

**HEALTH & SAFETY EXECUTIVE  
NUCLEAR DIRECTORATE  
ASSESSMENT REPORT**

**New Build**

**Step 2 Fault Analysis Assessment of AECL Submission for the ACR1000**

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 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 AECL submission of the Advanced Candu Reactor 1000 (ACR-1000).

The main conclusion of this report is that the AECL 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 (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 in 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 would lead to the issuing of the Design Acceptance Confirmation referred to above.

The objective of this report is therefore to assess AECL’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 AECL Step 2 submission used during this assessment was located at S:\New Reactor Build\RP Submission\AECL Submission – Sep 2007 (Ref 6). Within the submission AECL supplied the document, “Preliminary Review of ACR-1000 Compliance with 2006 UK Safety Assessment Principles”, which presented a discussion on how the ACR-1000 design addressed the HSE Safety Assessment Principles for Nuclear Facilities, (SAPs) Ref 7.

### Stability under normal operation

The ACR-1000 core design is inherently stable against rapid spatial flux/power oscillations by virtue of the relatively small core size, and of the fuel bundle design, namely fuel enrichment, lattice pitch and material distribution. These are such that the neutron migration length is relatively small, resulting in a tightly coupled core. Important reactor core characteristics are:

- a) The temperature, power and core void coefficients of reactivity are all negative for the ACR. This means that the reactor behaviour is stable for minor deviations in temperature, power or coolant density requiring fewer interventions by the operator. For larger deviations caused by fault situations leading to reactor temperature and power increases and possibly coolant voiding, the resulting negative feedback process help to control the severity of the fault. For example, an increase in power also tends to increase the core void and the fuel temperature. This leads to reduced reactivity, which assists by reducing the rate of increase of the power, void and fuel temperature back to their original values.
- b) In normal operation, the reactor power is steady, or changing in a controlled fashion and the coolant flow is stable. Any fluctuations in power and flow are of small amplitude, and therefore the coolant temperature does not change significantly. CANDU reactors have a long history of good operational performance, and ACR-1000 is designed to meet or exceed this performance. Abnormal transients, such as a turbine trip, reactor trip, or loss of electrical power to one or more heat transport pumps, are taken into account in the loading cycle calculations.
- c) The small coolant density coefficient of reactivity in ACR-1000 means that the reactivity transient resulting from cold water injection into the core would be modest.
- d) The design requirements on the zone-control absorber rods include spatial flux-shape control - the rods automatically adjust their positions in a hunting mode to eliminate zonal flux tilts.
- e) The power coefficient of the ACR-1000 core is negative, and hence any overpower transient will be self-damping.

### **Successful outcomes from various fault scenarios**

The ACR-1000 systematic review of plant design identifies the scenarios or mechanisms that may lead to the occurrence of initiating events that could lead to a radiological hazard and therefore require assessment. A comprehensive list of initiating events is provided and the events are grouped by their bounding effects. For each initiating event, the progression of the fault is modelled, using purpose built computer codes where necessary, including modelling the response of protection systems and operator action where appropriate.

The analysis:

- a) Incorporates sufficient margins in the analysis assumptions to off-set uncertainties associated with plant performance, operational measurements, and plant and accident modelling;
- b) Applies the single failure criterion to all safety systems;
- c) Accounts for consequential failures that may occur as a result of the initiating event;
- d) Credits actions of systems only where the systems are qualified for the accident conditions or when their actions may have a detrimental effect on the consequences of the analysed accident;
- e) Considers the effects of the ageing of components, systems and structures;
- f) Accounts for the possibility of the equipment being taken out of service for maintenance; and
- g) Credits operator actions only when there are:
  - unambiguous indications of the need for such actions,
  - adequate procedures and sufficient time to perform the required actions, and
  - environmental conditions that do not prohibit such actions.

### **Reliable extraction of heat from the core by the post trip cooling systems following various initiating faults**

The ultimate heat sink provides cooling water for the essential service water systems during power generation, normal shutdown and cooldown, and accident conditions. Sea/lake/river water is the ultimate heat sink when Class III and Class IV power supplies are available, and it provides suction to the service water pumps. The heat sinks which transfer heat to the ultimate heat sink include:

- a) The Essential Service Water system,
- b) The Essential Cooling Water system,
- c) The Plant Service Water System,
- d) The Plant Cooling Water System.

The following design bases apply to these heat sinks:

- i) The heat sink is capable of providing a continuous supply of cooling water to permit safe shutdown and cool-down of the plant following an accident.
- ii) The heat sink is a highly reliable source of cooling water capable of performing the safety function required during and after the following postulated design basis events.

## **2.2 Standards and Criteria**

The fault assessment strategy for Step 2 is given in ND DIV 6 Assessment Report AR07015, Ref 3. 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 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). During Step 2 NII will conduct an assessment of the proposed design against those principles in the HSE Safety Assessment Principles for Nuclear Facilities (SAPs) that are deemed relevant to fundamental design aspects. The Safety Assessment Principles for Nuclear Facilities, recently revised and updated in 2006, are used to guide regulatory assessment and decision making. The SAPs relevant to Fault Analysis are contained in the Fault Analysis section ie 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.

AECL supplied a compliance document (Ref 6) to outline how they believe the HSE Safety Assessment Principles will be complied with. The summary as to how AECL claim they will comply with the requirements of the relevant SAPs in the area of fault analysis is contained in Annex 3. In all areas AECL claim they 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 AECL claims the following:

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

### **Initiating faults SAP FA.2**

AECL claim to have identified and taken account of the most limiting faults on the plant. A list of postulated initiating events is provided. The eight categories of initiating events are grouped into AOOs, 2 categories of DBAs, and two categories of BDBAs. The 'Systematic Review of Plant Design for Identification of Initiating Events' will be available at a later stage.

*O1. Confirmation will be required that AECL 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, which have been used by AECL, to conclude that all faults within the design base envelope will not lead to unacceptable consequences. AECL has claimed that those codes and models used have been subjected to a quality assurance program for their use, validation and appropriateness. 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**

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**

The ACR-1000 incorporates two fast-acting, fully capable, diverse, and separate shutdown systems, which are physically and functionally independent of each other. The first system consists of mechanical shutoff rods, which drop into the core when a trip signal de-energises the clutches that hold the shutoff rods out of the core. The design of the shutoff rods is based on proven CANDU 6 design.

The second system injects a concentrated solution of gadolinium nitrate into the low-pressure moderator to quickly render the core subcritical.

AECL claim that all the transients are capable of being controlled by the liquid injection system without any assistance from the control rods.

*O4. Confirmation will be required that the full range of assumed faults can be effectively controlled by the diverse shutdown system acting alone*

## **Operating Limits and Conditions SAP FA.2**

The approach to the transient analysis appears appropriate and AECL claim to meet the requirements of 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 AECL 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**

The severe accident analysis is used to determine measures to further reduce the risk. AECL claim that the severe accident analysis program provides the overall strategy on severe accidents. Beyond Design Basis Accidents (BDBAs) are highly unlikely as a result of engineered safety systems. However, accidents that do progress to severe core damage have a potentially significant impact upon public health and safety. Hence, regulations focus both on prevention and mitigation of consequences of severe accidents.

*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. AECL has supplied HSE with 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 and 4 as outlined in the planning documents, will be to confirm the adequacy of the arguments and evidence.

### **4. RECOMMENDATIONS**

R1. Undertake detailed Fault Analysis assessment of AECL'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 AECL of models, computer codes used in the transient analysis
- pessimising the data used and plant conditions to achieve conservative results
- confirm the range of faults the divers shutdown system can effectively control
- the consistency of operating limits and conditions with those directly derived the fault analysis
- review of the containment scenario following a severe core accident

## 5. REFERENCES

1. HSE. Nuclear Power Station Generic Design Assessment – Guidance to Requesting Parties, Version 2, 16 July 2007.
2. HSE ND DIV 6 Unit 6D Operating Plan, 2 August 2007 – 31 March 2008.
3. HSE ND DIV 6 Assessment Report “Step 2 Fault Studies & PSA Assessment Strategy”, Assessment Report No 07015. HSE, ND– BMS G/AST/001, “Assessment Guidance – Assessment Process”, Issue 002, 28 February 2003.
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. AECL “Preliminary Review of ACR-1000 Compliance with 2006 UK Safety Assessment Principles”, 10820-01321-ASD-008-H, Revision 0, September 2007.
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

<b>SAP Number</b>	<b>SAP Title</b>	<b>Assessed Category</b>	<b>WENRA Ref.</b>	<b>IAEA Ref.</b>
<b>EKP</b>	<b>Key engineering</b>			
EKP.2	Fault tolerance	S2	E2.1	
EKP.3	Defence in depth	S2	E2.1	
<b>ERC –</b>	<b>Reactor Core</b>			
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)
<b>EHT –</b>	<b>Heat Transport systems</b>			
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
<b>FA –</b>	<b>Fault analysis general</b>			
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)
<b>FA –</b>	<b>Design basis analysis</b>			
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		
	<b>PSA</b>		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	
<b>FA –</b>	<b>Severe accident analysis</b>			
FA.15	Fault sequences	S2		5.42 6.5
FA.16	Use of severe accident analysis	LA		
	<b>Theoretical Models</b>			
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		

	<b>Numerical Targets for Fault Analysis</b>			
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 Step2

SAP Number	SAP Title	Assessed Category
<b>EKP</b>	<b>Key engineering</b>	
EKP.2	Fault tolerance	S2
EKP.3	Defence in depth	S2
<b>ERC –</b>	<b>Reactor Core</b>	
ECR.1	Design and Operation of Reactors	S2
ECR.2	Shutdown systems	S2
ECR.3	Stability in normal operation	S2
<b>EHT –</b>	<b>Heat Transport systems</b>	
EHT.1	Design	S2
EHT.2	Coolant inventory and flow	S2
EHT.3	Heat sinks	S2
EHT.4	Failure of heat transport system	S2
<b>FA –</b>	<b>Fault analysis general</b>	
FA.1	Design basis analysis, PSA and severe accident analysis	S2
FA.2	Identification of initiating faults	S2
FA.3	Fault sequences	S2
<b>FA –</b>	<b>Design basis analysis</b>	
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
	<b>PSA</b>	
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
<b>FA –</b>	<b>Severe accident analysis</b>	
FA.15	Fault sequences	S2
FA.16	Use of severe accident analysis	LA
	<b>Theoretical Models</b>	
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 Step2

Assessment Topic/SAP	Assessment
<b>Key engineering</b>	
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.	
<b>Reactor Core</b>	
<p><b>Design and Operation of Reactors</b></p> <p>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.</p> <p>Guidance SAP paragraphs 440 - 443</p> <p>440 The above principle covers normal operation, refuelling, testing and shutdown and design basis fault conditions. The fundamental safety functions are:</p> <ul style="list-style-type: none"> <li>a) control of reactivity (including re-criticality following an event);</li> <li>b) removal of heat from the core;</li> <li>c) confinement or containment of radioactive substances.</li> </ul> <p>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.</p> <p>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.</p> <p>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.</p>	<p>The RP claims that the ACR-1000 core design takes into consideration all operating modes and routine operating manoeuvres including power level changes, refuelling, shutdown and restart. Furthermore, analyses are performed to predict core response under postulated fault conditions to ensure that certain critical parameters are within specific safety limits. They show that the fundamental safety functions are delivered with a degree of confidence such that the safety goals are met.</p> <p>The RP additionally claims that the primary design requirements on the shutdown systems are to ensure safe shutdown when either shutdown system is actuated. Each shutdown system must be capable of inserting negative reactivity at an appropriate rate and have sufficient reactivity depth to maintain a subcritical core state. All design-basis accident events are analyzed to demonstrate that the shutdown systems meet effectiveness criteria and that all safety criteria are met. These criteria cover reactivity control, heat generation and removal, in-core-component temperatures, and ultimately potential radiological doses to the public.</p>
<p><b>Shutdown systems</b></p> <p>Principle ERC.2 At least two diverse systems should be provided for shutting down a civil reactor.</p> <p>Guidance SAP paragraphs 444 – 445</p> <p>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.</p> <p>445 Reactor shutdown and subsequent hold-down should not be inhibited by mechanical failure,</p>	<p>The ACR-1000 incorporates two fast-acting, fully capable, diverse, and separate shutdown systems, which are physically and functionally independent of each other.</p> <p>The first system consists of mechanical shutoff rods, which drop into the core when a trip signal de-energizes the clutches that hold the shutoff rods out of the core. The design of the shutoff rods is based on proven CANDU 6 design.</p> <p>The second system injects a concentrated solution of gadolinium nitrate into the low-pressure moderator to quickly render the core subcritical.</p> <p>In both shutdown systems, the instrumentation to measure each of the parameters is quadrupled and trips the reactor</p>

<p>distortion, erosion, corrosion etc of plant components, or by the physical behaviour of the reactor coolant, under normal operation or design basis fault conditions.</p>	<p>automatically on a two-out-of-four logic basis via computerized shutdown.</p>
<p><b>Stability in normal operation</b></p> <p>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.</p> <p>SAP Guidance paragraphs 446 – 455</p> <p>446 An increase in reactivity or reduction in coolant flow, caused by the unplanned:</p> <ul style="list-style-type: none"> <li>a) movement within the core;</li> <li>b) loss from the core; or</li> <li>c) addition to the core;</li> </ul> <p>of any component, object or substance should be prevented.</p> <p>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:</p> <ul style="list-style-type: none"> <li>a) fuel geometry changes that have an adverse effect on heat transport;</li> <li>b) failure of the primary coolant circuit.</li> </ul> <p><i>Note:</i> Where these mechanisms cannot be prevented by design, protective measures should be available to maintain the plant in a safe condition.</p> <p>448 The structural integrity limits for the core structure and its components (including the fuel) should ensure that their geometry will be suitably maintained.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>452 The design of the core and its components should take account of any identified safety-related factors, including:</p> <ul style="list-style-type: none"> <li>a) irradiation;</li> <li>b) chemical and physical processes;</li> <li>c) static and dynamic mechanical loads;</li> <li>d) thermal distortion;</li> <li>e) thermally-induced stress; and</li> </ul>	<p>The ACR-1000 core design is inherently stable against rapid spatial flux/power oscillations by virtue of the relatively small core size, and of the fuel bundle design and lattice arrangement, namely fuel enrichment, lattice pitch and material distribution are such that the neutron migration length is relatively small, resulting in a tightly coupled core.</p> <p>Important reactor core characteristics are summarised below:</p> <ul style="list-style-type: none"> <li>a) The temperature, power and core void coefficients of reactivity are all negative for ACR. This means that the reactor behaviour is stable. For example, an increase in power also tends to increase the core void and the fuel temperature. This leads to reduced reactivity, which tends to bring the power, void and fuel temperature back to their original values.</li> <li>b) In normal operation, the reactor power is steady, or changing in a controlled fashion, and the coolant flow is stable. Any fluctuations in power and flow are of small amplitude, and therefore the coolant temperature does not change significantly. CANDU reactors have a long history of good operational performance, and ACR-1000 is designed to meet or exceed this performance. Abnormal transients, such as a turbine trip, reactor trip, or loss of electrical power to one or more heat transport pumps, are taken into account in the loading cycles calculations.</li> <li>c) The small coolant density coefficient of reactivity in ACR-1000 means that the reactivity transient resulting from cold water injection into the core would be modest.</li> <li>d) The design requirements on the zone-control absorber rods include spatial flux-shape control - the rods automatically adjust their positions in a hunting mode to eliminate zonal flux tilts.</li> <li>e) The power coefficient of the ACR-1000 core is negative, and hence any overpower transient will be self-damping.</li> </ul>

<p>f) variations in manufacture.</p> <p>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.</p> <p>454 Core components should be mutually compatible and compatible with the remainder of the plant.</p>	
<b>Heat Transport systems</b>	
<p>Design</p> <p>Principle EHT.1 Heat transport systems should be designed so that heat can be removed or added as required.</p> <p>SAP Guidance paragraph 459</p> <p>459 Sufficient capacity should be available to do this at an adequate rate.</p>	<p>The heat sources/loads and their uncertainties are provided in the design description and design manual documents for the relevant heat transport systems. These systems are designed to be capable of adequately removing the heat; i.e., adequate fluid flow rates are provided for heat removal. There is no requirement to provide external heating to the core.</p>
<p>Coolant inventory and flow</p> <p>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.</p> <p>Guidance SAP paragraph 460 – 462</p> <p>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.</p> <p>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.</p> <p>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.</p>	<p>During normal operation and shutdown conditions, the steam generators transfer the residual heat from the heat transport system to turbine condenser. The heat is then transferred to the ultimate heat sink through the condenser cooling water system. In this mode of operation, the feedwater is provided from the deaerator tank by the main feedwater system. In accident conditions, the heat transport system pumps may not be operable, in which case the fuel is cooled by natural circulation, referred to as thermosyphoning. If both the condenser and the main feedwater system are not operable, the water is supplied from other sources, and the residual heat is rejected by discharging steam in steam generators directly to the atmosphere by opening Main Steam Safety Valves (MSSV). If both the condenser and the main feedwater system are not operable, the water is supplied from other sources, and the residual heat is rejected by discharging steam in steam generators directly to the atmosphere by opening Main Steam Safety Valves (MSSV). The water to the steam generators for this operation can be supplied from three different sources:</p> <ul style="list-style-type: none"> <li>. Deaerator tank using auxiliary feedwater pump,</li> <li>. Reserve feedwater tank,</li> <li>. Reserve water tank.</li> </ul>
<p>Heat sinks</p> <p>Principle EHT.3 A suitable and sufficient heat sink should be provided.</p> <p>SAP Guidance paragraph 463</p> <p>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.</p>	<p>The ultimate heat sink provides cooling water for the essential service water systems during power generation, normal shutdown and cooldown, and accident conditions. Sea/lake/river water is the ultimate heat sink when Class III and Class IV power supplies are available, and it provides suction to the service water pumps. The heat sinks which transfer heat to the ultimate heat sink, include:</p> <ol style="list-style-type: none"> <li>a) The Essential Service Water system,</li> <li>b) The Essential Cooling Water system,</li> <li>c) The Plant Service Water System,</li> <li>d) The Plant Cooling Water System.</li> </ol> <p>The following design bases apply to these heat sinks:</p> <ol style="list-style-type: none"> <li>a) The heat sink is capable of providing a continuous supply of cooling water to permit safe shutdown and cooldown of the plant following an accident.</li> <li>b) The heat sink is a highly reliable source of cooling water capable of performing the safety function required during and after the following postulated design basis events:</li> </ol>

	The most severe natural phenomena including the design basis earthquake (DBE).
<p><b>Failure of heat transport system</b></p> <p>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.</p> <p>SAP Guidance paragraph 464 – 466</p> <p>464 Provision should be made to:</p> <ul style="list-style-type: none"> <li>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;</li> <li>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;</li> <li>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.</li> </ul> <p>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.</p> <p>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.</p>	<p>The Advanced CANDU Reactor (ACR) design complies with this principle. CANDU designs apply the ASME code rules for pressure boundary design, and provide for heat transport system failure prevention through overpressure protection equipment and stress analysis. These analyses provide the required feedback to ensure the system design is adequate.</p> <p>Nuclear safety analyses are performed to ensure adequacy of the design with respect to systems and plant behaviour during postulated accidents in ensuring that any releases remain within applicable limits.</p> <p>Changes in geometry of the pressure tubes due to irradiation over time are accommodated by bearings and positioners, and periodic inspections are done that include dimensional measurements of the pressure tubes.</p>
<b>Criticality safety</b>	
<p><b>Safety measures</b></p> <p>Principle ECR.1 Wherever significant amount of fissile materials may be present, there should be a system of safety measures to minimise the likelihood of unplanned criticality.</p> <p>471 The hierarchy of controls set out in the Key engineering principles sub-section (<i>paragraph 135 ff.</i>) is appropriate for criticality safety, and gives preference to minimising the amount of fissile material present, consistent with the process requirements. For non-reactor facilities, the principal means of passive engineering control of criticality should be geometrical constraint. Where</p>	<p>The ACR-1000 plant fully complies with the requirements of ECR 1. As the facility is a nuclear power plant, adequate provisions have been made in the design, monitoring and operating procedures to ensure that unplanned criticality is prevented.</p> <p>The application of this principle to a nuclear power plant is consistent with IAEA guidelines and Canadian practices already met by existing CANDU plants. As the ACR-1000 plant is a nuclear power generating plant, significant effort has been expended on analysis and testing of the NPP core, the core behaviour, the fissile fuel behaviour, and other related items. These analyses have covered a variety of normal and accident conditions.</p>

<p>sub-criticality cannot be maintained through geometrical constraint alone, additional engineered safety measures should be specified, such as fixed neutron absorbers. Reliance on neutron absorbers requires assurance of their continued presence and effectiveness.</p> <p>472 Further safety measures may need to be specified such as:</p> <ul style="list-style-type: none"> <li>a) controlling the mass and isotopic composition of the fissile material present in a nuclear process;</li> <li>b) controlling the concentration of fissile material in solutions; and</li> <li>c) controlling the amount of neutron moderating and reflecting material associated with the fissile material.</li> </ul> <p>473 The design and operation of plant and equipment dealing with fissile material should be such as to facilitate the termination of a criticality incident.</p>	<p>The reactor is supplied with a full complement of instrumentation and systems related to control of the criticality of the reactor. Thus, the possibility of unplanned criticality is remote. During maintenance outages, there is a possibility that some of the control instrumentation and systems may be unavailable. In this event, the reactor is put into the "Guaranteed Shutdown State" (GSS). GSS is achieved by addition of sufficient gadolinium into the heavy water in the calandria to overpoison the moderator. Additionally, the moderator purification system can be disabled to ensure that the gadolinium cannot be inadvertently removed.</p> <p>New Fuel Storage and Handling Design Bases includes a requirement that fuel will be stored and handled in a manner that prevents criticality. Criticality prevention is considered in the handling and storage of new fuel, using techniques such as fuel separation and selected material as neutron absorbers. The Spent Fuel storage system consists of baskets, stacking frames, a manbridge, and miscellaneous manual operated tools that are used to manipulate the fuel and storage baskets from above the bay.</p>
<p>Double contingency approach</p> <p>Principle ECR.2 A criticality safety case should incorporate the double contingency approach.</p> <p>474 The double contingency approach requires that unintended criticality cannot occur unless at least two unlikely, independent concurrent changes in the conditions originally specified as essential to criticality safety have occurred.</p> <p>475 For long-term storage of radioactive waste containing fissile materials, traditional deterministic criticality assessments can lead to very conservative limits on fissile materials. Consideration should be given to a risk-informed approach that balances the risks from an unplanned criticality against other factors, such as the dose accrued as a result of the preparation of waste packages.</p>	<p>The RP claims that they apply the double contingency principle. Section 4.2.2 of ANS-8.1 is adopted for the ACR-1000 nuclear criticality safety. This requirement states: <i>"Process designs should incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible"</i>.</p> <p>Contingency scenarios along the ACR-1000 fuel route that could potentially lead to criticality events are identified in the ACR-1000 nuclear criticality safety evaluation document.</p> <p>The method of selection of credible abnormal conditions for the ACR-1000 nuclear criticality analyses should be documented in the ACR-1000 nuclear criticality safety evaluation report.</p>
<b>Fault analysis general</b>	
<b>General</b>	
<p>Design basis analysis, PSA and severe accident analysis</p> <p>Principle FA.1 Fault analysis should be carried out comprising design basis analysis, suitable and sufficient PSA, and suitable and sufficient severe accident analysis.</p>	<p>The ACR-1000 safety analysis program comprises design basis analysis, suitable and sufficient PSA and sufficient severe accident analysis. Comprehensive safety analyses and safety assessments are carried out to verify that the ACR-1000 design meets safety requirements for the plant.</p> <p><b>Safety Analysis Process</b></p> <p>The safety analysis for the ACR-1000 is approached through a process that includes:</p> <ul style="list-style-type: none"> <li>a) Identifying initiating events;</li> <li>b) Classifying events and identifying bounding event sequences;</li> <li>c) Selecting an appropriate analysis method for each event to be analysed;</li> <li>d) Conducting the analysis; and</li> <li>e) Assessing the results against the acceptance criteria.</li> </ul> <p>The safety analysis deals primarily with radiological hazards. Some non-radiological hazards are identified, such as fires and floods; however, the focus of the analysis is on their impact on reactor safety.</p>
<p>Identification of initiating faults</p>	<p>A systematic review of the plant design is performed as part of the Level 1 PSA to identify</p>

<p>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.</p> <p>SAP Guidance paragraph 504</p> <p>504 The process for identifying faults should be systematic, auditable and comprehensive, and should include:</p> <ul style="list-style-type: none"> <li>a) significant inventories of radioactive material and also radioactive sources that may be lost or damaged;</li> <li>b) planned operating modes and configurations, including shutdown states, decommissioning operations, and any other activities which could present a radiological risk; and</li> <li>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.</li> </ul> <p>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.</p>	<p>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.</p> <p>During normal operation of the ACR-1000 plant various amounts of radioactive materials are present within its systems and structures. It is assumed that any accident scenario must necessarily involve the displacement of radioactive material from its normal location. From the review of radioactive sources to the identification of initiating events and their classification or grouping, the two major developmental steps to be carried out are:</p> <ul style="list-style-type: none"> <li>a) Establishing the set of Internal Events by employing the Master Logic Diagram analysis, and</li> <li>b) Establishing the set of common cause/external events.</li> </ul>
<p>Fault sequences</p> <p>Principle FA.3 Fault sequences should be developed from the initiating faults and their potential consequences analysed.</p> <p>SAP Guidance paragraphs 505 – 510</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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, e.g. 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.)</p> <p>509 The calculated doses should include those arising from the potential release of radioactive material, direct radiation, and criticality incidents.</p> <p>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</p>	<p>The design basis fault sequences for the Advanced CANDU Reactor (ACR) are developed as part of the DBA and PSA.</p> <p>Deterministic safety analysis are performed to determine accident sequences. The internal events PSA covers the evaluation of the accident sequences by performing accident sequence event tree analysis. The event tree reflects system relationship and accident phenomenology that determine whether or not the sequences lead to core damage.</p> <p>The starting point of the event tree is the initiating faults (events) which are internal events occurring within the plant. In the event trees the mitigating systems probabilities are calculated by developing fault tree models for each particular system, which include random failures from components and equipment within the plant, unavailability of components due to routine maintenance, errors due to operator actions and component common cause failures. Initiating events caused by events like internal fire, internal flood and earthquakes are also covered in Level I PSA external event analysis.</p>

(paragraph 623 f.) could be reached.	
<b>Design basis analysis</b>	
<p>Fault tolerance</p> <p>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.</p> <p>SAP Guidance paragraph 513</p> <p>513 If possible, DBA should be carried out as part of the engineering design. Where this is not possible (e.g. 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.).</p>	<p>To demonstrate the engineering design of the plant is robust and that the safety systems are effective, detailed safety analyses of design basis accidents are performed by AECL as part of the design process, consistent with the practice in previous CANDU designs.</p> <p>Consistent with current trends in Canadian nuclear regulations, design basis accidents are events with estimated frequencies higher than 10<sup>-5</sup> per year. In fact, events with frequencies higher than 10<sup>-2</sup> per year are referred to anticipated operational occurrences; the acceptance criteria for these events are more stringent than for design basis accidents.</p>
<p>Initiating Events</p> <p>Principle FA.5 The safety case should list all initiating faults that are included within the design basis analysis of the facility.</p> <p>Guidance SAP paragraph 514, 515</p> <p>514 Initiating faults identified in Principle FA.2 should be considered for inclusion in this list, but the following need not be included:</p> <ul style="list-style-type: none"> <li>a) faults in the facility that have an initiating frequency lower than about 1 x 10<sup>-5</sup> pa;-</li> <li>b) failures of structures, systems or components for which appropriate specific arguments have been made;</li> <li>c) natural hazards that conservatively have a predicted frequency of being exceeded of less than 1 in 10 000 years;</li> <li>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.).</li> </ul> <p>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.</p> <p>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.</p>	<p>A list of all initiating events that are included within the design basis of the Advanced CANDU Reactor (ACR) plant represents the basis for the safety case. This list is developed based on a Systematic Review of the Plant Design for Identification of Initiating Events.</p> <p>The ACR-1000 systematic review of plant design identifies the scenarios or mechanisms that may lead to the occurrence of initiating events that could lead to a radiological hazard and therefore require assessment. A comprehensive list of initiating events is provided and the events are grouped by their bounding effects. A number of sources of information are examined to ensure the completeness of the list of initiating events. These include:</p> <ul style="list-style-type: none"> <li>. Close examination of the design of ACR-1000 systems (all systems containing significant radioactive inventories are considered).</li> <li>. Events listed in IAEA TECDOC 719 and NUREG/CR-5750.</li> <li>. Previous CANDU Safety Analyses.</li> <li>. Past CANDU Operating Experience.</li> </ul>
<p>Fault sequences</p> <p>Principle FA.6 For each initiating fault in the design basis, the relevant design basis fault sequences should be identified.</p> <p>Guidance SAP paragraph 516 - 518</p> <p>516 Correct performance of safety-related and non-safety equipment should not be assumed where this would alleviate the consequences.</p> <p>517 Each design basis fault sequence should include as</p>	<p>The RP claims that for each initiating fault in the design basis, deterministic safety analysis is performed to determine the fault sequences.</p> <p>For each initiating fault in the design basis, deterministic safety analysis is performed to determine the fault sequences. The analysis allows high confidence in demonstrating conformity with the acceptance criteria. To achieve the desirable high confidence, safety analysis:</p> <ol style="list-style-type: none"> <li>1. Are performed by qualified analysts in accordance with a QA process</li> </ol>

<p>appropriate:</p> <ul style="list-style-type: none"> <li>a) failures consequential upon the initiating fault, and failures expected to occur in combination with that initiating fault arising from a common cause;</li> <li>b) single failures in the safety measures in accordance with the single failure criterion;</li> <li>c) the worst normally permitted configuration of equipment outages for maintenance, test or repair;</li> <li>d) the most onerous permitted operating state within the inherent capacity of the facility;</li> </ul> <p>Sequences with very low expected frequencies need not be included in the DBA.</p> <p>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.</p> <p>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.</p> <p>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.</p>	<ul style="list-style-type: none"> <li>2. Apply a systematic analysis method,</li> <li>3. Use verified and validated models and computer codes,</li> <li>4. Use justified assumptions,</li> <li>5. Account for uncertainties in the safety analysis models and inputs,</li> <li>6. Build in a degree of conservatism commensurate with the severity of the analysed event and the associated uncertainties, and</li> <li>7. Be subjected to a review process. The analysis method includes: <ul style="list-style-type: none"> <li>1. Identification of the scenarios to be analysed as required to attain the analysis objectives, including sensitivity analyses;</li> <li>2. Identification of the applicable acceptance criteria and limits;</li> <li>3. Collection of the information that describes the analysed plant and all permissible plant states;</li> <li>4. Defining the assumptions regarding the plant operating state, the availability and performance of the plant systems, and the operators' actions;</li> <li>5. Identification of the important phenomena of the analysed accident transients;</li> <li>6. Selection of the computational methods or computer codes, models, and correlations that have been validated for the intended applications;</li> <li>7. Identification of significant uncertainties associated with plant performance, operational measurements, and plant and accident modelling;</li> <li>8. Preparation of input data for the analysis;</li> <li>9. Conducting calculations predicting the event transient, starting from the initial steady state up to the pre-defined end-state;</li> <li>10. Verification of calculation results for physical and logical consistency; and</li> <li>11. Processing and documenting the calculations results to demonstrate conformance with the acceptance criteria.</li> </ul> </li> </ul> <p>Safety analysis are based on complete and accurate plant design and operational information and supported by experimental data. Assumptions made to simplify the analysis, as well as assumptions concerning the availability and performance of the systems and operators are identified and justified.</p> <p>The analysis:</p> <ul style="list-style-type: none"> <li>a) Incorporates sufficient margins in the analysis assumptions to off-set uncertainties associated with plant performance, operational measurements, and plant and accident modelling;</li> <li>b) Applies the single failure criterion to all safety systems;</li> <li>c) Accounts for consequential failures that may occur as a result of the initiating event;</li> <li>d) Credits actions of systems only where the systems are qualified for the accident conditions or when their actions may have a detrimental effect on the consequences of the analysed accident;</li> <li>e) Considers the effects of the aging of components, systems and structures;</li> <li>f) Account for the possibility of the equipment being taken out of service for maintenance; and</li> <li>g) Credits operator actions only when there are: <ul style="list-style-type: none"> <li>1) unambiguous indications of the need for such actions,</li> <li>2) adequate procedures and sufficient time to perform the required actions, and</li> <li>3) environmental conditions that do not prohibit such actions.</li> </ul> </li> </ul>
<p>Consequences</p> <p>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.</p> <p>Guidance SAP paragraph 521 – 524</p> <p>521 The analysis should demonstrate, so far as is</p>	<p>As for other CANDU designs, the analysis is normally performed using conservative assumptions. The analyses are also performed using tools that are adequately qualified.</p> <p>The ACR-1000 safety analysis requirements are consistent with those that have been applied in analysis of previous CANDU plant designs and they ensure that the analysis is sufficiently conservative to provide adequate confidence that Regulatory limits are met for all design basis events that the plant is adequately safe, and the design is robust.</p>

<p>reasonably practicable, that:</p> <ul style="list-style-type: none"> <li>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;</li> <li>b) there is no release of radioactivity; and</li> <li>c) no person receives a significant dose of radiation.</li> </ul> <p>522 Relocation means the material is no longer in its designated place of residence or confinement.</p> <p>523 Where releases occur, then doses to persons should be limited. The numerical targets for doses to persons are set out in Target 4 (<i>paragraph 599 f.</i>).</p> <p>524 Design basis analysis may also contribute to accident management strategies and emergency plans.</p>	<p>Some of the important requirements that yield conservative results are as follows:</p> <ul style="list-style-type: none"> <li>. The analyst must select the facility operating state which is demonstrably the worst (or "bounding") for each accident to be analysed, or develop some alternative strategy to ensure that all permitted operating states are covered. The analyst must select values of the key plant variables important to safety as initial conditions for the simulation which lead to the worst ("bounding") consequences for the plant state to be considered. Engineered Safety Features (ESF) are simulated assuming performance characteristics at the Minimum Allowable Performance Standard (MAPS) limits, with allowance for uncertainties.</li> <li>. In any particular simulation, only one of the two shutdown systems is credited with shutting down the reactor. This is to demonstrate that either shutdown system, acting alone, is capable of arresting the transient and rendering and maintaining the reactor subcritical.</li> <li>. Normal process and control system response, which may either lessen or worsen the severity of the process upset, is modelled except where such response is disabled by identified common or cross-linked failures.</li> <li>. Uncertainties due to modelling of physical phenomena by the computer codes are handled in one of two ways: the uncertainty can either be inserted into the model as a bias, or an allowance for uncertainty can be added to the calculated result or incorporated into the margin requirement. In the first method, each phenomenon is considered independently, so that the final calculated result is bounding without consideration of the probability of the combined result. In the second method, the uncertainties due to individual effects are combined statistically to obtain an overall uncertainty.</li> </ul>
<p>Linking of initiating faults, fault sequences and safety measures</p> <p>Principle FA.8 DBA should provide a clear and auditable linking of initiating faults, fault sequences and safety measures.</p> <p>Guidance SAP paragraph 525</p> <p>525 The analysis should demonstrate that:</p> <ul style="list-style-type: none"> <li>a) the design basis initiating faults are addressed;</li> <li>b) safety functions have been identified for the design;</li> <li>c) the performance requirements for the safety measures have been identified; and</li> <li>d) suitable and sufficient safety measures are provided.</li> </ul>	<p>Safety analysis documentation provides a clear and auditable linking of initiating faults, fault sequences and safety measures. The safety analysis results are documented to</p> <ul style="list-style-type: none"> <li>a) Describe the technical basis for the analysed event and key phenomena and processes,</li> <li>b) Present information describing the analysis method and assumptions,</li> <li>c) Present analysis results in a way facilitating their understanding and drawing conclusions concerning conformance to the acceptance criteria, and</li> <li>d) Facilitate update of the analysis.</li> </ul> <p>The safety analysis documentation includes:</p> <ul style="list-style-type: none"> <li>a) Safety analysis basis documents describing the assumptions, methodology and acceptance criteria used in the analyses,</li> <li>b) Analysis reports documenting the actual analysis, its results, conclusions and recommendations if applicable,</li> <li>c) Safety analysis data list, which is a compilation of the data used in the various deterministic safety analyses.</li> </ul> <p>A safety analysis report (SAR) is also prepared to provide a comprehensive demonstration of the safety adequacy of the plant. The safety analysis report is an important link between the operating organisation and the regulatory body, since it is one of the main documents which support the operating licence for the reactor.</p>
<p>Further use of DBA</p> <p>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</p> <p>SAP paragraph 526</p> <p>526 DBA should provide the basis for:</p> <ul style="list-style-type: none"> <li>a) safety limits, i.e. the actuator trip settings and performance requirements for safety systems and safety-related equipment;</li> </ul>	<p>The requirements of this principle are satisfied by standard CANDU design, analysis and operating practices. More precisely:</p> <ul style="list-style-type: none"> <li>a) The Safety Design Guide for safety and systems important to safety provides the safety functions and requirements of these systems. Chapter 15 of both the Preliminary and Final Safety Analysis Reports for each CANDU plant provides the trip setpoints for each of the five safety systems (SDS1, SDS2, ECCS, EFWS, and Containment). The data being used in the safety analyses, including trip settings and performance requirements, are documented in the Safety Analysis Data List (SADL). The Minimum Allowable Performance Standards (MAPS) limits for safety systems are a key part of the SADL and are demonstrated to be adequate through detailed assessments of safety system</li> </ul>

<ul style="list-style-type: none"> <li>b) conditions governing permitted plant configurations and the availability of safety systems and safety-related equipment;</li> <li>c) the safe operating envelope defined as operating limits and conditions in the operating rules for the facility; and</li> <li>d) the preparation of the facility operating instructions for implementing the safe operating envelope, and other operating instructions needed to implement the safety measures.</li> </ul>	<p>effectiveness (e.g., trip coverage analysis, dose assessments, ECCS effectiveness).</p> <p>b) The Minimum Allowable Performance Standards (MAPS) limits are provided to the plant operations group for the preparation of the Operating Limits and Conditions. The accident analysis contains a number of assumptions and credits on the process and mitigating systems and on the operator that determine the plant operational limits and operating rules (Safe Operating Envelope or Operating Limits and Conditions).</p> <p>c) Accident analysis also identifies actions that must be taken by the operator to restore the plant to a stable safe condition, which forms the basis for the Emergency Operating Procedures.</p>
<b>PSA</b>	
<p>Principle FA 10 Need for PSA. Suitable and sufficient PSA should be performed as part of the fault analysis and design development and analysis.</p> <p><b>Guidance SAP paragraphs 529</b></p>	
<p>Principle FA 11 :Validity. PSA should reflect the current design and operation of the facility or site.</p> <p><b>Guidance SAP paragraphs 530 -531</b></p>	
<p>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.</p> <p>Guidance SAP paragraphs (none)</p>	
<p>Principle FA 13: Adequate representation. The PSA model should provide an adequate representation of the site and its facilities</p> <p><b>Guidance SAP paragraphs 532 -540</b></p>	
<p>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.</p> <p><b>Guidance SAP paragraphs 541 -542</b></p>	
PSA Related Numerical Targets. NT.1	
<b>Severe accident analysis</b>	
<p>Fault sequences</p> <p>Principle FA.15 Fault sequences beyond the design basis that have the potential to lead to a severe accident should be analysed.</p> <p>Guidance SAP paragraph 545 - 548</p> <p>545 This should include:</p> <ul style="list-style-type: none"> <li>a) determination of the magnitude and characteristics of their radiological consequences, including societal effects; and</li> <li>b) demonstration that there is no sudden escalation of consequences just beyond the design basis.</li> </ul> <p>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.</p> <p>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.</p> <p>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.</p>	<p>The Advanced CANDU Reactor (ACR) Severe Accidents Analysis Program ensures compliance with this principle.</p> <p>The objective of the ACR-1000 Severe Accidents Analysis Program is to explore the consequences of severe beyond design basis accidents. It provides the basis for establishing mitigation measures for severe accident management in order to minimize public risk. The goal of this program is to demonstrate that the risk contribution posed by high-consequence, low-frequency events, which are not considered in normal accident analysis, is acceptable. The analysis will evaluate both probability and consequences of severe accidents, in order to estimate the cumulative frequency of various categories of severe accident events. This information will be used as the basis to identify cost effective design mitigation at an early stage in the project. Codes such as MAAP-CANDU are used to analyse severe accident progression.</p>

<p>Use of severe accident analysis</p> <p>Principle FA.16 The severe accident analysis should be used in the consideration of further risk-reducing measures.</p> <p>Guidance SAP paragraph 549 - 550</p> <p>549 The severe accident analysis should provide information:</p> <ul style="list-style-type: none"> <li>a) to assist in the identification of any further reasonably practicable preventative or mitigating measures beyond those derived from the design basis;</li> <li>b) to form a suitable basis for accident management strategies;</li> <li>c) to support the preparation of emergency plans for the protection of people; and</li> <li>d) to support the PSA of the facility's design and operation.</li> </ul> <p>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.</p>	<p>The severe accident analysis is used in the consideration of further risk-reducing measures.</p> <p>The severe accident analysis is used to determine measures to further reduce the risk. The severe accident analysis program provides the overall strategy on severe accident. Beyond Design Basis Accidents (BDBAs) are highly unlikely as a result of engineered safety systems. However, accidents that do progress to severe core damage have a potentially significant impact upon public health and safety. Hence, regulations focus both on prevention and mitigation of consequences of severe accidents.</p>
<b>Assurance of validity of data and models</b>	
<p>Theoretical models</p> <p>Principle FA.17 Theoretical models should adequately represent the facility and site.</p>	<p>The safety analysis of the design basis events will be performed using detailed models and computer codes that have been adequately validated and verified. Detailed analysis input information for design basis events will be prepared and documented in separate AB reports. The theoretical models used for the ACR-1000 are validated in compliance with the Canadian standard CSA 286.7.</p>
<p>Calculation methods</p> <p>Principle FA.18 Computational methods used for the analyses should adequately represent the physical and chemical processes taking place.</p> <p>Guidance SAP paragraph 552 - 557</p> <p>552 Where possible, the analytical models should be validated by comparison with actual experience, appropriate experiments or tests.</p> <p>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.</p> <p>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.</p> <p>555 Where validation against experiments or tests is not possible, a comparison with other, different, calculational methods may be acceptable.</p> <p>556 Where possible, independent checks using diverse methods or analytical models should be carried out to supplement the original analysis.</p> <p>557 The radiological analysis should include any direct radiation and any inhalation, absorption and ingestion of radioactive material and should also</p>	<p>The computer program development, validation and application at AECL are performed in compliance with the "AECL Quality Assurance Manual for Analytical, Scientific and Design Computer Codes". The current version of this manual has incorporated the CNSC comments and has been made consistent with CSA Standard N286.7 and the CNSC Regulatory Guide, G-149. All validation and verification activities of computer programs used in the safety analysis of Advanced CANDU Reactor (ACR) will be carried out, documented and controlled as per this manual.</p> <p>A number of theoretical computer models are employed in support of the design of CANDU plants over the past decades. The models for the ACR-1000 are based on the traditional CANDU approach. For new ACR-1000 features, systems or components there is a research and development program to validate the assumptions used in the computer models.</p>

<p>take account of the physical and chemical form of the radioactive material released.</p>	
<p>Use of data</p> <p>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.</p> <p>Guidance SAP paragraph 558,559</p> <p>558 Where uncertainty in the data exists, an appropriate safety margin should be provided.</p> <p>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.</p>	<p>The credibility of this safety-related information depends to a great extent on the degree of conservatism incorporated into the safety analysis and on the qualification of the individual safety analysis activities and tools such as computer programs, analysis methods, and input information. Qualification of the data sets used in the analysis is a requirement of the "AECL Quality Assurance Manual for Analytical, Scientific and Design Computer Codes". Preparation of a Safety Analysis Data List (SADL) is a key element of the analysis process. This list is checked by system designers to ensure the accuracy and validity of data. The data used in design and safety analysis will be either the existing valid data or based on specific experimental results. One of the normal practices is that conservative assumptions will be made in the design and related safety analysis to cover any uncertainties including those in available data. Extrapolation from available data will be avoided, or will be done with appropriate justification.</p>
<p>Computer models</p> <p>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.</p> <p>Guidance SAP paragraph 560 - 563</p> <p>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.</p> <p>561 The procedures should, where appropriate, address code and dataset verification, version control, testing, documentation, user training, peer review and endorsement.</p> <p>562 The procedures should specify independent verification of computer codes and datasets to confirm consistency with the supporting documentation.</p> <p>563 The process of inputting data into a model should be independently verified.</p>	<p>Computer models and datasets used in support of the analysis of the ACR-1000 are developed, maintained and applied in accordance with the AECL quality assurance procedures. The computer codes used in the safety analysis of the ACR-1000 are validated, verified, documented, and controlled as per the AECL Quality Assurance Manual for Analytical, Scientific and Design Computer Codes and CSA Standard N286.7. The codes used in the ACR design and safety analysis are qualified for their application. In most cases the codes are already qualified for use in ACR applications. In some cases, the existing analytical codes may need incremental validation for new applications that are specific to the ACR configuration or design parameters. In very few instances, modifications may be required for some codes to address new features of the ACR design. Any modification to an existing computer code or extension to the validation basis meets the requirements of AECL's Software Quality Assurance Program. The ACR program uses the validated Canadian Industry Standard Toolset (IST) of safety analysis codes as a basis to carry out the safety analyses required for reactor licensing. The IST codes are further extended and validated for ACR application as necessary. AECL's Interpretation/Compliance Support</p>
<p>Documentation</p> <p>Principle FA.21 Documentation should be provided to facilitate review of the adequacy of the analytical models and data&gt;</p> <p>Guidance SAP paragraph 564</p> <p>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.</p>	<p>The analytical model and data are fully documented such that it can facilitate the review and allow to be independently reviewed. The analytical model and data are documented in compliance with Canadian standard N286.7 AECL uses formal documents to control the essential information for its scope of activities. The formal documents are controlled to ensure that they are easily retrievable, that they are prepared by personnel having access to the relevant information, that they are available for users, and that only the latest revisions are in use. This document control system is used throughout all life-cycle phases of nuclear facilities. AECL's company-wide sub-tier quality assurance manuals and supporting procedures describe the specific requirements for the preparation, review, approval, issue, and revision of documents.</p>
<p>Sensitivity studies</p>	<p>As per Canadian regulatory documents S-310 and S-294, sensitivity studies are performed.</p>

<p>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.</p> <p>Guidance SAP paragraph 565</p> <p>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.</p>	<p>The regulatory document S-294 requires that sensitivity analysis, uncertainty analysis and importance measures be performed as part of the PSA.</p> <p>Systematic review of the deterministic safety analysis results is also required to ensure that they are correct and meet their initial goal. The results are assessed against the relevant requirements, applicable experimental data, expert judgment, comparison with similar calculations and sensitivity analyses.</p>
<p>Data collection</p> <p>Principle FA.23 Data should be collected throughout the operating life of the facility to check or update the fault analysis</p> <p>565 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.</p>	<p>In Canada, collection of data by the licensee throughout the operating life of the plant is a requirement of the CNSC and is enforced through Regulatory Documents S-99, "Reporting Requirements for Operating Nuclear Power Plants" and S-98 'Reliability Programs For Nuclear Power Plants'. Among the reports required to be submitted to the CNSC are Event Reports and Reliability Reports. These cover 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.</p> <p>AECL will provide support to the Advanced CANDU Reactor (ACR) plant owner/utility, as required to set up these processes consistent with the approach successfully adopted by the Canadian Utilities.</p>