UK EPR	
	Title: **COMPARISON of EPR design with HSE/NII SAPs**
	UKEPR-0005-001 Issue 00

Total number of pages: 162	Page No.: I / III
Chapter Pilot: Ph. CHAUMIN *Name/Initials* P. CHAUMIN *Date* *30/06/2008*	
Approved for EDF by: G. KAUFFMANN *Name/Initials* *Date* *30-06-08*	Approved for AREVA by: C. WOOLDRIDGE *Name/Initials* C.Wooldridge *Date* *30-06-2008*

REVISION HISTORY

Issue	Description	Date
00	First issue	30-06-08

For information address:

AREVA NP SAS
An AREVA and Siemens Company
Tour AREVA
92084 Paris La Défense Cedex
France

EDF
Division Ingénierie Nucléaire
Centre National d'Equipement Nucléaire
165-173, avenue Pierre Brossolette
BP900
92542 Montrouge
France

TABLE OF CONTENTS

1. REFERENCES

[1] Health and Safety Executive (HSE). Safety Assessment Principles for Nuclear Facilities, 2006 Edition Revision 1 (January 2008).

[2] Health and Safety Executive (HSE). NSD Guidance on Demonstration of ALARP, A N Hall, T/AST/005 Issue 3, December 2006.

2. CONTEXT

The UK HSE has developed Safety Assessment Principles (SAPs), against which it assesses safety submissions for civil nuclear facilities in the UK [1]. The SAPs are deemed to express HSE/NII views on relevant good practice in reactor design and operation. Whilst the concept of compliance cannot be strictly applied between a design and an assessment principle, it has nonetheless been decided to perform a comparison between the EPR design and the expectations of the SAPs. This comparison is intended to be a contribution to the demonstration that the EPR design process has followed “relevant good practice”, as required by the guidance from HSE/NII in application of the ALARP principle [2].

The EPR design was developed within a French and German framework involving both national Safety Authorities. The Safety Authorities produced a specific set of recommendations for the design of new PWRs, known as the “Technical Guidelines”, which were the fundamental requirements applied to the EPR design. Subsequently, the EPR design was compared against international standards such as IAEA safety guidelines, EURs and WENRA reference levels. These guidelines and principles do not correspond in all respects to the recommended practices suggested in the SAPs. Nonetheless it is considered that all the key nuclear safety requirements embodied in the SAPs are met by the EPR design, and in particular that EPR achieves the fundamental objective that the radiological risk to workers and the public is as low as reasonably practicable, which is the basic legal requirement underpinning UK nuclear safety regulations.

It should be noted that a number of SAPs refer to matters which are not directly relevant to the Generic Design Assessment (e.g. related to operation, or site specific). In some of these cases, responses have been provided based on EDF practice in France. In other cases, the SAP is stated to be "out of scope". (However, the current SAPs compliance analysis is not intended to provide a strict definition of the scope and limits of Generic Design Assessment.)

The assessment of the EPR design against the SAPs is provided in the appendix below.

APPENDIX

SAP	Comment
FP.1 The prime responsibility for safety must rest with the person or organisation responsible for the facilities and activities that give rise to radiation risks	The EPR is considered to comply with the SAP. AREVA and EDF are responsible for the design of the EPR. The design phase of the EPR has been performed under control of a specific Quality and Project Management and of the respective Quality Management Systems of AREVA and EDF. Information on Quality and Project Management is presented in the PCSR Chapter 21. Similar quality processes will be implemented in the erection, operation and decommissioning phases of the EPR.
FP.2 Effective leadership and management for safety must be established and sustained in organisations concerned with, and facilities and activities that give rise to, radiation risks	The EPR is considered to comply with the SAP. AREVA and EDF are responsible for the design of the EPR. Both companies have together or separately designed, manufactured, erected and operated a large number of nuclear power plants in France and in other countries. Both companies have a large amount of experience in the setting up of organisations sustaining effective leadership and management for safety. This experience includes effective safety management of design, manufacture or other services procured by a large number of sub-contractors. Operating requirements of future operators were incorporated early in the EPR conceptual design phase by utility involvement. Effective leadership and management of safety will be sustained in all phases in the plant lifetime, including the operation phase. EPR Quality and Project Management is described in PCSR Chapter 21 (for the GDA and post-GDA phases).
FP.3 Protection must be optimised to provide the highest level of safety that is reasonably practicable	The EPR is considered to comply with the SAP. The EPR design process has first taken full credit of design experience from the existing Nuclear Power Plants in France and Germany, through the involvement of plant designers and the operating utilities. The EPR was given ambitious safety objectives: deterministic and probabilistic objectives were set for design basis events and hypothetical events, including severe accident sequences, on radiation protection performance and on environmental performance. The different phases of the EPR design have allowed an iterative optimisation process, the result of which is considered to be the highest level of safety that is reasonably practicable.

SAP	Comment
FP.4 The dutyholder must demonstrate effective understanding of the hazards and their control for a nuclear site or facility through a comprehensive and systematic process of safety assessment.	The EPR is considered to comply with the SAP. Safety assessment of the EPR is possible through the different steps of the Safety Reports. The PCSR and its supporting documentation, including general operating rules, give the safety requirements and their implementation in the design of the reactor core, the primary coolant boundary, the containment and other civil structures, the engineered safety features and other auxiliary systems, the electrical power supply, the control and instrumentation and the operating principles. The resulting behaviour of the plant in all circumstances is described in the event analysis, PSA and hazard studies. Waste discharge during operation and decommissioning is also addressed. Consideration in the PCSR of the complete facility lifetime, of all possible events including hazards and hypothetical severe accidents give evidence of a comprehensive and systematic process of safety assessment.
FP.5 Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm.	The EPR is considered to comply with the SAP. Radiation risks to individuals can be divided into risks to plant workers during normal operation, off-site risks from solid, liquid or gaseous wastes, and risks from accidental events. The EPR has minimised the radiation risk to workers through a radiation protection optimisation process described in PCSR Chapter 12. EPR off-site risks from solid, liquid or gaseous wastes have also been optimised and are described in PCSR Chapters 11 and 20 (dedicated to decommissioning). The EPR containment design minimises the radiation risks from accidental events (to workers as well as to off-site individuals), even in the case of severe accidents. Accident events are described in PCSR Chapters 14 (design basis events) and 16 (risk reduction category events).
FP.6 All reasonably practicable steps must be taken to prevent and mitigate nuclear or radiation accidents.	The EPR is considered to comply with the SAP. The EPR design follows the defence in depth philosophy and provides prevention and mitigation features, for each event family. The EPR designers have chosen an evolutionary design to take maximum benefit from the large experience

SAP	Comment
	feedback from the previous generation of nuclear plants, and in order to ensure the reliability of components by means of reasonable technological steps. Compared to the previous generation II plants, the EPR design includes improvements in fuel design, reactor design, containment design and in the general layout of the plant. This gives the EPR improved capability to mitigate design basis events (e.g. LOCAs and Steam Generator Tube Rupture, SGTR), and greater robustness against internal and external hazards (e.g. fire, seismic events, airplane crash). In addition, the EPR design incorporates an additional level of defence in depth, by providing effective mitigation features for severe accidents. The compliance of EPR with the ALARP principle is demonstrated in PCSR Chapter 17.
FP.7 Arrangements must be made for emergency preparedness and response in case of nuclear or radiation incidents.	The EPR is considered to comply with the SAP. Emergency preparedness and response to nuclear or radiation incidents is the responsibility of the dutyholder and involves local and national UK Authorities. Emergency planning arrangements for a given facility depend on the site. The information exchange and decision making process must be agreed between all the involved parties. Aspects of the UK EPR design relevant to emergency preparedness described in the PCSR include mitigation of severe accident events (Chapter 16), the Man Machine Interface, Emergency Operating Procedures (PCSR Chapter 18), the related I&C systems (Chapter 7) and the Main Control Room habitability conditions (Sub-chapters 6.4 and 9.4).
FP.8 People, present and future, must be protected against radiation risks.	The EPR is considered to comply with the SAP. The EPR design minimises the radiation risks to workers by meeting ambitious radiation protection objectives. The EPR design minimises the radiation risks to persons off-site by meeting ambitious environmental performance objectives. The effective containment of the EPR results in a very low risk of accidents with significant radiological consequences (including severe accidents). The long term strategy for waste management covering operational waste, spent fuel and decommissioning waste ensures that people in the future will be protected from radioactive materials produced by the EPR. .

SAP	Comment
	A detailed discussion of the radiological consequences of accidents can be found in PCSR Chapters 14 and 16, on waste discharges and waste management in PCSR Chapters 11 and 20, and on radiological protection in PCSR Chapter 12.
MS.1 Directors, managers and leaders at all levels should focus the organisation on achieving and sustaining high standards of safety and on delivering the characteristics of a high reliability organisation.	The EPR is considered to comply with the SAP. Within the AREVA and EDF organisations, a strong Safety Culture is applied at all stages of product and facility life cycles: design, construction, operations, shutdown and dismantling. Within both AREVA and EDF, executive management establishes organisational structures consistent with the legal provisions of the relevant countries in which they operate. The organisations are based on the principle that achieving and sustaining high standards of safety requires a system of clearly defined responsibilities, thus ensuring that each person at each level of the organisation has the skills required to exercise their vested responsibility as regards safety, has sufficient authority, and has the necessary technical, financial and human resources for the mission. An independent organisation reporting to the Executive Board is responsible for inspections and reports on the accomplishment of policy and associated objectives. The involvement of directors, managers and leaders is effective through the decisions taken and provision of the necessary resources for developing, maintaining and continuously improving Quality and Environment (Q&E) Management System The Q&E Management Systems comply with stringent national (French Order of August 10, 1984 and in addition for AREVA American Appendix B of 10 CFR 50, German KTA 1401, Finnish YVL 1.4) and international (ISO 9001, ISO 14001, and IAEA 50-C-Q) codes and standards for Nuclear facilities. The Q&E Management Systems developed, maintained and effectively implemented by the co-applicants AREVA and EDF are presented in Chapter 21 of the UK EPR PCSR. Compliance with codes and standards and effective implementation of such Q&E Management Systems are regularly assessed by the management through management reviews. These reviews take into account the results of: external inspections/audits respectively carried out by the Regulators of various countries, audits by accredited independent third parties leading to the issuance of official certificates of authorisation (ISO certificates, ASME certificates), Customer audits, and the lessons learned process. AREVA and EDF have also put their Continuous Improvement and Sustainable Development approach at the heart of their

SAP	Comment
	strategy. Results of inspections/audits, both internal and external, are capitalised as lessons learned and analysed as part of a continuous performance improvement initiative relating to safety. Sustainable Development and Continuous Improvement organisations support and help managers and staff to implement Sustainable Development commitments and make sure that each individual is concerned about these issues in their daily activities.
MS.2 The organisation should have the capability to secure and maintain the safety of its undertakings.	The EPR is considered to comply with the SAP. As key players in the energy market, AREVA and EDF have established and developed policies for securing human resources and skills, and for ensuring the availability of resources in terms of technical expertise and management skills to serve worldwide needs. Measures have been developed by AREVA and EDF to attract, retain and develop the best talents, and to transfer knowledge from senior staff to the leaders of tomorrow. These measures have been significantly and successfully extended during the last few years to cope with the risk of a shortage of qualified engineers in the global energy market in which demand is increasing rapidly. Chapter 21 of the UK EPR PCSR presents measures employed in order for AREVA and EDF to remain capable organisations for securing and maintaining the safety of their undertakings. Personnel review, the core process of the talent development, is based on performance and potential assessment, succession and development planning covering the evolution of organisations and necessary skills, recruitments planning, training, mobility, succession planning for key people, and performance recognition and reward linked to objective setting and appraisal. The effectiveness of the established organisational structures is assessed regularly by management and, when necessary, changes to the organisation are implemented in a careful but consequential manner. Contractors are involved in activities such as, but not limited to, design, supply, manufacturing, erection activities which may have strong impacts on the safety of the Nuclear Power Plant. AREVA and EDF as “intelligent customers” have developed and systematically implemented measures in order to ensure that requirements for safety are defined and disseminated in the supply chain and that a strong safety culture is effective at all levels of that chain.

SAP	Comment
	Safety requirements are taken into account by AREVA and EDF for the selection and qualification of contractors before starting safety-related activities. During the performance of contracts, surveillance of documentation required from contractors is implemented depending on the safety classification of products; inspections and tests on manufacturing activities are carried out; audits at contractors' premises and on NPP sites are organised according to defined procedures, by qualified inspectors and qualified auditors for checking that requirements for safety are properly understood by the contractors and their implementation is effective. AREVA and EDF seek lasting partnerships with contractors as a means of offering its customers the best possible level of service. Amongst the various inputs to feed-back analyses, unplanned events are systematically recorded and analysed according to standard processes. This, in addition to the in-depth analyses of issues resulting from inspections, audit and surveillance processes, ensures a permanent focus on potential consequence on safety. Corrective and preventive actions are documented in a suitable manner to prevent loss of knowledge and to ensure that the organisation at all levels gets the right information in a timely manner. The capture and communication of information concerning management and technical aspects is a key issue for ensuring that those who need to make safety-related decisions have the necessary information available. Communication networks and applications have been developed for filing and preserving documents and records in order that information is retrievable and readable during the retention time defined to comply with legal and contractual requirements. Provisions for the control of documents and records are described in the Q&E Management System as explained in Chapter 21 of the UK EPR PCSR.
MS.3 Decisions at all levels that affect safety should be rational, objective, transparent and prudent.	The EPR is considered to comply with the SAP. AREVA and EDF Q&E Management Systems define provisions for the decision making process. Responsibilities, methods and tools, and necessary input data from lessons learned, from feedback, from root cause analyses of deficiencies and from technological development monitoring, are clearly established, communicated and

SAP	Comment
	available in the processes and procedures through the internal networks. Depending on the safety classification of activities and equipment defined by the safety units of the organisations, when technical decisions are to be made, specific meetings or design reviews are organised. Competent personnel participate in such meetings or reviews and records of discussions and decisions are kept. For the UKEPR Generic Design Assessment (GDA), the Project organisation, roles and responsibilities are defined in specific Project procedures and are summarised in Chapter 21 of the UK EPR PCSR. In particular, the GDA Project is led by qualified Project Managers who have been nominated by and report to AREVA and EDF senior management. The Project Managers are supported by a project team and by technical teams. Regular meetings at all management levels are established to discuss progress and agree actions. As explained in Chapter 21 of the PCSR, at the start of UK EPR Generic Design Assessment, AREVA and EDF management decided to implement an Independent Nuclear Safety Assessment (INSA) process to independently assess documents prepared and reviewed by the AREVA/EDF technical teams and to address significant safety issues. Conclusions of the INSA reviews are presented for discussion to a Design Safety Review Committee (DSRC) composed of independent senior experts from AREVA, EDF, AMEC and Rolls Royce who then make recommendations to the GDA Project. A GDA Steering Committee comprising senior AREVA and EDF management is also established to assure governance of the GDA Project. The Steering Committee is also available to arbitrate any divergent views that cannot be resolved by the Project Managers, should they occur.
MS.4 Lessons should be learned from internal and external sources to continually improve leadership, organisational capability, safety decision making and safety performance.	The EPR is considered to comply with the SAP. Both EDF and AREVA have developed comprehensive programmes to collect, analyse and act upon lessons learned from experience feedback, implemented in the Quality Management Systems referenced in Chapter 21 of the UK EPR PCSR. These programmes aim to implement improvements derived from identified weaknesses, deficiencies or errors that occur within the organisation at the different stages of business activities (e.g. design, construction, operation, manufacturing and procurement), by means of self-detection, benchmarking, inspections, audits and surveillance which address, in particular, organisational, safety management, product quality.

SAP	Comment
	Issues are investigated to identify root causes and trends (including those related to human factors), to initiate corrective and preventive actions as appropriate and to check their effectiveness. Failure factors from the nuclear industry worldwide are also taken into consideration for the continuous improvement processes developed by EDF and AREVA. Experts from EDF and AREVA participate in international conferences, meetings, workshops in addition to working groups of international organisations such as ISO, IAEA or ASME to ensure awareness and understanding of the latest methods, technical developments and issues. This overall system has fed the EPR design with inputs from the beginning, including feedback experience from the utilities (French and German), manufacturers and Safety Authorities. For the UK EPR, a design change process has been implemented including a link to the reference Flamanville 3 design change process which provides input into the UK EPR design of experience gained during the Flamanville 3 final design and construction phase.
SC.1 The process for producing safety cases should be designed and operated commensurate with the hazard, using concepts applied to high reliability engineered systems. **and** **SC.2 The safety case process should produce safety cases that facilitate safe operation.** **and**	These SAPs refer to the Safety Case process which must be followed by the dutyholder operating a NPP in the UK. The responsibility for compliance will therefore rest with the dutyholder licensee. The submissions being made for GDA are believed to be compliant with the requirements of these SAPs in respect of the plant design. The EPR is a Generation 3+ reactor whose evolutionary design benefits from global international experience acquired at the PWR system operational level in western countries, and French and German engineering design experience. For the purpose of GDA, the Safety Case submitted is closely based on the FA3 Preliminary Safety Analysis Report (PSAR), submitted to the French safety authorities for the Flamanville 3 design, but adapted to fit the UK context in order to consider UK regulatory requirements for nuclear installations and supplementary safety design objectives. EPR design and optimisation, and consequently the PSAR, were extensively reviewed during the fifteen year design and optimisation period.

SAP	Comment
SC.3 For each life-cycle stage, control of radiological hazards should be demonstrated by a valid safety case that takes into account the implication from previous stages and for future stages.	The process of design development was conducted under the oversight of the French and German Safety Authorities and their technical support organisations. From the start of the EPR design to the issuing of the Flamanville 3 construction license (DAC), all the recommendations of the French Regulator have been underwritten by analysis performed by its Technical Support Organisation, IRSN (Institute for Nuclear Safety and Radiation protection). Over the whole period, about ninety EPR design assessment reports were issued by IRSN comprising more than six thousand pages of detailed technical analysis. These reports were tabled at meetings of the French Standing Group for Nuclear Reactors (GPR), an independent advisory body established to support the French Regulator, consisting of scientists and engineers from France and other European countries and the USA. In addition, review of the EPR design has been achieved by the Finnish Safety Regulator (STUK), prior to the granting of the Construction License for OL3 in February 2005. As a result, the Flamanville 3 design had been subjected to a much broader and thorough examination at the stage of submission of the Preliminary Safety Report, compared to previous plant designs. Experts from several European countries have contributed to the examination. The French regulator ASN completed technical examination of the FA3 PSAR in September 2006. Information given in the PCSR and the PCER is clearly and logically structured in order to facilitate easy assess and further use. The "Introduction to the Safety, Security and Environmental Report (SSER)" document presents the contents of the PCSR and PCER, and provides a glossary of the acronyms used in the safety case and a full set of definitions. The PCSR comprises 21 chapters containing in particular the following elements: • general description of the nuclear and conventional plant installations and their main features, • presentation of safety analysis rules and the general design basis for structures, equipment and systems, • preliminary analysis of each system, explaining the measures adopted to comply with the stated nuclear safety

SAP	Comment
	requirements, • general description of the operation of the unit, • principles that will be applied to ensure the quality of the design, construction, operation and decommissioning, • complete analysis of the accidents considered and an assessment of their potential radiological consequences, • description of measures taken to mitigate accident situations, including severe accidents, and internal and external hazards, • main results of the Probabilistic Safety Analysis (PSA), • a description of the steps taken in the design with regard to radiological protection, including minimisation of collective dose, control of radioactive discharges. Consideration is also given to measures to facilitate the eventual decommissioning of the installation. This PCSR is intended to justify the safety of the design throughout the whole plant's life cycle, from construction through operation to decommissioning, including on-site spent fuel and radioactive waste management issues. An Integrated Waste Strategy (IWS) for managing radioactive waste produced by the plant during its life cycle is presented in PCSR Chapter 11. Although it is not practicable to present details of all the design solutions for the on-site storage of active waste at this stage of GDA, sufficient information is provided to give confidence that waste materials can be safely managed on a long term basis, prior to transfer to national repositories as prescribed by the UK Government. Chapter 20 of the PCSR also provides information about decommissioning.
SC.4 A safety case should be accurate, objective and demonstrably complete for its intended purpose.	The EPR is considered to comply with the SAP. PCSR Chapter 14 provides a full fault studies analysis, with description of the codes and methods utilised. Internal hazards studies are described in Chapter 13. A level 1 and 2 PSA has been developed and implemented in support of the EPR design. In addition, a specific off-site PSA has model been developed for UK EPR in support of the ALARP assessment. Chapter 17 of the PCSR provides an ALARP

SAP	Comment
	analysis and a review of PSA results compared to the SAPs numerical targets for risk.
SC.5 Safety cases should identify areas of optimism and uncertainty, together with their significance, in addition to strengths and claimed conservatism.	The EPR is considered to comply with the SAP. The EPR is an evolutionary reactor that takes full advantage of the experience from previous generation of PWRs, in particular of the latest French and German reactors. The uncertainty in the design is thus reduced. Uncertainties have been taken into account at each stage of the design. The EPR design follows the defence-in-depth approach as presented in IAEA Safety Standard on nuclear reactor design NS-R-1. The EPR design benefits from a long and extensive review period, as described in the response to SAP SC.1, that has led to improvements in and optimisation of the design. Prior to reactor operation in the UK a Pre-Operation Safety Report would be issued containing final design details and relevant details of the construction and commissioning of FA3.
SC.6 The safety case for a facility or site should identify the important aspects of operation and management required for maintaining safety.	The EPR is considered to comply with the SAP. The PCSR considers operation and maintenance aspects such as : - the operating limits for mechanical systems and components (Sub-chapter 3.4), - radiological protection (Sub-chapter 18.2) - operating principles (Sub-chapter 18.2) including normal operation and emergency operation, - commissioning of the plant (Chapter 19). The PCSR does not contain details of operating procedures such as Technical Specifications, accident management procedures, maintenance programmes, emergency planning arrangements, commissioning procedures, radiation protection arrangements for operating staff etc. These operating and commissioning documents will be produced during the plant construction phase and would be presented in a Pre-Operational Safety Report, for agreement before the plant was

SAP	Comment
	put into service. The specific processes by which the documents will be produced will be presented in Step 4 of GDA in an update of the PCSR.
SC.7 A safety case should be actively maintained throughout each of the life stages.	This SAP is not relevant for the GDA submission.
SC.8 Ownership of the safety case should reside within the dutyholder's organisation with those who have direct responsibility for safety.	This SAP is not relevant for the GDA submission.
ST.1 Account should be taken of all relevant factors that might affect the protection of individuals and populations from radiological risk when assessing the siting of a new facility.	The EPR is considered to comply with the SAP. Sub-chapter 2.1 of the PCSR presents a summary of the site data used in the safety analysis. These data are considered to be typical of UK coastal sites in England and Wales on which nuclear power plants have been sited, which is consistent with the Government expectations mentioned in the White Paper on Nuclear Power - January 2008, "Applications to build new nuclear power stations will focus on areas in the vicinity of existing nuclear facilities". The data given in the PCSR do not cover all the site data that would be used in a site-specific safety analysis, and therefore further analyses will be carried out at the site-specific stage. The dutyholder applicants will define the information in their application for a license. This site-specific content will include information concerning density and distribution of population, natural and man-made hazards.
ST.2 The safety case should demonstrate that the characteristics of the population	The EPR is considered to comply with the SAP. Sub-chapter 2.1 of the PCSR states that, for the individual dose assessment, emergency response is not considered (e.g.

SAP	Comment
off-site would allow for an effective off-site emergency response.	in support of the Design Basis Analysis and the Risk Reduction Analysis, as well as for the comparison against the SAPs numerical target 8). This is consistent with the requirements and objectives of: - Firstly, the design basis (PCC) and the design extension (RRC-A) conditions, stating that there should be no requirement for protective countermeasures for the public living nearby, i.e. no evacuation, no need for sheltering and no need for distribution of iodine tablets. - Secondly, the severe accidents (RRC-B), stating that their impact over time and space should be limited: • Limited need for sheltering, • No requirement for emergency evacuation beyond the immediate vicinity of the site, • No permanent relocation, • No long-term restriction on the consumption of foodstuffs. Further, in the framework of the comparison to the SAPs numerical target 9 (societal impact), Sub-chapter 2.1 indicates that demographic data and emergency planning actions are considered in the methodology applied in the Level 3 Probabilistic Safety Assessment (see Sub-chapter 15.5). This methodology makes use of evaluations carried out previously for the Gas Cooled reactor sites; and the bounding site (among existing UK nuclear sites where new nuclear power stations are likely to be built), in terms of societal impact, is considered in the generic UK EPR analysis. However, the characteristics of the population off-site and the emergency response plans will be addressed by the dutyholder applicants when applying for a site licence.
ST.3 The safety case should include information on local physical data relevant to the dispersion of released radioactivity and its potential effects on people.	The EPR is considered to comply with the SAP Sub-chapter 2.1 of the PCSR states that the dispersion of released radioactivity is modelled using standard physical data for the individual dose assessments (e.g. in support of the Design Basis Analysis and the Risk Reduction Analysis, as well as for the comparison against the SAPs numerical target 8) and that these standard physical data are expected to cover the conditions at UK sites to a large extent. The other local data used in these assessments relate to life habits, including food consumption and exposure conditions, with orders of magnitude that are consistent with UK data.

SAP	Comment
	Additionally, in the framework of the comparison against the SAPs numerical target 9 (societal impact), the methodology applied in the Level 3 PSA is based on evaluations performed previously for the Gas Cooled reactor sites (see Sub-chapter 15.5), which make use of local physical data. The bounding site (among existing UK nuclear sites where new nuclear power stations are likely to be built) in terms of societal impact is considered in the generic UK EPR analysis. However, the local physical data will be addressed by the dutyholder applicants when applying for a site licence.
ST.4 Natural and man-made external hazards should be considered if they have the potential to adversely affect the siting decision.	The EPR is considered to comply with the SAP. For a given site location, the site licence applicant will provide all site-specific information. Nevertheless, with regard to natural and man-made external hazards, the EPR design has defined load cases derived from generic and enveloping external hazard events. The list of external hazards is given in PCSR Chapter 13. The assumptions on site-specific data used for the safety case defined in the PCSR are given in PCSR Chapter 2, including some demographic or meteorological assumptions needed for off-site dose calculations. For a particular site, the applicant will be required to check the actual site data are enveloped by the assumed values. If necessary, additional site-specific design features may have to be designed in order to meet the EPR safety objectives at a particular site.
ST.5 The safety case should take account of any hazardous installations that might be affected by an incident at the nuclear facility.	The EPR is considered to comply with the SAP. The effects of an incident on an EPR power plant on any off-site hazardous installation can be estimated from the radiological consequences assessment of accidents reported in PCSR Chapters 14 and 16. Even in the case of a severe accident, the risks are very low: the EPR design objective is to keep required off-site protection measures very limited in space and time duration, except for events of extremely low frequency. A list of neighbouring hazardous installations is site specific and will be drawn by the applicant for a site licence.
ST.6 On multi-facility sites, the safety case should consider the site as a whole to establish that	The EPR is considered to comply with the SAP. The EPR is designed to be an autonomous unit, the safety of which is assured by its own safety systems. No safety-related

SAP	Comment
hazards from interactions between facilities have been taken into account.	system is shared between several EPR units on the same site, or between an EPR unit and another facility on the same site. Interactions between facilities on a particular site are site specific and would be addressed in a site license application.
ST.7 The safety case should be revised to take account of off-site changes that could affect safety on a nuclear site.	The EPR is considered to comply with the SAP. As mentioned in response to ST.1, sub-chapter 2.1 of PCSR presents a summary of the site data used in the safety analysis. Further analyses taking into account specific data will be carried out at the site-specific stage The potential off-site changes (natural and man-made) that could affect safety on the site will be addressed by the dutyholder applicants of the license. Nevertheless, the general robustness of the EPR design makes it likely that off-site changes have been considered by the EPR.
EKP.1 The underpinning safety aim for any nuclear facility should be an inherently safe design, consistent with the operational purposes of the facility. **and** **EKP.2 The sensitivity of the facility to potential faults should be minimised.**	The EPR is considered to comply with these SAPs. The EPR is an evolutionary PWR. Its design is based on the defence in depth approach as for existing western PWRs. The design achieves a balance between an inherently safe design and a fault tolerant design. It has the following features assisting the achievement of inherently safe design and low sensitivity to potential faults: 1) Inherently safe reactivity feedback One of the main requirements of the EPR core design is that all reactivity coefficients should be negative. By this means, power and reactivity transients are inherently counteracted in such a way that increase of fuel temperature, moderator temperature or void fraction decreases core reactivity. Sub-chapter 4.3, section 4 of the PCSR shows that the fuel temperature coefficient and coolant void coefficient are negative. The design ensures that the moderator temperature coefficient stays negative between 0% and 100 % power, whatever the stage of operation (beginning, middle or end of cycle).

SAP	Comment
	2) Conservative design, that lowers the risk of radioactivity release due to rupture of piping, is achieved by: • Safety classification of all piping containing contaminated fluid (see Sub-chapter 3.2 of the PCSR) • Elimination of risk of loss of integrity of the main equipment of the RCS: Reactor Vessel, Steam Generators, RCP casings and Pressuriser • Application of break preclusion concept to main primary piping (see PCSR Sub-chapter 5.2) • Application of break preclusion concept to main secondary primary piping (see PCSR Sub-chapter 10.5) • Absence of lower head penetrations on the RPV for in-core instrumentation thus eliminating failure mechanism at that location 3) Improved margins in the general design of main components: • The large core size results in a substantially reduced average core power density (about 9% lower than in Sizewell B). This lowers the risk of excessive cladding temperature. Core parameters are maintained well below fuel integrity limits • The main components' size (especially the steam generator secondary side and the pressuriser volume) has been increased compared to the current design. This smooths the plant response to abnormal transients 4) Lower core elevation relative to the cold leg cross-over piping which limits core uncovery risk after a LOCA. 5) In the event of reactor coolant pump unavailability, natural circulation in the reactor coolant system is established between the core and the steam generators due to the elevation of the steam generators above the core, and the routing of the reactor coolant lines. 6) The robustness of the plant to internal and external hazards: • External hazards originating outside of the plant (examples are earthquake and airplane crash) or internal hazards originating in the plant (examples are fire or pipe whipping) are considered in the design.

SAP	Comment
	• Physical protection against external hazards prevents release of the radioactivity materials in the reactor core and the fuel pool and damage to systems needed for safe shutdown • Plant design against internal hazards is such that internal hazards must not induce nuclear accidents (PCC-3 and PCC-4 events) and must not remove more than one level of redundancy of mitigating systems (see PCSR Chapter 13 for more details). • Reactor coolant pump disintegration is prevented: at nominal speed by design, manufacture and inspection; at over-speed due to LOCA by application of the break preclusion concept of the primary piping (see section 4.3.2.1.2 of PCSR Sub-chapter 13.2) • Due to layout arrangements, turbine missiles will not cause damage to structures, systems and components relevant to safety (see section 4.3.1 of PCSR Sub-chapter 13.2). 7) Low sensitivity of the EPR to potential faults, achieved by the automatic functions of the Reactor Control Surveillance and Limitation System (RCSL, PCSR Chapter 7); • In normal operating conditions, the RCSL maintains the plant operating parameters within their normal allowed range of variation and initiates corrective measures (in particular interlocks, control rod movement inhibitions, partial trip and turbine slowdown) to prevent exceeding the Limiting Conditions of Operation so as to prevent actuation of the protection functions. Under fault conditions, when the intervention of the RCSL system cannot control the deviation, the protection functions are actuated.
EKP.3 A nuclear facility should be so designed and operated that defence in depth against potentially significant faults or failures is achieved by the provision of several levels of protection.	The EPR is considered to comply with the SAP. The EPR safety approach is based on the concept of providing successive lines of defence to mitigate the effects of technical or human failures, as prescribed in IAEA Standard NS-R-1 referenced in SAP EKP.3 (see PCSR Chapter 3). The EPR design objective has been to make significant improvements in each level of defence compared to earlier PWRs (Generation 2). The EPR defence in depth approach is described in PCSR Chapter 3. Key aspects are:

SAP	Comment
	• increased safety margins (achieved for example by reducing peak fuel linear rating); increased volume of major primary and secondary system components to give increased response time in abnormal conditions. These measures help prevent fault escalation (PCSR Chapter 3). • improved design of safeguard systems to help prevent core melt following internal events and hazards, including improved segregation and protection against internal and external hazards (PCSR Chapter 3). The 4–train system for safety injection allows core cooling to be achieved with one safety train unavailable due to a LOCA, one train unavailable due to maintenance and a third train unavailable due to a random failure. Risk of core melt is further reduced by specific devices (RRC-A features) to protect against common mode failures of safety systems (PCSR Chapter 16). Examples are, provision of 2 diverse back-up diesel generators for use following CCF of the 4 Emergency Diesel Generators, provision of a dedicated ATWS protection signal, provision of dedicated procedures for cooling by primary feed and bleed following CCF of the Emergency Feedwater System. • severe accidents have been taken into account in the EPR design stage, and physical measures implemented to ensure "practical elimination" of core melt events and sequences that could have a significant radiological impact on the environment (PCSR Chapter 16). These measures include provision of a dedicated primary pressure relief system to prevent high pressure core melt ejection into the containment, provision of passive hydrogen recombiners, provision of a spreading area for retaining molten corium inside the containment, and provision of a dedicated containment cooling system for severe accidents. The radiological objective is that only very limited countermeasures should be necessary in core melt situations, i.e.: - limited sheltering duration for the public, - no need for emergency evacuation beyond the immediate vicinity of the plant, - no permanent relocation, - no long term restrictions on the consumption of foodstuffs. Operational aspects of the defence in depth approach, such as Technical Specifications and Emergency Operating Procedures, will be available at a later stage.
EKP.4 The safety function(s) to be delivered within the facility	The EPR is considered to comply with the SAP.

<table>
<tr><th>SAP</th><th>Comment</th></tr>
<tr><td>should be identified by a structured analysis</td><td>
In order to ensure the safety of a Nuclear Power Plant, three safety functions must be fulfilled in all cases:

control of reactivity,
removal of heat from the core,
confinement or containment of radioactive substances.

In accordance with the concept of defence in depth, these safety functions are mainly achieved by two means:

firstly, the creation of barriers between radioactive materials and the environment to prevent unacceptable radiological discharges
secondly the installation of safety systems to mitigate accidents so as to restrict their consequences to an acceptable level

<u>Identification of barriers</u>
Beyond the three traditional and easily identified barriers of a PWR (fuel, primary system and reactor building), due attention is paid to all equipment that can lead to a discharge of radioactivity significantly greater than that existing in the environment.
Activity is considered as being significantly greater than that existing in the environment when both the following conditions are met:

the activity concentration of the contained fluid exceeds 1 MBq/l
the activity concentration of the contained fluid exceeds by a factor 1000 that existing in the environment

This equipment is identified and mechanically classified.
<u>Identification of other safety functions</u>
The fault analysis is carried through an extensive list of events:
</td></tr>
</table>

SAP	Comment
	1) Design basis accident analyses that cover all single events having a potential to impair one of the safety function previously mentioned. These events range from the most probable events PCC-2 to a list of improbable PCC-4 events 2) RRC-A events (Risk Reduction Category) introduced to complement the deterministic design basis analyses (PCCs or Plant Condition Categories). These sequences consider multiple failures conditions, identified using PSA studies as making a significant contribution to the global core damage risk. 3) The beyond design basis event of a core melt (RRC-B sequences) 4) The consideration of all external and internal hazards. For each PCC event presented in PCSR Chapter 14, the equipment necessary to detect the fault and reach an acceptable controlled state is identified (this equipment is F1A safety classified). In the long term analyses of events, all the non F1A equipment necessary to reach the safe state is identified and safety classified F1B. For each RRC-A event developed in PCSR Sub-chapter 16.1 equipment necessary to reach a final state is identified (this equipment is F2 safety classified, unless already classified to a higher level) All functions required to prevent significant discharges in RRC-B sequences and those specifically designed to monitor and control internal and external hazards (when necessary from an event-driven approach) must be identified and F2 safety classified, unless already classified to a higher level. A broad overview of the safety classification of the EPR structures, systems and components is presented in Sub-chapter 3.2 of the PCSR.
EKP.5 Safety measures should be identified to deliver the required safety function(s).	The EPR is considered to comply with the SAP. To implement the safety functions identified in accordance with the EKP.5 principle; the EPR safety measures follow the hierarchy below:

SAP	Comment
	Passive Safety Measures As explained in Sub-chapter 17.3 of the PCSR, a systematic assessment of passive safety measures that do not rely on control systems, active safety systems or human intervention was performed. Acceptance criteria included simplicity, impact on plant operation, on safety and on cost. Accepted measures are listed in Sub-chapter 2.2, section 4.2 of the PCSR; reasons for the selection of other active systems are developed in Sub-chapter 2.2, section 4.3. Automatically initiated active engineered safety measures. When passive safety measures were not favoured, automatically initiated active engineered safety measures are imposed for all action required within 30 minutes of the first alarm in the control room. The classical automatic initiation of Reactor Trip and of Safeguard Systems was extended during the design phase of the EPR by the addition of a partial cooldown system and of an isolation sequence that allows an automatic management of a SGTR accident until a controlled state. Before the first manual action of the operator, the failed SG is isolated and the internal leakage to the secondary system brought to a minimum and automatically stopped. Active engineered safety measures that need to be manually brought into service in response to the fault These are only acceptable for actions required more than 30 minutes after the first alarm (or 60 minutes if local plant action is required). In that case, the operator has had sufficient time to make a diagnosis of the main parameters of the plant, and to choose the procedure that will lead to a permanent safe state. Administrative safety measures The objective of events analyses is to limit the reliance on administrative measures to mitigate the consequences of accidents. Mitigation safety measures (e.g. filtration or scrubbing) Consistent with the SAPs requirement, filtered venting of the containment was rejected for containment pressure relief in

<table>
<tr><th>SAP</th><th>Comment</th></tr>
<tr><td></td><td>the EPR design. Instead, a containment heat removal system, described in Sub-chapter 6.2, section 7 of the PCSR, was preferred to the system used in some Generation 2 PWRs, where the Reactor Building can be depressurised to the atmosphere through multiple filters.</td></tr>
<tr><td>ECS.1 The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be categorised based on their significance with regard to safety.

and

ECS.2 Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance with regard to safety.</td><td>The EPR is considered to comply with these SAPs.

The detailed implementation of these principles is also reported in PCSR Chapter 3
Fundamentally, the EPR uses two main classification systems: the first is termed “mechanical” and addresses pressure issues and the barrier role of mechanical components (static approach); the second one is termed “functional” and addresses the performance of systems required by the accidents analyses (dynamic approach).
Both the mechanical and functional classifications have evolved from the initial approach used on early PWR designs.
The barrier approach, unchanged for the primary circuit, has been extended to cover the concept of activity retention, when both of the following conditions occur:
the activity concentration of the contained fluid exceeds 1 MBq/l
the activity concentration of the contained fluid exceeds that existing in the environment by a factor of 1000.
The functional classification has been adapted to address long term extension of the accident analyses. Classification F1A is applied to the main safety systems (subject to the single failure design criterion at the system level). Classification F1B is applied to systems required for longer term operation of the plant towards sustainable safe shutdown: it requires the concept of functional redundancy corresponding to the IAEA definition of the single failure principle.
As the two classifications are complementary there is not an automatic correspondence between mechanical and functional classification levels. Even though a “typical” safeguard system is likely to be F1A / M2, other combinations are possible: e.g. F1A / M1 for primary circuit isolation, or F1A / M3 for most of the emergency</td></tr>
</table>

SAP	Comment
	feedwater system. On the other hand a few interface requirements are postulated, e.g. no less than M3 for a mechanical equipment performing a F1 function, no less than F2 for the isolation between two different levels of mechanical classification (see PCSR Chapter 3, in connection with paragraph 155 of ECS.2). Mechanical and functional classifications give a comprehensive definition of component significance with regard to safety. Other so-called “classifications” describe how this significance is interpreted in terms of relevant requirements in a specific technical field: C for buildings, E for I&C, EE for electrical equipment and SC for seismic requirements.
ECS.3 Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate standards.	The EPR is considered to comply with the SAP. The objective of EPR safety classification is precisely to achieve through design, manufacturing and operating requirements, an acceptable quality of systems, components and civil structures involved in the plant safety. The safety classified systems, components and structures are arranged in classes, with corresponding requirements dependent on the safety functions to be performed. The most stringent requirements correspond to the most important safety functions. The following requirements may apply dependent on safety classification (see PCSR Chapter 3): for <u>systems</u> • single failure criterion • physical separation • emergency power supply • periodic tests for <u>components</u> • qualification • use of design and construction codes for <u>both systems and components</u> • design against earthquake

SAP	Comment
	• quality assurance During the plant life, the classified systems, structures and components will be inspected and tested regularly to reveal any degradation which might lead to abnormal operating conditions or inadequate safety system performance.
ECS.4 For structures, systems and components that are important to safety, for which there are no appropriate established codes or standards, an approach derived from existing codes or standards for similar equipment, in applications with similar safety significance, may be applied. **and** **ECS.5 In the absence of applicable or relevant codes and standards, the results of experience, tests, analysis, or a combination thereof, should be applied to demonstrate that the item will perform its safety function(s) to a level commensurate with its classification.**	The EPR is considered to comply with these SAPs. The EPR design is an evolution of previous and well proven French and German designs. Accordingly, wherever possible, i.e. in most cases, it uses only components, the design of which • is in accordance with codes and standards which are well known and widely accepted for nuclear application, • has performed adequately in extensive past experience in similar nuclear applications. Where an appropriate (nuclear) code or standard is not available, the design approach is justified by using • existing codes or standards used for similar equipment, in applications with comparable safety significance, • experience, tests and analyses derived from relevant good practice, research programmes and/or widely accepted methods. The thermal-hydraulic and mechanical design of the first PWRs was based mainly on an experimental approach. For early designs, no computer codes were available to model complex structures (such as the RPV) and associated fluid flows. Reliance was instead placed on extensive testing of major equipment to confirm its performance. In recent years, progress in computer codes, particularly in Computational Flow Dynamics (CFD), has allowed modelling of complex structures using accurate 3D numerical models, and the solution of complex physical problems (e.g. jet impact, flow reversal, vortices, buoyancy effect, jet mixing, thermal coupling, etc.). The design of the EPR is therefore underwritten by both 3D calculations and experimental results, handled in a complementary manner. Further information is presented in PCSR Chapter 3 (Codes and standards).
EQU.1 Qualification procedures should be in place to confirm that structures, systems and	The EPR is considered to comply with the SAP. The purpose of qualification is to demonstrate that the equipment can fulfil its required function during accident conditions

SAP	Comment
components that are important to safety will perform their required safety function(s) throughout their operational lives.	PCC, RRC-A and RRC-B. The equipment requiring qualification is that which is needed to operate so that the systems can fulfil their safety function. The loading conditions to be taken into account are those resulting from internal and environmental conditions corresponding to the conditions for which the equipment is required to function (PCC, RRC-A, RRC-B). Depending on its safety role and the conditions for which the equipment is required to operate, qualification requirements are drawn up and incorporated into the equipment design using the technical design specifications. In addition to the operating conditions, the qualification procedure takes account of: - the effects of ageing, i.e. the cumulative effects of the environmental conditions corresponding to normal operating conditions before the occurrence of the accident taken into account for qualification, - the effects of seismic stresses on the equipment required to be qualified for use in PCC conditions. These effects are taken into account on a case-by-case basis for equipment required for use in RRC-A or RRC-B events (see Sub-chapter 3.2). Concerning the qualification programmes and the verification of compliance (See Sub-chapter 3.6 of the PCSR), several methods are used in the qualification procedure: - Qualification by testing: this consists of subjecting equipment to loads representative of the operating conditions in which it must fulfil its safety function. - Qualification by analysis: qualification by analysis generally differs from qualification by testing because it does not involve specific tests. o *Qualification by calculation:* Qualification by calculation consists of demonstrating that the loads experienced by the equipment have consequences for the equipment that are acceptable. o *Qualification by operating experience*: Qualification by operating experience consists of determining the equipment’s ability to carry out its safety functions by analysing past history of representative equipment in industrial operation. In practice, this method is rarely used in isolation. It is usually used to complete and confirm the behaviour of an equipment component, whose qualification is demonstrated using other methods. - Qualification by analogy: qualification by analogy consists of comparing, based on logical rules, the equipment to be qualified with “similar” equipment, already qualified. - Mixed methods: combinations of the methods presented above can sometimes be used. These combinations vary according to the equipment under consideration. In all cases, each part of the mixed method must comply with the

SAP	Comment
	conditions corresponding to the selected method. All parts together must fully demonstrate the capability of the equipment to fulfil its safety function. For qualification of equipment, the reference document is the international standard CEI 60780. The following three qualification practices, which are compatible with this standard, can be used: - French practice based on the RCC-E (see Sub-chapter 3.8) and the associated specifications, - German practice based on KTA rules - American practice based on IEEE rules Following a review of European qualification practices, it is recognised that all these practices have the same objective, i.e. to demonstrate that equipment operates as expected in the environmental conditions and under specified loads. They have all been developed based on similar principles and, for methods involving testing, use the same steps and include identical operating conditions and parameters. However, it is not possible to demonstrate identical equivalence of single tests making up each of the qualification sequences. This variety of solutions for one qualification requirement does not imply a different level of safety. It reflects the different approach of individual test methods and the personal preferences of decision-makers and testers together with the dependency of parameters on design and installation data which may differ from one project to the next. Each of the above practices is applicable provided the qualification is verified for a requirement that is equal to or more severe than that of the EPR.
EDR.1 Due account should be taken of the need for structures, systems and components important to safety to be designed to be inherently safe or to fail in a safe manner and potential failure modes should be identified, using a formal analysis where appropriate.	The EPR is considered to comply with the SAP. EPR structures, systems and components (SSCs) important to safety are designed according to the general design requirements indicated in PCSR Chapter 3. Safety classification of the SSCs is carried out using complementary approaches, and is extensively described in PCSR Chapter 3. The EPR classification principles result in stringent requirements in terms of design and reliability. Moreover, redundant trains of the main safety systems (one per Safeguard Building) are strictly separated into four divisions. This operational separation is provided for electrical and mechanical safety systems. The four divisions of safety

SAP	Comment
	systems are consistent with the N+2 safety concept. With four divisions, one division can be out-of-service for maintenance and one division can fail to operate, while the remaining two divisions are available to perform the necessary safety functions even if one is ineffective due to the initiating event. This approach is complemented by PSA analyses where the potential failure modes of systems and equipment are extensively evaluated.
EDR.2 Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety.	The EPR is considered to comply with the SAP. Compliance of the EPR is confirmed in PCSR Chapters 3, 14 and 13. A very high level overview of the system design principles is given as follows: <u>Redundancy:</u> the EPR design requires application of the single failure criterion at the system level to F1A classified systems; rules for PCC studies insure functional redundancy for F1B functions, corresponding to IAEA requirement for functional redundancy. At a third level, redundancy is implemented as necessary through PSA analyses and corresponding RRC scenarios to achieve EPR probabilistic safety objectives. <u>Diversity</u>: there is no a priori design rule applicable to diversity. Diversity is implemented as required to protect against common cause failures of F1 systems, when it is possible to achieve diversity without lowering safety performance. This is the case, in particular, for RRC complex sequences: examples are requirement for diverse Station Black-Out diesels, or diverse reactor trip function for ATWS scenarios. <u>Segregation</u>: a number of layout rules are applied to implement the principle of segregation, albeit highly simplified as a result of the overall 4 division layout concept. The design ensures that the occurrence of a failure, internal or hazard-made, that affects a safety train must not result in the loss of another train. <u>Reliability:</u> reliability claims in the PSA must be substantiated and uncertainties included in the PSA analysis. However there is no a priori reliability requirement applied to a given safety function. Such specifications are only used by the designer as internal targets to ensure global consistency of the final assessment or to facilitate the relationship with subcontractors. Final acceptability is given first by achieving compliance with global safety objectives (global targets for core melt frequency and ‘practical elimination’ of certain accident sequences) and even though those targets are met,

SAP	Comment
	additional reliability may have to be provided to reduce the weight of major risk scenarios.
EDR.3 Common cause failure (CCF) should be explicitly addressed where a structure, system or component important to safety employs redundant or diverse components, measurements or actions to provide high reliability.	The EPR is considered to comply with the SAP. Common cause failure is addressed for structures, systems and components important to safety. Reduced sensitivity to failures, including human errors, is achieved by: • adequate design margins, automation, high reliability of the devices in their expected environment and in the organisation of the operating team, • protection against common mode failures by design against load cases (e.g. earthquake), • high degree of autonomy allowing large grace periods for operator actions. Diversity is implemented as required to protect against common cause failures of F1 systems, when it is possible to achieve diversity without lowering safety performance. This is the case, in particular, for RRC complex sequences where F1 systems are backed by F2 systems to mitigate accident consequences: examples are requirement for diverse Station Black-Out diesels, or diverse reactor trip function for ATWS scenarios (PCSR Chapter 16). Section 3.1 of the PCSR confirms that the EPR classification principles are consistent with the SAP proposals. The need and effectiveness of additional dedicated safety measures, such as diversity, are assessed via PSA and supporting studies in the framework of the RRC approach.
EDR.4 During any normally permissible state of plant availability no single failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.	The EPR is considered to comply with the SAP. The design of structures, systems and components important to safety takes into account the single failure in order to ensure that more than the minimum number of components is provided to carry out any essential function. This requirement for redundancy assists in ensuring high reliability of safety classified systems designed to maintain the plant within its deterministic design basis (see PCSR Chapter 3). The single failure is taken into account for F1A safety classified systems and F1B safety classified functions at the design stage. The failure taken into account is a random failure independent of the initiating event, which necessitates the system

SAP	Comment
	operation. A short term single failure is considered for active components. For passive components the single failure is postulated in the long term (more than 24 hours after the initiating event). Consequential failures resulting from the postulated single failure are also considered when applying the single failure principle (when means are not available to detect the occurrence of a failure and restore the function of the affected system or component in a short time period). A single active failure is also taken into account in the design of systems protecting against internal hazards.
ERL.1 The reliability claimed for any structure, system or component important to safety should take into account its novelty, the experience relevant to its proposed environment, and the uncertainties in operating and fault conditions, physical data and design methods.	The EPR is considered to comply with this SAP. The reliability claimed for the design of any EPR structure, system or component (SCC) important to safety is stated, qualitatively, in accordance with its role in the safety demonstration (e.g. safety classification, level of redundancy, qualification requirements, compliance with standards, …), and, quantitatively, according to the values used into the Probabilistic Safety Assessment (PSA) developed during the early design phases. Those SCC reliability characteristics are mainly: failure rates, probabilities of failure on demand, and mean times to repair. Some SCC reliability requirements (e.g. unavailability for maintenance, acceptable outage downtime) were specified taking account of the potential impact of their unavailability in the preliminary EPR Generation Risk Assessment (GRA). The EPR design uses many SCCs previously successfully used in French and German Plant. Thus, SCC reliability data used in the first PSA or GRA performed during the early phases of the design were derived mainly from operational plant experience feedback from France and Germany when the technology was known and the operating conditions were judged similar. These were supplemented by the EG&G generic reliability database or specific known data banks for safety-related SCC not yet precisely defined, innovating or without sufficient experience feedback. Those data were validated before they had been used in the studies. The following minimum information was analysed: • source of experience feedback, • method of gathering raw data,

SAP	Comment
	• period of observation and operation assumptions, • nature of the samples (technological characteristics, equipment limits, etc.), • calculation methods and assumptions used.
ERL.2 The measures whereby the claimed reliability of systems and components will be achieved in practice should be stated.	The EPR is considered to comply with this SAP. During SCC development, when contracting for SCC purchase, dedicated reliability analysis based on the claimed reliability is required from the supplier. The process for assessing the SCC provisional reliability is based on suitable qualitative and quantitative dependability analysis: • Dependability analysis infers that the SCC are trustworthy and capable of performing their global missions, either for plant safety or for plant availability. As far as possible, those analyses show that chosen technical solutions avoid or limit problems encountered in operating plants. • Failure Mode and Effect Analysis (FMEA) is required to identify the independent failure contributions to SCC overall mission critical failures. This would include both random and systematic failures. • Dependability models (such as fault trees) are built to assess the failure combinations or common modes leading to the overall SCC mission failure and identify the most critical paths. • Assessment of the elementary reliability data that involves: a justification of the product failure rates, a justification of the quality levels of the components, a state of the technology, a qualification inspections and acceptance reference document (by examination of the part lists compared with the components actually used, including the examination of the manufacturing process). There will be a requirement on the dutyholder to maintain a record of component reliability, based on operational experience to confirm that the PSA assumptions remain valid.
	The EPR is considered to comply with the SAP.

SAP	Comment
ERL.3 Where reliable and rapid protective action is required, automatically initiated engineered safety features should be provided.	The Protection System (see PCSR Chapter 7) implements the necessary short-term automatic-only actuation of safety systems which are used to mitigate the consequences of PCC events and accomplish similar actions in case of RRC-A accidents. As a general design rule, automation is adopted when it improves significantly safety, availability or cost and applies more particularly to tasks that otherwise would likely represent a source of human errors (e.g. those requiring a short response time or the assimilation of a large amount of information). As a consequence, and in accordance with the Design Basis Faults analysis rules, all actions required within 30 minutes of an accident to reach a controlled or safe shutdown state are automated. Further actions could have a manual character according to the following rules: • a manual action performed from the Main Control Room may take place no sooner than 30 minutes after the first item of significant information has been received by the operator, • a local manual action, i.e. a manual action that must be performed outside the main control room, may occur no sooner than one hour after the first item of significant information has been received by the operator.
ERL.4 Where multiple safety-related systems and/or other means are claimed to reduce the frequency of a fault sequence, the reduction in frequency should have a margin of conservatism with allowance for uncertainties.	The EPR is considered to comply with this SAP. The claim of reduction in the frequency of fault sequences is addressed in the EPR PSA. Considering the PSA associated with procedural operator actions, different types of safety-related systems are considered: • systems designed to mitigate the consequences of fault sequences identified in the Design Basis events (PCC), • systems designed to reduce the Core Damage Frequency of sequences considered in Design Extension Conditions (RRC-A), • systems designed to reduce or limit the Release Frequency of sequences considered in Severe Accidents (RRC-B). Non safety-systems are also credited in the PSA when they impact the onset of initiating events or when they can

SAP	Comment
	realistically be used after such events. For PSA purposes, success criteria are defined for all those mitigating systems on a realistic basis for sets of fault sequences which represent group of initiating events. The success criteria used for a specific group is the most stringent criteria of all the individual events within the group. Sensitivity studies are performed on significant assumptions, i.e. those which have a significant impact on the PSA results. Mean values of reliability parameters are generally used when performing reliability analysis of the system mission corresponding to the identified success criteria or when assessing the initiating events frequencies. Uncertainties are addressed in dedicated studies to give an indication of the level of confidence in the PSA results.
ECM.1 Before operating any facility or process that may affect safety it should be subject to commissioning tests to demonstrate that, as built, the design intent claimed in the safety case has been achieved.	The EPR is considered to comply with the SAP. Commissioning tests are carried out progressively between the erection, installation and the start of normal operation of the various plant systems. The commissioning tests are defined to: • Ensure that all operational aspects of system functions are tested, including safety-classified functions, taking into account off-site tests, where relevant. • Fulfil the requirements of commissioning test documentation. The plant commissioning phase ranges from erection to commercial operation. The tests are organised into two test categories: • Pre-operational tests and • Initial start-up tests (operational tests). Plant commissioning tests cover all the operations performed on equipment, systems and structures – notably those that are safety-classified – in order to ensure that they behave as specified in the design requirements. <u>Pre-operational test programme</u> • *Phase I*: includes preliminary tests and controls, first start-up of equipment, functions or function groups, not

SAP	Comment
	involving any interaction with the reactor coolant system (or its auxiliary systems) or the secondary-side systems; • *Phase II*: includes cold and hot functional tests of the reactor coolant and secondary-side systems before fuel loading. Initial start-up test programme: • *Phase III*: includes core loading, cold and hot pre-critical tests and actual start-up, including a “Demonstration Run”, up to “Commercial Operation Date”. Commissioning test requirements and programme of the EPR are described in PCSR Chapter 19.
EMT.1 Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case.	The EPR is considered to comply with the SAP. In-service inspection requirements of the Main Primary System and of the Main Secondary System are defined in accordance with the break preclusion requirements. They are discussed in the PCSR Sub-chapters 5.2 and 10.5 respectively. In-service inspection requirements for safeguard systems are defined in the PCSR Sub-chapter 6.5. The EPR containment building is designed to undergo a full pressure test every ten years. One of the main features in the EPR design is its capacity to permit maintenance during power operation without impairing the safety of the plant. The corresponding safety requirements are discussed in PCSR Sub-chapter 18.2. Testing requirements are part of the process engineering: each elementary system description in the PCSR includes a paragraph on “Testing, inspection and maintenance”. This can be found for each system in PCSR Chapters 5 to 11. I&C systems testing and maintenance requirements are defined in PCSR Chapter 7. Refer to the EMT.7 response below for in-service testing methodology.
EMT.2 Structures, systems and components important to safety	EPR is considered to comply with the SAP.

SAP	Comment
should receive regular and systematic examination, inspection, maintenance and testing.	The in-service testing methodology given below as a response to SAP EMT.7 includes frequency determination. In-service inspection is addressed in PCSR Sub-chapters 5.2, 6.5 and 10.5. Maintenance is addressed in PCSR Sub-chapter 18.2 and in each system related sub-chapter or section. Refer to the SAP EMT.1 response above.
EMT.3 Structures, systems and components important to safety should be tested before they are installed to conditions equal to, at least, the most severe expected in all modes of normal operational service.	The EPR is considered to comply with the SAP. The EPR qualification requirements and qualification programme are described in PCSR Sub-chapter 3.6. Several methods are used in the qualification procedures: qualification by testing, qualification by analysis, qualification by calculation (demonstrating that the load consequences are acceptable),.qualification by operating experience (analysing past history of representative equipment in industrial operation), qualification by analogy (comparing, based on logical rules, equipment with “similar” equipment, already qualified), and combinations of these methods. The RRC-E technical code provides further requirements and methodology for qualification of electrical equipment.
EMT.4 The validity of equipment qualification for structures, systems and components important to safety should not be unacceptably degraded by any modification or by carrying out of any maintenance, inspection or testing activity.	The EPR is considered to comply with the SAP. Conditions for maintaining qualification during manufacturing and operation are given in PCSR Sub-chapter 3.6. In particular, the documentation ensuring compliance with requirements is listed in this sub-chapter. The dutyholder will be required to maintain compliance with these requirements during plant operation.
EMT.5 Commissioning and in-service inspection and test procedures should be adopted that ensure initial and continuing quality and reliability.	The EPR is considered to comply with the SAP. The aim of commissioning tests is to demonstrate the initial plant component and system capability for safe and reliable operation. The method for defining commissioning tests is described in PCSR Sub-chapter 19.1.The aim of in-service tests is to demonstrate the same throughout the plant lifetime. In-service test procedures for UK EPR will be subject to further

SAP	Comment
	engineering studies, as explained in the EMT.7 response below. In-service inspection is described in PCSR Sub-chapters 5.2, 10.5 and 6.5 (see the EMT.1 response above). Maintenance strategy is discussed in PCSR Sub-chapter 18.2. See also the EMT.6 response below.
EMT.6 Provision should be made for testing, maintaining, monitoring and inspecting structures, systems and components important to safety in service or at intervals through out plant life commensurate with the reliability required of each item.	The EPR is considered to comply with the SAP. The EPR maintenance strategy is based, whenever possible, on the Reliability Centred Maintenance (RCM) approach, the aim of which is clearly to ensure the required level of reliability for structures, systems and components. The RCM approach is not, however, applied everywhere; exceptions are: • families of identical equipment, for which sampling methods are justified, • equipment within the Main Primary Circuit (MCP) or the Main Secondary Circuit, for which RCM is not relevant, or that are subject to other regulatory requirements. In-service inspection of this equipment is described in PCSR Sub-chapters 5.2 and 10.5. • civil engineering structures, for which RCM is not relevant. The EPR testing strategy is not yet fully defined. However, the analysis of periodic testing will include a study relating the test frequency to the overall reliability of each system, in addition to the test feasibility included in the system engineering. In the EPR, test equipment is used mainly for I&C testing. The requirements for testing I&C functions are given in PCSR Chapter 7. The way preventive maintenance is taken into account in the design of the EPR is explained in PCSR Sub-chapter 18.2.
EMT.7 In-service functional testing of systems, structures and components important to safety should prove the complete system	The EPR is considered to comply with the SAP. EPR design development has fully acknowledged this general principle and the requirement for periodic testing is considered as the most basic requirement for safety classified components.

<table>
<tr><th>SAP</th><th>Comment</th></tr>
<tr><td>and the safety-related function of each component.</td><td>Due to the fact that testing is carried out during the plant operational phase, the detailed implementation of testing is not included in the PCSR, but safety principles and general requirements are stated in PCSR Chapters 18, 6, 7 and 9.

In-service testing is addressed as follows:
For safety systems, an analysis of periodic testing is performed, which includes a study of the comprehensiveness of the proposed testing regime. The conclusions of this analysis are included in the “General Rules for Operation”. Similar documents will be created for an EPR in the UK context.
For mechanical structures subject to pressurised system and/or specific nuclear equipment regulations, through the implementation of the applicable regulations. Some adaptation of these requirements may be necessary to meet specific UK requirements.
For civil works, through specific maintenance and inspection programmes, which may also require UK adaptation.
Specific UK requirements for testing will be identified and developed later in the EPR licensing process.</td></tr>
<tr><td>EMT.8 Structures, systems and components important to safety should be inspected and/or revalidated after any internal or external event that might have challenged their design basis.</td><td>The EPR is considered to comply with the SAP.

Defining procedures of inspection following events is not within the scope of the GDA. All design safety requirements and criteria are given in the PCSR and other engineering documents. Development of inspection procedures will be the responsibility of the dutyholder.</td></tr>
<tr><td>EAD.1 The safe working life of structures, systems and components that are important to safety should be evaluated and defined at the design stage.

and</td><td>The EPR is considered to comply with these SAPs.

Ageing and degradation issues are addressed by the following measures:

<u>Equipment qualification (See Chapter 3 of PSCR) :</u>

Depending on its safety role and the conditions for which the equipment is required to operate, qualification requirements are drawn up and incorporated into the equipment design via design specifications. In addition to the operating conditions,</td></tr>
</table>

SAP	Comment
EAD.2 Adequate margins should exist throughout the life of a facility to allow for the effects of materials ageing and degradation processes on structures, systems and components that are important to safety. **and** **EAD.3 Where material properties could change with time and affect safety, provision should be made for periodic measurement of the properties.** **and** **EAD.4 Where parameters relevant to the design of plant could change with time and affect safety, provision should be made for their periodic measurement.**	the qualification procedure takes account of the effects of ageing, i.e. the cumulative effects of the environmental conditions to which the equipment is subjected before the occurrence of the accident condition being considered for qualification. For the purpose of environmental qualification, different zones are considered for defining ranges of environmental conditions. For example, the Reactor Building is subdivided into two sub-zones: the zone which is accessible during operation (the service compartment) and the zone with restricted access during operation (the reactor compartment). The dose rates in normal operation differ significantly in the two zones, requiring different ageing irradiations to be considered. <u>Treatment of Reactor Pressure Vessel (see Chapter 5 of the PCSR)</u> In the surveillance programme, the evaluation of the radiation damage is based on pre-irradiation testing of Charpy V-notch and tensile specimens and post-irradiation testing of Charpy V-notch, tensile, and 1/2 T (thickness) compact tension [CTJ] fracture mechanics test specimens. The programme is at evaluating the effect of irradiation on the fracture toughness of reactor vessel steels based on an approach combining transition temperature and fracture mechanics. The vessel monitoring programme uses specimen capsules housed in holders attached to the outside of the internal vessel barrel, and positioned directly opposite the central section of the core. These capsules can be removed when the vessel head and the upper core support structure are removed. All capsules contain vessel steel specimens of the selected base metal located in the core region of the reactor and of the core weld metal and the associated heat-affected zone metal. Each capsule encloses tensile test specimens, Charpy V-notch specimens (which contain weld metal and metal from the heat-affected zone) and compact tensile specimens. Archive materials are kept in sufficient quantities for additional capsules. Activation and fission dosimeters are placed in drilled filler blocks. The dosimeters allow the evaluation of the flux experienced by the specimens. In addition, thermal monitors made of low melting point alloys are included to monitor the maximum temperature of the specimens. The specimens are enclosed in a tight-fitting stainless steel sheath to prevent corrosion and ensure good thermal conductivity. The complete capsule is helium leak tested. As part of the surveillance programme, a report on residual elements will be made for monitored materials and deposited weld metal. <u>Treatment of Civil structures (See Chapters 1 and 3 of PSCR)</u> : Details of the schedule of loads and load combinations that are used in the design of EPR safety classified civil structures,

SAP	Comment
	and the applicable limits, are specified in Part 1 of the EPR Technical Code for Civil Works (ETC-C) and summarised in PCSR Chapter 3. The load cases specified cover normal operational, testing and fault loading conditions. The analysis methods in ETC-C have been developed and validated using experience feedback from construction and operation of French NPPs. Loading conditions corresponding to the plant construction and operational phases are considered in order to ensure the security, stability and durability of the EPR civil structures. Design calculations for the civil structures allow for a 60 year plant service lifetime (particularly for the calculation of shrinkage/creep and pre-stressing losses). Therefore, there is confidence that the structures can fulfil their safety functional requirements over the lifetime of the facility. Part 3 of the ETC-C specifies the instrumentation requirements for monitoring the condition of the containment structures during the construction and operating phases, and during testing. Results are used to confirm the functional capability of the containment building over its service life • In addition, during the plant life, the classified systems, structures and components will be inspected and tested regularly to reveal any degradation which might lead to abnormal operating conditions or inadequate safety system performance.
EAD.5 A process for reviewing the obsolescence of structures, systems and components important to safety should be in place.	EAD.5 is not considered to be within the scope of the GDA. The dutyholder will be required to develop a process for review of obsolescence.
ELO.1 The design and layout should facilitate access for necessary activities and minimise adverse interactions during such activities.	The EPR is considered to comply with the SAP. Accessibility is taken into account in the design of EPR. The design of the layout is consistent with layout standards which take into account equipment accessibility.

SAP	Comment
	Design principles covering accessibility design and organisation of maintenance are based on use of codes and standards and experience feedback from operational French and German NPPs. Criteria are defined for controlling the atmosphere in rooms to which access is required. Details are described in Chapter 9 on ventilation, in particular with regard to air renewal, toxic gas control, nitrogen, etc. Sub-chapter 12.3 of the PCSR describes the radiation protection design in rooms in different buildings. Sub-chapter 18.2 of the PCSR presents design measures taken into account to allow for equipment maintenance. Sub-chapter 12.5 presents the design principles applied for post accident accessibility.
ELO.2 Unauthorised access to or interference with safety systems and their reference data and with safety-related structures and components should be prevented.	The management of plant security is not addressed in this document.
ELO.3 Site and facility layout should minimise the movement of nuclear matter.	This is not within the scope of the GDA, and will be addressed in the site licensing phase.
ELO.4 The design and layout of the site and its facilities, the plant within a facility and support facilities and services should be such that the effects of incidents are minimised.	The EPR is considered to comply with the SAP. Several principles and objectives stated in this SAP can't be fully addressed during the GDA phase (e.g. paragraph 207, or operational aspects). In addition to the response to the EDR 2 principle about redundancy, diversity and segregation, more specific consideration is given to: • paragraph 206 a), effects of incident and hazards on structures systems and components, within PCSR

SAP	Comment
	Chapters 13 and 3, • paragraph 206 b), interactions between safety structures, within PCSR Chapter 3. In addition to the level of protection already achieved in the design of previous PWR plants, the overall 4 division layout concept and the increased level of load cases taken into account in the design of safety systems have been the main sources of improvement of the EPR approach. With regard to recovery actions following an event, a general requirement on the time available applies to every PCC study, and will have to be substantiated on the basis of written procedures. Furthermore, every major operator action is included in the probabilistic assessment, whose human factors model takes into account all aspects of feedback from 58 French reactors (operational, simulator and theoretical studies). A complementary specific assessment of access conditions will be performed (e.g. radiation protection) on a case by case basis.
EHA.1 External and internal hazards that could affect the safety of the facility should be identified and treated as events that can give rise to possible initiating faults.	EPR is protected against the following external hazards (see PCSR Chapters 3 and 13): • Earthquake, • Aircraft crash, • External explosion, • Lightning and electromagnetic disturbances, • Groundwater, • Extreme meteorological conditions (high and low temperatures, snow, wind, rain, etc.), • External flooding, • Drought, • Ice formation, • Toxic, corrosive or flammable gas. Protection against the external hazards is achieved by designing the F1 classified safety equipment to withstand the loads associated with the hazard event, or by providing physical separation between redundant elements of a safety classified system so that their safety function can be performed despite the occurrence of the hazard. This design objective is to ensure that protection is provided against PCC design basis events despite the simultaneous occurrence of the external hazard.

SAP	Comment
	The following internal hazards are addressed in the EPR design (see PCSR Chapter 13): • Pipework leaks and breaks, • Failure of tanks, pumps and valves, • Internal missiles, • Dropped loads, • Internal explosions, • Fire, • Internal flooding. The EPR design objective is to ensure that internal hazards: a) do not prevent the carrying out of F1 safety functions; b) do not trigger PCC-3/4 events c) do not compromise the divisional separation of safety trains. If a PCC-2 event is triggered by a hazard, the design of the safety systems ensures that a safe shutdown state can be achieved, despite the occurrence of the hazard and the occurrence of an additional single failure, and allowing for the possibility that a redundant element of a safety system may be unavailable due to maintenance. For internal hazards triggered by a PCC or RRC event, the design ensures that a final safe state can be achieved despite the adverse effects of the hazard on safety structures, components and equipment.
EHA.2 For each type of external hazard either site specific or, if this is not appropriate, best available relevant data should be used to determine the relationship between event magnitudes and their frequencies.	The EPR is considered to comply with these SAPs. The EPR design against hazards is based on the load case method in which safety classified equipment is designed to withstand the effect of loadings due to credible internal and external hazards that could affect the unit. The load case methodology, which is the conventional PWR approach to hazard design, results in the specification of load cases that bound all credible hazard events and event combinations. Two major improvements to the traditional hazards approach have been implemented in EPR.

SAP	Comment
and **EHA.3 For each internal or external hazard, which cannot be excluded on the basis of either low frequency or insignificant consequence, a design basis event should be derived.** **and** **EHA.4 The design basis event for an internal and external hazard should conservatively have a predicted frequency of exceedance in accordance with the fault analysis requirements (FA.5).**	• The number and level of the load cases have been increased to take into account experience feedback from more than 30 years of operation, incidents, studies and other events in the field of PWR or nuclear operation, including recent developments (e.g. climate change studies, consideration of the threat of aircraft impact following the 9/11 event etc). • To confirm that the risk of core melt from hazard events is small, and comparable to the risk from internal plant events, internal and external hazards have been included in the scope of the PSA. This has enabled a check to be carried out that the level of load cases applied (probability or frequency of return) and the robustness of the design measures implemented, are consistent with the EPR global safety objective for core melt frequency, in other terms that the design is coherent and homogeneous. It will be demonstrated that for typical UK sites, the magnitude of hazard events considered in the UK EPR design basis is consistent with the fault analysis requirements, when data becomes available for relevant sites later in the GDA process. The final PSA demonstration for the UK EPR will aim to comply with EHA.2 (acknowledged as normal good practice), EHA.3 (replacing “design basis events” by “initiating events” with their selection process) and EHA.4.
EHA.5 Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition.	The EPR is considered to comply with the SAP. Where the hazard directly affects the operator (e.g. toxic gases), the consequences are addressed independently of the operating conditions. Concerning hazards causing damage to the equipment, the design approach is to protect every safety function required by the PCCs. The PCCs have been defined as the bounding cases of all postulated internal faults, in each frequency category, on the NSSS process and include, in their definition, the requirement of the most adverse conditions. This protection is achieved by designing the equipment to withstand the loads associated with the hazard event, or by providing physical separation between redundant elements so that the safety function can be performed despite the occurrence of the hazard.
EHA.6 Analyses should take into account simultaneous effects,	The EPR is considered to comply with the SAP.

SAP	Comment
common cause failure, defence in depth and consequential effects.	Combinations of internal and external hazards are addressed in the EPR design (see PCSR Chapter 13). Hazard loadings are combined when a link exists between the hazard conditions (e.g. flooding with extreme rainfall), where a hazard may arise as a consequence of another hazard (e.g. fire induced by aircraft crash) or where combining conditions from unrelated hazards is considered prudent for introducing conservatism into the design assessment, e.g. fire, postulated to occur after a controlled state has been reached following a PCC event or two weeks after a design basis earthquake or an RRC event. Safety classified systems and equipment required to bring the reactor to a final safety state in PCC design basis events are protected against internal and external hazards, either by being designed to withstand the hazard loads or by physical segregation of redundant trains of a safety system. In addition, the possibility of common cause failure of safety systems due to the hazard is addressed in the reactor design against total losses of redundant equipment (Risk Reduction Category A event).
EHA.7 A small change in DBA parameters should not lead to a disproportionate increase in radiological consequences.	The EPR is considered to comply with the SAP. This requirement is generally acknowledged in the whole field of safety analysis and not only for the protection against hazards. Concerning DBA events, consistency with this principle is one of the main results expected from the use of conservative assumptions and rules. In particular, the choice of the events themselves (load cases for hazards) is often the best demonstration of compliance. In the framework of hazard studies, it is for example the case when the design takes into account all physically possible events in a given family (on-site or off-site explosions, load drops, …). In some cases the response can be very different. Concerning weather conditions, extremely high temperatures can be anticipated in the sense where a shutdown of the plant may be required before they occur. After several hours, the decrease in risk largely outweighs the additional loss of capability of cooling systems. For other topics, the implementation of this principle may need to be substantiated by sensitivity and uncertainty analyses. Even if it is implemented through a large number of diverse ways, this principle remains one of the basics of nuclear safety and is acknowledged by the EPR design approach beyond the framework of DBA, for the robustness assessment of RRC and severe accident studies.
EHA.8 The total predicted frequency of aircraft crash, including helicopters and other	The EPR is considered to comply with the SAP. The general approach, applicable to the EPR design, is consistent with the French Fundamental Safety Guide (RFS) I.2.a.

SAP	Comment
airborne vehicles, on or near any facility housing structures, systems and components important to safety should be determined.	The predicted frequency of all crashes (gathered in three main aircraft categories) is determined for each relevant building, using the best available site data, to form the first term (P1) of the global probability of unacceptable consequences. The two other terms are the probability (P2) of a subsequent failure of a safety function (here defined as reactor shutdown, residual heat removal, spent fuel storage and radioactive effluents treatment), and the probability (P3) of an unacceptable release of activity at the site boundary. These two probabilities P1 and P2, are generally taken as 0 or 1 on the basis of simple and conservative criteria proposed in the RFS (notably, for P2, the ability of the building to withstand the crash). It may be noted that the EPR robustness towards aircraft crashes has been considerably improved taking into account the assumption of a military aircraft and then of a large commercial aircraft. This assumption was included on a pure deterministic basis without any reference to a predicted frequency.
EHA.9 The seismology and geology of the area around the site and the geology of the site should be evaluated to derive a design basis earthquake (DBE).	The EPR is considered to comply with the SAP. At the standard design stage, the seismic response of each standard building is calculated using the set of standard conditions: EUR 0.25g ground spectrum associated with six different ground conditions. These analyses supply the floor spectra for the design and/or qualification of the safety-related structures, systems and components. The seismic response of each building is also calculated for the site specific ground conditions, associated with the corresponding EUR spectrum which is set at 0.25g for standard structures and at a suitable level, given the site seismicity, for the site structures. These analyses supply the seismic stresses for the civil structures. The choice of the level of seismic event in these calculations and the conservative nature of the seismic design process ensure the existence of safety margins with respect to earthquakes. Nevertheless, verification will be performed for each specific site. It will be initially based on comparison of the seismic loads used for the design and the seismic displacements to be considered in accordance with the SAPs. Where this comparison does not demonstrate a safety margin, a more detailed analysis of a selection of plant items will be performed based on conservative parameters (modelling of ground conditions, damping …) and even experimental data. An “inspection earthquake” is defined for EPR, as the level below which there would not be any requirement for specific verification or inspection of the safety significant components before return to service, or continued normal operation. It corresponds to a maximum horizontal floor acceleration of 0.05g (free field) which is consistent with a site intensity below VI on the MSK scale.

SAP	Comment
	The general approach for earthquakes is presented in PCSR Sub-chapter 13.1, section 2.
EHA.10 The design of facility should include protective measures against the effects of electromagnetic interference.	The EPR is considered to comply with the SAP. The EPR approach is global; it relies upon design rules specifying the measures implemented to reduce the consequences of electromagnetic disturbance on equipment. These measures are: • Reinforcement of concrete, limiting the penetration of external disturbances, • Earth and ground networks, reducing the perturbing currents and hence their effects, • Connection to the earth network of the shielding of cables where they enter a building, preventing disturbances through cables, • Use of different and segregated cable trays for cables of different nature, • Shielding of cables and connection of both ends to the earth network, • Devices (e.g. diodes) preventing transients when inductive loads are switched on, Finally, immunity tests are performed on equipment to ensure continuity of operation. These tests cover all the possible perturbations: lightning strike going through, and being reduced by, the above barriers, switching of inductive loads, electrostatic discharges, conducted or radiated electromagnetic waves. Where equipment is located outside the building and cannot take benefit from the civil works protection, requirements for electromagnetic immunity are identical as regards: electrostatic discharges, wireless telecommunications, switching of

SAP	Comment
	inductive loads. On the other hand, local measures have to be implemented to prevent lightning caused disturbances. More detail is presented in PCSR Sub-chapter 13.1, section 7, including reference to the applicable CEI standards.
EHA.11 Nuclear facilities should withstand extreme weather conditions that meet the design basis event criteria.	The EPR is considered to comply with the SAP. As stated in PCSR Sub-chapter 13.1, section 6, EPR design takes into account extreme weather conditions such as snow, wind (including generated missiles), extreme cold temperatures in air (up to -35°C) and water (frazil ice phenomenon), extreme high temperatures in air (up to 42°C) and water (up to 26°C) with associated assumptions on humidity, as well as drought. These values will be confirmed for each UK EPR site. The design aims to cover potential realistic climate developments during the lifetime of the plant, beyond those initially considered. The combinations of hazard events (external hazards, internal hazards and other than hazards), which are taken into account in the design of civil structures, are presented in the ETC-C civil design code for EPR.
EHA.12 Nuclear facilities should withstand flooding conditions that meet the design basis event criteria.	The EPR is considered to comply with the SAP. Basically, the protection of the nuclear island platform from the risk of flooding from the sea is ensured by its level. Following an event which occurred at the Blayais power plant in the south west of France in 1999, the methodology used to determine the prescribed levels has been thoroughly revised to include all relevant phenomena (see PCSR Sub-chapter 13.1, section 5) and all necessary margins (uncertainties, climate changes, …). The UK EPR will take benefit from the conclusions of this work, based on several years of engineering and R&D, and extensively reviewed by the French safety authority. In addition, the main other sources of flooding taken into account in the EPR design are (see PCSR Sub-chapter 13.2, section 8): • Pipework leaks and breaks

<table>
<tr><th>SAP</th><th>Comment</th></tr>
<tr><td></td><td>Actuation of fire protection systems
Rainfall
Effects of an earthquake on non-seismic structures</td></tr>
<tr><td>EHA.13 The on-site use, storage or generation, of hazardous materials should be minimised and controlled and located so that any accident to, or release of, the materials will not jeopardise the establishing of safe conditions on the facility.</td><td>The EPR is considered to comply with the SAP.

The load case approach for hazards allows a generally simple and conservative way to ensure that the operation of the plant is consistent with the safety demonstration. More detail is given in the submission as follows:
explosions, internal or external to the buildings in PCSR Sub-chapter 13.2, section 6 and PCSR Sub-chapter 13.1, section 4
fire in PCSR Sub-chapter 13.2, section 7
Toxic gas analysis is proposed to be finalised on a site specific basis.</td></tr>
<tr><td>EHA.14 Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.</td><td>The EPR is considered to comply with the SAP

The hazard conditions identified in EHA.14 are addressed within the EPR design. A summary of the design approach with reference to the EPR PCSR is given below.

<u>Fire</u>

Fire protection is described in PCSR Chapter 13. The safety objective for fire protection is to ensure that the safety functions are performed in the event of a fire inside the installation, which implies that:
a fire must not cause the loss of more than one set of redundant equipment in an F1 system;
the non-redundant systems and equipment, which perform the safety functions must be protected against the effects of a fire in order to ensure continuous operation;
a fire associated with a PCC 2-4 event must not compromise the habitability of the control room.</td></tr>
</table>

SAP	Comment
	• A remote shutdown station is supplied in case of unavailability of the main control room. The ignition of any combustible material present in the plant perimeter is considered as a potential fire source, except for low and very low voltage electrical cables and equipment or materials protected by a housing or box. A fire is assumed to occur during normal plant conditions (from full power to shutdown condition) or in a post-accident condition once a controlled condition has been achieved. The three types of measures are implemented to protect against fires: • Prevention, • Containment, • Control. Details are given in the PCSR and ETC-F (EPR technical code for fire). Missiles, Toxic Gas Release, Explosions EPR design principles require that industrial installations and transport routes which may pose a risk to the plant are identified for the site. The risks to be considered include: explosion: compression wave, ground movements, missiles, thermal radiation and smoke due to fires and movement of toxic, corrosive or radioactive gases (see PCSR Chapter 13). The EPR is designed to withstand a design basis explosion compression wave due to an external explosion, as described in PCSR Chapter 13. The EPR is designed to withstand the impact of general and military aviation, and the impact of a large civilian airliner, including effects of fuel fires. Detailed justification and necessary adjustment of the design measures against hazards associated with the specific site will be carried out when a site is selected for the UK EPR. Dropped Loads The design principles for protection against dropped loads are given in PCSR Chapter 13. Protection against dropped loads is based on the following preventive measures:

SAP	Comment
	• Classification of the lifting devices depending on the nuclear safety consequences of a postulated dropped load from the associated lifting device. • Installation or design rules for potential targets, • Operating rules for lifting devices: restriction of operating periods, limitation in lift heights, use of prescribed routes for transporting heavy loads etc. For each lifting device used in safety classified buildings, it must be demonstrated that the risk prevention is appropriate and the consequences of any postulated dropped load are acceptable. <u>Pipe Failure Effects</u> PCSR Chapter 13 described the design principles applied to protect safety classified structures and mechanical, electrical and instrumentation & control system components against the consequences of pipework leaks and breaks. The following potential consequences are considered when necessary after high energy pipe break: Mechanical and thermal effects in the vicinity • Jet impact forces. • Pipe whip. • Reaction forces. Global effects on room ambient conditions • Humidity. • Pressure increase • Temperature. • Radiation. • Flooding. Effects internal to the ruptured pipe

SAP	Comment
	• Flow forces. • Pressure wave forces Pipe restraints are provided where necessary to mitigate the consequences of pipe breaks on the surrounding equipment. <u>External and Internal Flooding</u> EPR design principles require that the EPR site is protected against external flooding from a range of water sources including river and coastal flooding, dam burst and flooding due to abnormal rainfall and groundwater levels (see PCSR Chapter 13). The different types of protection against external flooding are: • setting of the platform level and volumetric protection, • use of fixed or mobile protection devices, • design of a suitable water drainage system. The design of flooding protection measures is site specific and is based on design basis flooding events at a given return period. For the UK EPR the design basis flooding events will be defined specific to the site chosen and will conform to the return period required by hazard analysis of UK sited plants. The principles of EPR design against internal flooding are described in PCSR Chapter 13 Internal flooding may damage equipment or civil engineering structures, or prevent correct operation of the equipment. The following potential initiators of flooding are addressed: • Leaks and breaks in pressure retaining components • Incorrect system alignment, • Flooding by water from neighbouring buildings, • Spurious operation of the fire protection system, use of mobile fire extinguishing equipment, • Overfilling of tanks, • Consequence of isolation device failure.

SAP	Comment
	The equipment and structures deemed liable to fail in case of flooding are: • All electrical and I&C equipment, apart from cables whose terminals are not flooded and other waterproof equipment, • Certain sections of the civil engineering structures, if they are not able to withstand the floodwater pressure or temperature, • All non-waterproof mechanical equipment. The EPR is designed so equipment required to carry out F1 main safety functions is adequately protected against internal hazards, including flooding, either by physical protection, or segregation to ensure that not more than one redundant element of a safety system can be affected by the hazard.
EHA.15 The design of the facility should prevent water from adversely affecting structures, systems and components important to safety.	The EPR is considered to comply with the SAP. See the response to EHA.12 above.
EHA.16 Fire detection and fire-fighting systems of a capacity and capability commensurate with the credible worst-case scenarios should be provided.	The EPR is considered to comply with the SAP. Limiting the spread of a fire (containment) is achieved by dividing the buildings into fire compartments which use physical or geographical separation principles. Redundant trains in the F1 safety classified systems are installed in different areas, fire compartments or fire cells. Installed fire barriers or physical separation ensure that only one of the redundant trains in an F1 system may be endangered by a single fire. Detection and fire fighting devices are installed to detect and fight the fire and to control it as quickly as possible. The purpose of the detection system is to quickly detect the start of a fire, to locate the fire, to trigger an alarm and in some instances, to initiate automatic actions. Fire fighting devices, which are fixed or portable depending on the nature of the fire and the type of equipment to be protected, are provided.

SAP	Comment
	Concerning the 'worst case' situation, the functional failure of all equipment without adequately justified protection is postulated in the compartment or cell where the fire breaks out. In addition, the countermeasures needed to protect safety systems are seismically designed.
EHA.17 Non-combustible or fire-retardant and heat-resistant materials should be used throughout the facility.	The EPR is considered to comply with the SAP. According to the "defence-in-depth" principle, fire protection includes fire prevention, fire detection, extinguishing (fire controlling) and mitigation of fire effects (fire containing). Priority is given to measures preventing the risks and consequences of fire by 1) limitation of fire loads; choosing non-flammable or hardly inflammable equipment and fluids as far as possible. 2) using fire retardant cables throughout the facility 3) avoiding ignition sources in the vicinity of combustible materials Should a fire occur, all its consequences are studied. All the barriers and thermal screens are designed to be effective taking in account the severity and the duration of the reference fire (see PCSR Chapter 13).
EPS.1 Removable closures, the failure of a removable closure to a pressurised component or system that could lead to a major release of radioactivity should be prevented.	The EPR is considered to comply with the SAP. Adequate design and manufacturing precautions are taken to ensure the prevention of failure of removable closures, for every metallic pressure vessel component. This consideration is present at all stages of the design procedure, i.e.: • Closure cover, studs, nuts and gasket material selection. This is performed considering the intrinsic properties of the material with respects to different criteria and including its resistance in operating conditions. • Material procurement. The procurement has to fulfil specifications meant to ensure the assumed requirements are effectively produced. • Component design. The geometry should give the greatest chance of realising a defect free and/or defect tolerant component. Also, stress evaluations are performed using methods and criteria according to well-proven construction codes (RCC-M, ASME). Possibility of repair and replacement is also taken into account as shown

SAP	Comment
	in the PCSR Sub-chapter 5.4, section 4.3.4. • Component manufacturing. The component manufacturer is evaluated and approved. • Mechanical testing. This is meant to ensure, by actual verification, that the minimum mechanical characteristics, and especially those important for the envisaged application, are indeed met by the product under consideration. • Inspections. Essentially in the form of non–destructive examinations, this step is specifically devoted to the verification of the absence of unacceptable defect in the manufactured component. For example, when applied to the pressuriser manhole, this means that pre-service inspection of studs and nuts is specified and performed using visual examination as well as ultrasonic testing techniques. Volumetric pre and in-service inspection of the ligaments between each stud hole in the plate are also requested and typically imply ultrasonic testing or radiographic examination techniques. This is quite similar to what is performed on the circular weld around the manhole which is also part of the pressure retaining boundary of the pressuriser. On site, procedures exist that prevent the opening of any hole in conditions which would not be safe.
EPS.2 Flow limiting devices should be provided to piping systems that are connected to or form branches from a main pressure circuit, to minimise the consequences of postulated breaches.	The EPR is considered to comply with the SAP. Small branch connections attached to the main pressure circuit by welds are used for measurement devices, such as flowrate sensors. The small diameter used for these branches minimises the consequence of breaches and is a method of limiting the flow without a requirement for dedicated flow limiting devices. The only use of a flow limiting device is the flow restrictor placed in the outlet nozzle of the steam generator, which limits the discharge flowrate in case of a steam line break.
EPS.3 Adequate pressure relief systems should be provided for pressurised systems and provision should be made for periodic testing.	The EPR is considered to comply with the SAP. Pressurised systems are provided with safety valves so that the system integrity is ensured in the event of overpressure. The main relief valves are safety classified components subject to periodic testing. Examples of relief valves used for pressurised system protection are given below:

SAP	Comment
	<u>Pressuriser Safety Relief Valves (PSRVs)</u> These relief valves are used to protect the RCP [RCS] and reactor vessel against overpressure events in at-power states and shutdown conditions. To protect the RCP [RCS] against overpressure events at power, the opening pressures of the main safety valves on each protection line are staggered. In this case, the PSRVs operate in automatic mode via spring-loaded pilots. To protect the RCP [RCS] against overpressure events when the reactor is in a shutdown condition or during the long-term depressurisation, PSRVs are operated via solenoid pilot valves triggered by a specific I&C system, or in remote control mode. Protection of the RCS system against overpressure is described in PCSR Sub-chapter 5.4, section 7. <u>Safety relief valves for RHRS protection</u> These spring-loaded pressure relief valves protect the RRA [RHR] against overpressure after the RRA [RHR] is connected to the RCP [RCS] during cooldown. If primary coolant system overpressurisation occurs during these states, the spring-loaded pressure relief valves are required to open before the pressuriser relief valves. Protection of the RRA [RHR] system against overpressure is described in PCSR Sub-chapter 6.3. <u>Main Steam Relief Valves for MSSS protection</u> These relief valves ensure protection of the Main Steam Supply System and of the Steam Generator against overpressure. Protection of the MSS system against overpressure is described in PCSR Sub-chapter 10.3 and 6.8.
EPS.4 Overpressure protection should be consistent with any pressure-temperature limits of operation.	The EPR is considered to comply with the SAP. Overpressure protection analyses are presented in Chapter 3 of the PCSR; the methods and criteria applied are in accordance with the RCC-M code. Overpressurisation is considered in both hot and cold conditions, with pessimistic assumptions being made with regard to both thermal-hydraulic conditions and the safety device setpoints.

SAP	Comment
	For example, the pressure setpoints of the Pressuriser Safety Relief Valves (PSRVs) are changed depending whether the reactor is at power or in a shutdown state, thus protecting the reactor against overpressure in these different operation modes. More details of the design and operation of the PSRVs are presented in Sub-chapter 5.4 of the PCSR.
EPS.5 Pressure discharge routes should be provided with suitable means to ensure that any release of radioactivity from the facility to the environment is minimised.	The EPR is considered to comply with the SAP. The first means of minimising potential radioactivity releases is by monitoring radioactivity levels of the main primary coolant during normal operation, with the obligation to shut down the plant if abnormal activity appears; therefore the amount of radioactivity release through potential primary water or steam release to the environment is limited. Collection of the potential primary water/steam leakages is dealt with in the following manner: <u>The pressuriser relief lines</u> In order to prevent reactor coolant discharge into the reactor building during normal operation (potential leaks of the pressure safety relief valves) and during pressure safety relief valve testing, the pressuriser relief system discharges into the Pressuriser Relief Tank (PRT), which is a closed tank located inside the containment. From this tank, primary water is discharged to the Waste Treatment System (refer to Chapter 11 of the PCSR) by the Nuclear Vent and Drain System (RPE) [NVDS]. There is no discharge to the PRT during category 2 overpressure events (refer to Sub-chapter 5.5 section 5 and Sub-chapter 3.4, section 1.5 of the PCSR). If the expected final operating pressure/temperature values in the PRT are exceeded, fluid is discharged to the reactor building after mechanical rupture of bursting disks. This discharge can only occur during category 3 or 4 over-pressure accidents and RRC events. In that case, protection of the public is ensured by the containment. For these transients, the acceptability of the releases is demonstrated by the transient analyses presented in the PCSR. <u>Other safety valves of contaminated systems</u> These are connected to the RPE [NVDS] for treatment.

SAP	Comment
	The Reactor Coolant Pumps seal leakage recovery Refer to PCSR Sub-chapter 5.4, section 1 for more information The shaft line sealing system is made up of three seals arranged in series and a standstill seal system. The first shaft seal is a controlled leak-off seal, it provides the majority of the pressure drop. Primary water is recovered by the RCV [CVCS] before being re-injected to the RCP [RCS] by the charging pumps Seals no. 2 and 3 provide the remaining pressure drop, with a small leak to the vents and drains system (RPE) [NVDS]. The standstill seal system is a device used to block leakage from the third and last seal. Valves The risk of stem packing box leakage is dealt with in different ways. It can be avoided by using hermetically sealed valves such as the PSRVs (totally encased in a pressure resisting casing) or by bellows. Sub-chapter 5.4, section 6 of the PCSR shows that multiple packing with a leak-off collection route is implemented for certain types of valves. In that case, leakage recovery pipes are routed to the nearest RPE [NVDS] header system. The primary leakages are then routed to the radioactive waste management systems, which provide containment, measurements and control of radioactive discharges to the environment during normal operation and fault studies. The RPE [NVDS] collects all the liquid waste produced both inside (and outside) the containment and a part of the gaseous waste in the reactor building, and transports it to the associated storage and treatment facilities prior to monitoring and discharge. In this respect, the RPE [NVDS] contributes to compliance with the authorised discharge limits for liquid and gaseous waste. The liquid effluent collection system is designed to enable the controlled re-injection into the reactor building of highly-contaminated liquid effluent present in the nuclear auxiliary building or in the fuel building in a post-accident situation. The TEG [GWPS] system enables treatment and decay of primary gaseous effluent derived from treatment of the primary

SAP	Comment
	coolant or present in the cover gas of tanks containing primary coolant. It contributes to the functions of radioactive containment and limitation of discharge in normal operation. The design therefore ensures that any release of radioactivity from the facility to the environment is minimised.
EMC.1 The safety case should be especially robust and the corresponding assessment suitably demanding, in order that an engineering judgement can be made for two key requirements: **a) the metal component or structure should be as defect-free as possible;** **b) the metal component or structure should be tolerant of defects.**	The EPR is considered to comply with the SAP. The PCSR lists material specifications used for the principal pressure-retaining applications in Class M1 primary components and reactor coolant system piping. Material specifications with grades, classes, or types are included for the reactor vessel components, steam generator components, reactor coolant pump, pressuriser and main coolant lines. The materials used for the reactor coolant pressure boundary conform to the RCC-M Code Rules. According to their safety importance, adequate design and manufacturing precautions are taken to ensure every metallic structural component is as defect-free and as defect-tolerant as possible, at all stages of the process, such as: • Material selection. This is performed considering the intrinsic properties of the material with respect to different criteria, including its resistance to fracture. A well-proven material for the kind of application under consideration is preferred. Specific requirements going beyond Code rules may be added to suit the needs of a given application. • Material procurement. The procurement process has to meet steel-making, forging and heat treatment specifications that are designed to ensure the required mechanical properties are achieved. • Component design. Whenever possible, the design used components with characteristics (geometry: size and shape) that give the greatest chance of being defect free and/or being tolerant to defects. • Component manufacturing. Past experience in the field is an important consideration in the selection of a manufacturer. For important components, the RCC-M code requires prior qualification of the manufacturer (M 140 for shop and product and M160 for cast components). The component manufacturer must be evaluated and approved and their capability periodically checked and verified. • Mechanical testing. This is intended to ensure that minimum mechanical characteristics, especially those important for the envisaged application, are met by the product under consideration.

SAP	Comment
	• Inspection. The inspection step which involves non–destructive examination, is verifies the absence of defects in the manufactured component. Both surface and volumetric inspections are conducted. • Fracture mechanics analyses. To give additional confidence in the product and in the entire procedure, fracture mechanics analyses are performed assuming postulated defects. The objective is to confirm tolerance to defects, by demonstrating that defects that may be undetected, given the detection means available and applied, are still stable under all loads. The "break preclusion" demonstration is an example of such an approach. For additional information on defects, see PCSR Chapters 5, 6 and 10.
EMC.2 The safety case and its assessment should include a comprehensive examination of relevant scientific and technical issues, taking account of precedent when available.	The EPR is considered to comply with the SAP. Structures, systems and components of the EPR are classified according to nuclear safety classification, mechanical classification, seismic category, and designed to appropriate codes and standards rules. Depending on this classification, the safety case defines a domain where each component or structure important to safety should be operated and controlled throughout the entire plant operating life. The UK PCSR presents justification and demonstration of relevant scientific and technical issues important for the safety case. Extensive use is made of available operating experience from similar French and/or German NPPs. The safety case is considered to take account of and use all the available scientific and technical knowledge obtained in the PWR field. In both AREVA and EDF, a comprehensive survey of relevant scientific and technical issues is being conducted and continuously updated through • information delivered by the unit dedicated to technological tracking (intelligence), • participation in international workshops, seminars or congresses, • examination of the various issues raised by members of the FROG (Framatome Owners' Group), • participation in continuing programmes of R&D, notably in association with other nuclear industry members, etc

SAP	Comment
	For additional information on technical issues, see PCSR Chapters 3, 5, 10 and 17.
EMC.3 Evidence should be provided to demonstrate that the necessary level of integrity has been achieved for the most demanding situations.	The EPR is considered to comply with the SAP. Evidence that the necessary level of integrity is achieved for the most demanding situations is given through: • the definition of a set of conditions as required by the RCC-M Code for Class 1 equipment and • ensuring that components important to safety are operated and controlled within a well-defined safe operating envelope throughout the operating life. This set of design, service and test conditions considers all Component Condition Categories (CCCs), including accidental conditions, expected or postulated to occur during operation, with the relevant transients. Generally speaking, the evaluation the behaviour of each component under these conditions is performed on a damage prevention basis following the RCC-M Code rules and includes an evaluation of fatigue due to cyclic stresses. For additional information on evidence of necessary level of integrity, see PCSR Chapters 3, 5 ("non breakable components"), 10 and 17.
EMC.4 Design, manufacture and installation activities should be subject to procedural control.	The EPR is considered to comply with the SAP. AREVA and EDF work to quality assurance programmes which ensure that procedural control is applied throughout design, manufacture and installation activities including design changes. Both AREVA and EDF's past experiences in this area are internationally acknowledged. Procedures associated with design under configuration control are followed and reflected in all technical documents. For additional information on procedural control, see PCSR Chapters 3 and 21.

SAP	Comment
EMC.5 It should be demonstrated that safety-related components and structures are both free from significant defects and are tolerant of defects.	The EPR is considered to comply with the SAP. The requirement to maintain all safety-related components as defect free and as defect tolerant as possible is applied at all stages of the design and construction process. Details have been given in the response to EMC.1. For additional information on defects, see PCSR Chapters 5, 6 and 10.
EMC.6 During manufacture and throughout the operational life the existence of defects of concern should be able to be established by appropriate means.	The EPR is considered to comply with the SAP. Throughout EPR manufacturing and operation, appropriate means for defect identification, characterisation and evaluation are implemented. This is achieved through the performance of rigorous inspections during manufacturing, using non destructive examinations (radiographic, ultrasonic, magnetic particle and dye penetrant examinations). Regular in-service inspections are also carried out according to RCC-M requirements to ensure that the situation prevailing at beginning of life is not adversely altered during operation. On this issue, see also the response to SAP EMC.1. For additional information on defects, see PCSR Sub-chapter 3.8 (RCC-M) and Chapter 21.
EMC.7 For safety-related components and structures, the schedule of design loadings (including combinations of loadings), together with conservative estimates of their frequency of occurrence should be used as the basis for design	The EPR is considered to comply with the SAP. Following the requirements of RCC-M, the design basis for the EPR uses a set of load cases which are chosen to be conservative in terms of both magnitude and frequency, i.e. number of occurrences. The conservative estimation of all envisaged, single or combined, events covers the entire lifetime of the equipment and is applied as a basis for design. It is specified in the Design Specification. In accordance with RCC-M requirements, reactor service conditions are divided into

SAP	Comment
against normal operating, plant transient, testing, fault and internal or external hazard conditions.	• Levels A and B (normal and upset), • Level C (emergency) and • Level D (fault) categories. Level D conditions include limiting accidents, such as loss of primary coolant (LOCA), design basis earthquake (DBE), etc. Depending on the level of the service conditions, primary and/or secondary loads are considered. In contrast to externally applied primary loads, secondary loads produce self-limiting stresses due to structural self-constraint. Thermal loads are an example of such secondary loads. Level A conditions, which include start up/shut down, are considered in fatigue assessment/analysis to demonstrate that safe design life requirements are met (60 year life for the EPR). The fatigue assessment is made according to the RCC-M Code. For additional information on loadings, see PCSR Chapters 3 (design conditions and loads, load combination rules) and 5.
EMC.8 Geometry and access arrangements should have regard to the requirements for examination.	The EPR is considered to comply with the SAP. During the design phase of EPR, the requirement for inspectability has been a primary consideration for the plant designers. Regular in-service inspection is recognised as being of paramount importance for the safe operation of a nuclear power plant and ease of inspection is considered crucial for reliable continuous and safe operation. Access provisions have thus been considered and implemented in order to simplify and reduce the inspection work and simultaneously reduce the radiation dose to which inspectors may be subjected. Test and inspection plans are written in advance of pre-service inspections, involving both safety and component specialists. The RPV upper shell is an example of application of the inspectability philosophy. The RPV flange and the nozzle shell of the EPR is an integral forged piece. Previously, this zone has been fabricated in two pieces (shells) connected via a circumferential weld. The elimination of this weld reduces the inspection requirements for the zone and is especially valuable considering this is a region with a complex shape and thick walls. The set-on mounting of the nozzles also contributes to a higher accessibility, thus allowing an easier inspection.

SAP	Comment
	For additional information on examination requirements, see PCSR Chapters 3, 5 (inspection access) and 19.
EMC.9 The choice of product form of metal components or their constituent parts should have regard to enabling examination and to minimising the number and length of welds in the component.	The EPR is considered to comply with the SAP. The concern to ensure easy inspection of parts and components that need to be periodically examined includes the choice of material and product form. The best possible compromise between the various requirements, including both integrity and inspectability, is chosen. For example, the RPV is made from ring forgings connected by means of circumferential welds, thus eliminating longitudinal welds that would be subjected to higher stresses. The EPR has been designed with the requirement, supported by French Safety Authorities, that the number and length of welds should, as far as possible, be minimised. Here again optimisation principles are applied: when welds are retained that could be eliminated, it is because they their advantages outweigh the associated drawbacks. In such cases, controllability is assessed and verified. Welding is performed following state-of-the-art procedures (i.e. controlled welding parameters) involving stringent qualification requirements (with test and production coupons). The welds are then subjected to strict quality control (the welds in the nuclear category are required to be up to 100% radiographed; ultrasonic and liquid dye penetrant tests are also used to check against cracks). For additional information on product form, see PCSR Chapters 5, 6, 9 and 10.
EMC.10 The positioning of welds should have regard to high-stress locations and adverse environments.	The EPR is considered to comply with the SAP. Weld integrity is a key issue in the design of reliable nuclear pressure retaining components. Indeed, welds are recognised as potential weak points for structural integrity and as such are the object of constant attention. The position of welds is only one aspect of the general structural resistance problem; others are related to the nature of the base metal, weld quality, shape, length, loads, environment, inspectability, etc.

SAP	Comment

	The EPR weld features result from a compromise between various opposing requirements such as:
	
	• material requirements: homogeneous welds are preferred to dissimilar welds; filler material is selected to have characteristics corresponding to the expected mechanical behaviour,
	• inspectability: for example, in general, forged austenitic stainless steel is preferred over cast stainless steel because of the better ultrasound transmission in the forged form which is favourable for volumetric examination. A notable exception is the reactor coolant pump bowl where the complex shape does not favour use of a forged piece and where casting has always been successfully used to meet RCC-M requirements regarding material and qualification of the first part in a series.
	• welding characteristics: automatic vs. manual welding, weld parameter control
	• weld shape: narrow groove welding is used mainly
	• weld length : as far as possible, length is reduced to decrease the probability of defect occurrence,
	• weld position : as much as possible, weld positions are chosen so as to
	    o avoid the neighbourhood of geometric singularities, stress concentration zones, vessel thick-walled portions, etc.
	    o allow easy inspection; thus, care is taken to choose places limiting or avoiding any interference with other structures or with civil works,
	    o be submitted to moderate loads: if possible, highly stressed areas are avoided so as to maximise the margins to any appreciable potential damage,
	    o be faced with limited environmental constraints: these include irradiation, corrosion and temperature effects with emphasis given to possible degradation related to ageing,
	
	The cylindrical shell of the RPV can be taken as an example. It consists of two sections, an upper and lower part.
	
	To minimise the number of large welds, which reduces the frequency of in-service inspections, the upper part of the RPV is machined from a single forging and fabricated with eight nozzles. Since the nozzles are fabricated into the massive plate used in the RPV shell, most of the reinforcement needed for the nozzle design is provided by the vessel material itself. Therefore, the nozzles used in this design are of the “set-on” type requiring a less substantial weld bead than would

SAP	Comment
	otherwise be required. On the other hand, the lower part consists in 2 shells with a circumferential weld at mid core height. This feature, which is present in all existing French RPVs, is maintained in the EPR because • operating experience is highly positive, • comparison with past conditions in this area is favourable: in the EPR, this mid-core zone experiences a lower flux level (notably, due to the heavy reflector) even considering the envisioned 60 years lifetime, • stringent material requirements are applied to ensure a low end of life RTNDT (low phosphorus and copper contents). Also, a single core shell design is not feasible due to the large dimensions of the EPR RPV. At present, a larger core shell would not permit removal of all welds out of the core zone but would increase the weight and volume of the ingot (increasing risks of defects and reducing the number of potential manufacturers). For additional information on weld position, see PCSR Chapters 5, 9 and 10. Chapter 17 contains a discussion on the reasonable practicability of removing the RPV weld at mid-core height.
EMC.11 Failure modes should be gradual and predictable.	The EPR is considered to comply with the SAP. The stress report of a component is produced to demonstrate that all possible failure modes, given the various load conditions the component may be subjected to, are adequately addressed. Following Code requirements ensures the prevention of any damage related to the following failure modes • Excessive elastic deformation including elastic instability • Excessive plastic deformation • Plastic instability – incremental collapse • High strain-low cycle fatigue

SAP	Comment
	• Fast fracture with provisions taken for any corrosion phenomenon that could take part in the degradation process. Sudden or catastrophic failure is the least predictable failure mode and, therefore, adequate precautions need to be taken systematically to ensure adequate safety margins. In this field, much of the confidence is derived from the choice of material which should exhibit mechanical properties compatible with the role it is to play. For example, a non negligible domain for plastic behaviour, bringing an appreciable ductility margin, is one requirement. Minimal criteria for fracture toughness are also specified. As stated above, a high level of integrity is then provided by the design requirements of the RCC-M Code. Finally, the break preclusion (leak before break) concept also participates in the exclusion of fast fracture. This approach has received a large international recognition and approval. It demonstrates that a detectable leak appears from a postulated through-wall flaw well before flaw growth is given any chance to lead to a size that could result in failure. For additional information on failure modes, see PCSR Chapters 5 and 10 (break preclusion, prevention of potential damage).
EMC.12 Designs in which components of a metal pressure boundary could exhibit brittle behaviour should be avoided.	The EPR is considered to comply with the SAP. All precautions are taken at design, fabrication and operation stages to ensure an extremely high quality is achieved in the equipment, especially components of the pressure boundary. This contributes to the demonstration of a low probability of failure, notably brittle fracture, under every condition from normal to accidental. This point is verified through computations for the entire lifetime of the component under investigation and takes into account the possible embrittlement due to irradiation. Various considerations contribute to this demonstration: • well proven, ductile materials are preferred whenever possible,

SAP	Comment
	• fabrication is checked against the presence of defects (cracks, notches, indentations, etc.), • loads are kept at a low and acceptable level taking into consideration thermal transients, residual stress, stress concentration, etc. • design operation takes place at temperature levels that preclude the possibility of brittle failure. Generally speaking, reactor components are operated at temperatures which ensure the material fracture toughness to be in upper shelf conditions. For the RPV, the reference temperature at nil ductility transition (RTNDT) is measured or evaluated at different times in the component life to avoid any risk of brittle fracture although various ageing mechanisms may take place. For additional information on precluding brittle behaviour, see PCSR Chapters 5, 9 and 10.
EMC.13 Materials employed in manufacture and installation should be shown to be suitable for the purpose of enabling an adequate design to be manufactured, operated, examined and maintained throughout the life of the facility.	The EPR is considered to comply with the SAP. The essential principles used for the material selection of the EPR are: • Selection and standardisation of materials to ensure an optimal combination of functional, design and fabrication features. • High toughness of the materials to avoid fast fracture of the components and systems over the whole plant lifetime of 60 years. • Adequate workability for avoiding non-conformances in welding and forming. • Corrosion resistance in all operation conditions (normal operation, shutdown), in combination with consistent fluid chemistry. • Selection of materials which do not show significant ageing (temperature, irradiation, environment). • Use of materials for which there is long-term manufacturing and operating experience: licensing of new materials only proposed after rigorous qualification. • Selection, standardisation and specification of adequate and optimised semi-finished products and their

SAP	Comment
	manufacturing / processing techniques. The prevention of ageing risks and other damage mechanisms (erosion-cavitation, erosion corrosion, intergranular corrosion, stress corrosion cracking, fatigue, fast fracture) is obtained in the first place through an appropriate choice of material grades, and their procurement conditions, depending on the intended use. The technical constraints lead to the choice of materials that are: • well known to manufacturers, • result from optimisation of conventional commercial grades over a period of time, • a result of a constant striving to achieve good reproducibility of properties, • of a uniform structure and free from significant fabrication defects. The nuclear construction codes require: • Narrower chemical analysis ranges for major components, reactor coolant piping or steam generator tube materials. • Very strict control of impurities and inclusions. • Stringent non-destructive testing at all stages in manufacture. • Detailed testing of the first fabricated component. • Recording of essential variables governing properties required during use, in the supplier's technical fabrication programme. The following principal parameters are those used to define the selection of materials, depending on the application: • Tensile strength governing sizing, • Operating temperatures, • Thermal properties,

SAP	Comment
	• Ductility and toughness, governing fast fracture prevention, • Possibility to manufacture large components, • Weldability, if needed, • General corrosion behaviour, • Erosion-Corrosion prevention, • Intergranular corrosion prevention, • Stress corrosion cracking prevention, • Ageing under neutron irradiation, • Thermal ageing prevention, • Limitation of dosimetry, • Controllability during manufacturing and operation. Main principles for material selection are: • Manufacturing aspects: Workability is considered due to forming methods being increasingly used in the manufacture of components. This permits reducing the total number of welds, improving shop schedules at the fabrication stage and reducing the corresponding inspection requirements. An important contribution to good weldability and material properties can be made by using modern steel-making practices to achieve low sulphur and trace-element contents, high homogeneity and avoidance of macro- and micro-segregation. Requirements imposed on the base metal must also be satisfied by the weld metal and the heat affected zones (HAZ). From this point of view, the weldability of the base metal, the selection of filler metals and the optimisation of welding parameters are all important technical factors. During the stress-relief heat treatment of ferritic steels, the coarse-grain zone of the HAZ is subjected to relaxation processes which may lead to micro-separations along the former austenitic grain boundaries as the result of a

SAP	Comment
	high-temperature creep process. This phenomenon can be reliably controlled, both in welded joints and under overlay claddings, by selecting suitable optimised materials and welding techniques, monitoring the layer build-up and heat input and optimising heat treatment sequences. • Corrosion resistance: To avoid corrosion products in the primary circuit for piping systems and components in contact with primary water, stainless steels are used. The surfaces of ferritic components are clad using austenitic stainless steel weld metal or austenitic stainless steel product forms (plates, pipes, forging and castings) are used. o If the environment is in contact with air (i.e. saturated with air), to avoid corrosion all piping systems and components are made from austenitic stainless steel. o All piping systems and components with stagnant fluid condition are designed using austenitic stainless steels to avoid corrosion. o Piping systems or components with two phase flow or flashing conditions are designed using CrMo-alloy ferritic steel grades, austenitic stainless steel or martensitic stainless steel. With respect to susceptibility to intergranular corrosion, austenitic stainless steels with optimised chemical composition will be used: o Austenitic stainless steel with low carbon content (up to 0.035% unless prevention is ensured by an appropriate test) o Austenitic stainless steels stabilised with Niobium or Titanium o Cast austenitic-ferritic stainless steel for which carbon content does not exceed 0.040% and ferrite content (as calculated with Schaeffler diagram) is between 12 and 20%. • Inspection: Design and material choices must be compatible with Construction and Operation inspections. For this reason, cast austenitic steels are avoided where possible in class 1 and 2 piping systems subjected to in-service inspections, or a specific evaluation of inspectability aspects is conducted.

SAP	Comment
	As a result: • Material selection principles for primary components are: For the QC1 components, the RCC-M is the basis design code. The EPR material selection rules and material specifications (or material data sheets /MDS) are defined accordingly in the RCC-M code, for each main component of the primary system (RCC-M section II. Materials part 1 & 2). For each elementary part or sub-component, the RCC-M material or specification datasheet describes in all details, the material to be selected, the scope of application, chemical analysis, melting and manufacturing process, mechanical properties, heat treatment, testing and acceptance procedures. For QC1 components (main primary components), the rules and requirements for material selection are given in the RCC-M section 1 B2000: B.2100 (General), B.2200 (scope of application), B.2300 (susceptibility to intergranular corrosion and associated steel grades selection requirements), B.2400 (Cobalt content)... The procurement specifications refer to the RCC-M. For the EPR, these procurement specifications can be used to supplement or precise the RCC-M materials datasheets on specific points such as material identification, limitations in content of residual elements, additional testing. Co-based hardfacing alloys (Stellites) are avoided in the primary system wherever possible, except for applications where no equivalent practice is currently qualified. Such applications are listed in Chapter 3. • Material selection principles for auxiliary systems and components are. For auxiliary mechanical components, material selection is depending on the classification of the component and also on the component manufacturer know-how, on the technology and design of the component, on the functions to be fulfilled by each part of the component (acting forces, surface behaviour, static or dynamic parts...). For pumps and valves, the materials selected and proposed by the manufacturer for the pressure retaining parts, as well as for the main internal parts (e.g. shaft or stem for pumps and valves), are defined according the RCC-M design code (RCC-M B2000 or C 2000). The corresponding material specifications are also defined and included in the RCC-M (tables B 2200, C 2200). For other pumps/valves small internal parts, other materials not referred to in the RCC-M are proposed. Some

SAP	Comment
	materials are also forbidden, as indicated in the equipment specification. For piping, heat exchangers or tanks, the materials to be selected and proposed by the manufacturer refer to the RCC-M design code or equivalent. The material specifications are those included in the RCC-M (tables B 2200 and C 2200). • Material selection principles for Secondary Systems and Components are: The main steam lines contain superheated steam (single phase flow) under non-stagnant conditions. Therefore components are designed using carbon ferritic steel grades. No problems due to corrosion and erosion corrosion are expected. In the water/steam circuits (single phase flow or two phase flow and flashing conditions), carbon steels or low alloy ferritic steels are used. During normal operation on ferritic surfaces spontaneous formation of a magnetite layer takes place (>150°C) which protects the ferritic surface against further general corrosion. When a significant risk of corrosion-erosion is suspected, Cr-Mo steels or stainless steels are used.
EMC.14 Manufacture and installation should use proven techniques and approved procedures to minimise the occurrence of defects that might affect the required integrity of components or structures. **and** **EMC.15 Materials identification, storage and issue should be closely controlled.**	SAPs EMC 14, 15, 16, 19 and 20 are not considered to be, strictly speaking, within the scope of the Generic Design Assessment process for Design Acceptance Confirmation of the EPR in the UK. Nevertheless, it can be stated at this stage that the QA programme in place for EDF and AREVA for EPR defines provisions to ensure compliance with the applicable safety requirements, Codes, standards, and specific requirements, throughout Design, Procurement, Fabrication, Inspection, Testing, Erection and Commissioning. This includes in particular: • Control of manufacture and installation techniques and procedures using proven techniques and approved procedures (EMC.14). • Control of materials through material identification, storage and protection (EMC.15). • Control of the potential for contamination of materials during manufacture and installation (EMC.16).

SAP	Comment
and **EMC.16 The potential for contamination of materials during manufacture and installation should be controlled to ensure the integrity of components and structures is not compromised.** **and** **EMC.18 Manufacture and installation operations should be subject to appropriate third-party independent inspection to check that processes and procedures are being carried out as required.** **and** **EMC.19 Where non-conformities with the procedures are judged to have a detrimental effect on integrity or significant defects are found and remedial work is necessary, the remedial work should be carried out to an approved procedure and should be subject to the same requirements as the original.** **and**	• Manufacturing and installation surveillance (checking that the appropriate quality level of the equipment is achieved) will be subject to appropriate independent inspection; this will be defined at the time (EMC.18). • Control of non-conformances with applicable requirements and provisions to keep all affected items under control until an approved solution has been correctly implemented with regard to the original requirements (EMC.19). • Control of quality records of manufacturing, installation and testing activities which require to be retained in accordance with applicable regulatory requirements for "lifetime records" or "non-permanent records" (EMC.20).

SAP	Comment
EMC.20 Detailed records of manufacturing, installation and testing activities should be made and be retained in such a way as to allow review at any time during subsequent operation.	
EMC.17 Provision should be made for examination during manufacture and installation to demonstrate the required standard of workmanship has been achieved.	The EPR is considered to comply with the SAP Examinations during manufacturing of equipment and installation are performed according the rules given by the technical codes or standards applied. Codes and standards used in the EPR design are addressed in PCSR Sub-chapter 3.8. As an example, RCC-M follows the French industrial practice and benefits from experience from manufacture, inspection and operation of French units. Examinations performed by all the parties directly concerned are applied over the whole cycle of equipment realisation; these activities consist of the checking of the preliminary documents (welding data book, qualifications, specifications) as well as the follow-up of the non destructive and destructive tests performed for each important step of the in-factory manufacturing and the on-site construction. Inspection and testing programmes issued comply with the requirements of the applicable codes (e.g. RCC-M section III for the NDT). Notably, they detail the area of the examination, and the method, extent and frequency of the control. These examinations taking place during manufacture are reliably capable of showing that the part has been manufactured to the required standard. Otherwise, surveillance (or audit) is also performed in order to have confidence in the capacity of the suppliers to implement procedures and processes that leads to the control of equipment quality.
EMC.21 Throughout their operating life, safety-related components and structures should	The EPR is considered to comply with the SAP. As requested by mechanical codes and good practice imposed on all safety-related equipment, the mechanical

SAP	Comment
be operated and controlled within defined limits consistent with the safe operating envelope defined in the safety case.	components are designed with appropriate safety margins. Design pressures and temperatures are used, along with stringent stress criteria, to ensure that each system, structure or component will tolerate its working conditions without any risk of mechanical failure throughout operating life. The thermal-hydraulic conditions of the RCS and of the secondary systems are constantly monitored, and are input to the normal reactor power control system, which maintains the reactor pressure and temperature within the normal range. Transients are constantly analysed to ensure that there is no risk of fatigue ruptures occurring, while brittle fracture is prevented by design and operating features. If design conditions are exceeded, the RCSL can induce countermeasures that limit the risk of abnormal loading. If all these measures are not sufficient, reactor trip, along with operation of the safety valves, ensures that pressure always remains within the allowed range determined by the codes. The same principles are applied to the safety of other mechanical systems. The systems are all designed to be operated safely within their design conditions. Good practice and international standards are followed, to avoid any risk of adverse consequences resulting from overpressure, through the combined effects of monitoring and operation of safety valves. All safety-related systems, structures and equipment are identified. Further to the QA within the design process, a QA programme is employed to ensure that they are built, checked, operated and maintained in an appropriate manner.
EMC.22 Materials compatibility for components should be considered for any operational or maintenance activities.	The EPR is considered to comply with the SAP. This issue is addressed essentially through the adequate choice of materials at the design stage. In the EPR, pressure-retaining systems, components and parts are required to be designed, manufactured and installed in accordance with the requirements of the RCC-M Code. This Code defines the materials acceptable for a given application and requirements ensuring material compatibility with any operational or maintenance activity. For additional information on material compatibility, see PCSR Sub-chapter 3.8 (RCC-M).

SAP	Comment
EMC.23 For metal pressure vessels and circuits, particularly ferritic steel items, the operating regime should ensure that they display ductile behaviour when significantly stressed.	The EPR is considered to comply with the SAP. The requirement for ductile behaviour is addressed essentially through the combination of the following provisions : 1. Adequate choice of material : In the EPR, pressure-retaining systems, components and parts (notably, large components manufactured from ferritic steel, such as the Reactor Pressure Vessel) are required to be designed, manufactured and installed in accordance with the requirements of the RCC-M Code. This Code defines the materials acceptable for a given application with their minimum mechanical characteristics. For materials used in components important to safety, these include minimum fracture requirements such as fracture toughness values. 2. Conservative set of loading conditions : Specified operating conditions for those pressure retaining components are conservatively defined and generally involve operating temperatures above the Nil Ductility Transition Reference Temperature, RTNDT, thus allowing for an appropriate margin to this temperature. This provides assurance that ductile behaviour will prevail in real operating conditions. 3. Reliable assessment of fracture behaviour : The RCC-M Code covers both prevention of « non-ductile failure » and « ductile tearing ». Beginning of life mechanical properties are extrapolated to their end of life values which are considered in the assessment, thus allowing for a safe evaluation of the component fracture behaviour throughout its entire lifetime. For additional information on ductile behaviour, see PCSR Chapters 3 and 5 (fast fracture analysis).
EMC.24 Facility operations should be monitored and recorded to demonstrate compliance with the operating limits and to allow review against the safe operating envelope defined in the safety	The EPR is considered to comply with the SAP Main pressure and temperature transients on the most loaded systems will be monitored during operation in order to check that components always remain within the safety limits and the reactor design basis hypotheses. In this context, the General Operating Rules establish a set of rules specific to operation of the unit which ensures that the unit is kept within the normal operating domain.

SAP	Comment
case.	If the operating envelope is breached, mechanical analysis of components would be updated in order to take account of the evolution of the transient data base. A dedicated process will be established during operation to analyse and count the occurrences of each selected transient.
EMC.25 Means should be available to detect, locate, monitor and manage leakage that could indicate the potential for an unsafe condition to develop or give rise to a significant radiological effect.	The EPR is considered to comply with the SAP. In order to meet requirements associated with additional levels of defence in depth, the EPR has a leak detection system which detects, locates and measures leaks from the reactor coolant system to prevent a hypothetical through-wall defect leading to a pipe break. In the event that the flow rate exceeds certain defined limits, this system initiates alarms in Main Control Room (see description of this system in Sub-chapter 5.2 of the PCSR). The system allows the operators to make an early diagnosis of the situation and also to initiate, if necessary, actions to limit the consequences of the leak. In case of leaks that lead to incidental or accidental conditions, the operation is defined in accordance with State Oriented Approach. This approach (described in Sub-chapter 18.2 of the PCSR) is a self-adapting process (constant diagnosis of the plant condition). In practice, when the operator is confronted with a given accident, he has a diagnosis of the state of the plant based on the six critical safety functions (given in Sub-chapter 18.2). This assessment makes it possible to identify the appropriate procedure together with associated operational actions. As the diagnosis evolves (for example a leak that develops significant radiological effect), there is a re-evaluation and an identification of a more suitable procedure if necessary. Moreover, the EPR is designed to minimise the risk of containment by-pass events. In particular, the risk of containment by-pass via Steam Generator Tube Rupture has been analysed in the design (refer to Sub-chapter 16.3 of the PCSR) Note : The radiological effects of a leak are detected by Plant Radiation Monitoring System (described in Sub-chapter 12.3 of the PCSR)

SAP	Comment
EMC.26 Detailed assessment should be carried out where monitoring is claimed to provide forewarning of significant failure.	The EPR is considered to comply with the SAP. Forewarning of significant failure is provided on the EPR by : • design provisions • in-service inspection testing (principles presented in the PCSR Chapter 5 and Sub-chapter 6.5), in-service testing (frequency of these tests takes into account feedback experience on equipment failure) and preventive maintenance (taking into account the failure modes and also feedback experience) • monitoring Even if the break preclusion concept for the primary coolant line and the main steam line is mainly based on design provisions, it is reinforced by the existence of a leak detection system. This system contributes to the detection of leakage from the primary system as well as from the secondary system and auxiliary systems .It initiates alarms in the event that the flow rate exceeds certain defined limits. Chapter 18 addresses the way the information is provided in the Main Control Room .The operating procedures address the actions to be performed. It is demonstrated that, for all the sensitive zones there is a sufficient margin between: • the size of the smallest detectable through wall crack, and • the size of the unstable through wall crack. Continuous vibration monitoring on main coolant pumps and monitoring of pumps motor temperature are performed to avoid any degradation. This allows the operators to react on alarms and trip the pumps before damage.
EMC.27 Provision should be made for examination that is reliably capable of demonstrating that the component or structure is manufactured to the required standard and is fit for purpose at all times during service.	The EPR is considered to comply with the SAP. Information related to examination during manufacture is given in the response to EMC.17. In addition, rules for the management of the In-Service-Inspection of equipment will be issued to describe the basic procedures for monitoring in operation, performed on mechanical equipment and structures, including periodic tests, hydrostatic tests and Non Destructive Testing. PCSR Sub-chapter 6.5 addresses some of these provisions.

SAP	Comment
	The maintenance policy will take into account these arrangements and also integrate rules for replacement or repair of equipment. This maintenance organisation enables prevention of failures before they affect the function of the equipment. Each in-service examination technique (NDT) implemented must be qualified to demonstrate that the claimed performance is reliably achieved, in order to give evidence that the component is fit for purpose throughout its life cycle.
EMC.28 An adequate margin should exist between the nature of defects of concern and the capability of the examination to detect and characterise a defect.	The EPR is considered to comply with the SAP. For the EPR project, a detailed analysis, notably based on the available experience feedback on the French fleet, has led to the selection of NDT techniques which will be implemented for the pre-service and in-service inspections. In accordance with the French regulation related to operation, NDT qualifications are required when they are applied to main primary and secondary components. The purpose of the qualification is to demonstrate that the technique selected, as being the most suitable according to the constructional and operating constraints (geometry of components size and shape, type of materials, accessibility of the areas, radiological concerns, …), enables detection of defects whose characteristics have been previously defined, based on predicted potential damage in selected areas. In some cases, qualifications of the NDT method could lead to implementation of test programmes on mock-ups including representative simulation of the sought defects. Thus, it can be proven that, whatever the applied parameters of the NDT method, the implementation of the qualified technique guarantees that the detection of the flaws is reliably achieved in every case.
EMC.29 Examination of components and structures should be sufficiently redundant and diverse.	The EPR is considered to comply with the SAP An example of redundancy and diversity is in the welding examinations during manufacturing, where both ultrasonic and radiographic examinations take place.

SAP	Comment
	The RCC-M code defines the non destructive tests to be performed: the table S 7710.1 in Section IV of RCC-M requires full penetration butt welds to be examined by magnetic particle and radiographic means. In addition, ultrasonic examination is to be performed where the wall thickness of the adjoining piece is greater than 10 mm. However, it is understood that for manufacture of components, for example the transition ring and flanges of the RPV (see chapter M 2113 of Section II of RCC-M) there is a requirement for volumetric examination using ultrasonic means, and a surface examination. As a general rule, it should be noted that the French practice is to develop a single inspection technique which is guaranteed 100% success of detecting a known defect size. In some particular cases for the pre-service and in-service inspection, there can be a requirement to implement two different NDT methods (e.g. volumetric methods for transition welds of pipes) but if it is proven that a single method can detect all degradation mechanisms, the implementation of only one method is acceptable (see Sub-chapter 13.2 of the PCSR). The qualification of the NDT technique according to the French regulation enables this requirement to be met.
EMC.30 Personnel, equipment and procedures should be qualified to an extent consistent with the overall safety case and the contribution of examination to the structural integrity aspect of the safety case.	The EPR is considered to comply with the SAP. Classification of equipment according to the RCC-M complies with the safety classification for each item and appropriate provisions are made to specify personnel, equipment and procedures qualification consistently. For example, high standards of manufacturing are required for equipment important to safety (such as those items contributing to the integrity of the pressure boundary of the reactor coolant system). The manufactured parts are subjected to qualification report (section II, chapter M140) containing the manufacturing programme and tests conducted to verify the product properties. A qualification of the manufacturing shop is also required, including the shop facilities, personnel and management, and industrial experience. The scope is to ensure that a manufacturer is capable of satisfactorily fabricating the required parts. Concerning the manufacturing inspection, section III of RCC-M gives details of the examination techniques to be used for parts and components. As an example, parts of the RPV must be 100% examined by ultrasonic methods. Moreover,

SAP	Comment
	RCC-M Section MC8000 requires that the examination must be carried out by qualified and certified personnel. For welding operation, RCC-M Section IV requires welding procedure qualification, qualification of welders and operators, qualification of filler materials and technical qualification of production workshops. Finally, RCC-M Section V deals with forming operation; some procedures (for example expanding tubes in heat exchanger tube plates) are required to be qualified in Section F4400. In addition, surveillance could be performed by dedicated entities within owner and vendor organisations to verify the implementation of this set of qualifications.
EMC.31 In-service repairs and modifications should be carefully controlled through a formal procedure for change.	Compliance with this SAP is outside the scope of the GDA process.
EMC.32 Stress analysis (including when displacements are the limiting parameter) should be carried out as necessary to support substantiation of the design and should demonstrate the component has an adequate life, taking into account time-dependent degradation processes.	The EPR is considered to comply with the SAP. This issue is essentially addressed through the establishment of component stress reports. Stress reports are established in support of the design of the EPR components, notably pressure retaining parts and including piping. The RCC-M Code provides the basis for the analyses in the reports. Widely accepted methods are used and documented in the demonstration. The various steps concern • modelling, • load determination and load combination • analysis method • mechanical resistance check through acceptance criteria verification Loads or displacement controlled loadings and monotonic and cyclic loadings are all taken into consideration. Time-dependent degradation processes, including fatigue, are analysed under the latter type of loadings. Ageing is also taken

SAP	Comment
	into account through consideration of end of life mechanical characteristics. Earthquake loads are modelled using simple static analyses, floor response spectrum analyses or time history analyses. For systematic assessment, qualified computer software is used. When commercial codes are employed, the supplier's validation is supplemented by a qualification procedure through which AREVA or EDF verify the applicability of the code for nuclear applications. For additional information on stress analysis, see PCSR Chapters 3, 5, 6, 9 and 10.
EMC.33 The data used in analyses and acceptance criteria should be clearly conservative, taking account of uncertainties in the data and the contribution to the safety case.	The EPR is considered to comply with the SAP. All EPR pressure boundary materials are required to meet the RCC-M Code requirements. Minimum mechanical characteristics (e.g. strength and Charpy toughness requirements) are specified in the Code, and are verified and documented in end of fabrication reports. Analyses, calculations and evaluations, performed to verify the design, all use conservative methods. Input data (load values, applicable temperatures, transient characteristics, numbers of occurrences and acceptance criteria) are also systematically established or chosen with significant margins. For additional information on use of data, see PCSR Chapter 3.
EMC.34 Where high reliability is required for components and structures and where otherwise appropriate, the sizes of crack-like defects of structural concern should be calculated using verified and validated fracture mechanics methods with verified application.	The EPR is considered to comply with the SAP. During the EPR design and manufacturing phases, rigorous precautions are taken so as to ensure, as far as possible, defect-free components. All unacceptable defects are required to be either eliminated or repaired in accordance with the requirements of the RCC-M Code. In-service inspections are carried out periodically on critical components. If a defect is found, the detected defect is assessed for continued operation using the methodology and rules presented in the RCC-M Code, or those established

SAP	Comment
	from validated fracture mechanics methods. These exhibit built-in conservatisms. Permissible maximum defect size can be calculated for the application under the expected loads, and comparison can be made with the actual measured defect size. For additional information on fracture mechanics methods, see PCSR Chapter 3.
ECE.1 The required safety functional performance of the civil engineering structures under normal operating and fault conditions should be specified.	The EPR is considered to comply with the SAP. PCSR Chapter 3 confirms that the EPR civil structures that have a role in providing the three basic safety functions of reactivity control, core cooling and containment of radioactive materials, are designated as category 1 safety classified structures. The required safety functional performance of the safety classified civil structures, under normal and fault conditions, is specified in ETC-C (EPR Technical Code of for Civil Works), a specific nuclear design code for EPR safety classified civil structures developed by EDF and German Utilities. ETC-C describes the principles and requirements for safety, serviceability and durability conditions of concrete and steel structures for normal operational loads, plant transients and fault conditions, including internal and external hazards. Load combinations that must be taken into account in the design are specified. A summary of the requirements of ETC-C is given in PCSR Chapter 3. ETC-C has evolved from earlier civil works standards developed for French NPPs. The rules for design, construction and testing specified by the code have been validated using extensive experience feedback from construction and operation of French NPPs.
ECE.2 For structures requiring the highest levels of reliability, several related but independent arguments should be used.	The EPR is considered to comply with the SAP. EPR civil structures are designed to the ETC-C, described in Sub-chapter 3.8 of the PCSR. ETC-C contains rules concerning design, construction QA, resistance tests and containment monitoring. It also gives the inspection rules applicable during operation. The requirements of design, construction and inspection are consistent with the level of classification of the structures. Sub-chapter 6.5 of the PCSR describes the in-service inspection principles. The design life of the plant is taken into account in the design calculations for civil structures.

SAP	Comment
	The choice of the concrete quality for the reactor building (high performance concrete) was previously tested in the Civaux 2 unit, with favourable feedback. Protection against internal and external hazards is an integral part of the structural design. A Seismic Margin Assessment is in progress to demonstrate adequacy of margins in the seismic assessment. Sub-chapter 3.3 of the PCSR presents some design provisions used for the safety classified civil structures. The design of non-classified structure considers the potential consequences of failure for safety-related structures. Design solutions seek, if possible, to avoid occurrence of hazards.
ECE.3 It should be demonstrated that safety-related structures are sufficiently free of defects so that their functions are not compromised, that identified defects are tolerable, and that the existence of defects that could compromise their safety function can be established through their life-cycle.	The EPR is considered to comply with the SAP. EPR civil structures are designed to the ETC-C, described in Sub-chapter 3.8 of the PCSR. ETC-C contains the rules used for the design, i.e. design requirements, construction QA, resistance tests and containment monitoring. It also gives the inspection rules applicable during operation. The requirements of design, construction and inspection are consistent with the level of classification of the structures. Sub-chapter 6.5 describes the in-service inspection principles. Category 1 civil works are seismically qualified, as required by ETC-C. The QA surveillance programme and management of defects are described in Chapter 21. Civil structures are designed against external hazards, as described in Chapter 13 of the PCSR. For the containment, Chapter 6 of the PCSR describes the load cases considered for the design, and the safety and functional requirements, for the reactor and peripheral buildings. Confidence that safety functions are not compromised by defects in structures is based on use of correct methods and materials for construction, fabrication and assembly of safety-related structures, based on proven codes and standards. Tests during construction and commissioning, and in service inspections, give confidence that the plant will conform to safety requirements.

SAP	Comment
ECE.4 Investigations should be carried out to determine the suitability of natural site materials to support the foundation loading specified for normal operation and fault conditions.	The EPR is considered to comply with the SAP. Seismic methodology is described in Sub-chapters 3.3 and 3.8, taking into account ground characteristics. When the site is known, calculations with the site-specific values will be carried out.
ECE.5 The design of foundations should utilise information derived from geological site investigation.	The EPR is considered to comply with the SAP, however it is beyond the scope of the GDA process. Geological investigations are used for the site implementation of the plant. Chapter 2.2 presents a summary of the relevant environmental and site characteristics.
ECE.6 For safety-related structures, load development and a schedule of load combinations within the design basis together with their frequency should be used as the basis for the design against operating, testing and fault conditions.	The EPR is considered to comply with the SAP. Details of the schedule of loads and load combinations that are used in the design of EPR safety classified civil structures, and the applicable limits, are specified in Part 1 of the EPR Technical Code for Civil Works (ETC-C) and summarised in PCSR Chapter 3. The load cases specified cover normal operational, testing and fault loading conditions. As required by the SAP, the behaviour requirements of structures under the applied load cases take into account the degree of damage which is acceptable given the anticipated frequency of occurrence of the different loading conditions. The different behaviour requirements are: • Complete functionality of the structure. This requires that the deformation of the structure and materials is limited with no requirement for repair • Partial functionality of the structure. This requires a continued capability for reactor operation subject to any necessary repairs. • Maintaining the containment function. This is applicable in situations when it is not planned to restart the plant.

SAP	Comment
	Achievement of this requirement ensures the safety objective of limiting the radiological impact of accidents. The design approach results in the creation of safety margins in the structural design for normal situations. Part 3 of the ETC-C specifies the instrumentation requirements for monitoring the condition of the containment structures during the construction and operating phases, and during testing. Results of the monitoring will be available for use in periodic safety reviews and post event analysis of civil structures, as required by the SAP.
ECE.7 The foundations should be designed to support the structural loadings specified for normal operation and fault conditions.	The EPR is considered to comply with the SAP. The foundations are designed with respect of the operational and safety requirements, and comply with ETC-C.. Sub-chapter 3.3 describes the requirements for each building, including the pumping station and tunnels. Chapter 2 summarises generic site data used in the UK EPR design. Sub-chapter 2.1 describes the enveloping data which are used for external hazards. Seismic design is described in Sub-chapters 3.3 and 3.8.
ECE.8 Designs should allow key load bearing elements to be inspected and, if necessary, maintained.	The EPR is considered to comply with the SAP. Sub-chapter 6.5 presents the in-service inspection principles. Inspections cover maintenance controls. Access is allowed to the key load-bearing elements for inspection. Measurement devices are defined for tracking differential movements during the plant lifetime. Chapter 3 presents requirements applicable to the design civil structures and mechanical equipment, which are dependent on the level of classification. ETC-C describes the rules applicable to the design and testing of EPR civil structures.
ECE.9 The design of	Chapter 13 describes the requirements of external flooding.

SAP	Comment
embankments, natural and excavated slopes, river levees and sea defences close to a nuclear facility should be such so as to protect and not to jeopardise the safety of the facility.	The design of embankments, natural and excavated slopes, river or sea defences are site specific and outside the scope of GDA.
ECE.10 The design should be such that the facility remains stable against possible changes in the ground-water conditions.	The EPR is considered to comply with the SAP. Details of the design against groundwater are site specific and outside the scope of GDA. A periodic re-evaluation of groundwater data would be made during the time life of the plant.
ECE.11 The design should take account of the possible presence of naturally occurring explosive gases or vapour in underground structures such as tunnels, trenches and basements.	The EPR is considered to comply with the SAP. A geological survey will be made before installation of the plant, which will exclude occurrence of this natural hazard. Consequently, no explicit case is studied for gas explosions which occur due to underground structures. Sub-chapter 13.1 identifies the external hazards which are taken into account in the UK EPR. The external hazards which are used to define the design include compression waves, ground movements, and earthquake.
ECE.12 Structural analysis or model testing should be carried out to support the design and should demonstrate that the structure can fulfil its safety functional requirements over the lifetime of the facility.	The EPR is considered to comply with the SAP. Details of the schedule of loads and load combinations that are used in the design of EPR safety classified civil structures, and the applicable limits, are specified in Part 1 of the EPR Technical Code for Civil Works (ETC-C) and summarised in PCSR Chapter 3. The load cases specified cover normal operational, testing and fault loading conditions. The analysis methods in ETC-C have been developed and validated using experience feedback from construction and operation of French NPPs.

SAP	Comment
	Loading conditions corresponding to the plant construction and operational phases are considered in order to ensure the security, stability and durability of the EPR civil structures. To allow for a provisional service lifetime of the plant of 60 years, and a construction time of 5 years, design calculations for the civil structures assume a life of 65 years (particularly for the calculation of shrinkage/creep and pre-stressing losses). Therefore there is confidence that the structures can fulfil their safety functional requirements over the lifetime of the facility. Part 3 of the ETC-C specifies the instrumentation requirements for monitoring the condition of the containment structures during the construction and operating phases, and during testing. Results are used to confirm the functional capability of the containment building over its service life.
ECE.13 The data used in any analysis should be such that the analysis is demonstrably conservative.	The EPR is considered to comply with the SAP. Chapter 3 describes the safety principles which apply to the system structural design. The overriding concept of the design is defence in depth. The design must include sufficient margins to be safe under onerous load combinations. Design safety margins are specified in codes and standards, as described in Sub-chapter 3.8. These codes ensure that design loads are enveloping. An SMA is in progress to demonstrate the adequacy of margins in the seismic assessment.
ECE.14 Studies should be carried out to determine the sensitivity of analytical results to the assumptions made, the data used, and the methods of calculation.	The EPR is considered to comply with the SAP. The civil structural analyses are performed based on ETC-C, which is an evolution of EUROCODES. Safety factors are used based on experience gained in European countries, including the analysis of structures which collapsed. Moreover, the combination of loadings applied to structures combines individual loads with amplification factors giving significant safety margins, due to the fact that these load combinations are unlikely to occur simultaneously. Concerning specific loadings, the EPR design gives comfortable margins based in particular on the following:

SAP	Comment
	• earthquake: a Seismic Margin Assessment is used as a sensitivity study, • LOCA pressure inside the containment: EDF have used a scaled mock-up (MAEVA: 1/3 scale in diameter and 1/1 scale in the thickness of the wall) to test the structure beyond the design pressure. • non-accidental external hazards use a similar approach to that for seismic hazards.
ECE.15 Where analyses have been carried out on civil structures to derive static and dynamic structural loadings for the design, the methods used should be adequately validated.	The EPR is considered to comply with the SAP. Civil structural analyses are performed using computer codes (3D finite elements codes or other codes). These computer codes used extensively for existing French NPPs and are qualified through a process which has been reviewed as part of the EPR licensing process for Flamanville 3. .
ECE.16 Civil construction materials should be compliant with the design methodologies used, and shown to be suitable for the purpose of enabling the design to be constructed, operated, inspected and maintained throughout the life of the facility.	The EPR is considered to comply with the SAP. Standard codes, and French standards are applied to concrete characteristics, in accordance with ETC-C. ETC-C describes the design rules, methodology, for design, building and testing phases. This code is described in Sub-chapter 3.8. Chapter 21 confirms that the EDF and AREVA organisations include QA principles in construction activities and impose QA requirements on equipment suppliers and construction organisations. The QA processes of the different companies ensure consistency of the construction with design requirements.
ECE.17 The construction should use appropriate materials, proven techniques and approved procedures to minimise the occurrence of defects that might affects the required integrity of	The EPR is considered to comply with the SAP. Chapter 21 describes the organisation of the UK EPR project during GDA and the construction and operating phase. All the companies involved are required to be QA certified and satisfy specific QA requirements. Sub-chapter 3. 8 presents the ETC-C civil code used to design and build the plant.

SAP	Comment
structures.	Qualification requirements for civil structures and equipment are defined depending on the Safety duty. The requirement of material quality, seismic requirements etc. are written in design requirement documents, and in the contacts for the suppliers, in conformance with the EDF and AREVA QA systems (see Chapter 21) Chapter 3 describes the different requirements for the concrete, equipment, materials, etc. Confidence that safety functions are not compromised by defects in structures is based on the use of correct methods and materials for construction, fabrication and assembly of safety-related structures, based on proven codes and standards. Tests and in service inspection during construction and commissioning, give confidence that the plant will conform to safety requirements.
ECE.18 Provision should be made for inspection during construction to demonstrate that the required standard of workmanship has been achieved.	The EPR is considered to comply with the SAP. Sub-chapter 21.2 presents the QA organisation of EDF and AREVA, which includes requirements for quality surveillance of construction. The ISO 9001 standard takes into account design organisation and construction organisation. ETC-C presents requirements for construction quality (Sub-chapter 3.8). The construction organisation, including organisation of commissioning tests, is beyond the scope of GDA. However, Chapter 19 presents the commissioning organisation. The objective of the commissioning tests is to demonstrate that the installed plant meets its safety duty.
ECE.19 Where construction non-conformities are judged to have a detrimental effect on integrity or significant defect are detected, remedial measures should achieve the original design intent.	The EPR is considered to comply with the SAP. EDF and AREVA procedures for plant construction include non-conformity procedures. Chapter 21 presents the QA organisation. The ISO 9001 standard includes reference to a non-conformities process. This is beyond the scope of GDA. However, it may be noted that, for the FA3 construction project there is a non conformity

SAP	Comment
	process for construction defects. If any defect is found, a specific analysis must be done to confirm acceptability or to decide on a change. The demonstration that the safety functions are not compromised by structural defects is achieved by use of appropriate methods and materials for construction or fabrication and assembly of safety-related structures, based on use of codes and standards. Tests and in service inspection during construction and commissioning, give confidence that the plant conforms to safety requirements.
ECE.20 Provision should be made for inspection during service that is capable of demonstrating that the structure can meet its safety functional requirements.	The EPR is considered to comply with the SAP. Chapter 3 of the PCSR describes the EPR design codes, which include margins to ensure the lifetime of structures and equipment. These codes present the requirements for testing materials to ensure the quality and availability, including periodic testing and in-service inspection. Sub-chapter 6.5 describes in-service inspection for damages to pipework, etc. Sub-chapter 18.2 describes preventive maintenance procedures.
ECE.21 Pre-stressed concrete pressure vessels and containment structures should be subjected to a proof pressure test, which may be repeated during the life of the facility.	The EPR is considered to comply with the SAP. The ETC-C code for civil works, and the RCC-M code for materials, define the periodic tests which must be performed during the life of the plant. PCSR Chapter 6 discusses the periodic leak tightness tests and pressure tests for the containment.
ECE.22 Civil engineering structures that retain or prevent leakage should be tested against	The EPR is considered to comply with the SAP. Leaktightness may be required from the civil engineering structures and related ventilation systems, to prevent or reduce

SAP	Comment
leak tightness requirements prior to operation to demonstrate that the design intent has been met.	radiological consequences. To ensure the containment safety function, relevant tests (leaktightness, and/or ventilation performance, …) are planned during commissioning and periodically thereafter. Specific provisions for habitability of the main control room are provided, in order to protect operators from outside contamination or other outside hazardous substances (see Chapter 9).
ECE.23 Provisions should be made for the routine inspection of sea and river flood defences to determine their continued fitness for purpose.	This is not within the scope of the GDA and will be addressed in the site licensing phase.
ECE.24 There should be arrangements to monitor foundation settlement of major facilities during and after construction, and the information should be fed back into design reviews.	The EPR is considered to comply with the SAP. ETC-C describes how settlement is addressed in the design of EPR civil structures. Sub-chapter 3.3 summarises the design principles. Differential settlement between the reactor building and adjacent buildings is inspected periodically. The objective of the design is to minimise the consequences of small differential settlements on safety-related systems.
ESS.1 All nuclear facilities should be provided with safety systems that reduce the frequency or limit the consequences of fault sequences, and that achieve and maintain a defined safe state.	The EPR is considered to comply with the SAP. The EPR reactor is provided with safety systems (see PCSR Chapters 5 and 6) designed to limit the consequences of design basis accidents and to achieve and maintain a safe state. PCSR Chapter 7 describes I&C controls involved in the safety functions (control of reactivity, removal of heat from the core and confinement or containment of radioactive substances). I&C controls ensure the execution of automatic actions identified in the safety case, according to the event classification. PCSR Chapter 14 (Design basis analysis) and Chapter 16 (Design extension conditions and severe accident analysis)

SAP	Comment
	demonstrate how the safety systems are used to mitigate consequences in the case of PCC (design basis accident) events and RRCs (design extension accidents and severe accidents).
ESS.2 The extent of safety system provisions, their functions, levels of protection necessary to achieve defence in depth and required reliabilities should be determined.	The EPR is considered to comply with the SAP. The safety of the EPR unit is based on the concept of defence in depth, which is based on five levels of defence (prevention of departure from normal operation, preventive measures in case of abnormal operation, accident mitigation measures limiting the effects of PCC events, measures to reduce the risk of core melt and to limit the radioactivity releases in the event of a core melt, and on-site and off-site measures to mitigate radiological consequences) as described in PCSR Chapter 3. PCSR Chapter 6 provides a description of the safety systems and the requirements related to their safety functions. In addition, PCSR Chapters 14 and 16 (safety analyses for design basis conditions, and design extension and severe accidents) and PCSR Chapter 15 (probabilistic safety analyses) demonstrate that the safety systems have sufficient capability to ensure core protection and mitigation of postulated initiating events consequences.
ESS.3 Adequate provisions should be made to enable the monitoring of the plant state in relation to safety and to enable the taking of any necessary safety actions.	The EPR is considered to comply with the SAP. The EPR safety systems are monitored as described in PCSR Chapter 7. In the ***Main Control Room***, all the means necessary to control and monitor the plant in operation (within specified operating limits and conditions) are available to operators. If the Main Control Room is unavailable (e.g. due to fire), the operators are able to carry out monitoring and control of the plant from a ***Remote Shutdown Station***, to allow a safe shutdown state to be reached and maintained.
ESS.4 Variables used to initiate a safety system action should be identified and shown to be	The EPR is considered to comply with the SAP. Relevant parameters in the EPR power plant are continuously monitored and controlled to ensure that the reactor remains

SAP	Comment
sufficient for the purpose of protecting the facility.	within its operating range. The variables monitored are physical data representative of the reactor operating state. The operating range of the variables used to activate a safety system is chosen based on the safety and functional requirements of each system (see Chapter 6 of the PCSR for more details on the system design). Variables used to initiate automatic short-term actions, and their setpoints, are used in the fault analyses developed in Chapter 14 of the PCSR (see Sub-chapter 14.1 for the variables and setpoints associated with each safety system). The corresponding sensors provide signals to the Protection System and are F1A safety classified. Justification that all the required sensors have been identified and that the setpoints are correct is confirmed by the results of the transient analyses. The Protection Functions and information on the monitored parameters are supplied in tables in PCSR Sub-chapter 7.3. As the analysis of initiating events is extended to the achievement of the safe shutdown state, procedures followed by the operator are modelled in the analyses: the sensors necessary for correct diagnosis of faults are identified and the corresponding setpoints are justified. These sensors are classified F1B. The same process is followed when studying the RRC-A events to identify and justify the sensors required for short and long term analyses. When non-F1 sensors are required, they are identified and assigned an F2 safety classification. The automatic actuation of safety systems involved in the accident mitigation is modelled in the PSA (see Chapter 15). The analysis of the results of the PSA support studies, which are performed with best estimate assumptions, allows relevant signals to be identified for modelling the fault sequences.
ESS.5 The interfaces required between a safety system and the plant to detect a fault sequence and bring about a safe facility state should be engineered by means that have a direct, known, timely	The EPR is considered to comply with the SAP. The Instrumentation and Control system continuously monitors plant physical variables and generates signals to actuate systems producing corrective actions if a deviation from the normal operating range is detected (see Chapter 7 of the PCSR for more details). Some relief devices are also directly activated when a specific variable reaches the designated setpoint (e.g. a safety valve opens if its pressure setpoint is exceeded).

SAP	Comment
and unambiguous relationship with plant behaviour.	Safety analyses presented in Chapters 14 and 16 of the UK EPR PCSR show the adequacy of the monitored parameters and the safety systems actuation. These analyses show the impact of the safety system actions on the plant behaviour, taking into account uncertainties and time delays in the sensor response, and confirm that safety criteria are met. After an incident or accident, and after a suitable grace period for fault diagnosis, credit can be taken for operator intervention to restore safe operation of the plant. Emergency Operating Procedures based on the monitoring of the six safety functions and systems availability (see the definition of State Oriented Approach in Sub-chapter 18.2 of the PCSR) allow the operators to identify the most suitable strategy for reaching a safe state.
ESS.6 Where it is not possible to use a directly related variable to detect a fault sequence, the variable chosen should have a known relationship with the fault sequence.	The EPR is considered to comply with the SAP. In PCC-1 events, i.e. during all phases of normal operation, the main safety-related parameters of the EPR power plant are continuously monitored and controlled to ensure that the reactor remains within its operating range. Should a fault sequence occur, adequate response is provided by manual or automatic intervention of safety systems, in order to ensure radiological limits are not exceeded. In most cases, the variable used to detect a fault sequence is directly linked to the monitored parameter (e.g. neutron flux detectors to detect core overpower). In some specific cases, a variable, or set of variables, can be used to perform an indirect determination of the phenomena to be detected. The safety analyses demonstrate that the chosen variables are appropriate. An example of such an indirect link is provided by the low DNBR surveillance and protection channel. By monitoring parameters such as core temperature, pressure, flowrate and power distribution, the on-site low DNBR algorithm ensures that no rod damage is caused by the Departure from Nucleate Boiling phenomenon. The algorithm uses these parameters to determine the local core thermal-hydraulic conditions and applies a critical heat flux (CHF) correlation based on experimental data obtained in CHF tests (see Chapter 4 of the PCSR). The justification for the variables chosen for detection of the fault is finally confirmed in the transient analyses (see Chapters 14 and 16 of the PCSR), which demonstrate that corrective actions initiated by the chosen variables allow safety criteria to be met.

SAP	Comment
ESS.7 The protection system should employ diversity in the detection of fault sequences, preferably by the use of different variables, and in the initiation of safety systems action to terminate the sequences.	The EPR is considered to comply with the SAP. The I&C architecture is designed to distribute diverse I&C functions into an appropriate number of different safety I&C systems to avoid common cause failures and thus to meet the required probabilistic targets. Two complementary types of diversity are implemented in the design in order to reduce the risk of common mode failures as defined below. <u>Functional Diversity</u> - Functional diversity provides two separate I&C functions based upon two different methods of detecting a condition in order to initiate the same type of protective action. <u>Equipment Diversity</u> - Equipment diversity consists of providing two different hardware platforms in order to preclude a common mode failure taking out a function. The separate I&C systems have adequate independence and diversity features to minimise the risk of common mode failures (hardware and software) in accordance with plant probabilistic targets. I & C controls for protection systems actuation are extensively described in PCSR Chapter 7.
ESS.8 A safety system should be automatically initiated and normally no human intervention should be necessary following the start of a requirement for protective action.	The EPR is considered to comply with the SAP. The Protection System is described in PCSR Chapter 7. As a general design rule, automation is adopted when it significantly improves safety, availability or cost, and is applied more particularly to tasks that otherwise would be a potential source of human errors (e.g. those requiring a short response time or the assimilation of a large amount of information). In the case of a design basis event, all the functions necessary to reach the controlled state[1] (namely “F1A” functions, as described in PCSR Chapter 3) are initiated by the Protection System (PS). The functions required to reach the safe state (namely “F1B” functions) are either automatically generated in the Safety Automation System (SAS) or manually initiated.

[1] The **controlled state** is defined as a state where the fast transient resulting from a PCC-1 to PCC-4 event is finished. The plant is stabilised and where the core is sub critical, the heat removal is ensured in the short term, the core coolant inventory is stable and activity releases remain tolerable.

SAP	Comment
	Depending upon the different tasks of the I&C functions, contradictory commands could be given by the different I&C functions to particular actuators. Therefore, general priority rules are established so that any potential command will be assigned a defined priority level. The following general rules are applied for all actuators in the plant: • Higher classified functions have priority over commands from lower classified functions. The order of priority is: (1) F1A function, which has priority over (2) F1B function which has priority over (3) F2 functions and non classified functions; • The order of priority between different categories of I&C functions within the quality related class is: (1) highest priority for control of design basis accidents and design extended conditions, then (2) limitation function, and at the lowest level, (3) limitation of operating condition; • The principal order of priority within each I&C category in all classes is: (1) highest priority for component and system protection, then (2) automatic action, and at the lowest level, (3) manual action. Automatic control functions may be switched off if the process conditions allow.
ESS.9 Where human intervention is necessary following the start of a requirement for protective action, then the time before such intervention is required should be demonstrated to be sufficient.	The EPR is considered to comply with the SAP. In most safety studies, the controlled state of the reactor is achieved by automatic actions. For some specific cases (e.g. for some instances of boron dilution), manual actions are required. A general rule applied for EPR safety studies is that no manual action from the main control room can be credited within a grace period of 30 minutes from the first significant information transmitted to the operator. If a local manual action is required (i.e. outside the main control room), the grace period is extended to 1 hour. Safety studies presented in Chapters 14 and 16 show that safety criteria are met taking into account these rules.

SAP	Comment
ESS.10 The capability of a safety system, and of each of its constituent sub-systems and components, should be defined.	The EPR is considered to comply with the SAP. The capability and sizing of each safety system, including all of the parts constituting the systems, is described in the related PCSR sub-chapters. For instance, the capability of the Safety Injection System is described in PCSR Sub-chapter 6.3 and the Extra Boration System in Sub-chapter 6.7. The PCSR sub-chapter dedicated to each safety system describes: • How the safety systems are defined to handle all operating states and all safety functions (for instance the control of the reactivity during PCC and RRC events), • The design assumptions which have been considered • How the safety systems are designed to handle seismic events, and internal and external hazards • The tests, inspections and maintenances that are performed • Their operating conditions In addition, Chapters 14 and 16 describe which safety systems are called upon to operate during design basis accidents, design extension accidents and severe accidents. Finally, PCSR Sub-chapter 18.2 describes the corrective and preventive maintenance operations on safety systems and their components carried out to confirm that the required system functional capabilities are achieved.
ESS.11 The adequacy of the system design as the means of achieving the specified function and reliability should be demonstrated for each system.	The PCSR for the UK EPR addresses this requirement, with the exception of providing a Fault and Protection Schedule as requested in the notes to the SAP. The Design Basis Analysis (DBA), given in Chapter 14 of the PCSR, addresses the consequences for nuclear safety of a large number of postulated faults considered within the design basis. The list of faults considered in the DBA is based on a

SAP	Comment
	comprehensive survey of potential and hypothetical events, including operating experience feedback analysis from the existing fleet of NPPs. The safety functions challenged, and the safety systems used to mitigate the postulated design basis faults, are identified in Chapter 14. The design basis analysis demonstrates that radiological criteria are met for all accidents. Moreover, for each analysis, a specific paragraph identifies those cases where the design of a specific safety system is determined by consideration of that particular event. Table 24 of Sub-chapter 14.1 presents a summary of the safety functions and associated systems used for both the Design Basis and Design Extension/Severe Accident events. The probabilistic safety analysis summarised in PCSR Chapter 15 considers a large set of internal events, internal hazards and potential external hazards. The PSA is based on a systematic search for potential initiating events using the methodology detailed in IAEA-TECDOC-719, which involves: • Engineering evaluation or technical study of plant (see PCSR Chapter 14 ‘Design Basis Analysis’) • Previous PSAs • Previous lists of IEs such as in NUREG/CR 3862 • Analysis of operating experience for actual plant • FMEA of EPR systems. The complete list of the initiating events addressed in the PSA is presented in Sub-chapter 15.0, and Sub-chapter 15.5 for the off-site consequences PSA. The fault sequences mitigation is presented in the different sub-chapters of Chapter 15 where it is possible to identify: • The fault analysed • The plant response in terms of protection actuated (systems challenged…) including signals and operator action • The success criteria for the safety systems involved in mitigation of the event. The reliability of the safety systems is analysed using fault tree methodology reported in the PSA supporting documentation

SAP	Comment
	• The consequences of the accident sequences and their frequencies. As stated in Sub-chapter 17.3 of the PCSR, PSA has been used in the EPR design process since the basic design phase in order to identify the potential weaknesses in the design. Consequently, the system reliability has been improved to ensure that the risk of radiological release risk is as low as reasonably practicable. Examples of system improvements that were implemented following PSA analysis are: • Introduction of diversity in the on-site electrical power source by addition of two 'Station Black-Out' diesels • Improvement of the protection against an interfacing system LOCA
ESS.12 Adequate provisions should be made to prevent the infringement of any service requirement of a safety system, its sub-systems and components.	The EPR is considered to comply with the SAP. EPR safety systems and all parts of these systems, including support systems, are designed to operate under a wide range of conditions, including adverse environmental conditions, seismic events and following external and internal hazards. All damage modes, service requirements and design conditions, are considered at the design stage, in particular, in accordance with RCC-M requirements, those relating to temperature, pressure, erosion, cavitation, vibration, and fatigue associated with local thermal-hydraulic phenomena. The operating rules take account of these service requirements and limits of operation.
ESS.13 There should be a direct means of confirming to operating personnel: **a) that a demand for safety system action has arisen;** **b) that the safety actuation systems have operated fully; and** **c) whether any limiting condition**	The EPR is considered to comply with the SAP. The information presented to operating personnel is discussed in the Man Machine Interface section of the PCSR. This includes the role and classification of alarms. Severity-4 alarms are specifically dedicated to inform operators of demands for safety system action. They are used to trigger entry into Emergency Operating Procedures (EOPs). Additional information is presented to operators to provide confirmatory information on correct safety system operation (including any exceedance of time allowed for action) and alarms are displayed in case of system failure. (Safety system surveillance is part of the EOP requirements, and corrective actions, including changes to the accident management strategy are proposed to operators).

SAP	Comment
for which the safety system has been qualified has been exceeded.	The design principles of alarms are presented, together with the MMI in PCSR Sub-chapter 18.1. Accident operating procedures are presented in PCSR Sub-chapter 18.2.
ESS.14 Safety system actions and associated alarms should not be self-resetting, irrespective of the subsequent state of the initiating fault.	The EPR is considered to comply with the SAP. For the main safety functions (i.e. control of reactivity, removal of heat from the core, and confinement or containment of radioactive substances), the action signal for the associated safety system (i.e. safety injection, steam generator emergency feed, and containment isolation) is stored, and memory resetting is performed manually, with a delay imposed in the I&C programming. The manual action to reset the system is part of the operating procedure, and is linked to the management strategy of the initiating event. The design of the protection system is described in PCSR Chapter 7 (with additional detail in Appendix 7B) and the EOP principles are given in PCSR Sub-chapter 18.2.
ESS.15 No means should be provided, or be readily available, by which the configuration of a safety system, its operational logic or the associated data (trip levels etc) may be altered, other than by specifically engineered and adequately secured maintenance/testing provisions used under strict administrative control.	The EPR is considered to comply with the SAP. Where possible, the functional configuration of safety systems (e.g. valve alignment) is monitored, and configuration alarms are displayed to operators. The I&C application software is configured off-line through a set of software engineering tools. These tools are used for initial coding, integration, commissioning and validation, as well as for maintenance and modification throughout plant lifetime. For maintenance purposes (software downloading, parameter modification, component replacement), the maintenance team is able to work on the Protection System without impairing the operability of the system. Configuration alarms are part of system functional engineering and are described in system design manuals. The EPR I&C procedures and tools are described in PCSR Sub-chapter 7.6.

SAP	Comment
ESS.16 Where practicable, following a safety system action, maintaining a safe facility state should not depend on an external source of energy.	The EPR is considered to comply with the SAP. In the EPR design, a general safety requirement on support systems is that they have a level of safety classification and qualification consistent with the main safety systems. This applies fully to power supply systems. Each of the four safety trains has its own source of energy (main diesel generators) which is able to run the safety systems of the train: safety injection, steam generator emergency feed, cooling systems, emergency boration. In addition, some safety equipment obtains a passive power supply from batteries (e.g. I&C cabinet, containment isolation valves). The EPR power supply to safety systems is described in PCSR Chapter 8. Details of the containment isolation system are given in PCSR Sub-chapter 6.2. Details of the I&C power supply are given in PCSR Chapter 7.
ESS.17 Foreseeable faults within a safety system that could cause any single plant variable, or combination of variables, to change to significantly less safe values should be identified and, as necessary, avoidance measures or appropriate protective features provided.	The EPR is considered to comply with the SAP. The EPR plant variables (e.g. primary pressure and temperature, pressuriser level, steam generator pressure, level and flow rates, neutron fluxes ...) are monitored through different levels of defence in depth. Small and slow changes of variables are displayed to operators by alarms. For larger or faster changes, the limitation functions in the I&C system are actuated in order to avoid protection actions. If necessary, the protection functions in the I&C system are able to trip the reactor or to actuate engineered safety features. These protection functions are designed in accordance with the EPR four separate safety train concept. Additional diverse I&C functions are provided in the EPR design to cope with some potential failures in safety systems, in events identified as “RRC initiating events” (Risk Reduction Category). The EPR I&C functions are described in PCSR Chapter 7.
ESS.18 No fault, no internal or external hazard should disable a safety system.	The EPR is considered to comply with the SAP. The EPR safety systems (extensively described in PCSR Chapter 6) are physically separate, independent and isolated from other systems. PCSR Chapter 13 explains how safety systems are protected against external and internal hazards. In addition, safety studies demonstrate that in case of one protection system failure, the safety function can be ensured with

SAP	Comment
	other safety systems allowing the reactor to reach a safe state.
ESS.19 A safety system should be dedicated to the single task of performing its safety function.	The EPR is considered to largely comply with the SAP. ESS.19 has not been considered as a principle during the design phase of the EPR, but the choice between combined and separated functions has been made on the basis of a case by case analysis of advantages and drawbacks. In the UK EPR design the protection and safety monitoring system is separate and distinct from the non-safety-related control systems. In some cases, the protection and safety monitoring system provides signals to the non-safety-related control system. These signals are transferred to the control system via isolation devices that are classified as protection and safety monitoring system components. A discussion is provided in PCSR Chapter 7. In general, the safety-related fluid systems are dedicated, and do not have non-safety functions. One key exception is the RIS/RRA (SIS/RHR) system. This system provides operational functions (normal cooling of the RCS, control of temperature during shutdown …) and also safety functions (boration, decay heat in accidental conditions, containment function, ...). The system is safety classified and operational functions cannot jeopardise the safety function. • The 4 RIS/RRA [SIS/RHRS] trains are structurally separated from one another, supplied by a separate electrical system and cooled by a separate RRI [CCWS] train, • Each train can operate either in residual heat removal mode or in LHSI mode, but not at the same time. o when the reactor is not in a shutdown state, the RIS/RRA [SIS/RHRS] is placed in safety injection mode to ensure the safety injection function. o when the reactor is in a shutdown state with all RRA [RHRS] trains in operation, the MHSI pumps are used to ensure the safety injection function independently (with high output minimum flow line opens), Thus, the RRA [RHRS] (used in normal operation mode) and RIS [SIS] (used in emergency operation mode) can be considered as functionally independent systems.

SAP	Comment
	The RIS/RRA (SIS/RHR) system is described in PCSR Section 6.3.
ESS.20 Connections between any part of a safety system (other than the safety system support features) and a system external to the plant should be avoided.	The EPR is considered to comply with the SAP. All EPR safety systems are designed to operate independently of connections to systems external to the plant. In the case of off-site electrical supplies, the unit is connected to the external network via a main connection and an auxiliary connection (which supply all of the unit auxiliaries in all normal operating and accident situations). However, in the case of a loss of off-site power being detected by I&C Reactor Protection System, the reactor is tripped and the electrical supply is provided by means of main diesel generators, or the ultimate diesel generators (in the case of failure of the main diesel generators), both of which are internal to the plant. Therefore, the safeguard systems are capable of performing their function without external power. In case of problems with the supply of cooling water external to the plant, an alternative source of cooling water will be provided, the design of which is site-specific. Hence, cooling water is supplied to essential safeguard systems in all situations.
ESS.21 The design of a safety system should avoid complexity, apply a fail-safe approach and incorporate the means of revealing internal faults from the time of their occurrence.	The EPR is considered to comply with the SAP. The EPR safety systems incorporate means of revealing internal malfunction, and the Protection System is designed to withstand single failure, even during maintenance or periodic testing. Self tests and periodic tests are implemented to detect any component failures, and test frequencies are calculated based on the reliability expected of the tested function. PCSR Chapter 6 describes in-service inspection performed. This preventive maintenance operation consists of carrying out non-destructive examinations and checks on equipment. These checks and examinations constitute the maintenance and monitoring programme.
ESS.22 A safety system should avoid spurious operation at a frequency that might directly or	The EPR is considered to comply with the SAP. Passive equipment e.g. relief valves, are designed to avoid spurious actuation.

SAP	Comment
indirectly degrade safety.	Monitoring systems and other safety equipment are actuated by I&C systems (in particular by the Protection System) using redundant sensors and instrumentation. Four separated electrical divisions are employed using two-out-of-four logic or two-out-of-three logic (depending on safety classification) to avoid spurious actuation. Design of I&C to prevent spurious actuation is discussed in PCSR Chapter 7.
ESS.23 In determining the safety systems provisions, allowance should be made for the unavailability of equipment.	The EPR is considered to comply with the SAP. Redundant trains of the main safety systems (one per Safeguard Building) are strictly separated into four divisions. The four divisions of the safety systems are consistent with the N+2 safety concept. With four divisions, one division can be out-of-service for maintenance and one division can fail to operate, while the remaining two divisions are available to perform the necessary safety functions, even if one is ineffective due to the initiating event. Moreover, self tests and periodic tests are implemented to detect any component failures. They consist of periodically checking the systems which perform safety functions. In case of unavailability of equipment, maintenance (followed by re-qualification tests after the maintenance work) can be performed. The maintenance is preventative or corrective, depending on the safety system state (i.e. operational or not). Testing and maintenance of equipment is described in PCSR Chapters 6 and 7.
ESS.24 The minimum amount of operational safety system equipment for which any specified facility operation will be permitted should be defined and shown to meet the single failure criterion.	The EPR is considered to comply with the SAP. All safety systems are designed with redundant components in accordance with the single-failure criterion (PCSR, Sub-chapter 3.1, section 2.5.6). Chapter 14 of the PCSR provides accident analyses performed assuming the worst single failure. These analyses account for single failure as well as assuming plant unavailability for maintenance. The allowable unavailability of equipment specified in the Technical Specification for limiting conditions of operation is justified by the accident analyses. In case of unavailability of a system, the allowed time for repair will be defined in the general rules of operation.

SAP	Comment
ESS.25 The vetoing or the taking out of service of any safety system function should be avoided.	The EPR is considered to comply with the SAP. For each plant state, the Technical Specifications define the safety systems required to ensure the safety functions with respect to the single failure criterion.. Safety functions are redundant and removal of one train is only authorised in normal operation for maintenance purposes, given that this removal is consistent with the Technical Specifications. The Protection System, which is constantly in operation, is designed with four levels of redundancy with a 2oo4 voting logic that considers possible degradation of voting (maintenance failure) in such a way that the system remains operational even in the case of failure of several channels. Protective functions may in some cases be inhibited through permissive conditions. This is only authorised only if the plant status does not request these functions. Permissives allow the taking out of service of some protection signals in order to perform normal operations (such as the transition to shutdown conditions). This is handled in the operating procedures (Chapter 18 of the PCSR) through validation of the permissive.
ESS.26 Maintenance and testing of a safety system should not initiate a fault sequence.	The EPR is considered to comply with the SAP. The EPR design has largely taken into account maintenance and testing requirements of safety systems. See also the responses made to Safety Assessment Principle EMT.6. For mechanical and electrical components, the EPR four separate safety trains allow maintenance to be carried out on one train during power operation without impairing the system safety function; the remaining three trains are able to provide the required performance, with the assumption of an additional single failure on one of them. This is discussed in PCSR Sub-chapter 18.2.

SAP	Comment
	For the I&C systems, provisions are made in order to allow maintenance and testing. In the protection system, the various types of tests are performed in an overlapping manner in such a way that the instrumentation, the processing equipment, the actuator control and the interfaces between the parts are all tested. Provisions for maintenance and testing of each I&C function are described in the PCSR in a dedicated paragraph of the corresponding sub-chapter (7.3 to 7.6).
ESS.27 Where the system reliability is significantly dependent upon the performance of computer software, the establishment of and compliance with appropriate standards and practices throughout the software development life-cycle should be made, commensurate with the level of reliability required, by a demonstration of 'production excellence' and confidence-building' measures.	The EPR is considered to comply with the SAP. As described in PCSR Chapter 7, the Process Information and Control System (MCP [PICS]) is the I&C system that enables the computerised operation of the plant. It includes: • The operator workstations and the Plant Overview Panel (POP) installed in the Main Control Room (MCR); • The operator workstations installed in the Remote Shutdown Station (SDR[RSS]); • The operator workstation installed in the Technical Support Centre (TSC) for supervision; • The basic operator workstations (with fewer screens) that can be installed, in addition to the computerised operating means, in particular plant situations (e.g. commissioning), or for specific activities (e.g. maintenance). For level 1 and 2 programmable electronic systems, a software engineering method is applied which avoids manual programming of specific application software. This method is based on the re-use of pre-existing or specifically developed and qualified software. For example, the software of the digital automation systems is built from the following types of pre-existing software: • Identical parts of the operating system software which can be used in processing units of the same type, • Parts of the operating system software that must be configured according to the applications (e.g. to manage communication inside the distributed computer system), • Standardised function modules (libraries), which must be combined and configured to perform the specific

SAP	Comment
	application functions. By using standardised function modules, each having a clearly-defined parameter depending on input-output characteristics, the software is completely and unambiguously designed by selecting the required function modules, setting their parameters and defining the connections between the modules and external signals. As detailed in PCSR Chapter 7, a design verification strategy is applied, taking considerable advantage of the software engineering method and of the central data management and consistent documentation concept for all of the design specification data.
ESR.1 Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate locations on the facility.	The EPR is considered to comply with the SAP. As described in PCSR Chapter 18, a Remote Shutdown Station (RSS) is provided as a back-up to the Main Control Room, for use in the event that the latter becomes uninhabitable due to fire, gas, smoke, etc. The function of the RSS is to allow control of the Unit when the MCR is unavailable, but when there is no other failure or accident, apart from a possible loss of the external power supply. The RSS enables the Unit to be monitored and managed during all PCC-1 (normal operational) situations and includes the instrumentation and controls required to bring the reactor to, and maintain it in, a safe state. The EPR design assumes that, when operations are managed from the RSS, the external electrical supply may not be available so power may only be obtainable from the diesel generators supplying the emergency switchboards. Note that the design assumes the RSS will not be required to be available in incident and accident conditions (PCC-2 to PCC-4 and RRC) as the MCR is qualified to remain available under such conditions.
ESR.2 The reliability, accuracy, stability, response time, range and, where appropriate, the readability of instrumentation, should be adequate for this required service.	The EPR is considered to comply with the SAP. In the EPR design, the instrumentation complies with classification requirements, the single failure criterion and the periodic test requirements for the functions in which it is involved. As an example, instrumentation equipment fulfils the same requirements for the protection against internal and external hazards as the functions and systems to which it belongs. The EPR instrumentation systems is also selected in such a manner that the measuring range, the accuracy and other

SAP	Comment
	relevant features are consistent with the range and magnitude of the variation expected from the measured process parameters. EPR instrumentation equipment is designed to facilitate and minimise the need for calibration. Testing and verification are performed to ensure that instrumentation is properly calibrated and if necessary, recalibrated. Provisions are made to avoid errors during maintenance and calibration. Functional and safety requirements of EPR instrumentation are described in more detail in the PCSR Sub-chapter 7.5.
ESR.3 Adequate and reliable controls should be provided to maintain variables within specified ranges.	The EPR is considered to comply with the SAP. Three systems are involved in process control, all of which use digital I&C architecture: • The Process Automation System (PAS). The main role PAS is the monitoring and automation of the plant in all normal operating conditions. Additionally the system performs some monitoring and control of sub-functions related to risk reduction categories. It is therefore F2 classified. • The Reactor Control, Surveillance and Limitation System (RCSL). The role of the RCSL is to process F2 and NC I&C classified functions related to core control and monitoring, including automatic LCO (limiting conditions of operation) functions, and limitation functions for core and reactor coolant circuit parameters requiring control rod actuation. • The Process Information and Control System (PICS). This system is used by the operators to monitor and control the plant in all plant conditions. It is classified to perform F2 and NC operating and monitoring functions. It accesses information from control systems and presents the information to the operating personnel at workstations in the Main Control Room, Remote Shutdown Station and Technical Support Centre or at local to plant workstations during commissioning or maintenance activities. It generates alarms in case of process or system anomalies and provides the operators with guidance for implementing appropriate measures. PCSR Chapter 7 presents the I&C functions and systems.
ESR.4 The minimum control and	The EPR is considered to comply with the SAP.

SAP	Comment
instrumentation for which facility operation may be permitted should be specified and its adequacy substantiated.	Technical Specifications for Operation (TSOs) define: • what is required (including control and indication) for a given function to be considered available, • what functions are required to be available, including the functions devoted only to indication, and thus define the minimum control and instrumentation availability for which plant operation may be permitted. A TSO justification document is provided in order to substantiate the adequacy of TSOs requirements, when needed. Critical instrumentation functions must not be lost due to failure of a single component.
ESR.5 Where computers or programmable devices are used in safety-related systems, evidence should be provided that the hardware and software are designed, manufactured and installed to appropriate standards.	The EPR is considered to comply with the SAP. The description in PCSR Chapter 7 addresses this question (see also PCSR Chapter 1).
ESR.6 Safety-related system control and instrumentation should be operated from power supplies whose reliabilities and availabilities are consistent with the functions being performed.	The EPR is considered to comply with this SAP. The nuclear island power supply system is arranged in four independent divisions. It includes: • a main power supply for all the non-safety-related drives located in the nuclear island buildings. • an emergency power supply for all the safety-related drives of the unit. • an uninterruptible power supply (2 hours capacity at full load) for the instrumentation and control system, the control supplies for the electrical switchboards, and all the other loads that must remain live during the start-up of the diesel generators.

SAP	Comment
	• a severe accident dedicated uninterruptible power supply that supports management of severe accidents coincident with loss of all off-site power and all onsite emergency power supplies. • a power supply supporting the rod control mechanisms. The nuclear island emergency power supply is designed to supply power to the drives that perform safety functions, within acceptable static and dynamic voltage limits, in all operating modes and transient conditions. The reliability and availability requirements of the emergency power supply are such that it is not a determining factor in the unavailability of the systems to which it supplies power. The nuclear island power supply is described in PCSR Sub-chapter 8.3.
ESR.7 Adequate communications systems should be provided to enable information and instructions to be transmitted between locations and to provide external communications with auxiliary services and such other organisations as may be required.	The EPR is considered to comply with the SAP. However, as stated in PCSR Chapter 18, the design of systems to communicate outside the main control room (MCR) has not been finalised at the current stage of the FA3 EPR design. This is because, given the rapid pace of technological development in this area, it is considered more effective to defer the choice of communication systems until as near as possible to the Unit's set-to-work date. For similar reasons, detailed specification of the plant communication systems in the UK EPR is likely to take place after the conclusion of the GDA process.
ESR.8 Instrumentation should be provided to enable monitoring the location and quantities of radioactive substances that may escape from their engineered environment.	The EPR is considered to comply with the SAP. Monitoring of gaseous and liquid radioactive discharges and the associated devices is described in PCER Sub-chapter 7.3; PCSR Sub-chapter 12.3 describes the KRT system [PRMS]. Measurements of activity and volume of the radioactive liquid effluents from the EPR are carried out before transfer to the shared storage tanks to provide feedback on the discharges. The RPE [NVDS] collects all the liquid waste, drains and leaks produced both inside and outside the containment, and transports it to the associated storage and treatment facilities of the TEU prior to transfer to the shared storage tanks. Before discharge from the tanks, the liquid effluents in the tank are analysed in order to check that the discharge complies with the limits and conditions set in the discharge authorisation. In addition, continuous monitoring of the ongoing discharge is carried out as an additional precautionary measure to enable

SAP	Comment
	the discharge to be terminated if necessary. The TEP [CSTS] enables the measurement, storage, and treatment of primary liquid effluent recycled in the primary cooling system. Regarding gaseous discharges, monitoring of air activity in the ventilation ducts of the Nuclear Auxiliary Building (NAB), Safeguard Auxiliary Building (SAB) and Fuel Building (FB), prior to discharge to the stack, allows detection of increases in activity levels in an affected area. Planned and continuous discharges via the stack, as well as primary effluent discharge treated by the TEG [Gaseous Waste Processing System], are also monitored. Every room of the EPR unit likely to be contaminated is connected to the stack. In addition, area monitoring of the plant by the KRT (airborne activity monitoring and local dose rate monitoring), and activity monitoring of the NAB, SAB and FB sumps, help in detecting, giving warnings, and identifying the nature and extent of any unplanned releases, to allow remedial activities to be instigated.
ESR.9 Control systems should respond in a timely and stable manner to normal plant disturbances without causing demands on safety systems.	The EPR is considered to comply with the SAP. The EPR Reactor Control, Surveillance and Limitation system (RCSL) makes an important contribution to the normal plant operation (i.e. to control of PCC-1 plant conditions). The RCSL is designed to accommodate various plant disturbances without actuation of safety systems. Platform simulation tests in various conditions including the most severe PPC-1 transients are performed in order to verify the accurate response of the safety-related control systems such as the RCSL. Pre-operational and periodic tests are also carried out to ensure the adequacy of the design and the performance of the RCSL. The RCSL, including its rapid load reduction capability (also referred to as partial trip, see PCSR Sub-chapter 7.4), constitutes one of the major innovations of the EPR compared to earlier Generation II PWRs. The RCSL enhances the capability of the plant to deal with disturbances without actuating the Protection System.
ESR.10 Faults in control systems and other safety-related	The EPR is considered to comply with the SAP.

SAP	Comment
instrumentation should not cause an excessive frequency of demands on a safety system.	EPR design includes voting logic, Operating Aid Functions and limitation systems to reduce the likelihood that elementary faults in instrumentation or control systems will result in a demand on safety systems. The main parameters involved, linked to protection, are neutron flux, RCS pressure and temperature, pressuriser level, steam generator level, etc. For most of these parameters, the control system is complemented by an Operating Aid Function. When parameters move outside control range, the Operating Aid Function uses information voted from several sources to implement an actuator response specifically aimed at avoiding the occurrence of a safety system demand.
EES.1 Essential services should be provided to ensure the maintenance of a safe plant state in normal operation and fault conditions.	The EPR is considered to comply with the SAP. The EPR engineered safety features are described in PCSR Chapter 6. The essential services necessary to maintain these systems in an operational state are the electrical power supply and cooling water. Compressed air is rarely used in the EPR: only a few valves have pneumatic actuators and these revert to a safe position or a buffer tank in the case of air supply loss. The EPR electrical power is supplied by AC or DC sources according to the safety requirements of the supplied systems. EPR safety AC sources are supplied by two sets of diesel generators: four main emergency diesel generators and two ultimate diesel generators. A description of the EPR electrical power supplies is given in PCSR Chapter 8. The diesel generators are described in the PCSR Sub-chapter 9.5. The EPR component cooling and essential service water systems (CCWS and ESWS), and the ultimate cooling water system (UCWS) are described in PCSR Sub-chapter 9.2. The design of the ESWS and the UCWS depends on the site location, especially regarding the water intake. PCSR Sub-chapter 9.2, section 4 gives the safety requirements applied to the service water intake and filtering. Safety analysis will be completed later in the site license application process.
EES.2 Where a service is obtained from a source external to the nuclear site, that service	The EPR is considered to comply with the SAP. During normal operation of the EPR, AC electrical power is provided from two different off-site grid connections. In the case

SAP	Comment
should also be obtainable from a back-up source on the site.	of loss of off-site power (LOOP), safety systems are powered by the four main emergency diesel generators (EDGs). The four main EDGs are safety classified and consequently are protected from internal and external hazards. Nevertheless, should they fail, the necessary heat removal systems would be backed-up by the two ultimate diesel generators. A description of the EPR electrical power supplies and diesel generators is given in PCSR Chapter 8 and Sub-chapter 9.5. The steam generator emergency feed water system (EFWS) and the safety injection system (in ECCS mode) use water storage contained within the systems. For long term heat removal, the safety injection system (ECCS mode or Residual Heat Removal mode) is supported by cooling water obtained from off site (sea or river or lake). The engineered safety features and the support cooling systems are described in PCSR Chapter 6 and Sub-chapter 9.2 respectively.
EES.3 Each back-up source should have the capacity, duration, availability and reliability to meet the maximum requirements of its dependent systems.	The EPR is considered to comply with the SAP. The capacity and service duration of the EPR diesel generators is defined according to the RCC-E chapters C2400 andC2500. The main diesel generators are able to meet the demand requirements of the systems they support in the event of an accident combined with a loss of off-site power. Taking into account the importance of the diesel reliability in the overall PSA results, a reliability objective is specified to, and a reliability assessment required from, the equipment supplier. The capacity of the ultimate heat sink is defined by the heat removal requirement from all supported cooling systems with the most onerous assumptions, especially assumptions related to meteorological conditions (air and water temperatures, air humidity, water level). The cooling systems are described in PCSR Sub-chapter 9.2. The site data depend on the site location: typical values are given in the PCSR Chapter 2. The actual values for a given site location be assessed in the site license application.
EES.4 Where essential services are shared with other plants on a multi-facility site, the effect of the sharing should be taken into account in assessing the adequacy of the supply.	The SAP is considered not to apply to the EPR. The EPR is designed an independent unit. No sharing of safety classified systems with other EPRs or neighbouring facilities is foreseen. The grid connection to multi-facility site will be designed in accordance with the combined requirements of all facilities. This design would be assessed in a site license application.
EES.5 The capacity of the	The EPR is considered to comply with the SAP.

SAP	Comment
essential services to meet the demands of the supported safety functional requirement(s) should not be undermined by making cross-connections to services provided for non-safety functions.	The EPR grid connections are common to the conventional island and the nuclear island. The double independent Very High Voltage connection provides a reliable off-site power supply, including during maintenance of the main connection. In addition, the EPR is designed to withstand house load operation from the main generator, which provides a further contribution to the reliability of the normal power supply. The electrical protection features are designed according to a selectivity principle, in order to avoid fault propagation to safety classified power supplies. Emergency power is supplied to the conventional island from safety divisions 2 and 3 via connections designed to avoid fault propagation to the safety classified power supply, especially in case of internal hazards (e.g. fire). The EPR electrical power supplies (including the conventional island and the balance of plant) and the single line diagram are described in PCSR Chapter 8. The ultimate heat sink design for the EPR plant is site-dependent. As mentioned in response to SAP EES.1, the requirements for water intake and filtration are given in PCSR Sub-chapter 9.2, section 4. The consequences of the possible sharing of the water filtration will be analysed in a site license application.
EES.6 Alternative sources of essential services should be designed so that their reliability would not be prejudiced by adverse conditions in the services to which they provide a back-up.	The EPR is considered to comply with the SAP. The high reliability and independence of the EPR emergency power supply is ensured by a high quality and reliable grid switch-off and diesel start-up sequence. In addition, the ultimate diesel generators are diverse to the main emergency diesel generators. The grid disconnection and diesel loading sequence are described in the PCSR Sub-chapter 9.5.
EES.7 Protection devices provided for essential service components or systems should be limited to those that are necessary and that are consistent with facility requirements.	The EPR is considered to comply with the SAP. The EPR safety philosophy is to apply the same level of safety requirements to service systems as to the system that they supply. For the diesel generators, only the essential protection devices (i.e. over-speed protection) are operational when the generators are in emergency mode. For the Essential Service Water System, no protection signal is operational, other than the electrical protection, when it is started by the Protection System.

SAP	Comment
	Diesel generator and ESWS operation are described in PCSR Sub-chapters 9.2 and 9.5.
EES.8 Where a source external to the nuclear site is employed as the only source of the essential services needed to provide adequate protection, the specification and in particular the availability and reliability should be the same as for an on-site source.	The EPR is considered to comply with the SAP. The EPR uses no off-site power source for safety classified essential services.
EES.9 Essential services should be designed so that the simultaneous loss of both normal and back-up services will not lead to unacceptable consequences.	The EPR is considered to comply with the SAP. The EPR design imposes high reliability requirements on back-up systems. Nevertheless, a dedicated category of events, (called Risk Reduction Category A, RRC-A) is defined which covers cases of simultaneous loss of both normal and back-up services (e.g. loss of off-site power and the main diesel generators, loss of ultimate heat sink). Emergency Operating Procedures are designed, and if necessary additional mitigation features are provided, to prevent such sequences leading to unacceptable consequences. RRC-A events are assessed in PCSR Sub-chapter 16.1. The Level 1 PSA results are given in PSCR Sub-chapter 15.1.
EHF.1 A systematic approach to integrating human factors within the design, assessment and management of systems should be applied throughout the entire facility life-cycle.	The EPR is considered to comply with the SAP. Sub-chapter 18.1 of the PCSR describes the EPR Human Factors Engineering Programme; section 3.explains the safety requirements applicable to human factors in the design. The Human Factors Engineering Programme (HFE) covers the design, maintenance and testing during the operational lifetime. Chapter 12 of the PCSR describes human factors elements in the radiation protection design. Sub-chapter 12.2 presents

SAP	Comment
	information on source term reduction, and Sub-chapter 12.5 presents information on the steps taken to improve layout accessibility.
EHF.2 When designing systems, the allocation of safety actions between humans and technology should be substantiated and dependence on human actions to maintain a safe state should be minimised.	The EPR is considered to comply with the SAP. Sub-chapter 18.1, section 2.2 of the PCSR describes the role of the HFE programme in apportioning tasks between human operators and automatic systems. The allocation of actions between humans and technology is substantiated in PCSR Sub-chapter 18.1, section 4.1.3, including the automation principles and criteria. These principles are applied to actions irrespective of their safety significance. The approach ensures that the dependence on human action to maintain a safe state is reduced to those actions that are not suitable for handling by automatic systems.
EHF. 3 A systematic approach should be taken to identifying human actions that can impact on safety.	The EPR is considered to comply with the SAP. The human factors engineering programme takes into account human reliability. The design objective is to make the plant less sensitive to human errors using design measures, and emergency procedures via a State Oriented Approach. Sub-chapter 18.1 explains how human reliability is covered in the human factors engineering programme, and the consequences for the design (automation, control room, alarms, procedures …) and staff organisation (operators, supervisor, etc). Human errors are addressed in the Probabilistic Safety Analysis presented in Chapter 15. Human reliability is included in the event sequences modelled. The PSA studies provide verification of the robustness of the plant against human error.
EHF.4 Administrative controls used to remain within the safe operating envelope should be systematically identified.	The EPR is considered to comply with the SAP. Sub-chapter 18.1 of the PCSR describes the role of operating staff in the main control room, and the design of the MMI. The role of each operator is clearly defined.

SAP	Comment
	Sub-chapter 18.2 presents the operational procedures : • for normal operation, including maintenance actions, • for emergency actions • for severe accident actions. The actions are specific to the different operators: actions are different for an operator and a supervisor, for example.
EHF.5 Analysis should be carried out of task important to safety to determine demands on personnel in term of perception, decision making and action.	The EPR is considered to comply with the SAP. The human factors engineering programme addresses the issue of operational staff organisation (Sub-chapter 18.1, section 1.3), including the demands on personnel. It assists in specifying the resources required to enable the operation and maintenance teams to analyse, diagnose and carry out actions (Sub-chapter 18.1, section 2.2), covering the aspects of perception, decision making, and action. The HFE programme description in Sub-chapter 18.1 explains the way representative tasks are analysed, taking into account personnel numbers, skills and experience. This work may include the use of process simulators or mock-ups. The MMI description in Sub-chapter 18.1, section 4 describes the composition and role of operating personnel, indication and control requirements and alarm system characteristics, which contribute to perception, decision making, and the performance of actions.
EHF.6 Workspaces in which plant operations and maintenance are conducted should be designed to support reliable task performance, by taking of human perceptual and physical characteristics and the impact of environmental factors.	The EPR is considered to comply with the SAP. The HFE programme described in Sub-chapter 18.1 explains the how workspace and environmental conditions are investigated and analysed to determine how to achieve the desired human performance goals. This work may include use of tests and mock-ups.

SAP	Comment
EHF.7 User interfaces, comprising controls, indications, recording instrumentation and alarms should be provided at appropriate locations and should be suitable and sufficient to support effective monitoring and control of the plant during all plant states.	The EPR is considered to comply with the SAP. The MMI is designed to meet specific requirements, which have been developed by a panel of experienced plant operators by application of feedback experience from operating French NPPs. Tests have been defined to evaluate the tools which are considered necessary, such as alarms, displays, instrumentation, guidance levels etc. The tests utilise mock-ups to study different operational situations such as normal operation and emergency situations. The design of the MMI resulting from this work is implemented in the MCR. It covers both normal and emergency operation procedures. Additionally a simulator is used for testing different operational and accident situations, in order to test operating procedures, alarms, instrumentation actions etc. Sub-chapter 18.1 presents the design principles of the MMI and associated equipment. Sub-chapter 18.2 presents the principles used to develop operational, emergency and severe accident procedures.
EHF.8 A systematic approach to the identification and delivery of personnel competence should be applied.	Some general information concerning training is given in PCSR Chapter 18.1. The identification and delivery of personnel competence for operating the plant is the responsibility of the dutyholder and is outside the scope of GDA.
EHF.9 Procedures should be produced to support reliable human performance during activities that could impact on safety.	The EPR is considered to comply with the SAP. Procedures are developed in consultation with operators, taking into account feedback experience from existing plants. Emergency procedures are tested on a simulator. Fault studies are developed taking into account operator actions from emergency procedures. The Level 1 PSA in Chapter 15 assumes operator actions consistent with the strategy defined in the emergency operating procedures. Qualitative and quantitative PSA analyses will be used to assist in designing detailed operating procedures and

SAP	Comment
	for operator training, with emphasis on operation actions, failure of which could lead to a significant increase in the frequency of core damage. Sub-chapter 18.2 describes the emergency operating procedures and the severe accident management guides. Sub-chapter 18.2 describes the emergency and the severe accident procedures.
EHF.10 Risk assessment should identify and analyse human actions or omissions that might impact on safety.	The EPR is considered to comply with the SAP. The impact of human actions on safety is analysed in the PSA (see Chapter 15). The following types of human action are considered in the design phase PSA: • Human errors during operation and maintenance • Operator actions during post-accident recovery • Operator actions in severe accident management
ENM.1 A strategy (strategies) should be made and implemented for the management of nuclear matter.	The EPR is considered to comply with the SAP. Sub-chapter 9.1 of the PCSR describes the design of the new fuel dry storage racks, the safety requirements, and the loads assumed in the design. This chapter also describes the underwater fuel storage racks, the safety requirements, the load cases assumed for the design, and the operational principles.
ENM.2 Nuclear matter should not be generated on the site, or brought onto the site, unless	The EPR is considered to comply with the SAP. Sub-chapter 9.1 of the PCSR describes the management of new fuel, when coming onto the site, prior to loading.

SAP	Comment
sufficient and suitable arrangements are available for its safe management.	This chapter describes the also the underwater fuel storage racks, the safety requirements, the load cases for the design, and the operational principles.
ENM.3 Unnecessary or unintended generation, transfer or accumulation of nuclear matter should be avoided.	This is not within the scope of the GDA.
ENM.4 Nuclear matter should be appropriately controlled and accounted for at all times.	This is not within the scope of the GDA.
ENM.5 Nuclear matter should be characterised and segregated to facilitate its safe management.	This is not within the scope of the GDA.
ENM.6 When nuclear matter is to be stored on site for a significant period of time it should be stored in a condition of passive safety and in accordance with good engineering practice.	The EPR is considered to comply with the SAP. Sub-chapter 9.1 of the PCSR describes the new fuel dry storage rack, and the underwater fuel storage rack: it defines the equipment design basis and design characteristics. The dry fuel storage and the underwater fuel storage facility structures are classified as seismic category 1. They are designed against external and internal hazards, i.e. flooding, dropped loads, design basis earthquake, air plane crash, etc). The facility is designed to maintain its structural integrity following a safe shutdown earthquake and to perform its intended function following postulated initiating events and hazards. Non seismic equipment in the spent fuel storage racks is designed such that fuel failure could not result in Keff exceeding

SAP	Comment
	its maximum allowable value.
ENM.7 Storage of nuclear matter should be in a form and manner that allows it to be retrieved and, where appropriate, inspected.	The EPR is considered to comply with the SAP. Sub-chapter 9.1 of the PCSR describes the design of the spent fuel storage racks. The alignment of modules is checked on-site using a dummy fuel assembly. Insertion tests are carried out to confirm the adequacy of tolerances. In service-maintenance is not required on the storage racks. The fuel handling systems are designed to unload and load the core. They are designed to handle the fuel assemblies underwater from the time they enter the storage pool to the time they are placed in a transport cask for shipment off the site.
ENM.8 Nuclear material accountancy data should be analysed and reviewed periodically.	This is not within the scope of the GDA..
ECV.1 Radioactive substances should be contained and the generation of radioactive waste through the spread of contamination by leakage should be prevented.	The EPR is considered to comply with the SAP. In the Reactor Building, the EPR uses three physical barriers between radioactive materials and the environment: the fuel cladding, the reactor coolant pressure boundary, and the containment building. Each of these is designed to be leak tight. The EPR containment concept is a double walled building, with an inner steel liner. The EPR containment is designed to withstand pressure and temperature transients resulting from all initiating events considered in the design: design basis events as well as risk reduction categories events, including severe accidents, and to withstand internal and external hazards. The containment function includes isolation devices on each penetration, cooling systems, a hydrogen control system and an annulus filtration system. The EPR containment function is described in the following PCSR sub-chapters :

SAP	Comment
	• Design of category 1 civil structures, Sub-chapter 3.3 • Containment systems, Sub-chapter 6.2
ECV.2 Nuclear containment and associated systems should be designed to minimise radioactive releases to the environment in normal operation, fault and accident conditions.	The EPR is considered to comply with the SAP. In normal operation, all potential radioactive releases through air flow from containment and peripheral buildings are filtered by HEPA filters, and, if necessary by iodine filters. EPR gaseous releases are reduced by the efficiently designed TEG [GWPS] and TEP [CSTS] systems, running at constant gas volume flowrates during power operation. The liquid releases are minimised by the use of primary coolant recycling. Radioactive gases discharges are described in Sub-chapter 11.2. The GWPS and CSTS systems are described in PCSR Sub-chapters 11.4 and 9.3. In fault and accident conditions, the containment is isolated. The safeguard systems (Safety Injection) and the severe accident systems EVU (CHRS, Containment Heat Removal System) are designed to be leak tight. The rooms where they are located are dynamically confined in order to allow filtration of aerosols and iodine from residual leaks. Containment isolation is described in the PCSR Sub-Chapter 6.2. The HVAC systems are described in PCSR Sub-Chapter 9.4.
ECV.3 The primary means of confining radioactive substance should be by the provision of passive sealed containment systems and intrinsic safety features, in preference to the use of active dynamic systems and components.	The EPR is considered to comply with the SAP. The EPR containment is designed to ensure very low leakage in normal and fault conditions, including severe accidents, by means of static confinement of radioactive substances inside the Reactor Building. Any potential leak is routed to the plant stack via filtration systems, so no unfiltered material can reach the environment directly. The number of penetrations is minimised, by simplification of the safeguard systems, e.g. absence of headers on the Safety Injection system, and in-containment water storage. Containment penetrations are isolated by redundant valves, powered by secure power supplies. Maintenance activities on isolation valves and their support systems are considered in the design.

SAP	Comment
	EPR containment isolation is described in PCSR Sub-chapter 6.2. No discharge from the containment building is necessary in design basis or severe accident conditions. The only opening to the containment atmosphere is the small flow air renewal system used during access of personnel in power operation. The corresponding penetration is isolated with piping isolation technology. The containment HVAC systems are described in the PCSR Sub-chapter 9.4.
ECV.4 Where the radiological challenge dictate, waste storage vessels, process vessels, piping, ducting, and drains (including those that my serve as routes for escape or leakage from containment) and other plant items that act a containment for nuclear matter, should be provided with further containment barrier(s) that have sufficient capacity to deal with the leakage resulting from any design basis fault.	The EPR is considered to comply with the SAP. The EPR waste management systems have a barrier function and are classified in accordance with their radioactive inventory. Provisions are made in the layout, civil and ventilation design in respective buildings, to cope with potential leaks of these systems by means of passive containment barriers (leak-tight civil works) and dynamic confinement. The EPR waste management systems (gaseous, liquid, solid waste, radioactive or chemical) are described in PCSR Chapter 11.
ECV.5 The need for access by personnel to the containment should be minimised.	The EPR is considered to comply with the SAP. Access by personnel to the containment for maintenance activities is planned to take place a few days before and after outage, and for some planned or contingent maintenance activities. Specific design of the layout and of the ventilation systems is dedicated to allow such access (the two room design concept with dynamic containment) The safety containment function is unaffected by personnel access. The reactor building access conditions are addressed in PCSR Sub-chapter 12.3. Containment HVAC systems are described in PCSR Sub-chapter 9.4.

SAP	Comment
	There no requirement for access to the containment following an accident, except in cases when the equipment hatch has been previously opened (PCSR Sub-chapter 12.5).
ECV.6 Suitable monitoring devices with alarms and provisions for sampling should be provided to detect and assess changes in the stored radioactive substance or changes in the radioactivity of the materials within the containment.	The EPR is considered to comply with the SAP. The radioactive substances in the primary coolant are monitored in all conditions (normal operation and accidental conditions) through sampling and activity measurements on the Reactor Coolant System and on auxiliary systems. Changes in radioactivity in the containment are monitored in all conditions (normal operation and accident conditions) by measurements of the activity in the containment atmosphere. The nuclear sampling system is described in PCSR Sub-chapter 9.3. The KRT system [Plant Radiation Monitoring system] is described in PCSR Sub-chapter 12.3. The fissile content of the core is monitored indirectly by the reactivity control systems. These are described in PCSR Sub-chapter 4.5.
ECV.7 Appropriate sampling and monitoring systems and other provisions should be provided outside the containment to detect, locate, quantify and monitor leakages of nuclear matter from the containment boundaries under normal and accident conditions.	The EPR is considered to comply with the SAP. The Nuclear Vent and Drain System [NVDS] collects the liquid leakage from nuclear matter inside and outside the containment and transfers it to various systems according to the ability to be recycled, or according to its radiological characteristics. Systems where primary coolant could be circulated outside containment in normal operation or in accidental conditions are monitored through sampling and activity measurements on auxiliary and safeguard systems. In addition, the atmosphere of the rooms where such systems are located is monitored by activity measurements on HVAC systems. The NVDS is described in PCSR Sub-chapter 11.4. The nuclear sampling system is described in PCSR Sub-chapter 9.3. The KRT system [Plant Radiation Monitoring system] is described in PCSR Sub-chapter 12.3.

SAP	Comment
ECV.8 Where provisions are required for the import and export of nuclear matter into or from the facility, the number of such provisions should be minimised.	The EPR is considered to comply with the SAP. The generic equipment for the import of new nuclear fuel and export of spent fuel is located in the fuel building. A further part is site-specific (at the interface with public transportation) The fuel storage and spent fuel handling systems are described in PCSR Sub-chapter 9.1.
ECV.9 The design should ensure that controls on fissile content, radiation levels, the overall containment and ventilation standards are suitable and sufficient at all times.	The EPR is considered to comply with the SAP. The integrity of fuel assemblies is controlled at different stages, during their acceptance on the site, when they are unloaded from the reactor core, and also in case of damage detection. Fuel handling devices are designed with a high reliability level. The reactor building and fuel building ventilation systems are designed to minimise the effects of a fuel handling accidents (configuration change from open circuit ventilation to dynamic containment). Fuel handling systems are described in PCSR Sub-chapter 9.1. Containment and fuel building HVAC systems are described in PCSR Sub-chapter 9.4. Fuel handling accidents are analysed in PCSR Chapter 14.
ECV.10 The safety functions of the ventilation system should be clearly identified and the safety philosophy of the system in normal and fault conditions should be defined in terms of the relative priorities given to the functions associated with the system.	The EPR is considered to comply with the SAP. In the nuclear island and waste treatment buildings, where a ventilation system is used to perform dynamic containment of radioactive airborne substances, the corresponding safety function is identified and the corresponding configuration is given priority in the controls. In such configurations, the following functions are provided: (1) aerosol and iodine filtration before release to the environment via the stack and (2) prevention of contamination spreading in order to provide protect building occupants. Specific provisions for habitability of the main control room are provided, in order to protect operators from outside contamination or other outside hazardous substances. All HVAC systems, including main control room ventilation, containment and other nuclear ventilation, and non-radioactive ventilation systems are described, together with their safety classification, in PCSR Sub-chapter 9.4.

SAP	Comment
ERC.1 The design and operation of the reactor should ensure the fundamental safety functions are delivered with an appropriate degree of confidence for permitted operating modes of the reactor.	The EPR is considered to comply with the SAP. Analysis of Design Basis events (PCC) and Risk Reduction Category A (RRC-A) shows that the three basic safety functions of control of reactivity, removal of heat from the core and the confinement or containment of radioactive substances, are achieved in all permitted modes of reactor operation, including accidents in the spent fuel pool (see PCSR Chapters 14 and 16), with a high degree of confidence. The requirement to assume the most adverse Single Failure in PCC studies ensures that the safety functions can be achieved despite the most onerous failure (e.g. failure to insert the highest worth control rod assembly into the reactor core, loss of emergency diesel at the most onerous instant …).
ERC.2 At least two diverse systems should be provided for shutting down a civil reactor.	The EPR is considered to comply with the SAP. Core reactivity can be controlled by adjusting either the control rod insertion in the core or the soluble boron (boric acid) concentration in the primary coolant. The overall principles of the core reactivity control are explained in PCSR Chapter 4. For fault conditions that require quick negative reactivity insertion, the reactor is protected by a fast, gravity driven, insertion of all control rods and, as a back-up in case of failure to insert the control rods, by soluble boron injection in the primary coolant. There are 89 control rods; 53 of them are dedicated to the shutdown function and always fully withdrawn during the time the reactor core is critical. In case of a reactor trip actuation, the reactor protection system cuts off the electrical power supply for all the control rod mechanisms, therefore releasing the 89 rods which immediately insert into the core. The allowed insertion of the control rods used by the reactor control system is limited to maintain shutdown capability and to provide the shutdown margin which enables any design basis condition to be dealt with. The Control Rod Drive Mechanism (see PCSR Chapter 3) and the Rod Assembly Guide which are part of the internal structure of the reactor vessel (see PCSR Chapter 3) are designed and manufactured in accordance with the safety classification (described in PCSR Chapter 3).

SAP	Comment
	Soluble boron injection comes in addition to or as a back-up of insertion of the control rods. Soluble boron injection can be achieved either by the Extra Boration System (EBS) see PCSR Chapter 6, or by the Safety Injection System (SIS) see PCSR Chapter 6: both systems are safety classified, and are designed, manufactured and tested accordingly. Analysis of Risk Reduction Category A (RRC-A) events involving failure of the control rods to insert shows that the EBS system is functionally capable of safely shutting down the reactor to achieve a final safe state (see PCSR Chapter 16) independently of the control rods. The Chemical and Volume Control Systems (RCV), see PCSR Chapter 9, is used for reactor control to adjust the boron concentration during normal operation; it is not safety classified.
ERC.3 The core should be stable in normal operation and should not undergo sudden changes of condition when operating parameters go outside their specified range.	The EPR is considered to comply with the SAP. Reactor and core design is described in PCSR Chapter 4. The nuclear design evaluation (see PCSR Chapter 4) confirms that the reactor core has inherent characteristics which, together with corrective actions of the reactor control and protective systems, provide adequate core reactivity control. The design also provides for inherent stability against diametrical or radial and axial power oscillations and for control of induced axial power oscillation through the use of control rods. Design basis and functional requirements of the reactivity control systems are presented in PCSR Chapter 4. PCSR Chapter 4 presents the fuel design and the core thermal-hydraulic design. The thermal-hydraulic design analyses and calculations establish coolant flow parameters which ensure that adequate heat transfer is provided between the fuel cladding and the reactor coolant. The design assures that the core structure and components (such as fuel and internal equipment) allow sufficient coolant flow for heat removal.
ERC.4 The core should be designed so that safety-related	The EPR is considered to comply with the SAP.

SAP	Comment
parameters and conditions can be monitored in all operational and design basis fault conditions and appropriate recovery actions taken in the event of adverse conditions being detected.	Analysis of Design Basis events (PCC) and Risk Reduction Category A (RRC-A) shows that the three basic safety functions of control of reactivity, removal of heat from the core and the confinement or containment of radioactive substances, are achieved in all permitted modes of reactor operation, including accidents in the spent fuel pool (see PCSR Chapters 14 and 16), with a high degree of confidence. The requirement to assume the most adverse Single Failure in PCC studies ensures that the safety functions can be achieved despite the most onerous failure (e.g. failure to insert the highest worth control rod assembly into the reactor core, loss of emergency diesel at the most onerous instant …). The EPR core is designed to ensure that the heat produced by fuel assemblies is safely removed in all operational and design basis fault conditions (see PCSR Chapter 4, Reactor and Core Design). In particular, fuel assemblies are designed to have adequate rigidity (through guide thimbles, grids, nozzles…) and to avoid undesirable behaviour, such as rod bowing. (Margins for rod bowing are nevertheless taken into account in safety analyses, based on AREVA's experience as a fuel designer, to demonstrate that safety criteria are met.) By ensuring adequate heat removal and limited core geometry deformation, the EPR design ensures that recovery actions, such as fast insertion of Rod Cluster Control Assemblies, remain possible under normal, incident or accident conditions. Core instrumentation is chosen to adequately monitor each safety-related core parameter. It is selected in such a manner that measurements of range, accuracy and other relevant features are consistent with the range and magnitude of the variation expected in the process parameters being measured. Instrumentation requirements and classification are described further in PCSR Sub-chapter 7.5. In operation, fuel assembly leak tightness is monitored using activity measurements made in the primary fluid. These measurements allow for detection of fuel cladding failures and enable monitoring of their development. Fuel assemblies are designed so that their structure and parts can be suitably inspected before they are loaded into the core. Post-irradiation inspection to confirm fuel behaviour and performance is possible and would be normal practice in the case of a new fuel assembly design or a significant change to reactor operating conditions. The fuel handling system allows fuel to be removed from the reactor despite environmentally induced damage such as rod bowing, swelling or other damage occurring in normal operation or design basis fault conditions.

SAP	Comment
EHT.1 Heat transport systems should be designed so that heat can be removed or added as required.	The EPR is considered to comply with the SAP. Several systems are designed to transport and remove heat from: • The reactor core, • The spent fuel pool, • The containment. To remove heat from the reactor core is a safety function taken into account in the basic design of the plant, both in normal and accidental operation (there is no safety requirement for adding heat in the PWR process). The main heat transport system is made up of the Reactor coolant system (RCP) itself, the steam generators and the main steam lines (MSSS) on the secondary side from the steam generators to the turbine. • The reactor coolant system functions and its design flow rates are described in PCSR Chapter 5. • The secondary cooling system and in particular the MSSS system is described in PCSR Chapter 10. The Main Steam Relief Train (VDA) is capable of removing decay heat by dumping steam from the main steam system into the atmosphere in the event of turbine tripping with the condenser unavailable. It is described in PCSR Chapter 6. The Residual Heat Removal System (RRA) removes the reactor core heat in the following conditions: • In normal shutdown states with the core loaded when the steam generators can no longer perform this function (with reactor in State C to E). • In case of accident PCCs and RRCs to reach and maintain the safe state. This system is described in PCSR Chapter 6. When the RRA is actuated, the heat is then transported to the component cooling water system and essential service water system (RRI/SEC) by means of heat exchangers, which ensure sufficient heat transfer from the component cooling system to cold water. The RRI and SEC systems are described in PCSR Sub-chapter 9.1.

SAP	Comment
	The SEC [ESWS] system also contributes to the decay heat removal from the PTR [FPPS/FPCS] as part of the spent fuel pool cooling system. The Containment Heat Removal System (EVU) is used to ensure decay heat removal from the containment in case of severe accidents (RRC-B). The EVU system transfers the decay heat from the IRWST to the ultimate cooling water system using a dedicated cooling system, the SRU. This is described in PCSR Chapter 6
EHT.2 Sufficient coolant inventory and flow should be provided to maintain cooling within the safety limits for operational states and design basis fault conditions.	The EPR is considered to comply with the SAP. The Reactor Coolant System (RCP) design flow and its uncertainties for normal operation are described in PCSR Chapter 5. Design basis analyses from PCSR Chapter 14 show that the primary circuit inventory and cooling are sufficient, and maintained by active and passive systems. In these analyses, uncertainties on systems data are considered in a conservative way.
EHT.3 A suitable and sufficient heat sink should be provided.	The EPR is considered to comply with the SAP. The heat sink for the EPR safety classified cooling systems is provided by the SEC [ESWS] (Classified F1A) and the SRU [UCWS] (Classified F2). Some equipment uses atmospheric air as a heat sink. The SEC and SRU are supplied by backed-up electrical supplies. EPR design principles require that F1 and F2 systems are designed to carry out their safety functions in the presence of external hazards, including extreme conditions of air and water temperatures, as required by the SAP (see PCSR Chapter 13).
EHT.4 Provisions should be made in the design to prevent failure of the heat transport system that could adversely affect the heat transfer process, or safeguards should be available to maintain the	The EPR is considered to comply with the SAP. The break preclusion concept, which ensures that a break in a pipe can be ruled out by preventive measures, is described in PCSR Chapter 13. PCSR Chapters 14 and 16 show analyses of events leading to a loss of coolant inventory following a pressure boundary

SAP	Comment
facility in a safe condition and prevent any release in excess of safe limits.	failure, or to a decrease of heat removal by the secondary system. The alarms and signals from the Surveillance and Protection System, added to the relevant active and passive safety systems, prevent an uncontrolled loss of coolant flow or heat removal by the secondary system and enable a controlled and safe state to be reached. Furthermore, the activity is contained inside the containment in case of Loss of coolant accident (isolation of the containment). In normal operation, main physical (e.g. temperature and pressure) and chemical (e.g. boron concentration,) properties of the primary coolant system are monitored and controlled. The reactor coolant volume and chemical control is performed by the RCV [CVCS], described in PCSR Chapter 9. The activity in the primary coolant is monitored by the Nuclear Sampling System. The core cooling is performed by pressurised water: in these conditions, only steam and liquid phase can be mixed; there is no risk of unexpected chemical reactions between incompatible heat transport fluids.
EHT.5 The heat transport system should be designed to minimise radiological doses.	The EPR is considered to comply with the SAP. The EPR core design includes a heavy reflector that minimises the neutron flux on the reactor vessel. The reactor vessel is enclosed in the reactor pit, the concrete walls of which provide an efficient biological shield. For other neutron routes in the reactor building, biological shielding is provided as required. Other sources of radiological doses from the primary coolant arise from fission products coming through fuel cladding leaks and from corrosion products transported in the coolant itself or deposited on primary equipment. The EPR has been designed to minimise radiological doses using the following measures: material selection (free or low cobalt alloys), optimisation of the purification systems, chemistry control during power operation (pH management) and cold shutdown phases (oxygenation). In-service-inspection or maintenance activities can only start when radiological criteria are met in the primary coolant. As regards the choice of heat transfer fluid, the EPR benefits from the PWR concept. Heat is transferred to non-radioactive fluids :

SAP	Comment
	• Steam that powers the turbine via the steam generators in power operation, • the Component Cooling Water System via the Residual Heat Removal System (RRA [RHRS]) during shutdown states. There is no direct cooling of the primary system by the heat sink. The EPR design features to minimise radiological doses are described in PCSR Chapter 12.
ECR.1 Wherever significant amount of fissile materials may be present, there should be a system of safety measures to minimise the likelihood of unplanned criticality.	The EPR is considered to comply with the SAP. Wherever significant amount of fissile materials may be present (i.e. mainly in the reactor pressure vessel and the spent fuel pool), a system of safety measures has been implemented to minimise the likelihood of unplanned criticality. These measures include: a) <u>The design of the new fuel dry storage racks (see PCSR Sub-chapter 9.1)</u> This design : - avoids any criticality risks in the most conservative homogenous moderation conditions (immersion in pure water or pure steam), assuming that the individual cells of the rack contain new fuel with the maximum permitted enrichment. - prevents any geometrical deformation as a result of changes in operating or ambient conditions. The design must be stable against tipping; measures must be taken to prevent unintended movement of the fuel assemblies or of the storage rack itself. - prevents more than one fuel assembly being placed in a single storage cell or a fuel assembly being placed or jammed between two storage cells. b) <u>The functional design of core reactivity control</u> <u>(see PCSR Sub-chapter 4.5)</u>

SAP	Comment
	The safety functional requirement met by the functional design of the reactivity control is to control core reactivity, to enable the chain reaction to be stopped under all circumstances, and to allow the reactor to return to a safe state. Core reactivity is controlled under all normal operating conditions from start-up to shutdown by the use of two different means. The first consists of the Rod Cluster Control Assembly (RCCAs) and the second of variation in the concentration of soluble boron in the coolant. The general design bases and functional requirements used in the functional design of the reactivity control for EPR (e.g. maximum reactivity insertion, adequate shutdown margin or sub-critical state of the core) are described in the PCSR (see PCSR Sub-chapter 4.5). The functional design of reactivity control impacts the design of a large number of systems described in the PCSR: the Control Rod Drive System (CRDS), the Chemical and Volumetric Control System (RCV [CVCS]), the Extra Boration System (RBS [EBS]), the Safety Injection System (RIS [SIS]). c) <u>The design of underwater fuel storage racks (see PCSR Sub-chapter 9.1)</u> This design : - excludes all risks of criticality, not only in normal storage conditions but also in the case of zero boron concentration in the pool water. The potential storage of incomplete fuel assemblies (from which 1 to 3 fuel rods have been extracted) is taken into account. - prevents any geometrical deformation as a result of changes in operating or ambient conditions. The design must be stable against tipping; measures must be taken to prevent unintended movement of the fuel assemblies or of the storage rack itself. - prevents more than one fuel assembly being placed in a single storage cell or a fuel assembly being jammed between two storage cells. The analysis of Design Basis events (PCC) and Risk Reduction Category A (RRC-A) events demonstrates that the system

SAP	Comment
	of safety measures ensure that reactivity control is achieved in all permitted modes of reactor operation, including accidents in the spent fuel pool (see PCSR Chapters 14 and 16), with a high degree of confidence. Probabilistic safety assessment also addresses such events (see PCSR Chapter 15) and confirms the high level of prevention/mitigation of the design. The risk of fast reactivity insertion into the core following an external heterogeneous dilution has also been assessed (see PCSR Sub-chapter 16.3). Taking into account design measures, probabilistic analysis shows that the risk of forming a slug larger than 4 m^3 (“critical slug size”) and thus inducing a core melt, is negligible. In conclusion, given the design characteristics and the dedicated methods of prevention, it is deemed that the risk of fast reactivity insertion into the core following an external heterogeneous dilution event can be considered as “practically eliminated”.
ECR.2 A criticality safety case should incorporate the double contingency approach.	The EPR is considered to comply with the SAP. The double contingency approach (in the context of a reactor facility such as EPR), is incorporated into the safety analysis. The EPR reactor is designed so as to avoid a criticality accident. In particular: - a criticality accident cannot result from a single anomaly (failure of a component, function, human error, accidental situation (e.g. fire)) - if a criticality accident can result from the simultaneous occurrence of two anomalies, it must be demonstrated that: o the two anomalies are rigorously independent o the probability of occurrence of each of the two anomalies is sufficiently low o each anomaly can be highlighted by means of adequate and reliable monitoring
RP.1 Adequate protection against exposure to radiation and radioactive substances in normal operation should be provided in	The EPR is considered to comply with the SAP. Normal operation includes all outage types: refuelling only outage, normal outage with routine maintenance, ten year outage with a large ISI programme. The EPR occupational exposure has been optimised using experience feedback from

SAP	Comment
those parts of the facility to which access needs to be gained.	French nuclear plants. Different items contribute to radiation exposure improvement: fuel design, material selection, primary coolant chemistry, purification systems, maintenance requirements, layout and accessibility to equipment. Moreover, adequate structural protections have been provided for radiation protection in places where maintenance work will need to be performed. Each of these items has been optimised in the EPR design, as far as possible, whilst ensuring compatibility with safety requirements. The overall collective dose objective of the EPR is 0.35 man.Sv per year and per unit (for 18-month fuel cycles, averaged over 10 years and including 3 Normal Refuelling Outages, 2 Refuelling Only Outages and 1 ten-year outage). The assessment of the EPR dose uptake prediction is provided in PCSR Sub-chapter 12.4.
RP.2 Adequate protection against exposure to radiation and radioactive substances in accident conditions, should they occur, should be provided in those parts of the facility to which access needs to be gained. This should include prevention or mitigation of accident consequences.	The EPR is considered to comply with the SAP. The EPR safeguard systems are designed to be operated automatically, or from the main control room. Access to some equipment is considered only for systems used to maintain the long term cooling of the reactor core or the spent fuel. The few actions considered are described in PCSR Sub-chapter 12.5.
RP.3 Where appropriate, designated areas should be further divided, with associated controls, to restrict exposure and prevent the spread of radioactive substances.	The EPR is considered to comply with the SAP. The EPR radiation protection classification and zoning is described in PCSR Sub-chapters 12.1 and 12.3. Technical devices enabling access control are part of the above description. Organisational measures will be defined later, as part of the operational rules.
RP.4 Appropriate provisions for protecting persons entering	The EPR is considered to comply with the SAP.

SAP	Comment
and working in contaminated areas should be provided.	Shielding provisions and ventilation provisions are described in PCSR Sub-chapter 12.3. Room and staff monitoring is also described in PCSR Sub-chapter 12.3.
RP.5 Suitable and sufficient decontamination provisions for the people, the facility, its plant and equipment should be provided.	The EPR is considered to comply with the SAP. Showers are provided in the personnel hot change room for decontamination of people. Spent fuel casks and any waste containers are decontaminated until surface contamination is in accordance with the transportation regulations. Plant equipment, subject to any maintenance activity, especially equipment subject to in-service inspection, can be decontaminated by flushing and draining. The RPE system [Nuclear Vent and Drain System] is described in PCSR Chapter 11.
RP.6 Where shielding has been identified as a means of restricting dose, it should be effective under all conditions.	The EPR is considered to comply with the SAP. The main shielding material is standard concrete aggregate. Water is also used as a shielding material (in primary pipework, the steam generators, the reactor and the spent fuel pool. Other materials can be used: lead, shielding glass and specific neutron shields. For normal operation, all shielding provisions are permanent. Temporary shielding may be used later in the plant lifetime, to cope with hot spots. The EPR design has selected, as much as possible, valve technologies to prevent hot spot stabilisation. The EPR shielding provisions are described in PCSR Sub-chapter 12.3.
FA.1 Fault analysis should be carried out comprising design basis analysis, suitable and sufficient PSA, and suitable and	The EPR is considered to comply with the SAP. The fault analysis is carried out through:

SAP	Comment
sufficient severe accident analysis.	• Design Basis (PCC) accident analysis for the EPR described in PCSR Chapter 14. • Risk Reduction Categories RRC-A (multiple failure events) and RRC-B (severe accidents) described in PCSR Chapter 16. • A comprehensive PSA at Level 1, 2 and 3, presented in PCSR Chapter 15.
FA.2 Fault analysis should identify all initiating faults having the potential to lead to any person receiving a significant dose of radiation, or to a significant quantity of radioactive material escaping from its designated place of residence or confinement.	The EPR is considered to comply with the SAP. The list of Design Basis Events analysed in the EPR PCSR is presented in PCSR Chapter 14. This list is intended to cover all significant events having a potential to lead to a significant radiological release consequences at all locations in the plant and in all plant states.
FA.3 Fault sequences should be developed from the initiating faults and their potential consequences analysed.	The EPR is considered to comply with the SAP. Analysis of design basis fault sequences, developed from the Design Basis initiating events, is described in PCSR Chapter 14. A conservative methodology is used for the transient analysis, including the assumption of the most adverse single additional failure, and the most onerous preventive maintenance state. Radiological consequences analyses of the design basis fault sequences are described in PCSR Chapter 14. The design basis initiating events are included in the Level 1 PSA analysis, as required by SAP FA.3. An assessment of the societal consequences of within and beyond design basis faults against Target 9, as requested by SAP FA.3, is presented in Chapter 15 of the PCSR. Due to the extremely low frequency of large releases achieved by the EPR design (PCSR Chapter 15) Target 9 is achieved.
FA.4 DBA should be carried	The EPR is considered to comply with the SAP.

SAP	Comment
out to provide a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safety measures.	The design basis analysis is described in PCSR Chapter 14. The initiating events studied in this chapter are classified into several classes of events: • Increase of heat removal by the secondary system, • Decrease of heat removal by the secondary system, • Decrease in reactor coolant system flow rate, • Reactivity and power distribution anomalies, • Increase of water inventory in the primary system, • Reduction of water inventory in the primary system, • Radioactive releases from a subsystem. In the dedicated chapter, the analyses show that the relevant criteria for each event are met.
FA.5 The safety case should list all initiating faults that are included within the design basis analysis of the facility.	The EPR is considered to comply with the SAP. A table of design basis initiating events is given in PCSR Chapter 14.
FA.6 For each initiating fault in the design basis, the relevant design basis fault sequences should be identified.	The EPR is considered to comply with the SAP. Development of design basis fault sequences for the Design Basis initiating events is described in PCSR Chapter 14. The fault sequences considered address the identified requirements i.e.: • failures resulting from the initiating event and failures expected to occur in combination with that initiating event from common causes are included;

SAP	Comment
	• single failures in the safety measures are assumed in accordance with the single failure criterion; • the worst normally permitted configuration of equipment outages for maintenance, test or repair is assumed • the most onerous permitted operating state of the reactor is considered; Adverse conditions arising as a consequence of the fault are taken into account for equipment performing a safety function (see PCSR Chapter 3). All actions required within 30 minutes of a PCC accident to reach a controlled or safe shutdown state are automated, and further actions which could be of a manual nature are executed in accordance with written procedures (see PCSR Chapter 18).
FA.7 Analysis of design basis fault sequences should use appropriate tools and techniques, and be performed on a conservative basis to demonstrate that consequences are ALARP.	The EPR is considered to comply with the SAP. Analysis of Design Basis event sequences (PCCs) for the EPR is presented in PCSR Chapter 14. The analysis is carried out using validated models and conservative assumptions. The analysis shows that in all cases at least one of the physical barriers preventing a significant release of radioactivity into the environment remains intact and that the radiological consequences are small. An analysis of the radiological consequences of the Design Basis (PCC) events is presented in PCSR Chapter 14. This confirms that the radiation dose to members of the public in the vicinity of the plant at the time of the accident is well within the targets set for the EPR design, and also well below the BSL for Design Basis events given in Table 4 of the SAPs, meeting the requirement of paragraph 523 of SAP FA.7.
FA.8 DBA should provide a clear and auditable linking of initiating faults, fault sequences and safety measures.	The EPR is considered to comply with the SAP. Analysis of the Design Basis (PCC) events is described in PCSR Chapter 14. For each PCC sequence the F1 safety systems claimed to provide the basic safety functions are described. Demonstration that a safe state is achieved in the PCC event analysis demonstrates the functional capability of the F1 safety systems.

SAP	Comment
	Analysis of Risk Reduction Category A (RRC-A) presented in PCSR Chapter 16 similarly identifies the F2 safety systems that provide diverse protection in complex sequences involving CCF of F1 systems.
FA.9 DBA should provide an input into the safety classification and the engineering requirements for systems, structures and components performing a safety function; the limits and conditions for safe operation; and the identification of requirements for operator actions.	The EPR is considered to comply with the SAP. In accordance with standard practice, the PCC, RRC and severe accident analyses are used as the basis for confirming plant safety limits, the functional requirements for safety systems and equipment, availability requirements on safety-related plant, and for identifying required operator actions and available action times in accidents (see in particular PCSR Chapter 3 for safety classification and for equipment qualification and PCSR Chapter 18 for emergency operating procedures).
FA.10 Suitable and sufficient PSA should be performed as part of the fault analysis and the design development and analysis.	The EPR is considered to comply with the SAP. PSA has been performed as an integral part of the EPR design. Results of the PSA analysis for the UK EPR are given in PCSR Chapter 15. The numerical targets defined in the Safety Assessment Principles are used to evaluate and verify the UK EPR design. In addition to the SAPs numerical targets, specific safety objectives are considered in the design in accordance with the EPR Technical Guidelines. See Chapter 15 for more details.
FA.11 PSA should reflect the current design and operation of the facility or site.	The EPR is considered to comply with the SAP. The current French practice on operating plants aims at maximising the benefits from the series effect: PSA data update is performed on the basis of all operating feedback, the design and operation specificities are close to zero and, within the standard PSA model, the site dependant data are generally taken into account on an envelope basis. On the other hand, the use of PSA in day to day operation is quite low (e.g. no risk monitor). The major uses of PSA are concentrated on standard purposes: technical specifications, periodic safety reviews, operating feedback and incidents analyses etc.

SAP	Comment
	Additionally, EDF will propose in due course, implementation of the same approach on the EPR worldwide standard. However, at the GDA stage, the available PSA tools enable both a site and a standard approach to be contemplated.
FA.12 PSA should cover all significant sources of radioactivity and all relevant initiating faults identified at the facility or site.	The EPR is considered to comply with the SAP. The PSA presented in Chapter 15 of the PCSR considers internal events, and internal and external hazards affecting all significant sources of radioactive material in the plant (including the nuclear steam supply system, the fuel building, the nuclear auxiliary building and effluent treatment building. Initiating events cover all reactor states, including both at-power and shutdown conditions.
FA.13 The PSA model should provide an adequate representation of the site and its facilities.	The EPR is considered to comply with the SAP. As explained in PCSR Chapter 15, the EPR PSA model accounts for random component failures, failure of components due to the initiating event, common cause failures, and equipment unavailability due to maintenance. Best-estimate methods and data are used for supporting transient analyses, accident progression analyses, source term analyses, and radiological analyses, as requested by the SAP. Reliability data are derived mainly from operational feedback from France and Germany, supplemented by the EG&G generic reliability database (see PCSR Chapter 15). Initiating event frequencies are evaluated from operating feedback from French plants and international feedback. The PSA contains a comprehensive treatment of human errors, which are allowed for in equipment unavailability analysis and in treating the probability of failure to execute requested actions (see PCSR Chapter 15). The PSA analysis in the PCSR includes an uncertainty analysis (PCSR Chapter 15); risk results are presented at a range of confidence levels, rather than as a central estimate of risk.
FA.14 PSA should be used to	The EPR is considered to comply with the SAP.

SAP	Comment
inform the design process and help ensure the safe operation of the site and its facilities.	As far as design is concerned, and as stated in PCSR Sub-chapter 17.4, the EPR objectives of reinforcing defence in depth involved extensive use of probabilistic methods. PSA was used to quantitatively demonstrate implementation of the defence-in-depth concept as well as to show that a balance has been achieved between levels of protection and that the levels were independent of one another. PSA studies were performed at the design stage of the EPR to support the choice of design options, including the required level of redundancy and diversity of the safety systems. PSA was also used to select or reject changes to the main EPR design options during the Basic Design Optimisation Phase of EPR. With regard to the use of PSA during the plant life, see response to SAP FA 11 above.
FA.15 Fault sequences beyond the design basis that have the potential to lead to a severe accident should be analysed.	The EPR is considered to comply with the SAP. Paragraph 545: The analysis of fault sequences leading to and encompassing the progression of severe accidents, which in the EPR terminology are called scenarios, includes the fission product migration in the plant as well as their release to the environment. This fission product release is then used to predict the radiological consequences of a severe accident. In fulfilment of the SAP requirement, the PCSR considers the radiological consequences of core melt sequences (PCSR Chapter 16) Probabilistic analysis is used to identify RRC-A events (see PCSR Chapter 16). RRC-A analysis is used to demonstrate the efficiency of RCC-A features to mitigate the consequences of multiple failure events such as common cause failure of F1 classified safety systems. The RRC-A results are presented in PCSR Chapter 16. In carrying out the RRC-A studies particular attention is given to the uncertainties that can cause a “cliff edge” increases in risk (see PCSR Chapter 16). Finally, the analysis of severe accidents discriminates between representative and bounding scenarios. Representative scenarios are used for the design of severe accident mitigation systems and the analysis of their efficiency, while bounding scenarios involve onerous assumptions and are used to show that no cliff edge effects exist (e.g. due to possible early containment failure). Paragraph 546: The analysis includes the failure of physical barriers such as fuel and fuel cladding as well as the primary pressure

SAP	Comment
	boundary. The consequent effects of such failures, i.e. mass and energy release, fission product release into the containment as well as discharge of core melt from the reactor pressure vessel are factored in the analyses of severe accidents. While it is a deterministic design objective of the EPR to keep the containment function intact throughout the accident, the PSA Level 2 additionally quantifies modes of containment failure and associated risks, which arise from highly remote severe accident phenomena such as the consequences of high pressure core melt. Notably, high pressure core melt is deterministically excluded, as the EPR provides for redundant dedicated bleed valves, which transfer high pressure into low pressure core melt scenarios Paragraph 547: The severe accident analyses employ best-estimate assumptions, codes and methods in order to exhibit the margins involved in the safety design of the plant. In addition, bounding scenarios with onerous assumptions are used to examine the robustness of the EPR safety concept by showing that no cliff edge effects exist. Paragraph 548: It has been of paramount importance from the early design stages of the EPR to use codes and models which have undergone validation against representative experiments. These validated codes then allow the extrapolation of experimental findings to reactor scale. Consequently, the severe accident analyses are heavily backed by representative experiments. In addition, many tests have been performed in direct support of the development of the EPR specific severe accident mitigation measures and to prove their ability to function.
FA.16 The severe accident analysis should be used in the consideration of further risk-reducing measures.	The EPR is considered to comply with the SAP. Paragraph 549: Preparatory severe accident analyses have included the identification of phenomena which could potentially lead to early containment failure and have enabled their prevention by deliberate, reasonably practicable measures. The early design stages of the EPR design proved that letting the severe accident develop in an uncontrolled manner and

SAP	Comment
	design the last barrier against consequent loads was impracticable. In response, the EPR is equipped with dedicated, independent severe accident control systems, i.e. dedicated primary system depressurisation to prevent the effects of high pressure core melt sequences, a combustible gas control system to avoid hydrogen combustion modes threatening the containment integrity, a core catcher to prevent basemat attack by core melt and a containment heat removal system to control pressure and temperature. The design of these systems and the analysis of their efficiency rely upon so-called ‘representative’ scenarios. Beyond this, so-called ‘bounding’ scenarios involving onerous assumptions are used to assess the robustness of these systems. These analyses are also useful for the development of operating strategies for severe accidents (OSSA), which involve an optimised operational scheme for the severe accident control systems, notably the containment heat removal system, and mitigation actions in case these systems fail. The severe accident analyses also assist in the preparation of emergency plans in so far as they predict the radioactive source term to the environment, which is then used to determine the radiological consequences. Additionally, the execution of these plans may be supported by outside monitoring of doses. The PSA Level 2, which may be considered as a living PSA and updated regularly throughout the lifetime of the plant, assists in analysing the overall plant response to severe accidents, in identifying potential weak points and in defining appropriate measures. Paragraph 550: All severe accident analyses use best estimate assumptions, codes and methods to evaluate the actual behaviour of the plant in severe accidents to demonstrate the margins involved in the plant design.
FA.17 Theoretical models should adequately represent the facility and site	The EPR is considered to comply with the SAPs. The theoretical models of the EPR unit used for safety analysis use validated codes and models developed using standard quality assurance processes. The main analytical codes used to perform the design basis transient studies described in PCSR Chapter 14 are

SAP	Comment
and **FA.18 Caculational methods used for the analyses should adequately represent the physical and chemical processes taking place**	CATHARE, S-RELAP, SMART, FLICA, PANBOX, COBRA, MANTA and NLOOP. The main codes for performing the RRC-A (multiple failure) and RRC-B (severe accident) studies presented in PCSR Chapter 16 are MAAP4, COCOSYS, COSACO, WALTER, CORFLOW, CHEMASE, GASFLOW and COM3D. These codes have been systematically developed and validated against integral and separate effects tests at a range of size scales in French, German and international test facilities in R&D programmes developed over several decades. Where appropriate, comparisons have been made with operational transients in PWR plants. Details of the development and validation basis of the analysis codes are given in PCSR Chapter 14 and PCSR Chapter 16. Radiological analysis of within and beyond design basis accidents are described in PCSR Chapters 14 and 16. Effects of direct radiation, inhalation and ingestion of radioactivity and the physical and chemical form of the released material are modelled in calculating the dose to the critical individual, as required by the SAP.
FA.19 The data used in the analysis of safety-related aspects of plant performance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means. **and** **FA.20 Computer models and datasets used in support of the analysis should be developed, maintained and applied in accordance with appropriate quality assurance procedures.**	The EPR is considered to comply with the SAPs. Documents and design studies for UK EPR are produced and controlled within the Quality Management Systems (QMS) of both companies participating in the UK EPR GDA Project and of their subcontractors. These QMS comply with main international codes and standards (in particular ISO 9001:2000). They describe procedures (such as development and management of scientific engineering computer programs or input data validation) to be applied within the project, in particular when performing design engineering work (e.g. fault analysis studies). A description of codes used for Design Basis Analysis studies is presented in Appendix 14A of Chapter 14 of the PCSR. Along with DBA studies, PCSR Chapter 14 describes important phenomena and qualification of the codes, which allows confirmation of the adequacy of the physical models used to describe the transients. Probabilistic and deterministic analyses are presented in PCSR Chapters 15 and 14, respectively. For these analyses,

SAP	Comment
and **FA.21 Documentation should be provided to facilitate review of the adequacy of the analytical models and data.** **and** **FA.22 Studies should be carried out to determine the sensitivity of the fault analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation.**	pessimistic assumptions are used. When establishing methods for fault analyses, if conservative assumptions or the choice of pessimistic data is not obvious, sensitivity studies are performed.
FA.23 Data should be collected throughout the operating life of the facility to check or update the fault analysis.	See response for SAP FA.11 above.
FA.24 The fault analysis should be updated where necessary, and reviewed periodically.	The EPR will comply with the SAP. The update of the safety analyses is generally performed within the framework of the periodic safety reassessment of the plant (every 10 years in France). When changes occur on the plant, an assessment of the impact on the safety analysis is performed and if needed, some safety analyses are reperformed before implementation of the modifications.

SAP	Comment
	When experience feedback (incidents, unexpected deterioration detected ...) challenges the safety demonstration, a review of safety analysis is performed to check if it remains valid, and if necessary, new analysis is performed.
NT.1 A safety case should be assessed against numerical targets and legal limits for normal operation, design basis faults, and radiological accident risks to people on and off the site.	The EPR is considered to comply with the SAP. As shown hereunder in the discussion of the individual numerical targets and legal limits, the EPR design meets these limits or is anticipated to meet the limits. For some numerical targets, further analysis may be required to fully demonstrate meeting the limit because specific site information is required and is not available in the GDA. <u>Normal operation - any person on the site - Target 1 and Normal operation - any group on the site - Target 2</u> As stated in PCSR Sub-chapter 3.1, Safety Design Objective SDO-2 for the UK EPR is that the effective dose received by any operator annually should be below 10mSv. Compliance with this objective, which will ensure compliance with Targets 1 and 2, is addressed in PCSR Sub-chapter 12.4, section 4. It is concluded that given the dose levels currently experienced in operating French NPPs and the measures taken in EPR to achieve further dose reductions, there is confidence that the 10mSv/yr dose limit adopted for the UK EPR will be achievable. <u>Normal operation – any person off the site - Target 3</u> As stated in PCSR 3.1, Safety Design Objective SDO-3 for the UK EPR is that the maximum dose to an individual off-site due to normal operation of an EPR shall not exceed 0.3 mSv and shall not exceed 0.5 mSv for the total site containing the EPR. Compliance with this objective, which ensures Target 3 compliance, is addressed in PCER Chapter 11. The methodology used to carry out the Initial Radiological Assessment (IRA) is provided by the Environment Agency. Taking into account simple cautious assumptions (with conservatism), the Stage 2 IRA methodology gives an annual doses for the critical group of 63.0 µSv.y-1. This value ensures compliance SD0-3 objective. However, the annual dose calculated at Stage 2 is above the 20 µSv.y-1 BSO threshold. For the complementary PCER submission being prepared for November 2008, a “Stage 3” assessment is being carried out using a set of site parameters appropriate for the UK. There is confidence that this assessment will give an annual dose to the critical group close to the BSO level. <u>Design basis fault sequences – any person - Target 4</u> As mentioned in PCSR Sub-chapter 3.1, the safety approach applied to the EPR requires consideration of a limited number

SAP	Comment
	of representative internal faults and enveloping conditions liable to be encountered during operation and various associated reactor states. These initiating events are grouped together in four categories (Plant Condition Categories of events, PCCs) based on their estimated frequency of occurrence and their impact on the environment. For the EPR project, requirements on the radiological consequences of these accidents have been set at the design stage (see PCSR 3.1). Compliance with the design requirement is demonstrated in PCSR Sub-chapter 14.6. A comparison between Target 4 and EPR requirements on PCCs radiological consequences makes it possible to conclude that compliance to EPR requirements on PCCs radiological consequences induces compliance to Target 4, as far as off-site risks are concerned. The only potential exception concerns PCC-3 events whose frequency exceeds 1 x 10^{-3} pa and whose radiological consequences are above 1 mSV. PCSR Sub-chapter 14.6 shows that the only PCC-3 event whose radiological consequences are above 1 mSV is the steam generator tube rupture of 1 tube. The related initiating event frequency (see PCSR Sub-chapter 15.1) is below $1x10^{-3}$ pa. As a consequence, Target 4 compliance is achieved, as far as off-site risks are concerned. Concerning Target 4 on-site risks, no formal assessment against this target is presented at this stage of GDA. However given the bounding hypotheses used for assessing the radiation dose for the assessment of off-site risks, and the fact that protective measures (emergency procedures involving evacuation and sheltering) are easier to implement within the site, it is considered that the risk to workers would be smaller than the risk to the hypothetical person assumed in the off-site dose calculation (the hypothetical person is supposed to stay downwind at the site fence during 7 days following the initiating event), and the Target 4 compliance would therefore be met. <u>Individual risk of death from on-site accidents – any person on the site - Target 5 and Frequency dose targets for any single accident – any person on the site - Target 6</u> No formal assessment against Targets 5 and 6 are presented at this stage of GDA. However given the bounding hypothesis used for assessing the radiation dose for the assessment of off-site risks (see compliance to Targets 7 and 8 below), and the fact that protective measures (emergency procedures involving evacuation and sheltering) are easier to implement within the site, it is considered that the risk to workers would be smaller than the risk to hypothetical person assumed in the off-site dose calculation (the hypothetical person is supposed to stay downwind at the site fence during 7 days following the initiating event), and the Targets 5 and 6 compliance would therefore be met.

SAP	Comment
	<u>Individual risk to people off the site from accidents - Target 7</u> As mentioned in PCSR Sub-chapter 3.1, Safety Design Objective SDO-5 for the UK EPR states that the risk of fatality of any person off-site due to exposure to radiation from accidents will be below 10^{-6}/yr. Compliance with this objective, which ensures Target 7 compliance, is addressed in PCSR Sub-chapter 17.4. Using the results of the PSA analysis (see PCSR Chapter 15), the risk of death to the most exposed individual is estimated to be 4.2×10^{-7}/yr, which is considered highly pessimistic. This meets Safety Design Objective SDO-5 and therefore Target 7. <u>Frequency dose targets for accidents on an individual facility – any person off the site - Target 8</u> As mentioned in PCSR Sub-chapter 3.1, Safety Design Objective SDO-6 for the UK EPR states that the EPR design will ensure that the total frequency of accidents in each of the different dose categories is below the BSL. The design objective will be to achieve an accident frequency in each dose category that is below the BSO. Compliance with Target 8 is addressed in PCSR Chapter 15 and Sub-chapter 17.4. Using the results of the PSA analysis, it is demonstrated that the UK EPR design achieves a Broadly Acceptable level of risk in all Dose Bands, meeting the Safety Design Objective and therefore Target 8. <u>Total risk of 100 or more fatalities - Target 9</u> As mentioned in PCSR Sub-chapter 3.1, Safety Design Objective SDO-7 for the UK EPR states that the total risk of 100 or more fatalities, either immediate or eventual, from on-site accidents that result from exposure to ionising radiation, will be below 10^{-7}/yr. Compliance with this objective, which ensures Target 9 compliance, is addressed in PCSR Chapter 15 and Sub-chapter 17.4. Using the results of the PSA analysis, it is demonstrated that the frequency of the releases which have the potential to lead to more than 100 eventual fatalities, for a generic UK site, is below the BSO. This meets Safety Design Objective SDO-7 and therefore Target 9.
NT.2 There should be sufficient control of radiological hazards at all times.	The EPR is considered to comply with the SAP. The design basis analysis is described in PCSR Chapter 14. The initiating events studied in this chapter are classified into several classes of events:

SAP	Comment
	• Increase of heat removal by the secondary system, • Decrease of heat removal by the secondary system, • Decrease in reactor coolant system flow rate, • Reactivity and power distribution anomalies, • Increase of water inventory in the primary system, • Reduction of water inventory in the primary system, • Radioactive releases from a subsystem. In the dedicated chapter, the analyses show that the relevant criteria for each event are met. Control of radiological hazards is embedded in the defence-in-depth (see PCSR Sub-chapter 3.1) approach used by the EPR design, which consists of protection devices and control systems to prevent accidents, and engineered safety features and protective systems to mitigate accidents. Availability of safety features is required by Plant Technical Specifications. When the required safety features happen to be unavailable, Plant Technical Specifications define alternative means by which the plant can be operated in order to maintain an adequate level of protection (see PCSR Chapter 18). When needed, a safe shutdown state can be required taking into account PSA insights. These PSA insights are appropriate to the plant sate, whatever the period in which the risk occurs is. Besides, the PSA covers a wide range of plant states (e.g. plant outages), making it possible to detect significant contributions to radiological risk in all times during plant operation. As mentioned in PCSR Sub-chapter 15.7, analysis of dominant core damage sequences shows there are no 'outliers' in the EPR overall core damage frequency.
AM.1 A nuclear facility should be so designed and operated to ensure that it meets the needs of	The EPR is considered to comply with the SAP. Accident management strategies are included in the safety assessment of the EPR Plant Initiating Events (PIE): design

SAP	Comment
accident management and emergency preparedness.	basis events as well as risk reduction category events (RRC-A and RCC-B events) covering hypothetic fault sequences and severe accidents. Design basis events are assessed in PCSR Chapter 14. RRC events are assessed in PCSR Chapter 16. A definition of the instrumentation and equipment needed to reach a safe plant state is included in these accident management strategies. The classification rules are given in PCSR Sub-chapter 3.2; the related I&C is described in Chapter 7. The Man Machine Interface and the Emergency Operating Procedures are described in PCSR Sub-chapter 18.2, and the Main Control Room habitability conditions are addressed in Sub-chapter 9.4. Emergency preparedness and response in case of nuclear or radiation incidents is the responsibility of the dutyholder (see the response to SAP FP.7). Provisions exist within the EPR design to allow further emergency planning: notably technical support centre and related I&C features. The training of plant personnel in accident management procedures is also the responsibility of the dutyholder. This could be achieved with a full scale training simulator, which is beyond the scope of the GDA.
RW.1 A strategy should be produced and implemented for the management of radioactive waste on a site.	The EPR is considered to comply with the SAP. The EPR design includes the storage of radioactive liquid effluent in tanks and the monitored discharge into the water, the monitored emission of gaseous radioactive discharges, and the treatment and packaging of solid waste before transportation to the final depository, after a period of interim storage (as needed). The forms of radioactive waste generated permit stabilisation and disposal using available technologies. Waste management is described in PCSR Chapter 11. Details of monitoring can be found in PCER Chapter 7. The development of procedures for waste management on-site is the responsibility of the dutyholder applicant; these will be described in the operating organisation’s quality and environmental management system.
RW.2 The generation of radioactive waste should be prevented or, where this is not reasonably practicable, minimised in terms of quantity and activity.	The EPR is considered to comply with the SAP. PCSR Chapter 11 describes the radioactive waste arising during operation of the EPR unit and the techniques used to minimise radioactive waste generation. Minimisation in terms of quantity and activity is achieved by more efficient use of fuel, and efficient separation and treatment of the different types of radioactive waste through the waste treatment systems.

SAP	Comment
	Further minimisation will be the responsibility of the dutyholder applicant;, through the efficient management of the waste treatment systems.
RW.3 The accumulation of radioactive waste on site should be minimised.	The EPR is considered to comply with the SAP. Liquid waste is stored in tanks and is released into the water in an appropriate and monitored way. The sizing of tanks is adapted to the amount of liquid to be stored. The radioactive waste liquid release is addressed in PCSR Chapter 11. EPR process and operational solid radioactive waste management is addressed in PCSR Chapter 11. Radioactive solid waste is treated in the waste treatment building and put into packages, appropriate to the radioactive and chemical characteristics of the waste, ready for transport to a final disposal site (VLLW and LLW), or alternatively stored on site before final disposal (ILW). More information will be made available in an updated submission of PCSR Chapter 11 (Planned for November 2008), on interim storage facilities for safely storing ILW solid radioactive waste on-site for 100 years after the commissioning of the reactor. Minimisation of the arisings of solid radioactive waste (RW2) will help reduce the amount of waste stored at on-site any one time. The management of the waste to be stored on site will be the responsibility of the dutyholder applicant.
RW.4 Radioactive waste should be characterised and segregated to facilitate subsequent safe and effective management.	The EPR is considered to comply with the SAP. Radioactive waste is characterised as VLLW, LLW, ILW according to UK classification in order to facilitate subsequent management. Characterisation of radioactive waste is described in Sub-chapter 11.2 of the PCSR, to be further detailed in the November PCSR submission. Maintaining effective segregation between solid waste streams during EPR unit operation will be the responsibility of the dutyholder applicant.

SAP	Comment
RW.5 Radioactive waste should be stored in accordance with good engineering practice and in a passively safe condition.	The EPR is considered to comply with the SAP. Chapter 11 describes how solid radioactive waste is put in safe packages, adapted to the radioactive and chemical characteristics of the waste, and the duration of storage. The containers are stored in the waste treatment building storage area, which is designed to comply with nuclear safety requirements for such buildings in structural design and layout and ventilation aspects. The interim storage facilities for the storage of ILW over a period of 100 years, to be described in the November 2008 PCSR submission, will comply with the requirement for passively safe storage.
RW.6 Radioactive waste should be processed into a passively safe state as soon as is reasonably practicable.	The EPR is considered to comply with the SAP. The design of waste treatment equipment for radioactive waste includes the need to process wastes shortly after their arising. Management during operation of the EPR unit will be the responsibility of the dutyholder applicant.
RW.7 Information that might be required now and in the future for the safe management of radioactive waste should be recorded and preserved.	The EPR design process is considered to comply with the SAP. Under EDF/AREVA quality and environmental management systems, the design files are recorded and preserved. The quality management systems for the design phase are described in PCSR Chapter 21. Maintaining waste management records for EPR operation will be the responsibility of the dutyholder applicant.
DC.1 Facilities should be designed and operated so that	The EPR is considered to comply with the SAP.

SAP	Comment
they can be safely decommissioned.	PCSR Sub-chapter 20.2, sections 2, 3 and 4 illustrate the fact that the design focuses on arrangements which facilitate both decommissioning and maintenance. Moreover, a decommissioning plan will be produced, including an indication of the programme and duration of decommissioning, together with design provisions to facilitate decommissioning.
DC.2 A decommissioning strategy should be prepared and maintained for each site and should be integrated with other relevant strategies.	The EPR is considered to comply with the SAP. The EPR design facilitates the decommissioning of the plant at the end of its operational life. The implementation of the EPR takes into account the following: • choice of materials to reduce activation products and contamination, to minimise the use of hazardous and non-inert materials and to increase the use of recyclable materials; • design provisions to facilitate decommissioning work, removal of main components and structures, and personnel access during the dismantling phase; • arrangements relating to the circuits to allow measures to be taken to limit the contamination of systems, to make provisions to limit the spread of contamination, and to facilitate the decontamination of rooms and equipment; • existence of comprehensive documentation, storage and retrieval systems.
DC.3 Decommissioning should be carried out as soon as is reasonably practicable taking relevant factors into account.	The EPR is considered to comply with the SAP. Viable strategies are considered for decommissioning of a nuclear power plant: • immediate dismantling of the whole plant; • safe enclosure of the reactor and adjacent buildings with radioactive inventory followed by deferred dismantling.

SAP	Comment
	The final decommissioning strategy has to be decided by the owner, considering relevant factors which could be developed in the decommissioning plan.
DC.4 A decommissioning plan and programme should be prepared and maintained for each nuclear facility throughout its life-cycle to demonstrate that it can be safely decommissioned.	The EPR will comply with the SAP. A decommissioning plan will be produced, including an indication of the programme and duration of decommissioning, together with design provisions to facilitate decommissioning. The dismantling of a nuclear facility comprises several technical operations and administrative processes, the final result of which is the site regulatory delicensing. In most cases, the following sequence applies: • decision to permanently shut down the facility by the owner; • removal of fissile materials and radioactive liquids, while the nuclear-side plants are still operating, although in a simplified way; • depending on the technical requirements, demolition or refurbishment of the non-nuclear plant and possibly a reduction of the facility perimeter; • phased dismantling of the activated and contaminated equipment; • phased deactivation and decontamination of components; • after establishing what remains of the facility, partial or total delicensing; • a period of safestore, if required. The waste produced by these operations is removed from the site, possibly after interim storage on site. Finally, the remaining structures and the site itself are redeveloped according to the owner's requirements and the obligations to which the owner is bound under the terms of decommissioning.

SAP	Comment
	PCSR Sub-chapter 20.2, section 5 addresses the measures to be taken to retrieve and store the documentation necessary for decommissioning.
DC.5 The facility should be made passively safe before entering a care and maintenance phase.	The EPR will comply with the SAP. Fissile materials and radioactive liquids are removed from the facility and safely disposed of (as described in the response to SAP DC.4, above) before entering a care and maintenance phase.
DC.6 Throughout the whole life-cycle of a facility the documents and records that might be required for decommissioning purposes should be identified, prepared, updated and retained.	The EPR will comply with the SAP. As mentioned in PCSR Sub-chapter 20.2, section 5, particular attention will be given to the following documentation: • drawings and diagrams relevant to operations; • additional documentation permitting the use or modification, for alternative operations, of equipment and structures (e.g. design of handling machines, special tools, floors, load-bearing structures, manufacturing and equipment specifications, geo-technical test results); • photos and videos useful to illustrate the component assembly and erection, the carrying out of the earthworks and the parts of the structures which are subsequently hidden, the means for handling components, the routing plans, focusing on those parts which are to become highly activated and contaminated; • quantitative inventories; • a record of all of the operating incidents, together with their assessment and a record of all modifications made to the original facility; • all of the documents providing traceability in the areas of radiological cleanliness and the radiological inventory (mapping, smear tests, various samples, etc). The safety analysis is carried out at the first stage of the planning and has to be reviewed in case of evolutions during decommissioning.

SAP	Comment
DC.7 Organisational arrangements should be established and maintained to ensure safe and effective decommissioning of facilities.	DC.7 is not within the EPR design scope.
DC.8 The safety management system should be periodically reviewed and modified as necessary prior to and during decommissioning.	The EPR will comply with the SAP. As mentioned in PCSR Sub-chapter 20.1, section 3, the dismantling process chosen by the operator is defined (prior to implementation) through documents dealing with: • the scheduling and nature of the dismantling works, and the facility final state; • the origin, characterisation, quantity, treatment, packaging, transportation, disposal and recycling of nuclear waste and other kinds of waste as well as the management of these; • the risks to the public and workers, and the measures taken to detect, prevent and limit such risks; • the maintenance requirements for the facility and the auxiliary buildings during the dismantling phases; • the on site emergency plan; • the predicted impact of dismantling and the facility final state on the environment.