HSE
Health and Safety Executive

HEALTH & SAFETY EXECUTIVE
NUCLEAR DIRECTORATE
ASSESSMENT REPORT

New Build

Step 2 Fault Analysis Assessment of EDF_AREVA Submission for the EPR

HM Nuclear Installations Inspectorate
Redgrave Court
Merton Road
Bootle
Merseyside L20 7HS

1. INTRODUCTION

The Generic Design Assessment (GDA) “Guidance to Requesting Parties” document, Ref 1, outlines the two phase approach to licence new nuclear power stations in the UK. The overall assessment strategy for Step 2 is outlined in the Unit 6D Operating Plan, Ref 2, and the specific fault study assessment strategy for Step 2 is given in ND DIV 6 Assessment Report AR07015, Ref 3.

This approach, described in Ref 3, is consistent with ND’s assessment procedures guidance as outlined in Ref 4. Therefore this structure will be used in the assessment of the EDF/AREVA submission of the European Pressurized Water Reactor (EPR).

The main conclusion of this report is that the EDF/AREVA safety documentation is adequate for Step 2 of the GDA process.

.

2. ND Assessment

A proposal to licence new nuclear power stations in the UK is subjected to a two phase process as detailed in the Generic Design Assessment (GDA) – Guidance to Requesting Parties document, Ref 1. Phase 1 consists of 4 Steps and leads to the issuing of a Design Acceptance Confirmation. A Design Acceptance Confirmation means that the station design will be suitable for construction in the UK subject to a site specific licence being granted at the completion of Phase two.

This assessment report covers the fault analysis assessment carried out for Phase 1, Step 2. Phase 1, Step 2 of the GDA is called the “Fundamental Safety Overview” and covers an overview of the fundamental acceptability of the proposed design concept within the UK regulatory regime, Ref 1. It is written taking into account the requirements of our BMS manual Refs 4 & 5.

The overall assessment strategy for Step 2 is defined in the Unit 6D Operating Plan, Ref 2, and the specific Fault Studies & PSA strategy for Step 2 is given in ND DIV 6 Assessment Report AR07015, Ref 3.

As stated in the BMS guidance covering the NII assessment process, G/AST/001, Ref 4, “…..for a safety case to be effective it must provide three elements: *Claims, Evidence and Argument.*” The GDA addresses these elements in a stepwise approach. Phase 1, Step 2 addresses the claims. Phase 1, Step 3 addresses the arguments and Phase 1, Step 4 addresses the evidence. The completion of these Steps in Phase 1 constitutes the completion of the NII assessment covering the generic design and if completed satisfactorily would lead to the issuing of the Design Acceptance Confirmation referred to above.

The objective of this report is therefore to assess the adequacy of EDF/AREVA’s claims that the relevant Fault Study Safety Assessment Principles (SAPs) are met.

Assessment during Steps 3 & 4 will address the adequacy of the arguments and evidence supporting these claims respectively.

2.1 Requesting Parties Case

The EDF/AREVA Step 2 submission used during this assessment was located at S:\New Reactor Build\RP Submission\ EDF_AREVA Submission – Sep 2007. The submission was entitled, “UK-EPR Fundamental Safety Overview” (FSO) (Ref 6).

Within the FSO submission EDF/AREVA did not provide a document that directly addressed compliance with each of the SAPs (e.g. a route map indicating the section(s) of the FSO that addressed each SAP). However, within the FSO, it was stated that, *“For this Fundamental Safety Overview submitted for Step 2 of pre-licensing, a systematic review of EPR safety features against UK requirements is not available. However, a limited review has been undertaken which indicates that the EPR design already meets the majority of UK requirements”.* A Technical Query (TQ) – EPR000003 was raised requesting an explanation of how the EPR design complied with each of the SAPs, including a request that EDF/AREVA provide an early response against the key Fault Analysis SAPs.

EDF/AREVA’s response to TQ EPR000003 (Ref 7), shows that EDF/AREVA claim compliance with the key Fault Analysis SAPs.

The EDF/AREVA EPR Safety Philosophy

The EPR design philosophy is based on the following objectives related to the current generation of PWRs:

- increase redundancy and separation,
- reduce core damage frequency (CDF),
- reduce large release frequency (LRF),
- mitigate severe accidents,
- protect critical systems from external events,
- improve man-machine interface (MMI),
- extend response times for operator actions.

A cornerstone of the EPR design philosophy, the principle of “defence-in-depth,” has been improved on all levels, resulting in:

- reductions in radiological consequences and accident initiator frequencies,
- favourable transient plant behaviour,
- simplification of the safety systems and functional separation,
- elimination of common mode failures by physical separation and diverse back-up

Core Stability

The temperature, power and core void coefficients of reactivity are all negative for the EPR as expected. This means that the reactor behaviour is stable for minor deviations in temperature, power or coolant density requiring fewer interventions by the operator. For larger deviations caused by fault situations leading to reactor temperature and power increases and possibly coolant voiding, the resulting negative feedback process helps to control the severity of the fault. For example, an increase in power also tends to increase the fuel temperature and decrease the coolant density. This leads to reduced reactivity, which assists by reducing the rate of increase of the power, and fuel temperature returning these parameters back to their original values.

The EPR has no grey rods, which are used in other LWR designs for normal operation reactivity control. The core is cooled and moderated by light water at a pressure of 15.5 MPa. Normal operation reactivity control is provided by varying the concentration of soluble boron in the water reactor coolant or by control rods movements. The boron concentration in the coolant is varied to control slow reactivity changes necessary for compensating Xenon poisoning or burn-up effects during power operation and for compensating large reactivity changes associated with large temperature variations during cool down or heat-up phases.

Design Basis

Redundant 100% capacity safety systems (one per Safeguard Building) arranged in four trains are strictly separated into four divisions. This divisional separation is provided for electrical and mechanical safety systems. The four divisions of safety systems are consistent with an 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.

In the event of a loss of off-site power, each safeguard division is powered by a separate Emergency Diesel Generator (EDG). In addition to the four safety-related diesels that power various safeguards, two independent diesel generators are available to power essential equipment during a postulated Station Blackout (SBO) event - i.e. loss of off-site AC power with coincident failure of all four EDGs.

Water storage for safety injection is provided by the In-containment Refuelling Water Storage Tank (IRWST). Also inside containment, below the Reactor Pressure Vessel (RPV), is a dedicated spreading area for molten core material following a postulated worst-case severe accident.

The fuel pool is located outside the Reactor Building in a dedicated building to simplify access for fuel handling during plant operation and handling of fuel casks. As stated previously, the Fuel Building is protected against aircraft hazard and external explosions.

Initiating Faults

The events studied are selected on the basis of potential risk vis-à-vis meeting the principal safety functions:

- control over reactivity;

- cooling of the fuel elements; and
- containment of radioactivity.

They are classed in four categories of design basis conditions (PCC - Plant Condition Category) and in two categories of design extension categories (RRC - Risk Reduction Category).

The classification of the PCC is undertaken taking into account their estimated frequency of occurrence:

- PCC-1 : Normal operation transients Condition I events
- PCC-2 : Reference transients (10-2 / yr < f), Condition II events
- PCC-3 : Reference incidents (10-4 / yr < f < 10-2 / yr), Condition III events
- PCC-4 : Reference accidents (10-6 / yr < f < 10-4 / yr). Condition IV events

For both Condition I events (PCC-1 normal operation) and Condition II events (PCC-2 transients – events that might be expected to occur at least once during life of the unit), there is no loss of integrity of the fuel. For Condition II events and events of lower probability of occurrence that result in a plant shutdown, shutdown capabilities will bring the plant to a sub critical condition and maintain it in a safe shutdown state through the use of safety-related equipment.

For Condition I events, the controls, surveillance, and limitation systems automatically maintain the plant within Limiting Conditions for Operation (LCO) postulated for accident analyses and thus well below the integrity limits of the fuel cladding. These systems rely on efficient, accurate and reliable instrumentation concepts inherent in the design of the EPR.

For Condition II events, automatic countermeasures (limitations) are actuated to terminate abnormal transients at an early stage and return the plant to Condition I without a reactor trip when possible. The protection trip function relies on the accurate monitoring of essential core parameters and is actuated only in the absence of operator response or when automatic control actions do not succeed in terminating the transient.

Core-specific design criteria are defined below.

- Condition III events shall not cause more than a small fraction of the fuel elements in the reactor to be damaged

- For Condition III and IV events, the fuel melting at the hot spot shall not exceed 10% in volume. This criterion translates to a 10 % area limit at the axial elevation of the power peak.

- For Condition II events, the maximum linear heat generation rate shall be limited to meet the fuel clad, fuel rod, and fuel centreline temperature specified acceptable fuel design limits. These limits are typically a function of the fuel rod burn up with a safety analysis accounting for irradiation-induced changes.

Thermal Margin acceptance criteria
The thermal margin design basis provides a 95% probability (at a 95% confidence level) that Departure from Nucleate Boiling (DNB) will not occur on the limiting fuel rods during normal operation and anticipated transients (Condition I and II events).

By preventing DNB, adequate heat transfer between the fuel cladding and the reactor coolant is ensured. The prevention of DNB relies on appropriately defined limitation and protection functions based upon on-line DNBR calculations. These functions use fixed incore flux measurements to reconstruct the local thermal hydraulic conditions and calculate the minimum DNBR (MDNBR).

Uncertainties related to the fuel geometry and thermal-hydraulic model, are considered for determining the setpoints. The setpoint criterion is a 95% probability at a 95% confidence level that the DNB will not occur when the on-line calculated DNBR threshold is reached or when other protective functions have been actuated.

The methodology used for determining setpoints with respect to DNB depends on the type of reactor protection channels used to protect the core.

Three types of transients are considered as described below:

- **Transients for which the DNBR protection is sufficient (Type 1).**

These transients are relatively slow and DNB is avoided by setting the DNBR threshold of the DNBR protection channel at a limit that guarantees avoidance of DNB.

- **Transients that occur at power, but for which the DNBR protection channel is not sufficient (Type 2).**

These transients exceed the response time of the protection channel. For these transients, the protection is based on specific event detection (e.g.,“low pump speed” for detection of loss of RCS flow). Once the setpoints for these specific protections have been defined, the MDNBR during the corresponding transient(s) depends only on the initial condition(s) at which the event occurs. LCOs that define the worst initial conditions for these events are defined by appropriate accident analyses, thus preventing DNB limits from being exceeded during the transient. A surveillance/limitation function ensures that the actual DNBR always exceeds the DNBR threshold fixed for initial conditions of accidents (also called DNBRLCO -- mainly with regard to the loss of flow event). This setpoint takes into account all the uncertainties linked to the fuel geometry and those related to the surveillance/limitation functions.

- **Transients occurring at very low power or at subcritical conditions or leading to re-criticality at low temperature conditions (Type 3**).

For these events, the methods previously defined do not apply and specific protection functions and safety systems must intervene. The focus of the corresponding accident analyses for these transients is to characterize the protection and safety systems to ensure that the minimum DNBR limits that guarantee the integrity of the fuel are not violated during the accident.

Fuel Temperature Design Basis

For Condition I and II events, there is at least a 95% probability (at a 95% confidence level) that the fuel melting temperature is not exceeded in any part of the core. The melting temperature of UO2 corresponds to ~2810°C for unirradiated UO2, decreasing by ~ 7.6°C per 10000 MWd/MTU.

Precluding fuel melting preserves the fuel geometry, thus eliminating the possible adverse effects of molten fuel interacting with the fuel cladding.

Severe Accidents

Innovative features result in the low probability of energetic scenarios that could lead to early containment failure. Design provisions for the reduction of the residual risk, core melt mitigation, and the prevention of large releases are:

- prevention of high pressure core melt by a dedicated, high reliability, primary depressurisation system, which transfers high pressure to low pressure core melt sequences.

- features for corium spreading and cooling.

- prevention of hydrogen detonation by reducing the local hydrogen concentration in the containment at an early stage by establishing good atmospheric mixing of the containment atmosphere in combination with catalytic hydrogen recombiners, which reduce the global hydrogen amount.

- control of the containment pressure and temperature by a dedicated Containment Heat Removal System (CHRS) consisting of a spray system with recirculation through the cooling structure of the melt retention device.

- collection of all containment leaks in the annulus of the double wall containment and routing them through filters to the stack, as well as prevention of bypass of the confinement .

No attempt is made to provide external cooling of the reactor pressure vessel to contain the debris in-vessel following core melt. Rather, the concept of corium control relies on a dry core melt retention system to prevent steam explosion and to assure thin spreading of the hot corium to allow for its subsequent cooling. The concept of a core melt retention system is based on experimental results for hot corium. Therefore, design measures have been taken to assure that the corium will be hot at the moment of relocation into the retention system and this coupled with the chemical content of containment materials allows the corium to remain liquid and flow into the spreading compartment.

The EPR corium stabilisation concept is characterised by the following sequence of events:

1. vessel failure and consequential corium ejection into the reactor pit,

2. temporary corium retention in the reactor pit,
3. opening of the fuse hatch and corium flow through the discharge channel into the spreading compartment,
4. passive flooding and quenching of the spreading corium,
5. cooling and removal of the decay heat over the long-term.

Interaction of the corium with the structural concrete is thus avoided, since this could cause:

- embrittlement of the bearing structures which could affect the integrity of the metallic liner;
- long-term overheating and mechanical deformation of the foundation raft and the containment;
- prolonged release of non-condensable gases into the containment atmosphere due to interaction between the core melt and the structural concrete.

2.2 Standards and Criteria

The fault assessment strategy for Step 2 is given in ND DIV 6 Assessment Report AR07015, Ref 3, and indicates that ND will compare the design and the claims made by the Requesting Party's (RP) against the HSE Safety Assessment Principles (Ref 8). In accordance with this strategy, the relevant fault assessment SAPs on Reactor Core (ERC.1 – 3), Heat Transport Systems (EHT.1 – EHT.4), Fault Analysis section covering Design Basis Analysis (FA. 1 - 9) and Severe Accidents (FA.15 – 24), were selected for the Step 2 assessment.

To ensure that this selection covered an adequate set of fault assessment SAPs a further review was carried out against the WENRA reference levels, Ref 11, and the IAEA Nuclear Power Plant Design Requirements, Ref 12. The results of this review are shown in Annex 2 of the fault assessment strategy, Ref 3, where they are ordered under assessment topics. These key fault assessment SAPs were used during the assessment and appear in Annex 2 of this document. This assessment report has been written in accordance with the assessment procedures outlined in Refs 9 and 10.

2.3 ND ASSESSMENT

As already stated, the overall assessment strategy for Step 2 is outlined in the Unit 6D Operating Plan, Ref 2, and the specific fault study assessment strategy for Step 2 is given in ND DIV 6 Assessment Report AR07015, Ref 3.

Claims, arguments and ultimately evidence

The Fault Analysis SAPs selected for assessment of claims during Step 2 are shown in Annex 2 where they are ordered under assessment topic areas.

EDF/AREVA supplied a compliance document (Ref 7) to outline how it believes the HSE Safety Assessment Principles will be complied with. The summary, as to how EDF/AREVA claims it will comply with the requirements of the relevant SAPs, in the area of fault analysis, is contained in Annex 3. In all areas EDF/AREVA claims full compliance. The submission has supplied a great deal of information on the safety aspects of the design, and within the scope of the SAPs considered in Appendix 2, it is possible to confirm that EDF/AREVA claims the following:

1. Under normal operation the reactor core will be stable. This arises because core temperature, power and core void coefficients of reactivity are all negative SAP ERC.3
2. There are diverse and redundant cooling systems to extract reactor core heat under normal and fault conditions SAPs EHT.1 - 4
3. There are two diverse shutdown systems SAP ERC.2
4. Initiating faults have been taken into account as part of the Design Basis Analysis SAP FA.5
5. All Design Basis Accident faults meet the acceptability criteria SAP FA 4 & 5
6. Severe accidents have been considered in the design and means provided to mitigate the consequences and as reported in the PSA section, risk is adequately controlled SAPs FA.15 & 16.
7. Reactor fault scenarios have been undertaken using approved analytical techniques subjected to quality assurance SAPs FA.18 - 20

Initiating faults SAP FA.2

In section P2 of Volume 2 of the Submission, EDF/AREVA has outlined the list of faults that the EPR has been designed to be tolerate. The list appears exhaustive, in that it includes over-power reactivity transients from the hot condition, loss of coolant accidents requiring immediate response of safety injection systems, boiler tube faults with potential release through the containment system and cool down faults from the zero power condition.

O1. Confirmation will be required that EDF/AREVA have identified all significant faults.

Computer codes, their use and validation SAP FA.18

The results of the transient analyses are based on a suite of computer codes that have been used by EDF/AREVA to conclude that all faults within the design base envelope will not lead to unacceptable consequences. EDF/AREVA have claimed that these codes and models have been subjected to a quality assurance program for their use, validation and appropriateness. No information has been presented on that validation process. This will be followed up and verified in later Steps of the assessment process.

O2. Confirmation will be required that the computer codes used in the safety case have been appropriately validated.

Transient Analysis SAPs FA.19 & 22

EDF/AREVA did not provide any traditional transient analyses to support the conclusions that were made for the requirements of the design. At our request through Technical Query EPR000003, we received this material. It will be important to establish in later assessments that:

- conservative calculation methods and assumptions have been used to ensure the predictions are pessimistic
- the acceptance criteria for the successful outcome of the transient are appropriate
- the most limiting plant configuration and operating regime is assumed
- the results are not overly sensitive to small variations in input data
- plant data including response times of I&C detectors, trip logic and shutdown systems used, are modeled pessimistically

O3. Confirmation will be required that the calculational methods, data and acceptance criteria are suitably conservative and fit for purpose.

Diverse shutdown SAP ERC.2

Two diverse shutdown systems are provided. The Extra Boration System EBS is a safety-related system that performs the following functions:

- boration of the RCS in all anticipated operational transients and postulated accidents to reach a controlled state at all primary pressure levels,

- maintain the reactor in a shutdown state at any reactor temperature without control rods.

Response times and the range of faults that the EBS can successfully control is not declared.

O4. Confirmation will be required to define what range of faults the diverse shutdown system can effectively control

Operating Limits and Conditions SAP FA.2

The transient analysis appears to have been conducted appropriately and the claims made by EDF/AREVA meets the requirements of the HSE's Safety Assessment Principles as outlined in Annexes 2 and 3. It will be important in the assessment to establish that the direct link from the fault studies to the resulting operating limits and conditions imposed on the plant, to ensure that it remains in a safe operating envelope, is outlined in the future submissions. These would be pessimised and used as input data at the start of the transient analysis. Such plant parameters would be the inlet and outlet temperatures, pressure and thermal power. This is an important area that will be focused on in later assessment and is not expected to cause EDF/AREVA any difficulties.

O5. Confirmation will be required to confirm the consistency of operating limits and conditions on the plant with those directly derived from the fault analysis.

Severe accidents management SAPs FA.15 & 16

EDF/AREVA acknowledges the importance of severe accident management in mitigating the effects of Beyond Design Basis Accidents but has not indicated, at this stage, how this would be achieved in practice. This will be followed up in later Steps of the assessment process. The strategy has been to ensure that the molten core is made suitably safe within the concrete containment system. No attempt is made to try to hold the debris in the Reactor Pressure Vessel and the molten material is directed to a purpose made core catcher located below and lateral to the vessel. Here it can be cooled from all sides with water without resulting in steam explosions that could endanger the integrity of the concrete containment and supporting structures.

Once the well-defined geometry of the core has been lost, the uncertainties after such an event can produce a whole spectrum of possible results. We will need to be reassured during the next stages of assessment that the prevention of large scale steam corium explosions can be avoided with the system EDF/AREVA has provided.

O6. Confirmation will be required that the severe accident strategy, modeling methods, data and acceptance criteria are appropriate.

3. CONCLUSIONS

The submission meets the requirements of Step 2. EDF/AREVA have supplied HSE with sufficient material in relation to the area of fault studies and have made claims that the HSE's Safety Assessment Principles have been met in this area. Detailed assessment in Steps 3 and 4, as outlined in the planning documents, will be to confirm the adequacy of the arguments and evidence.

4. RECOMMENDATIONS

R1. Undertake detailed Fault Analysis assessment of EDF/AREVA's future safety documentation using the approach outlined in this document to verify the claims made.

R2. Focus on areas important to the Fault Studies assessment in relation to:

- the completeness of initiating faults
- the validation by EDF/AREVA of models, computer codes used in the transient analysis
- pessimising the data used and plant conditions to achieve conservative results
- define the range of faults the EBS can effectively control
- the consistency of operating limits and conditions with those directly derived from the fault analysis
- review of the containment scenario following a severe core accident

5. REFERENCES

1. HSE Nuclear Power Station Generic Design Assessment – Guidance to Requesting Parties, Version 2, 16 July 2007.
2. HSE ND DIV 6 Unit 6D Operating Plan, 2 August 2007 – 31 March 2008.
3. HSE ND DIV 6 Assessment Report “Step 2 Fault Studies & PSA Assessment Strategy”, Assessment Report No. AR07015
4. HSE ND – BMS G/AST/001, “Assessment Guidance – Assessment Process”, Issue 002, 28 February 2003.
5. HSE ND – BMS AST/003, “Assessment - Assessment Reporting”, Issue 002, 13 October 2003.
6. EDF /AREVA Submission
7. Technical Query EPR000003 “Compliance with HSE Safety Assessment Principles for Nuclear Installations (2006) Edition.
8. HSE Safety Assessment Principles for Nuclear Facilities, 2006 Edition.
9. HSE ND – BMS AST/001, “Assessment - Assessment Process”, Issue 002, 18 February 2003.
10. HSE ND – BMS AST/002, “Assessment - Assessment Activity management”, Issue 003, 16 April 2002.
11. Western European Nuclear Regulators Association (WENRA) Reactor Safety Reference Levels, January 2007.
12. IAEA Safety Standards Series – Safety of Nuclear Power Plants: Design – Requirements – No.NS-R-1.

Annex 1

Determination of Fault Analysis SAPs to be considered during Step 2 and a comparison with WENRA Reference Levels and IAEA Guidance Documents

SAP Number	SAP Title	Assessed Category	WENRA Ref.	IAEA Ref.
EKP	**Key engineering**			
EKP.2	Fault tolerance	S2	E2.1	
EKP.3	Defence in depth	S2	E2.1	
ERC –	**Reactor Core**			

ECR.1	Design and Operation of Reactors	S2	E2.1	2.10(2)
				2.10(3)
				2.10(4)

ECR.2	Shutdown systems	S2	G1.1 G2.1	2.10(2)
ECR.3	Stability in normal operation	S2	G2.2 G3.1	2.10(1)
EHT –	**Heat Transport systems**			
EHT.1	Design	S2	G4.2	5.45 6.68
EHT.2	Coolant inventory and flow	S2	E9.1	3.8 5.40 6.82
EHT.3	Heat sinks	S2	E2.1 E9.4 E10.7	2.9(1) 6.82
EHT.4	Failure of heat transport system	S2	E10.10	5.33 6.82
FA –	**Fault analysis general**			
FA.1	Design basis analysis, PSA and severe accident analysis	S2		

FA.2	Identification of initiating faults	S2		2.7(3)
				2.7(4)

FA.3	Fault sequences	S2	E9.3	6.80(1)
FA –	**Design basis analysis**			
FA.4	Fault tolerance	S2		
FA.5	Initiating Events	S2		
FA.6	Fault sequences	S2		
FA.7	Consequences	S2		
FA.8	Linking of initiating faults, fault sequences and safety measures	S2		
FA.9	Further use of DBA	S3		
	PSA		Note x	
FA.10	Need for PSA	S2	O1	
FA.11	Validity	S2	O1	
Fa.12	Scope and extent	S3	O1	
FA.13	Adequate representation	S2	O1	
FA.14	Use of PSA	S2(design)	O3	
FA –	**Severe accident analysis**			
FA.15	Fault sequences	S2		5.42 6.5
FA.16	Use of severe accident analysis	LA		
	Theoretical Models			
FA.17	Theoretical models	S3		
FA.18	Calculation methods	LA		
FA.19	Use of data	LA		
FA.20	Computer models	S3		
FA.21	Documentation	S2		
FA.22	Sensitivity studies	S2		
FA.23	Data collection	LA		

	Numerical Targets for Fault Analysis			
Target 4	Dose to any person from design basis sequences	S3		
Target 5	Individual risk from accidents - on site	S3		
Target 6	Dose for any single accident – on site	S3		
Target 7@	Individual Risk from accidents - off site	S2(broad indication)		
Target 8 @	Frequency of dose from accident - offsite	S2(high dose band)		
Target 9 @	Total risk of 100 or more fatalities	S2		

Key

S2 = Assessment commences at Step 2

S3 = Assessment commences at Step 3 or 4

NA = Not applicable

LA = Licence Applicant to address

WENRA Ref. = Refers to the clause in the WENRA document (Ref. 5) “WENRA Reactor Safety Reference Levels – January 2007”, see HSE website

IAEA Ref. = Refers to the clause in the IAEA document (Ref. 6) “IAEA Safety Standards Series – Safety of Nuclear Power Plants: Design – Requirements - No NS-R-1”, see IAEA website

@ The assessment will be a broad likelihood of the target being met based on extrapolation of the Step 2 results in the PSR. Fuller comparison is expected for Step 3

Note x – The PSA WENRA reference levels O1.1- 1.5 are met by PSA SAPs FA10-14, but not in a one to one correlation. O2 concerns validity and is met by the general FA assurance SAPs FA17-24. O3 is not applicable to the GDA as it is for existing plant. O4 is again not applicable for GDA as it is for Licence Applicants to comply with.

Annex 2

Table of Fault Analysis SAPs to be considered during Step 2

SAP Number	SAP Title	Assessed Category
EKP	**Key engineering**	
EKP.2	Fault tolerance	S2
EKP.3	Defence in depth	S2
ERC –	**Reactor Core**	
ECR.1	Design and Operation of Reactors	S2
ECR.2	Shutdown systems	S2
ECR.3	Stability in normal operation	S2
EHT –	**Heat Transport systems**	
EHT.1	Design	S2
EHT.2	Coolant inventory and flow	S2
EHT.3	Heat sinks	S2
EHT.4	Failure of heat transport system	S2
FA –	**Fault analysis general**	
FA.1	Design basis analysis, PSA and severe accident analysis	S2
FA.2	Identification of initiating faults	S2
FA.3	Fault sequences	S2
FA –	**Design basis analysis**	
FA.4	Fault tolerance	S2
FA.5	Initiating Events	S2
FA.6	Fault sequences	S2
FA.7	Consequences	S2
FA.8	Linking of initiating faults, fault sequences and safety measures	S2
FA.9	Further use of DBA	S3
	PSA	
FA.10	Need for PSA	S2
FA.11	Validity	S2
Fa.12	Scope and extent	S2
FA.13	Adequate representation	S3
FA.14	Use of PSA	S2(design)
NT	Numerical Targets 7,8 &9	S2
FA –	**Severe accident analysis**	
FA.15	Fault sequences	S2
FA.16	Use of severe accident analysis	LA
	Theoretical Models	
FA.17	Theoretical models	S3
FA.18	Calculation methods	LA
FA.19	Use of data	LA
FA.20	Computer models	S3
FA.21	Documentation	S2
FA.22	Sensitivity studies	S2
FA.23	Data collection	LA

Annex 3

Assessment template for Fault Analysis SAPs to be considered during Step 2

Assessment topic/SAP	Assessment
Key engineering principles	
Fault tolerance	
Fault tolerance Principle EKP.2 The sensitivity of the facility to potential faults should be minimised. *139* Any failure, process perturbation or mal-operation in a facility should produce a change in plant state towards a safer condition, or produce no significant response. If the change is to a less safe condition, then systems should have long time constants so that key parameters deviate only slowly from their desired values.	EPR design is considered to comply with the SAP. The EPR's low sensitivity to failure is achieved by: 1) Inherent characteristics and adequate design margins that provide favourable response periods to reactor transients and smooth the transients themselves; • The core design provides inherent safety features such as negative power reactivity coefficient and negative moderator temperature coefficient from low (zero) power to full power (see SSER 2.D.3.4) • The large core size (see SSER 1.A.1. table 1.1) results in a reduced average core power density, which has a beneficial effect on the margins to the core safety limits: the average linear power density of the fuel rods is 11 % lower than in the actual N4 plants and about 9% lower than in Sizewell B. • To smooth transients, the main components' sizes (especially the steam generator on the secondary side and the pressuriser on the primary side) have been increased compared to the current designs (see SSER 1.A.1. table 1.1). 2) The automatic functions of the Reactor Control Surveillance and Limitation System (RCSL, see SSER 2.G.4); In normal operating conditions, it 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 runback) 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.
Reactor Core	
Design and Operation of Reactors Principle ECR.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. Guidance SAP paragraphs 440 - 443 440 The above principle covers normal operation, refuelling, testing and shutdown and design basis fault conditions. The fundamental safety functions are: a) control of reactivity (including re-criticality following an event); b) removal of heat from the core; c) Confinement or containment of radioactive	EPR design is considered to comply with the SAP Analysis of Design Basis events (PCC) and Design Extension Conditions (RRC) show that the three basic safety functions of reactivity control, residual heat removal and the containment of radioactive substances, are achieved in all permitted modes of reactor operation, including accidents in the spent fuel pool (see SSER 2.P and 2.S), 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,…).

substances. 441 There should be suitable and sufficient margins between the normal operational values of safety-related parameters and the values at which the physical barriers to release of fission products are challenged. 442 The requirements for loading and unloading of fuel and core components, refuelling programmes, core monitoring and the criteria and strategy for dealing with fuel failures should be specified. 443 No single moveable fissile assembly, moderator or absorber when added to or removed from the core should increase the reactivity by an amount greater than the shutdown margin, with an appropriate allowance for uncertainty. The uncontrolled movement of reactivity control devices should be prevented.	
Shutdown systems Principle ERC.2 At least two diverse systems should be provided for shutting down a civil reactor. Guidance SAP paragraphs 444 – 445 444 Where a shutdown system is also used for the control of reactivity, a suitable and sufficient shutdown margin should be maintained at all times. 445 Reactor shutdown and subsequent hold-down should not be inhibited by mechanical failure, distortion, erosion, corrosion etc of plant components, or by the physical behaviour of the reactor coolant, under normal operation or design basis fault conditions.	EPR design 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 principle of the core reactivity control are explained in SSER 2.D.3.5, 6 and SSER 2.D.5. 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 SSER 2.C.6.4) and the Rod Assembly Guide which are part of the internal structure of the reactor vessel (see SSER 2.C.6.5) are designed and manufactured in accordance with the safety classification (described in SSER 2.C.1). 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 SSER 2.F.7, or by the Safety Injection System (SIS) see SSER 2.F.6: both systems are safety classified, and are designed, manufactured and tested accordingly. Analysis of Design Extension Conditions (RRC) 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 SSER 2.S.1.2) independently of the control rods The Chemical and Volume Control Systems (RCV), see SSER 2.I.3.2, is used for reactor control to adjust the boron concentration during normal operation; it is not safety classified.
Stability in normal operation Principle ERC.3 The core should be stable in normal operation and should not undergo sudden changes of condition when	EPR design is considered to comply with the SAP

operating parameters go outside their specified range. SAP Guidance paragraphs 446 – 455 446 An increase in reactivity or reduction in coolant flow, caused by the unplanned: a) movement within the core; b) loss from the core; or c) addition to the core; of any component, object or substance should be prevented. 447 The geometry of the core should be maintained within limits that enable the passage of sufficient coolant to remove heat from all parts of the core. Where appropriate, means should be provided to prevent any obstruction of the coolant flow that could lead to damage to the core as a result of overheating. In particular the overheating of fuel should be prevented where this would give rise to: a) fuel geometry changes that have an adverse effect on heat transport; b) failure of the primary coolant circuit. *Note:* Where these mechanisms cannot be prevented by design, protective measures should be available to maintain the plant in a safe condition. 448 The structural integrity limits for the core structure and its components (including the fuel) should ensure that their geometry will be suitably maintained. 449 Changes in temperature, coolant voiding, core geometry or the nuclear characteristics of components that could occur in normal operation or fault conditions should not cause uncontrollably large or rapid increases in reactivity. 450 Effects of changes in coolant condition or composition on the reactivity of the reactor core should be identified. The consequences of any adverse changes should be limited by the provision of protective systems or by reactor core design parameters. 451 There should be suitable and sufficient design margins to ensure that any reactivity changes do not lead to unacceptable consequences. Limits should be set for the maximum degree of positive reactivity. 452 The design of the core and its components should take account of any identified safety-related factors, including: a) irradiation; b) chemical and physical processes; c) static and dynamic mechanical loads; d) thermal distortion; e) thermally-induced stress; and f) variations in manufacture. 453 The core should be securely supported and positively located with respect to other components in the reactor to prevent gross unplanned movements of the structure of the core or adverse internal movements. 454 Core components should be mutually compatible and compatible with the remainder of the plant.	Reactor and core design is described in SSER 2.D. The nuclear design evaluation (see SSER 2.D.3) 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 SSER 2.D.5. SSER 2.D.2 presents the fuel design and SSER 2.D.4 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.
Heat Transport systems	
Design Principle EHT.1 Heat transport systems should be designed so	EPR design is considered to comply with the SAP Several systems are designed to transport and remove

that heat can be removed or added as required. SAP Guidance paragraph 459 459 Sufficient capacity should be available to do this at an adequate rate.	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 SSER 2.E.1.. The secondary cooling system and in particular the MSSS system is described in SSER 2.J.3. In normal operation, the Main Steam Relief trains (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 SSER 2.F.8. 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 the safe state (with reactor in State A or B). This system is described in SSER 2.F.3. 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 SSER 2.I.1 and 2. 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 (SRU) using a dedicated cooling system and its capacity is sufficient to perform this task in all system operating situations. This is described in SSER 2.F.2.
Coolant inventory and flow Principle 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. Guidance SAP paragraph 460 – 462 460 The various sources of heat to be added to or removed from any system and its component parts under normal and fault conditions should be quantified, and the uncertainties estimated in each case. 461 Inherent cooling processes such as natural circulation can be taken into account in assessing the effectiveness of the heat transport system, providing they are shown to be effective in the conditions for which they are claimed. 462 In the case of liquid heat transport systems, there should be a margin against failure of the operating heat transfer regime under anticipated normal and fault conditions and procedures. The minimum value of this margin should	EPR design is considered to comply with the SAP The Reactor Coolant System (RCP) design flow and its uncertainties for normal operation are described in SSER 2.E.1. Design basis analyses from SSER 2.P 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.

be stated and justified with reference to the uncertainties in the data and in the calculational methods employed.	
Heat sinks Principle EHT.3 A suitable and sufficient heat sink should be provided. SAP Guidance paragraph 463 463 Provision should be made for removal of heat to an adequate heat sink at any time throughout the life of the facility, irrespective of the availability or otherwise of external resources. Consideration should be given to the site-related environmental parameters such as variations in air and water temperatures, available levels and flow rates of water etc, to ensure adequate heat removal capacity at all times.	EPR design 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 SSER 2.C.3)
Failure of heat transport system Principle 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 facility in a safe condition and prevent any release in excess of safe limits. Heat transport systems should be designed so that heat can be removed or added as required. SAP Guidance paragraph 464 – 466 464 Provision should be made to: a) minimise the effects of faults within the facility that may propagate through the heat removal and ventilation systems. Personnel and structures, systems and components important to safety should be protected where necessary from the radiation, thermal and/or dynamic effects of any fault involving the heat transport fluids; b) prevent an uncontrolled loss of inventory coolant from the coolant pressure boundary. Provision should be made for the detection of significant loss of heat transport fluid or any diverse change in heat transport that might lead to an unsafe state. Provisions should be made in the design to minimise leakage of the coolant and keep it within specified limits. Isolation devices should be provided to limit any loss of radioactive fluid; c) where appropriate, provide a sufficient and reliable supply of reserve heat transfer fluid, separate from the normal supply, to be available in sufficient time in the event of any significant loss of heat transfer fluid. 465 The properties of any heat transport fluid, its composition and impurity levels should be so specified as to minimise adverse interactions with facility components and any degradation of the fluid caused by radiation. Appropriate chemical and physical parameters should be monitored and filtration, processing or other plant provided to ensure that the specified limits are maintained. 466 Where mutually incompatible heat transport fluids are used within the facility, provision should be made to prevent their mixing and, where appropriate, to prevent harm to personnel and safety-related structures in the event of such mixing.	EPR design 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 SSER 2.C.4. SSER 2.P and S show analyses of events leading to a loss of coolant inventory following a pressure boundary 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 SSER 2.I.3.2. The activity in the primary coolant is monitored by the Nuclear Sampling System. The core cooling is performed by pressurized 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.

Fault analysis general	
General	
Design basis analysis, PSA and severe accident analysis Principle FA.1 Fault analysis should be carried out comprising design basis analysis, suitable and sufficient PSA, and suitable and sufficient severe accident analysis.	EPR design is considered to comply with the SAP The faults analysis is carried out through: Design Basis (PCC) accident analysis for the EPR described in SSER 2.P. Design Extension Conditions (RRC-A) and severe accidents (RRC-B) described in SSER 2.S.2.1 and 2.S.2.2. Analysis of Preliminary PSA results, presented in SSER 2.R. (The updated SSER that will be issued for Step 3 of GDA will contain a comprehensive PSA at Level 1, 2 and 3)..
Identification of initiating faults Principle 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. SAP Guidance paragraph 504 504 The process for identifying faults should be systematic, auditable and comprehensive, and should include: a) significant inventories of radioactive material and also radioactive sources that may be lost or damaged; b) planned operating modes and configurations, including shutdown states, decommissioning operations, and any other activities which could present a radiological risk; and c) chemical and other internal hazards, man-made and natural external hazards, internal faults from plant failures and human error, and faults resulting from interactions with other activities on the site. Faults lacking the potential to lead to doses of 0.1 mSv to workers, or 0.01 mSv to a hypothetical person outside the site, are regarded as part of normal operation and may be excluded from the fault analysis. These are the levels of individual dose above which should be regarded as significant in Principle FA.2. A significant quantity of radioactive material is one which if released could give rise to a significant dose.	EPR design is considered to comply with the SAP The list of Design Basis Events analysed in the EPR SSER is presented in SSER 2.P.2.0. 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.
Fault sequences Principle FA.3 Fault sequences should be developed from the initiating faults and their potential consequences analysed. SAP Guidance paragraphs 505 – 510 505 The scope, content, level of detail and rigour of the analysis should be proportionate to the complexity of the facility and the hazard potential. 506 There should be a clear relation between the fault sequences used in DBA and severe accident analysis, and the fault sequence development of the PSA. 507 Transient analysis or other analyses should be carried out as appropriate to provide adequate understanding of the behaviour of the facility under fault conditions. 508 For fault sequences that lead to a release of radioactive material or to exposure to direct radiation, radiological consequence analysis should be performed to determine	EPR design is considered to comply with the SAP Analysis of design basis fault sequences developed from the Design Basis initiating events, is described in SSER 2.P.2. 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 SSER 2.P.3. 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 not included in the Step 2 SSER as it was not part of the design basis for the EPR. Due to the extremely low frequency of large releases

the maximum doses to a worker on the site, to a person outside the site, eg directly downwind of an airborne release, and to the reference group for any other off-site release pathways. (The detail of this analysis differs according to its application, see paragraphs 601, 607 and 621.) 509 The calculated doses should include those arising from the potential release of radioactive material, direct radiation, and criticality incidents. 510 Radiological analysis of societal effects from possible releases from the site should be carried out to determine whether the consequences specified in the societal risk target (Target 9 *(paragraph 623 f.)*) could be reached.	achieved by the EPR design (SSER 2.R.2) there is a strong confidence that Target 9 will be achieved. Compliance with the target will be confirmed formally in the SSER update being prepared for Step 3 of GDA.
Design basis analysis	
Fault tolerance Principle FA.4 DBA should be carried out to provide a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safety measures. SAP **Guidance paragraph** 513 513 If possible, DBA should be carried out as part of the engineering design. Where this is not possible (eg for review of existing facilities), the analysis should be developed in line with the engineering analysis to demonstrate that the safety function is met. In either case, it is important that the analysis fully reflects the engineering and iterates with it to engender improvements. It should also take account of the key principles sub-section *(paragraph 135 ff.).*	EPR design is considered to comply with the SAP The design basis analysis is described in SSER 2.P. 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.
Initiating Events Principle FA.5 The safety case should list all initiating faults that are included within the design basis analysis of the facility. Guidance SAP paragraph 514, 515 514 Initiating faults identified in Principle FA.2 should be considered for inclusion in this list, but the following need not be included: a) faults in the facility that have an initiating frequency lower than about 1 x 10^{-5} pa;- b) failures of structures, systems or components for which appropriate specific arguments have been made; c) natural hazards that conservatively have a predicted frequency of being exceeded of less than 1 in 10 000 years; d) those faults leading to unmitigated consequences which do not exceed the BSL for the respective initiating fault frequency in Target 4 *(paragraph 599 f.)*. *Note:* The risks from initiating faults in d) should be shown to be as low as reasonably practicable by application of relevant good engineering practice supported by deterministic and probabilistic analysis as appropriate. 515 Initiating fault frequencies should be determined on a best-estimate basis with the exception of natural hazards	EPR design is considered to comply with the SAP A table of design basis initiating events is given in SSER 2.P.2.0.

where a conservative approach should be adopted.	
Fault sequences Principle FA.6 For each initiating fault in the design basis, the relevant design basis fault sequences should be identified. Guidance SAP paragraph 516 - 518 516 Correct performance of safety-related and non-safety equipment should not be assumed where this would alleviate the consequences. 517 Each design basis fault sequence should include as appropriate: a) failures consequential upon the initiating fault, and failures expected to occur in combination with that initiating fault arising from a common cause; b) single failures in the safety measures in accordance with the single failure criterion; c) the worst normally permitted configuration of equipment outages for maintenance, test or repair; d) the most onerous permitted operating state within the inherent capacity of the facility; Sequences with very low expected frequencies need not be included in the DBA. 518 The analysis should establish that adverse conditions that may arise as a consequence of the fault sequence will not jeopardise the claimed performance of the safety measures. 519 Operator actions can be claimed as part of safety measures only if sufficient time is available, adequate information for fault diagnosis is presented, appropriate written procedures exist and compliance with them is assured, and suitable training has been provided. 520 Initiating events leading to fault sequences protected by the same safety measures may be grouped, and their frequencies summed, for the purposes of the DBA. Conversely, initiating events leading to similar fault sequences should not be subdivided to evade requirements for design basis safety measures.	EPR design is considered to comply with the SAP. Development of design basis fault sequences for the Design Basis initiating events, is described in SSER 2.P.2. 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; 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 SSER 2.C.7). 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 SSER 2.M.3).
Consequences Principle 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. Guidance SAP paragraph 521 – 524 521 The analysis should demonstrate, so far as is reasonably practicable, that: a) none of the physical barriers to prevent the escape or relocation of a significant quantity of radioactivity is breached or, if any are, then at least one barrier remains intact and without a threat to its integrity; b) there is no release of radioactivity; and c) no person receives a significant dose of radiation.	EPR design is considered to comply with the SAP Analysis of Design Basis event sequences (PCCs) for the EPR is presented in SSER 2.P.2. 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 SSER 2.P.3. 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

522 Relocation means the material is no longer in its designated place of residence or confinement. 523 Where releases occur, then doses to persons should be limited. The numerical targets for doses to persons are set out in Target 4 *(paragraph 599 f.)*. 524 Design basis analysis may also contribute to accident management strategies and emergency plans.	given in Table 4 of the SAPs, meeting the requirement of paragraph 523 of SAP FA.7.
Linking of initiating faults, fault sequences and safety measures Principle FA.8 DBA should provide a clear and auditable linking of initiating faults, fault sequences and safety measures. Guidance SAP paragraph 525 525 The analysis should demonstrate that: a) the design basis initiating faults are addressed; b) safety functions have been identified for the design; c) the performance requirements for the safety measures have been identified; and d) suitable and sufficient safety measures are provided.	EPR design is considered to comply with the SAP Analysis of the Design Basis (PCC) events is described in SSER 2.P.2. 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. Analysis of RRC Design Extension conditions presented in SSER 2.S similarly identifies the F2 safety systems that provide diverse protection in complex sequences involving CCF of F1 systems.
Further use of DBA Principle 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. Guidance SAP paragraph 526 526 DBA should provide the basis for: a) safety limits, ie the actuator trip settings and performance requirements for safety systems and safety-related equipment; b) conditions governing permitted plant configurations and the availability of safety systems and safety-related equipment; c) the safe operating envelope defined as operating limits and conditions in the operating rules for the facility; and d) the preparation of the facility operating instructions for implementing the safe operating envelope, and other operating instructions needed to implement the safety measures.	EPR design 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 SSER 2.C.2 for safety classification, SSER 2.C.7 for equipment qualification and SSER 2.M.3 for emergency operating procedures).
PSA	
Principle FA 10 Need for PSA. Suitable and sufficient PSA should be performed as part of the fault analysis and design development and analysis. **Guidance SAP paragraphs 529**	EPR design is considered to comply with the SAP PSA has been performed as an integral part of the EPR design. Results of the preliminary PSA analysis for the FA3 which is the reference design for the UK EPR are given in SSER 2.R. The EPR project uses as a safety objective the IAEA 10^{-5}/yr CMF target for future reactors (all events). To meet this objective, the following breakdown of internal targets has been proposed for the purpose of PSA studies (see SSER 2.R.0): core melt frequency due to internal events for power operation $<10^{-6}$/yr

	core melt frequency due to internal events for shutdown states $<10^{-6}$/yr core melt frequency due to internal hazards <3 10^{-6}/yr core melt frequency due to external hazards <5 10^{-6}/yr A further probabilistic objective is that no class of events should make a disproportionate contribution to the core melt frequency to achieve a balanced design. Moreover, any major sequence contributing to the overall risk may be analysed in the framework of RRC studies. Preliminary results of the Level 1 PSA for internal events in SSER 2.R.1 show that the probabilistic objectives are achieved, and that the risk of core melt due to internal events is evenly divided between the five event groups: LOCA, secondary cooling system events, loss of offsite power supplies, loss of heat sink events and ATWS. Results of the preliminary hazards PSA presented in SSER 2.R.4 show the target for internal hazards is achieved, and the target for external hazards achieved to within a slight shortfall. A more comprehensive PSA analysis for the UK EPR will be presented in the SSER update to be submitted for Step 3 of GDA.
Principle FA 11 :Validity. PSA should reflect the current design and operation of the facility or site. **Guidance SAP paragraphs 530 -531**	The current French practice on operating plants in these matters intend to maximise the benefits from the series effect: the 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… EDF will propose in due time to implement 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.
Principle FA 12: Scope and extent. PSA should cover all significant sources of radioactivity and all types of initiating faults identified at the facility or site. Guidance SAP paragraphs (none)	EPR design is considered to comply with the SAP The PSA presented in Chapter R of the Step 2 SSER considers internal events, internal and external hazards affecting the nuclear steam supply system as the dominant source of radioactive material in the plant. Initiating events cover all reactor states, including both at-power and shutdown conditions. For the Step 3 SSER, the PSA is being extended to cover events affecting the fuel building and events involving accidental release of radioactivity in the nuclear auxiliary building and effluent treatment building.
Principle FA 13: Adequate representation. The PSA model should provide an adequate representation of the site and its facilities **Guidance SAP paragraphs 532 -540**	EPR design is considered to comply with the SAP As explained in SSER 2.R.1, 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 SSER 2.R.1.2.1). Initiating event frequencies are evaluated from operating feedback from French plants and international feedback. The PSA contains a comprehensive treatment human errors, which are allowed for in equipment unavailability analysis and in treating the probability of failure to execute requested actions (see SSER 2.R.1.2.3). In the PSA analysis that will be presented in Step 3 of GDA, an uncertainty analysis will be included. Hence risk results will be presented at a range of confidence levels, rather than as a central estimate of risk, a requested by the SAP.
Principle FA 14: Use of PSA. PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities. **Guidance SAP paragraphs 541 -542**	EPR design is considered to comply with the SAP As far as design is concerned, and as stated in SSER 1.C.4.3, 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.
PSA Related Numerical Targets. NT.1	
Severe accident analysis	
Fault sequences Principle FA.15 Fault sequences beyond the design basis that have the potential to lead to a severe accident should be analysed. Guidance SAP paragraph 545 - 548 545 This should include: a) determination of the magnitude and characteristics of their radiological consequences, including societal effects; and b) demonstration that there is no sudden escalation of consequences just beyond the design basis. 546 The analysis should consider failures that could occur in the physical barriers preventing release of radioactive material, or in the shielding against direct radiation. 547 A best estimate approach should normally be followed. However, where uncertainties are such that a realistic analysis cannot be performed with confidence, a conservative or bounding case approach should be adopted to avoid optimistic conclusions being drawn. 548 Where severe accident uncertainties are judged to have a significant effect on the assessed risk, research aimed at confirming the modelling assumptions should be	EPR design 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 SSER considers the radiological consequences of core melt sequences (SSER 2.S.2.2 Probabilistic analysis is used to identify RRC-A beyond design basis conditions (see SSER 2.R.0). RRC-A analysis is used to demonstrate that no cliff edge increase in core damage frequency due to multiple failure events such as common cause failure of F1 classified safety systems. The RRC-A results are presented in SSER 2.S.1. In carrying out the RRC-A studies particular attention is given to the uncertainties that can cause a “cliff edge” increases in risk (see SSER 2.S.1.0).Analysis of RRC-A design extension conditions is also carried out to show there is no cliff edge increase in risk due to barrier failures beyond those considered in the design basis (e.g. 2A-LOCA, multiple steam

performed.	generator tube rupture, simultaneous Steam Line break with steam generator tube rupture etc) (see SSER 2.S.3). 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 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's 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.
Use of severe accident analysis Principle FA.16 The severe accident analysis should be used in the consideration of further risk-reducing measures. Guidance SAP paragraph 549 - 550 549 The severe accident analysis should provide information: a) to assist in the identification of any further reasonably practicable preventative or mitigating measures beyond those derived from the design basis; b) to form a suitable basis for accident management strategies; c) to support the preparation of emergency plans for the protection of people; and d) to support the PSA of the facility's design and operation.	EPR design 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 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 depressurization to prevent the effects of high pressure core melt sequences, a combustible gas control system

550 Measures identified under a) above need not involve the application of conservative engineering practices used in the DBA, but rather should be based upon realistic or best estimate assumptions, methods and analytical criteria.	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
Assurance of validity of data and models	
Theoretical models Principle FA.17 Theoretical models should adequately represent the facility and site.	EPR design 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 SSER 2.P are CATHARE, S-RELAP, SMART, FLICA, PANBOX, COBRA, MANTA and NLOOP. The main codes for performing the RRC design extension and severe studies presented in SSER 2.S 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. Further details of the development and validation basis of the analysis codes will be provided in the update of the SSER at Step 3 of GDA. Radiological analysis of within and beyond design basis accidents are described in SSER 2.P.3 and SSER 2.S.2.3. 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.
Calculation methods	

Principle FA.18 Calculation methods used for the analyses should adequately represent the physical and chemical processes taking place. Guidance SAP paragraph 552 - 557 552 Where possible, the analytical models should be validated by comparison with actual experience, appropriate experiments or tests. 553 The model should be validated for each application made in the safety analysis. The validation should be of the model as a whole or, where this is not practicable, on a module basis, against experiments that replicate as closely as possible the expected plant condition. 554 Care should be exercised in the interpretation of such experiments to take account of uncertainties in replicating the range of anticipated plant conditions. The limits of applicability of the analytical model should be identified. 555 Where validation against experiments or tests is not possible, a comparison with other, different, calculation methods may be acceptable. 556 Where possible, independent checks using diverse methods or analytical models should be carried out to supplement the original analysis. 557 The radiological analysis should include any direct radiation and any inhalation, absorption and ingestion of radioactive material and should also take account of the physical and chemical form of the radioactive material released.	SEE FA.17
Use of data Principle 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. **Guidance SAP paragraph** 558,559 558 Where uncertainty in the data exists, an appropriate safety margin should be provided. 559 The limits of applicability of the available data should be identified and extrapolation beyond these limits should not be used unless justified.557. The radiological analysis should include any direct radiation and any inhalation, absorption and ingestion of radioactive material and should also take account of the physical and chemical form of the radioactive material released.	EPR design 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 short description of codes used for Design Basis Analysis studies is presented in appendix 15A of the non-public version of the Flamanville 3 PSAR which was sent to HSE in response to TQ EPR00007. Along with DBA studies, SSER 2.P describes important phenomena and qualification of the used codes, which allows to check the adequacy of the models to the physics of the transient. Probabilistic and deterministic analyses are presented espectively in SSER 2.R and P. For these analyses, pessimistic assumptions are used. When building up methods for fault analyses, if the conservative assumption or the way to ensure the data is pessimistic is not obvious, sensitivity studies are performed.
Computer models	

Principle 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. Guidance SAP paragraph 560 - 563 560 These procedures should identify measures and controls to provide confidence that safety-related calculations are undertaken without error, to a level commensurate with the importance of the analysis being performed. 561 The procedures should, where appropriate, address code and dataset verification, version control, testing, documentation, user training, peer review and endorsement. 562 The procedures should specify independent verification of computer codes and datasets to confirm consistency with the supporting documentation. 563 The process of inputting data into a model should be independently verified.	SEE FA.19
Documentation Principle FA.21 Documentation should be provided to facilitate review of the adequacy of the analytical models and data> Guidance SAP paragraph 564 546 The documentation should include for example: Information showing that models and data are not employed outside their range of application; A description of the uncertainties in the model; and User guidelines and input description.	SEE FA.19
Sensitivity studies Principle 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. Guidance SAP paragraph 565 565 Where the predictions of the analysis are sensitive to the modelling assumptions, they should be supported by additional analysis using independent methods and computer codes.	SEE FA.19
Data collection Principle FA.23 Data should be collected throughout the operating life of the facility to check or update the fault analysis 566 This should include, but not be restricted to plant performance and failure data such as statistical data on initiating fault frequencies, component failure rates and plant unavailability during periods of maintenance or test, and data on external hazards.	See response for SAP FA.11 above.