Health and Safety Executive

HEALTH & SAFETY EXECUTIVE
NUCLEAR DIRECTORATE
ASSESSMENT REPORT

New Build

GDA Phase 1 - Step 2 Fault Analysis Assessment of the GE-H Submission for the ESBWR

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 license new nuclear power station 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 GE-Hitachi (GEH) submission of the Economic Simplified Boiling Water Reactor (ESBWR).

The main conclusion of this report is that the GEH 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. The report 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 GEH’s claim that the relevant fault study Safety Assessment Principles (SAPs) are met.

2.1 Requesting Parties Case

The GEH Step 2 submission used during this assessment was located at S:\New Reactor Build\RP Submission\GE Submission – Aug 2007. The submission is entitled, "UK Compliance document for ESBWR Design" Ref 6.

In response to TQ ESBWR 000001, GEH have provided a document that indicates how the ESBWR complies with the UK HSE Safety Assessment Principles. This presents information as to how the ESBWR design addressed each of the principles in the HSE Safety Assessment Principles (SAPs) for Nuclear Facilities, Ref 7.

Thermal and Hydraulic Design

Stability

In DCD 4.3.1, it is stated that the Doppler coefficient (ie the fuel temperature coefficient), the moderator void reactivity coefficient and the moderator temperature coefficient of reactivity shall be negative for power operating conditions, thereby providing negative reactivity feedback characteristics. This enhances the innate stability of the core in relation to temperature or power deviations.

The excess reactivity designed into the core is controlled by the control rod system supplemented by gadolinia-urania fuel rods. These integral fuel burnable absorber rods may be used to provide partial control of the excess reactivity available during the fuel cycle. The burnable absorber loading controls local peaking factors and lowers the reactivity of the fuel bundle. The burnable absorber performs this function by reducing the requirement for control rod inventory in the core at the beginning of the fuel cycle. Control rods are used during the cycle to compensate for reactivity changes due to burnup and also to control the power distribution.

Xenon Transients

Boiling water reactors do not have instability problems due to xenon. This has been demonstrated by:

• Never having observed xenon instabilities in operating BWRs;
• Special tests which have been conducted on operating BWRs in an attempt to force the reactor into xenon instability; and
• Calculations.

All of these indicators have proven that xenon transients are highly damped in a BWR due to the large negative moderator void feedback.

Principal Design Requirements

Initiating Faults

In DCD 15.0.1.2 of the submission GEH refer to the USNRC Regulations (10 CFR 50.49) in determining the scope of faults to be considered for analysis and the fact that the Standard Review Plan (SRP) treats all postulated abnormal initiating events with or without assuming a single active component failure or single operator error as if they are all design basis events. Therefore the following are classified as design basis events:

• Normal operation, including Anticipated Operator Occurrences (AOOs);
• Infrequent events;
• Accidents;
• External events; and
• Natural phenomena.

Acceptance criteria are defined for various fault conditions and as an example those for Anticipated Operational Occurrences are reproduced below.

Safety Analysis Acceptance Criteria for AOOs (taken from DCD Table 15.0-3)

• Pressures in the reactor coolant and main steam systems shall be maintained below 110% of their design values (i.e., not exceed ASME Code Service Level B), and the reactor steam dome pressure shall be maintained less than or equal to the Reactor Coolant System Pressure Safety Limit in the Technical Specifications.

• Fuel-cladding integrity should be maintained by ensuring that the reactor core is designed with appropriate margin during any conditions of normal operation, including the effects of AOOs. The minimum value of the critical power ratio (CPR) reached during the AOO should be such that 99.9 percent of the fuel rods in the core would not be expected to experience boiling transition during core-wide transients. (This criterion corresponds to the greater than 99.9% of the fuel rods in the core would be expected to avoid boiling transition related safety limit in the Technical Specifications.)

• Uniform cladding strain ≤ 1%.

• No fuel centreline (sic) melt.

• Reactor water level shall be maintained above the top of the core (i.e. active fuel).

• Containment and suppression pool pressures and temperatures shall be maintained below their design values.

• An AOO should not generate a more serious plant condition unless other faults occur independently.

• There is no loss of function of any fission product barrier (Safety Relief Valve or Depressurization Valve discharge does not apply).

Reactivity Control System
The Reactivity Control System consists of:

- Control rods and Control Rod Drive (CRD) system;
- Supplementary reactivity control in the form of gadolinia-urania fuel rods; and
- The Standby Liquid Control System.

Transient Analysis

The safety analysis of the design basis events will be performed using detailed models and computer codes that have been adequately validated and verified. Transient analysis models such as TRACG have been approved by the NRC (Reference DCD Chapter 15).

Severe Accidents

In the event of a severe accident in which the core melts through the reactor vessel, it is possible that the containment could be breached if the molten core is not sufficiently cooled. In addition, interactions between the core debris and concrete can generate large quantities of non-condensable gases, which could contribute to eventual containment failure.

The ESBWR design incorporates mitigating features to enhance core debris coolability. The lower drywell floor is designed with sufficient floor space to enhance debris spreading, and also contains the Basemat-Internal Melt Arrest and Coolability System (BiMAC) to protect the containment liner and basemat.

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 its Safety Assessment Principles (Ref 7). 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 8, 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.

GEH supplied a compliance document to outline how it believed the HSE Safety Assessment Principles will be complied with. The summary as to how GEH claim it will comply with the requirements of the relevant SAPs in the area of fault analysis is contained in Annex 3. In all areas GEH 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 GEH 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.

The technical information that will verify the above will be sought in later assessments. The US acceptance criteria will need to be compared and judged against appropriate UK requirements.

Initiating faults SAP FA.2

GEH has used the standard USNRC reference (10 CFR part 50) for defining the initiating faults that forms the basis of protection requirements. The DBAA requirements and assessment rules follow that defined by the NRC in the 10CFR 50 series. GEH constantly refers to the relevant subsection of this suite of documents and others when justifying the approach taken. As above, the US acceptance criteria will need to be compared and judged against appropriate UK requirements.

O1. Confirmation will be required that GEH has 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 GEH to conclude that all faults within the design base envelope will not lead to unacceptable consequences. GEH has claimed that these codes and models have been subjected to a quality assurance program for their use, validation and appropriateness. The validation process will have involved the USNRC who have expertise and independent methods of benchmarking GEH's results and it will be useful in the future parts of the assessment to have knowledge on how they went about assessing and approving GEH's codes. 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

A good start has been made in the transient analysis and 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 independent diverse shutdown systems are provided. The main system consists of control rod assemblies which perform the functions of power shaping, reactivity control, and scram reactivity insertion for safety shutdown response. The Standby Liquid Control (SLC) system is provided for the improbable event that insufficient control rods can be inserted in the reactor core to accomplish shutdown and keeps the reactor from going critical during cool-down in the normal manner. The major components of the SLC system, which are necessary for injection of sodium pentaborate solution (neutron absorber) into the reactor, are located within the Reactor Building. The SLC system can be manually initiated or in addition, can be automatically initiated for Anticipated Transients Without Scram (ATWS) and LOCA events. The SLC system contains two identical and separate trains. Each train provides 50% injection capacity. GEH claims the shutdown systems are of high integrity and reliability and that risk targets are met.

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 GEH 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. 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 GEH any difficulties.

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

Severe accident management SAPs FA.15 & 16

GEH acknowledges the importance of severe accident management in mitigating the effects of Beyond Design Basis Accidents and is developing a strategy to that end. There is provision for a system to catch any molten core and other debris in the unlikely event of a core melt. The inclusion of the Basemat-Internal Melt Arrest and Coolability System (BiMAC) device in the ESBWR design provides an engineered method to assure heat transfer between the debris bed and cooling water. BiMAC plays an important role in mitigating core melt scenarios. By flooding the lower drywell after the introduction of core material, the potential for energetic fuel/coolant interaction is minimized.

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. GEH has supplied sufficient material in relation to the area of fault studies such to be able to claim that the HSE's Safety Assessment Principles have been met in this area. Detail assessment in later stages as outlined in the planning documents will be to confirm these claims with detailed evidence.

4. RECOMMENDATIONS

R1. Undertake detailed Fault Analysis assessment of GEH'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 the RP of models, computer codes used in the transient analysis
- pessimising the data used to achieve conservative results
- define the range of faults the diverse shutdown system 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 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. GEH Submission
7. HSE. Safety Assessment Principles for Nuclear Facilities, 2006 Edition.
8. HSE ND – BMS AST/001, “Assessment - Assessment Process”, Issue 002, 18 February 2003.
9. HSE ND – BMS AST/002, “Assessment - Assessment Activity management”, Issue 003, 16 April 2002.
10. HSE ND – BMS AST/003, “Assessment - Assessment Reporting”, Issue 002, 13 October 2003.
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 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	
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.	The ESBWR complies with EKP.2. The Design Basis Assessment demonstrating the fault tolerance of the design is presented in PSR Section 2.5 and DCD Chapters 6 and 15. DCD Sections 6.2 and 6.3 specifically address the Containment systems and the Emergency Core Cooling Systems respectively. EKP.3 Defence in depth The ESBWR complies with EKP.3.
Defence in depth	
140 International consensus is that the appropriate strategy for achieving the overall safety objective is through the application of the concept of defence in depth. This should provide a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails. 141 The levels of protection should prevent faults, or if prevention fails should ensure detection, limit the potential consequences and prevent escalation. 142 The concept of defence in depth should be applied so that: a) deviations from normal operation and failures of structures, systems and components important to safety are prevented; b) any deviations from normal operation are allowed for by safety margins that enable detection and action that prevents escalation; c) inherent safety features of the facility, fail-safe design and safety measures are provided to prevent fault conditions that occur from progressing to accidents; d) additional measures are provided to mitigate the consequences of severe accidents. 143 Defence in depth is generally applied in five levels. The methodology ensures that if one level fails, it will be compensated for, or corrected by, the subsequent level. The aims for each level of protection are described in detail in IAEA Safety Standard NS-R-1[9], on which Table 1 is based. It should be noted that Table 1 deals with the application of defence in depth in the design of a facility, and does not deal with other important contributions such as human performance or equipment reliability. These topics are addressed in other sections of the SAPs.	The ESBWR complies with EKP.3. General plant design criteria are discussed in DCD Sub-section 1.2.1. Specific design criteria for different levels of safety according to importance are defined in DCD Section 3.1, whilst Engineered Safety Systems are discussed in DCD Chapter 6. The adequacy of these systems is demonstrated in the design basis in PSR Section 2.5 and DCD Sections 6.2, 6.3 and Chapter 15. Beyond design basis is discussed through the PSA presented in PSR Section 2.6. Level 5 mitigation will be a requirement of the Licensee.

Table 1 Objective of each level of protection and essential means of achieving them

Level	**Objective**	**Essential means**
Level 1	Prevention of abnormal operation and failures by design	Conservative design, construction, maintenance and operation in accordance with appropriate safety margins, engineering practices and quality levels
Level 2	Prevention and control of abnormal operation and detection of failures	Control, indication, alarm systems or other systems and operating procedures to prevent or minimise damage from failures
Level 3	Control of faults within the design basis	Engineered safety features, multiple barriers and accident or fault control procedures
Level 4	Control of severe plant conditions in which the design basis may be exceeded, including the prevention of fault progression and mitigation of the consequences of severe accidents	Additional measures and procedures to prevent or mitigate fault progression and for accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive substances	Emergency control and on- and off-site emergency response

144 An important aspect of the implementation of defence in depth is the provision of multiple, and as far as possible independent, barriers to the release of radioactive substances to the environment, and to ensure the confinement of radioactive substances at specified locations. The number of barriers will depend on the magnitude of the radiological hazard and the consequences of failure.

SAP	ESBWR response
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 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.	The ESBWR complies with ERC.1. Reactor design is covered in DCD Chapter 4. This includes fuel assembly and control rod design evaluations, control of reactivity, prevention of uncontrolled control rod movement, thermal hydraulic design, and shutdown margin with the highest reactivity control rod withdrawn. The design and safety analysis, which shows that there is adequate pressure margin between normal operating and most limiting abnormal event, for the (safety related) reactor coolant boundary is covered in DCD Section 5.2. Normal and post-accident core cooling systems are addressed in DCD Sub-section 5.4.8, DCD Section 6.3, and PSR Sub-section 2.12.2. Containment integrity safety analysis is provided in DCD Section 6.2. The ECCS LOCA performance analysis is provided in DCD Sub-section 6.3.3. The deterministic assessments of all other design basis events are provided in Chapter 15.

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.	The ESBWR complies with ERC.2. Reactivity control is addressed in DCD Section 4.6 (FMCRD) and control rod shutdown margin is addressed in DCD Sub-section 4.3.3. No single failure or malfunction of any type can cause an inserted control rod to withdraw. The Standby Liquid Control system design is addressed in DCD Sub-section 9.3.5, its shutdown capability is demonstrated in DCD Sub-sections 9.3.5.3 and 15.5.4.
Stability in normal operation Principle 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. 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.	The ESBWR complies with ERC.3. The ESBWR is designed to remain stable throughout the whole operating region, including plant start-up. The nuclear design is provided in DCD Section 4.3. Reactor core thermal and hydraulic design is covered in DCD Section 4.4. The thermal-hydraulic stability evaluations are provided in DCD Sub-section 4.3.3.6 and Appendix 4D.

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.	
Heat Transport systems	
Design Principle EHT.1 Heat transport systems should be designed so 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.	The ESBWR complies with EHT.1. Heat removal systems are discussed in DCD Chapter 5 (Isolation Condensers and Shutdown Cooling System) and DCD Chapter 10 (Main Condenser).
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 be stated and justified with reference to the uncertainties in the data and in the calculational methods employed.	The ESBWR complies with EHT.2. Coolant flow is by natural circulation sources of water described in DCD Section 4.4. Demonstration of adequate heat removal for Design Basis Accidents is provided in DCD Chapter 15 and Section 6.3

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.	The ESBWR complies with EHT.3. Heat removal systems are described in DCD Chapters 5 and 10.
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.	The ESBWR complies with EHT.4. The Reactor Coolant Systems are described in DCD Chapter 5, whilst the ECCS systems are described in DCD Section 6.3. The performance of these systems in response to Design Basis Events is presented in DCD Chapters 15 and Section 6.3.

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.	The ESBWR will comply with FA.1. ESBWR design basis analyses are presented in DCD Chapter 15 and Sections 6.2, 6.3 and 11.3. The Probabilistic Risk Assessment and severe accident analyses are presented in DCD Chapter 19. Hazards associated with non-core sources are addressed in DCD Chapter 15 deterministically. A full assessment of hazards associated with non-core sources of radioactivity will be discussed in the PCSR submission.
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.	The ESBWR complies with FA.2. Initiating internal event selection is discussed in DCD Chapter 15 as well as in the ESBWR PRA Section 2.3 (Ref. 3). External events are defined as follows: Fire - DCD Sub-section 9.5.1 and Appendix 9A. Fire protection of electrical cables - DCD Sub-section 8.3.3; Wind and Tornado - DCD Section 3.3; Floods - DCD Section 3.4; Missiles - DCD Section 3.5; Seismic - DCD Section 3.7.

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 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.	The ESBWR will comply with FA.3. The development of fault sequences is presented within PSR Section 2.6, DCD Chapter 19, and as detailed in Ref: GE Nuclear Energy, “ESBWR Design Certification Probabilistic Risk Assessment”, NEDO-33201 (Ref. 3). Currently only considers sequences leading to radiological consequences from core. Non-core fault sequences will be discussed in the PCSR submission.
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.)*.	The ESBWR complies with FA.4. This is addressed in PSR Section 2.5. These make reference to the detailed design basis analysis presented in DCD Chapter 15 and Sections 6.2 and 6.3, which provide a robust demonstration of the fault tolerance of the plant.

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 where a conservative approach should be adopted.	The ESBWR complies with FA.5. This is addressed in PSR Section 2.5 which makes reference to DCD Chapter 15 where a list is provided of all initiating faults considered and assessed with the Design Basis Analysis.

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.	The ESBWR complies with FA.6. This is addressed in PSR Section 2.5, which makes reference to DCD Chapter 15 and Sections 6.2 and 6.3 that defines the relevant design basis fault sequence for each initiating event considered in the Design Basis
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. 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.	The ESBWR complies with FA.7. This is addressed in PSR Section 2.5 and DCD Chapter 15 and Sections 6.2 and 6.3. Design considerations to meet ALARP are discussed in PSR Section 2.2 and DCD Sub-section 12.1.2 and Section 12.3.

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.	The ESBWR complies with FA.8. The Design Basis Analysis outlined in PSR Section 2.5 and the detail provided in DCD Sections 15.1 through to 15.5 provides a clear link between the initiating event, fault sequence and required number and performance of associated safety 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.	The ESBWR complies with FA.9. The Design Basis Analysis is outlined in PSR Section 2.5, with the detail provided in DCD Chapter 15 and Sections 6.2 and 6.3. Design Basis Analysis (DBA) is used to define safety systems status as well as optimising plant control settings, configurations, operating limits and the definition of the Technical Specifications in DCD Chapter 16.
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**	The ESBWR complies with FA.10. This is addressed in PSR Section 2.6 and in detail in Chapter 19 of the DCD and the ESBWR PRA (Ref. 3).
Principle FA 11 :Validity. PSA should reflect the current design and operation of the facility or site. **Guidance SAP paragraphs 530 -531**	The ESBWR complies with FA.11. The extant Issue 2 of the ESBWR PRA (Ref. 3) currently reflects the design as defined by Rev 3 of the DCD. Any design change control process encompasses any need to change the PRA. DCD Sub-section 19.4.2, describes the PRA update process.
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)	The ESBWR will comply with FA.12. The current PSA as described in PSR Section 2.6 and DCD Chapter 19 only covers core sources of radioactivity. Non-core sources of radioactivity will be discussed in the PCSR submission.

Principle FA 13: Adequate representation. The PSA model should provide an adequate representation of the site and its facilities **Guidance SAP paragraphs 532 -540**	The ESBWR complies with FA.13. This is addressed in PSR Section 2.6 and detailed in DCD Chapter 19. The details that address this principle are provided in NEDO 33201 (Reference 3).
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**	The ESBWR complies with FA.14. PSA has been used as an integral tool in the ESBWR design process from its beginnings and continues to provide design insights. Details are provided in Chapter 19 of the DCD and the ESBWR PRA (Ref. 3). The PSA will be handed over to the licensee.
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 performed.	The ESBWR complies with FA.15. This is covered in PSR Chapter 2.6 and detailed in DCD Chapter 19.

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. 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.	The ESBWR complies with FA.16. This is covered in the PSR Section 2.2 and in detail in the Severe Accident Management Design Alternatives (SAMDA) Report (Ref. 5), which utilises the PSA at looking at potential options for further reducing risk. The PRA will be used to support the preparation of emergency plans and accident management strategies.
Assurance of validity of data and models	
Theoretical models Principle FA.17 Theoretical models should adequately represent the facility and site.	The ESBWR complies with FA.17. Models such as TRACG have been approved by the NRC (Reference DCD Chapter 15). In addition, steps are taken to ensure the adequacy of models such as MAAP for PRA applications, as described in NEDO 33210 (Ref. 3), e.g. Sub-section 3.2.3.
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.	The ESBWR complies with FA.18. All models such as TRACG & MAAP used to support fault analysis have been approved for use by the USNRC as part of the 10CFR52 Design Certification process.

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.	The ESBWR complies with FA.19. This is addressed in PSR Sections 2.5 and 2.6 and detailed in DCD Chapters 15 and 19.
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.	The ESBWR complies with FA.20. The development of computer models and associated data sets have been developed, validated and verified in accordance with GEH Quality Assurance Programme (QAP) and addressed in PSR Section 2.9 and DCD Chapter 17. In addition industry validated and verified computer models are also used.
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.	The ESBWR complies with FA.21. PSR Sections 2.5 and 2.6 present the ESBWR Design Basis Analysis and Probabilistic Safety Analysis respectively. Details are presented in DCD Chapters 15 and 19 and Sections 6.2 and 6.3.

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.	The ESBWR complies with FA.22. Sensitivity of DBA results to variations in input conditions is included as part of the qualification of the analysis models, and appropriate conservatisms are used in the analyses. Sensitivity studies are presented in the ESBWR PRA (Ref. 3), Section 11, as referenced from DCD Chapter 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.	Whilst this is a Licensee requirement, it is recognised in the DCD the need for the License Applicant to update the PRA following construction, (DCD Chapter 19).