Health and Safety Executive

HEALTH & SAFETY EXECUTIVE
NUCLEAR DIRECTORATE
ASSESSMENT REPORT

New Build

Step 2 Fault Analysis Assessment of the Westinghouse Submission for the AP1000

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 Westinghouse submission of the Advanced PWR Reactor (APR).

The main conclusion of this report is that the Westinghouse safety documentation is adequate for the 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 – Guidance to Requesting Parties document (GDA), 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 2.

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 Westinghouse's claim 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 Westinghouse Step 2 submission used during this assessment was located at S:\New Reactor Build\RP Submission\Westinghouse Submission – Sep 2007. The submission is entitled, “UK Compliance document for AP1000 Design” (Ref 6).
Within the Westinghouse submission, there is a document (Ref 7) which outlines how the AP1000 design addressed each of the principles in the HSE Safety Assessment Principles for Nuclear Facilities, Ref 8, and includes cross references to the SSER which contained additional discussions on how the SAPs were addressed.

The Westinghouse Safety Case for the AP1000

The following is a summary of the claims made by the Requesting Party (RP, for this report Westinghouse), Westinghouse in relation to the safety of the AP 1000.
The Westinghouse AP1000 design includes advanced passive safety features and extensive plant simplifications to enhance the safety, construction, operation, and maintenance of the plant. The plant design uses proven technology, which builds on over 35 years of operating pressurized water reactor (PWR) experience. PWRs represent 76 percent of all light water reactors in the world and 67 percent of those PWRs are based on Westinghouse PWR technology.

The AP1000 design includes advanced passive safety features and extensive plant simplifications to enhance safety, reliability, construction, operation, maintenance, investment protection, and plant costs.
Major safety advances of the AP1000 design over conventional plant designs include the following:

- AP1000 safety features rely on natural driving forces, such as pressurized gas, gravity flow, natural circulation flow, and convection.
- AP1000 safety features do not use active components, such as pumps, fans, chillers, or diesel generators.
- AP1000 safety features are designed to function without active safety support systems, such as ac power, component cooling water, service water, and HVAC.
- Multiple levels of defence-in-depth provide for accident mitigation; this results in extremely low core damage probabilities.
- A few simple valves align and automatically actuate the passive safety systems. Most of these valves are designed to actuate to their safe positions upon loss of power or upon receipt of a safeguards actuation signal.
- The AP1000 design meets deterministic safety criteria with large margins.
- AP1000 safety features establish and maintain core cooling and containment integrity indefinitely, with no operator action or ac power, following design basis faults.
- AP1000 safety systems contain significantly fewer components, reducing required tests, inspections, and maintenance; their readiness is easily monitored.

The AP1000 passive safety features and other evolutionary developments improve the plant response against the Safety Assessment Principles in many areas compared to

current conventional PWR designs. The AP1000 safety philosophy provides for three levels of protection:

1. Accident resistance
2. Core damage prevention
3. Mitigation

Accident resistance provides plant design characteristics, which reduce the dependence on engineered safeguards systems to achieve safety and protect the utility's investment. The AP1000 plant design minimizes the occurrence and propagation of initiating events, which could lead to larger events and resulting challenges to safeguard systems. Accident resistance requirements include licensing design basis requirements, as well as safety margin basis requirements, to further increase accident resistance.

Thermal and Hydraulic Design

The thermal and hydraulic design of the reactor core provides adequate heat transfer compatible with the heat generation distribution in the core. This provides adequate heat removal by the reactor coolant system, the normal residual heat removal system, or the passive core cooling system.

Design Basis

The classification divides plant conditions into four categories according to anticipated frequency of occurrence and potential radiological consequences to the public. The four categories are as follows:

- Condition I: Normal operation and operational transients
- Condition II: Faults of moderate frequency
- Condition III: Infrequent faults
- Condition IV: Limiting faults

The following performance and safety criteria requirements are established for the thermal and hydraulic design of the fuel. The ability of the fuel to maintain the containment of radioactive fission products at elevated temperatures is an important safety feature of LWR reactors. For the AP1000 these are:

1. Fuel damage (defined as penetration of the fission product barrier; that is, the fuel rod clad) is not expected during normal operation and operational transients (Condition I) or any transient conditions arising from faults of moderate frequency (Condition II). It is not possible, however, to preclude a very small number of rod failures. These are within the capability of the plant cleanup system and are consistent with the plant design bases.
2. The reactor can be brought to a safe state following a Condition III event with only a small fraction of fuel rods damaged (as defined in the above definition), although sufficient fuel damage might occur to preclude resumption of operation without considerable outage time.
3. The reactor can be brought to a safe state and the core can be kept subcritical with acceptable heat transfer geometry following transients arising from Condition IV events.

To satisfy these requirements, the following design bases have been established for the thermal and hydraulic design of the reactor core.

Principal Design Requirements

The mechanical design and physical arrangement of the reactor components, together with the corrective actions of the reactor control, protection, and emergency cooling systems (when applicable) are designed to achieve these criteria, referred to as Principal Design Requirements:

1. Fuel damage, defined as penetration of the fuel cladding, is predicted not to occur during normal operation and anticipated operational transients.
2. Materials used in the fuel assembly and in-core control components are selected to be compatible in a pressurized water reactor environment.
3. For normal operation and anticipated transient conditions, the minimum DNBR calculated using the WRB-2M correlation is greater than or equal to 1.14.
4. Fuel melting will not occur at the overpower limit for Condition I or II events.
5. The maximum fuel rod cladding temperature following a loss-of-coolant accident is calculated to be less than 2200°F (1204°C).
6. For normal operation and anticipated transient conditions, the calculated core average linear power, including densification effects, is less than or equal to 5.718 kw/ft (18.97 kw/m) for the initial fuel cycle.
7. For normal operation and anticipated transient conditions, the calculated total heat flux hot channel factor, FQ, is less than or equal to 2.60 for the initial fuel cycle.
8. Calculated rod worth provide sufficient reactivity to account for the power defect from full power to zero power and provide the required shutdown margin, with allowance for the worst stuck rod.

Severe Accidents

In-vessel retention of molten core debris through water cooling of the external surface of the reactor vessel is a severe accident management feature of the AP1000. During postulated severe accidents, the accident management strategy to flood the reactor cavity with in-containment refueling water storage tank water and submerge the reactor vessel is credited with preventing vessel failure in the AP1000 probabilistic risk assessment. The water cools the external surface of the vessel and prevents molten debris in the lower head from failing the vessel wall and relocating
into containment. Retaining the debris in the reactor vessel protects containment integrity by eliminating the occurrence of ex-vessel severe accident phenomena, such as ex-vessel steam explosion and core-concrete interaction, which have large uncertainties with respect to containment integrity.
The AP1000 provides for in-vessel retention with features that promote external cooling of the reactor vessel:

• The reliable multi-stage reactor coolant system depressurization system results in low stresses on the vessel wall after the pressure is reduced.
• The vessel lower head has no vessel penetrations to provide a failure mode for the vessel other than creep failure of the wall itself.
• The floodable reactor cavity can submerge the vessel above the coolant loop elevation with water intentionally drained from the in-containment refuelling water storage tank.

• The reactor vessel insulation provides an engineered pathway for water-cooling the vessel and for venting steam from the reactor cavity.

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 RPs against its 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 objective of the Step 2 assessment is to identify any fundamental design aspects or safety shortfalls that could prevent the proposed design from being licensed in the UK (Ref. 1). The SAPs relevant to Fault Analysis are contained in the Fault Analysis section i.e. FA. 1 – 22, with some additions.

To confirm that the relevant selection of SAPs covered an adequate set of Fault Analysis SAPs for Step 2 a review of the WENRA reference levels (Ref 11) and IAEA Nuclear Power Plant (NPP) Design Requirements (Ref 12) was undertaken. The results of this review are shown in Annex 1 and it can be seen that the SAPs selected for Step 2 do cover the vast majority of relevant clauses in the referenced documents. The remaining areas will be considered in later steps of the assessment.

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.

Westinghouse 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 Westinghouse claims compliance with the requirements of the relevant SAPs in the area of fault analysis is contained in Annex 3. In all areas Westinghouse claims it will be able to comply. 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 Westinghouse 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 adequate cooling systems to extract reactor core heat under normal and fault conditions SAPs EHT.1 - 4
3. There are two independent shutdown systems SAP ERC.2
4. A comprehensive review of possible initiating faults has been undertaken 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 appear to have been undertaken using approved analytical techniques subjected to quality assurance SAPs FA.18 – 20.

Initiating faults SAP FA.2

Westinghouse has used the standard USNRC reference (10 CFR part 50) for defining the initiating faults that forms the basis of protection requirements. The adequacy of this will need to be established in future assessments.

O1. Confirmation will be required that the RP 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 the RP to conclude that all faults within the design base envelope will not lead to unacceptable consequences. Westinghouse 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 Westinghouse'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 Westinghouse's codes.

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

Transient Analysis SAPs FA.19 & 22

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 modelled 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 reactivity control systems are provided. These are rods (RCCAs and GRCAs), and chemical shim (Boric acid). The RCCAs and GRCAs are inserted into the core by the force of gravity. Both systems can provide shutdown and hold down following xenon decay. However, it is not clear, at this stage what "moderately frequent" reactivity faults the boric acid system could control without breaching designated acceptance limits. The issue is response time: i.e. how fast the boric acid can reach and enter the core and terminate any reactivity transient. Westinghouse 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 approach to the transient analysis appears appropriate and Westinghouse claims to meet the requirements of the HSE's Safety Assessment Principles (SAPs) 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; it is not expected to cause Westinghouse 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 (In-vessel debris retention) SAPs FA.15 & 16

The Risk-Oriented Accident Analysis Methodology (ROAAM) analysis of the in-vessel retention phenomena (References 19.39-1 and 19.39-2 of the Submission Ref 5) provides the basis for the application of the in-vessel retention accident management strategy to the AP600 (lower power variant of the AP1000) passive plant and quantification of vessel failure in the AP600 PRA. The ROAAM included an analysis of the in-vessel melt progression and evaluation of the structural and thermal challenges to the vessel during the relocation to the lower head, including in-vessel steam explosion. Testing and evaluation of the uncertainties associated with the thermal loads produced by the in-vessel circulating molten debris pool, and heat removal limitations due to boiling crisis on the exterior vessel surface were performed. The ROAAM concluded that the limiting challenge to the vessel integrity is the thermal loading produced during the steady-state

heat transfer to the lower head wall after complete debris relocation to the lower plenum. The in-vessel retention ROAAM analyses and testing showed that the water in the AP600 cavity will remove the heat produced by the molten debris bed in the lower head with significant margin while the structural integrity of the lower head was maintained.
In later steps of the assessment we will need to ensure that the AP1000 core can meet all relevant criteria, taking into account possible uncertainties in the process.

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. Westinghouse has supplied sufficient material in relation to the area of fault studies and has made claims that the HSE's Safety Assessment Principles have been met in this area. Detailed assessment in Steps 3 & 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 Westinghouse'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 Westinghouse 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 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 and in-vessel retention philosophy 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 07015
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. Westinghouse AP1000, “UK AP1000 Design Acceptance Application”, UKP-GW-GL-710, Revision 0.
7. Westinghouse AP1000, “UK Compliance Document for AP1000 Design, Section C, Safety Assessment Principles Roadmap for AP1000 Design”, UKP-GW-GL-710, Revision 0, Section C.
8. HSE Safety Assessment Principles for Nuclear Facilities, 2006 Edition.
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		
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.	
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 AP1000 is designed to maintain shutdown conditions even with the most reactive reactor Control assembly withdrawn. As discussed DCD subsection 4.3.1.4.12, the maximum reactivity insertion rate due to withdrawal of RCCAs or gray rod cluster assemblies (GRCAs) or by boron dilution is limited by the AP1000 plant design, hardware, and basic physics. During normal power operation, the maximum controlled reactivity insertion rate is limited. The maximum reactivity change rate for accidental withdrawal of two control banks is set such that peak linear heat rate and the departures from nucleate boiling ratio limitations are not challenged. The maximum reactivity worth of control rods and the maximum rates of reactivity insertion using control rods are limited to preclude rupture of the coolant pressure boundary or disruption of the core internals to a degree that would impair core cooling capacity due to a rod withdrawal or an ejection accident. Following any Condition IV occurrence, such as rod ejection or steam line break, the reactor can be brought to the shutdown condition, and the core maintains acceptable heat transfer geometry. DCD Section 15.4 discusses postulated events resulting in reactivity and power distribution anomalies. Reactivity changes could be caused by control rod motion or ejection, boron concentration changes, or addition of cold water to the reactor coolant system. Power distribution changes could be caused by control rod motion, misalignment, or ejection; or by static means, such as fuel assembly mislocation. Analyses have been performed and are presented in DCD Section 15.4 for the most limiting reactor and power distribution anomalies. In particular, the following incidents are discussed: • Uncontrolled rod cluster control assembly (RCCA) bank withdrawal from a sub critical or low-power start-up condition • Uncontrolled RCCA bank withdrawal at power • RCCA misalignment • Start-up of an inactive reactor coolant pump at an incorrect temperature • A malfunction or failure of the flow controller in a boiling water reactor recirculation loop that results in an increased reactor coolant flow rate (not applicable to the AP1000) • Chemical and volume control system malfunction that results in a decrease in the boron concentration in the reactor coolant • Inadvertent loading and operation of a fuel assembly in an improper position • Spectrum of RCCA ejection accidents The transients listed above previously have been analyzed. It has been determined that the most severe radiological consequences result from the complete rupture of a control rod drive mechanism housing, which is discussed in DCD Section 15.4.8

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 AP1000 design has addressed ERC.2. Two reactivity control systems are provided. These are RCCAs and GRCAs, and chemical shim (Boric acid). The RCCAs and GRCAs are inserted into the core by the force of gravity. During operation, the shutdown rod banks are fully withdrawn. The control rod system automatically maintains a programmed average reactor temperature compensating for reactivity effects associated with scheduled and transient load changes. See DCD Section 4.3 for additional information. The shutdown and control rod banks are designed to provide reactivity margin to shut down the reactor during normal operating conditions and during anticipated operational occurrences, without exceeding specified fuel design limits. The safety analyses assume the most restrictive time in the core operating cycle and that the most reactive control rod cluster assembly is in the fully withdrawn position. See DCD Chapter 15 for summaries of the analyses, assumptions, and results. The safety-related passive systems provide the required boration to establish and maintain safe shutdown condition for the reactor core. See DCD Section 6.3 for additional information.

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. 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.	The AP1000 design has addressed ERC.3. The feedback effect on core reactivity and power for fuel temperature and coolant voiding are negative, thereby contributing to the stability of power generation in the core.
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 AP1000 design has addressed EHT.1. The reactor coolant system transports heat from the reactor core to the steam generators. The reactor coolant flow rate is established by a detailed design procedure supported by operating plant performance data and component hydraulics experimental data. To ensure that adequate flow is always provided to the reactor core, the reactor coolant system flow rate is monitored by the protection and safety monitoring system and a reduction in flowrate will cause a reactor trip. Passive, safety-related systems perform the essential heat transport functions of removing heat from the reactor coolant system, the containment vessel, and the spent fuel pool following a design basis accident or when the normally used active systems are not available. They included the following: • The passive residual heat removal (PRHR) portion of the passive core cooling system consists of a single heat exchanger, which is submerged in the in-containment refueling water storage tank (IRWST) water. The PRHR can receive water from one of the two reactor coolant system hot legs and returns cooled water to the cold leg side channel head of one of the two AP1000 steam generators. The PRHR can remove core decay heat and reduce the reactor coolant system water temperature to cold shutdown conditions by natural circulation, and it is actuated when/if the normal means of heat removal via the steam generators is not available. The PRHR makes use of the IRWST water as a heat sink. The PRHR HX is described in DCD subsection 5.4.14. The PRHR function of the passive core cooling system has been extensively tested and analyzed, and it is described in DCD Section 6.3. • The passive containment cooling system is described in DCD Section 6.2.2. The passive containment cooling system functions to transfer heat from the outside of the containment steel shell using both convective heat transfer to naturally circulating air and evaporation of water to the air. The heated air and water vapour are discharged to the environment. The passive containment cooling system water flow onto the outside of the containment shell is initiated following any postulated event that results in an increase in the containment atmosphere pressure (and temperature). The passive containment cooling system is capable of removing sufficient heat to limit the containment peak pressure following the worst possible design basis accidents (a double-ended guillotine break of a cold leg or main steamline inside containment), and to subsequently reduce and maintain reduced containment pressure. The passive containment cooling system includes sufficient water to perform its function for 3 days with no operator action, and sufficient dependable onsite water is provided to continue heat removal for 4 additional days before supplemental water supplies (onsite or offsite are required). The passive containment cooling system has been extensively tested and conservatively analyzed as part of the safety analysis. The minimum required water volumes for safety-related containment cooling are specified in DCD Section 2.2.2.

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 be stated and justified with reference to the uncertainties in the data and in the calculational methods employed.	The AP1000 design has addressed EHT.2. The reactor coolant system design, including inventories for normal operations, is described in DCD Section 5.1. Design bases accident cooling is provided by the passive core cooling system, which is described in DCD Section 6.2. Design bases analyses that demonstrate the adequacy of cooling flow rates and inventory are described in DCD Chapter 15.
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 AP1000 design has addressed EHT.3. The AP1000 passive containment cooling system provides the safety-related heat sink used to transfer core decay heat (and reactor coolant sensible heat) to the environment following any postulated event, including the loss of the normal active heat sinks. The passive containment cooling system, as described in DCD Section 6.2, contains sufficient stored water for 7 days of operation with no reliance on external resources. After 7 days, additional supplies from offsite may be required to continue the passive containment cooling system function to apply water to the outside surface of the steel containment vessel. However, it is noted that the passive containment cooling system can continue to remove sufficient heat from the containment for an unlimited time by air natural circulation.

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 AP1000 design has addressed EHT.3. Adequate provisions (instrumentation and alarms) to detect significant loss of heat transport fluid before an unsafe state is reached, and inventory makeup provisions are provided where required. Also, appropriate isolation and drain collection capability is provided where postulated leakage would result in equipment damage or a large release of radioactivity. The effects of a failure of a heat transport system pressure boundary, which may propagate through the HVAC systems, have been minimized by segregation of potential high-energy pipe lines (energy sources), the installation of appropriate isolation dampers in HVAC ducting, and the segregation of plant areas and their HVAC systems. Analyses of the dynamic effects of pipe rupture are performed to determine the pressures and temperatures resulting from postulated breaks and to minimize the potential for structural damage. The AP1000 DCD provides a summary of the protection against the dynamic effects associated with postulated pipe ruptures in DCD Section 3.6.
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 AP1000 design has addressed FA.1. AP1000 design basis analyses are presented in DCD Chapter 15. The Probabilistic Risk Assessment and severe accident analyses are presented in DCD Chapter 19.

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 AP1000 design has addressed FA.2. The AP1000 initiating event analysis is described in Chapter 2 of the AP1000 PRA. Identification of the AP1000 internal initiating events is performed by the following tasks: • Evaluation of the initiating events applicable to the AP1000 by reviewing the initiating events reported in NUREG/CR-3862. • Evaluation of the applicability of initiating events considered in PRA and the plant-specific configuration and success criteria • Identification of additional plant-specific initiating events produced by failures or incorrect operation of the front-line or support systems. Following identification of a comprehensive set of initiating events, the events are categorized according to the plant response, possible consequential events, plant systems required, and subsequent plant-related effects. The categorization of initiating events reduces the number of initiating event groups to a manageable size for event trees analysis. Categorizing initiating events is an interactive process with developing the event trees. Event tree interactions ensure that once an event category has been developed, all initiators within the category are bounded by the sequences developed. Event trees model the functions required to maintain the plant in a safe, stable condition.
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 AP1000 design has addressed FA.3. Chapter 4 of the AP1000 PRA discusses fault sequence development. One core damage event tree is constructed for each initiating event category. The entry point of the event tree is the occurrence of an initiating event. The end point of an event tree sequence is either success or core damage. Each event tree describes the plant response to the most representative event in a category. In defining the plant response, credit is taken for safety and nonsafety systems as long as they are realistically expected to respond to the event. Moreover, credit is taken for proceduralized operator actions that are expected to be performed. Event tree top events are termed as nodes. Each node may branch into two or more outcomes (branches). In general, two-fold branching is used. Generally, the lower branches represent less favourable outcomes (for example, failure). A set of continuous branches from the initiating event to the end state defines an event sequence. The event trees define the core damage event sequences. In general, the top sequence in an event tree represents the expected response of the plant to the event. Initially, care is taken to place the event tree nodes in the order they would respond to the event. However, later in modelling, the order of the nodes may be rearranged to simplify the event tree. It is recognized that the event sequences will be quantified by fault tree linking. Thus the definition of plant systems/functions is streamlined to accommodate or expedite the fault tree linking process.
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.).*	AP1000 design has addressed FA.4. A detailed design basis analysis is provided in DCD Chapter 15. The following events are analyzed: Increase in heat removal from the primary system Decrease in heat removal by the secondary system Decrease in reactor coolant system flow rate Reactivity and power distribution anomalies Increase in reactor coolant inventory Decrease in reactor coolant inventory Radioactive release from a subsystem or component
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 AP1000 design has addressed FA.5. DCD Chapter 15 provides these descriptions. Each of the accidents analyzed in the AP1000 has a section titled “Identification of Causes and Accident Description.”

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 AP1000 design has addressed FA.6. DCD Chapter 15 provides a description of the fault sequences.

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 AP1000 design has addressed FA.7. The design basis accident analyses are discussed in DCD Chapter15. For the AP1000 analyses, the NRC identified a list of plant events to be analyzed. The NRC criteria are to apply a bounding approach to include all possible design bases fault consequences. For the AP1000, the NRC requires the ANSI 18.2 standard to be applied. The classification divides plant conditions into four categories according to anticipated frequency of occurrence and potential radiological consequences to the public. The four categories are as follows: • Condition I: Normal operation and operational transients • Condition II: Faults of moderate frequency • Condition III: Infrequent faults • Condition IV: Limiting faults The basic principle applied in relating design requirements to each of the conditions is that the most probable occurrences should yield the least radiological risk, and those extreme situations having the potential for the greatest risk should be those least likely to occur. Where applicable, reactor trip and engineered safeguards functioning are assumed to the extent allowed by considerations, such as the single failure criterion in fulfilling this principle.
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 AP1000 design has addressed FA.8. DCD Chapter 15 provides the design basis accident analysis. The design basis accident analyses are based on NRC Regulatory Guide 1.70. This regulatory guide has been used by license reactors both in the United States and internationally for over 40 years.

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.	
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 AP1000 design has addressed FA.10. NRC 10 CFR 52.47 requires that a design-specific PRA be performed to support Design Certification. The AP1000 PRA was done by considering risks due to all initiators and all modes of operations. The AP1000 PRA iterated with the AP1000 plant design to ensure risk insights were considered during the design phase. DCD Chapter 19 discusses the interaction between the design and the PRA.
Principle FA 11 :Validity. PSA should reflect the current design and operation of the facility or site. **Guidance SAP paragraphs 530 -531**	The AP1000 design has addressed FA.11. The AP1000 PRA was used in the Design Certification process to identify important safety insights and assumptions to support certification requirements, such as the reliability assurance program (RAP). The AP1000 PRA iterated with the AP1000 plant design to ensure risk insights were considered during the design phase. DCD Chapter 19 discusses the interaction between the design and the PRA. Duty Holder items identified in DCD Chapter 19 are designed to ensure that site-specific factors are addressed in the PRA once a site is chosen.

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 AP1000 design has addressed FA.12. The AP1000 PRA considers the reactor core as the largest source of radioactivity in the AP1000. Thus, the PRA quantifies risk due to initiating events that may challenge the core integrity. The AP1000 initiating event analysis is described in PRA Chapter 2. Identification of the AP1000 internal initiating events is performed by the following tasks: • Evaluation of the initiating events applicable to the AP1000 by reviewing the initiating events reported in NUREG/CR-3862. • Evaluation of the applicability of initiating events considered in past PRAs and the plant-specific configuration and success criteria • Identification of additional plant-specific initiating events produced by failures or incorrect operation of the front-line or support systems Following identification of a comprehensive set of initiating events, the events are categorized according to the plant response, possible consequential events, plant systems required, and subsequent plant-related effects. The categorization of initiating events reduces the number of initiating event groups to a manageable size for event trees analysis. Categorizing initiating events is an interactive process with developing the event trees. Event tree interactions ensure that once n event category has been developed, all initiators within the category are bounded by the consequences developed. Event trees model the functions required to maintain the plant in a safe, stable condition.
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 AP1000 design has addressed FA.13. NRC 10 CFR 52.47 requires that a design-specific PRA be performed to support Design Certification. The AP1000 PRA was performed by considering risks due to all initiators and all modes of operations. The PRA iterated with the AP1000 plant design to ensure risk insights were considered during the design phase. DCD Chapter 19 discusses the interaction between the design and the PRA. Duty Holder items identified in DCD Chapter 19 are designed to ensure that site-specific factors are addressed in the PRA once a site is chosen. The scope of the PRA accounts for contributions to the risk due to the following: • Random individual component failures • Components which are failed as a result of the initiating fault; • Common cause failures (and, as necessary, other dependent and consequential failures) • Unavailability due to testing and maintenance • Human errors Discussion of the scope of the PRA is throughout the PRA report, but specifically in the system notebooks, PRAs Chapters 8 through 28. Generic data sources have been used because plant-specific operational experience does not exist. However, a consistent approach to the use of generic data is discussed in PRA Chapter 32. The methodology for the human reliability analysis is documented in PRA Chapter 30.

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 AP1000 design has addressed FA.14. NRC 10 CFR 52.47 requires that a design-specific PRA be performed to support Design Certification. The AP1000 PRA was done by considering risks due to all initiators and all modes of operations. The AP1000 PRA iterated with the AP1000 plant design to ensure risk insights were considered during the design phase. AP1000 DCD Chapter 19 discusses the interaction between the design and the PRA. Duty Holder items identified in DCD Chapter 19 is designed to ensure that site-specific factors are addressed in the PRA once a site is chosen. The AP1000 Design Reliability Assurance Program (D-RAP) is implemented as an integral part of the AP1000 design process to provide confidence that reliability is designed into the plant and that the important reliability assumptions made as part of the AP1000 PRA will remain valid throughout plant life. The PRA quantifies plant response to a spectrum of initiating events to demonstrate the low probability of core damage and resultant risk to the public. PRA input includes specific values for the reliability of the various structures, systems, and components in the plant that are used to respond to postulated initiating events.
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 AP1000 design has addressed FA.15. A containment event tree displays the characteristics of the severe accident progression that impact the fission-product source term to the environment. It is used to provide the likelihood, magnitude, and timing of the possible accident progressions and the fission-product releases to the environment for each of the AP1000 accident classes. The containment event tree is a tool that provides a logical and practical structure for uniting the complex phenomenology of postulated severe accident event sequences. The event tree approach allows the analyst to determine the likelihood of a particular event sequence progression. This approach also permits evaluation of the impact of uncertainty of the event progression on the overall results and conclusions of the study. The treatment of severe accidents provided by the containment event tree provides assurance that important contributors to fission-product release are identified and evaluated in a structured and disciplined approach. The bases for the top events (or nodes) on the tree are supported by analyses, evaluations and testing, empirical data from past studies, and by the AP1000 design. A containment event tree has been developed for the AP1000 PRA at-power events and, it is documented in PRA Chapter 35. Containment release category frequencies are quantified and documented in PRA Chapter 43.

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 AP1000 design has addressed FA.16. A Severe Accident Mitigation Design Alternatives (SAMDA) evaluation documented in AP1000 DCD Chapter 1, Appendix 1B was performed to evaluate whether or not the safety benefit of the SAMDA outweighs the costs of incorporating the SAMDA in the plant. The SAMDA was conducted in accordance with applicable regulatory requirements as identified below. The AP1000 PRA was used to determine the safety benefit of the SAMDAs.
Assurance of validity of data and models	
Theoretical models Principle FA.17 Theoretical models should adequately represent the facility and site.	The AP1000 design has addressed FA.17. The AP1000 PRA Appendix A discusses the thermal-hydraulic analyses to support PRA success criteria. Included is a discussion of the software (such as MAAP and WCOBRA/TRAC) and the software models used for the thermal-hydraulic analyses.

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 AP1000 design has addressed FA.18. For AP1000, an extensive range of activities were completed as part of the design and the Design Certification activities to provide confidence in the design capabilities and reliability of the plant systems and equipment. Special attention was given to the safety-related, passive systems and their associated operating processes. These activities included the following: • Incorporation of operational experience (DCD Sections 1.9 and 3.1, and DCD Appendix 1A) • Conservative system design (DCD Sections 6.2, 6.3, and 6.4, and DCD Chapters 7 and 8) • Conservative design basis T/H analysis (DCD Section 15.0) • T/H analysis to support PRA success criteria (PRA Chapter 6 and PRA Appendix A) • PRAs, including importance and sensitivity studies (PRA Chapter 50) Conservative equipment and component design (DCD Chapter 3 and Section 3.11; ASME codes; ANS standards) • AP1000 plant, system, and equipment testing (DCD Section 1.5) • Emergency response guidelines thermal-hydraulic analysis • Plant pre-operational and in-service inspection and testing (DCD Sections 3.9.6, 5.2, 6.6, 16.1, 16.2, and 16.3) For the AP1000, extensive activities were completed as part of the Design Certification process to provide confidence in the design capabilities and reliability of the safety-related passive features. To specifically address the multiple-failure accident scenarios that are considered in the PRA, numerous analyses were performed, as documented in the following three reports: 1. PRA success criteria analyses in PRA Appendix A 2. Benchmarking of MAAP4 to NOTRUMP in Westinghouse Topical Report WCAP-14869 3. Thermal-hydraulic uncertainty evaluation in Westinghouse Topical Report WCAP-14800
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 AP1000 design has addressed FA.19. PRA Chapter 32 summarizes the reliability data used in the AP1000 PRA. Data from the URD is used where available. This database is specifically constructed for the advanced light water reactor passive plant; however, the data is primarily based on existing operating plant data. Westinghouse reviewed the data for applicability to the AP1000 plant. The components in the AP1000 plant are similar to, and are assumed to operate under similar conditions, as those in existing operating plants. Therefore, the data from the URD is applicable for AP1000. An uncertainty analysis was performed and documented in PRA Chapter 51. The core damage frequency cutset files were already obtained in the plant core damage frequency analysis. For the basic events and initiating event frequencies, core damage calculations are originally given in mean values for each basic event. An uncertainty analysis was performed for those basic events that show up in the core damage output files.

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 AP1000 design has addressed FA.20. The Westinghouse Quality Management System (QMS) was developed in accordance with Appendix B to 10 CFR Part 50. Analyses completed in support of the AP1000 design were performed and documented in accordance with the Westinghouse QMS.
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 AP1000 design has addressed FA.21. The AP1000 design basis accident analyses are summarized in AP1000 DCD Chapter 15. The AP1000 PRA is summarized in DCD Chapter 19. Further detail of the AP1000 PRA analyses is provided in the AP1000 PRA report.
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 AP1000 design has addressed FA.22. PRA Chapter 50 provides documentation of the PRA Sensitivity Studies. These analyses are chosen among numerous potential candidates to address the following issues: • Importance of individual basic events in their effect on plant core damage frequency • Importance of safety and non-safety systems in maintaining current plant core damage frequency • Importance of containment safeguards systems in maintaining current severe release frequency • Effect of human reliabilities as a group on plant core damage frequency • Special issues
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.	The AP1000 design does not address FA.23. This is in the Duty Holder scope.