

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

New Build

GDA Phase 1 - Step 2 AECL - ACR1000 Internal Hazard Assessment

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

1. INTRODUCTION

This assessment report records the Step 2 Internal Hazards assessment of the AECL ACR-1000 submission in accordance with the strategy outlined in the Unit 6D operating plan, Ref 2.

Overall, it was concluded that the AECL claims made against the key Internal Hazard Safety Assessment Principles (SAPs) used in Step 2 were reasonable. Supporting arguments and evidence will be required, during Steps 3 & 4, to ensure that the ACR-1000 design complies with the claims and, where reasonably practicable, the full range of Internal Hazard SAPs.

In preparation for Step 3 the assessment made a number of observations which identified further information to be provided by AECL in support of the claims.

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 Internal Hazard 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.

The overall assessment strategy for Step 2 is defined in the Unit 6D Operating Plan, Ref 2, and the specific Internal Hazard assessment strategy for Step 2 is given in ND DIV 6 Assessment Report AR07010, 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 assessment is therefore to consider whether AECL claim that the relevant Internal Hazard 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 the assessment was located at S:\New Reactor Build\RP Submission\AECL Submission – Sep 2007. The submission is entitled, “Safety, Security and Environmental Report” (SSER).

Within the submission, AECL document, “Preliminary Review of ACR-1000 Compliance with 2006 UK Safety Assessment Principles”, Ref 5, presented a discussion on how the ACR-1000 design addressed each of the principles in the HSE Safety Assessment Principles for Nuclear Facilities, Ref 6, and included cross references to the SSER which contained additional discussions on how the SAPs were addressed.

AECL claim that, “...*the ACR-1000 design is in principle compliant with the SAPs requirements*”. In the context of internal hazards, it is noted that the AECL claim covers compliance with all Internal Hazard SAPs.

2.2 Standards and Criteria

The assessment is conducted in accordance with ND BMS procedures, AST/001, AST/002 and AST/003, Refs 7–9 respectively, and informed by the guidance given in the Internal Hazards Technical Assessment Guide (TAG) T/AST/014, Ref 10.

The Internal Hazard assessment strategy for Step 2 is given in ND DIV 6 Assessment Report AR07010, Ref 3. In accordance with this strategy, the hazard SAPs, EHA.1 – EHA.17, Ref 6, were reviewed to identify key Internal Hazard SAPs that were relevant to the Step 2 assessment. To ensure that this selection covered an adequate set of Internal Hazard 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 Internal Hazards assessment strategy, Ref 3, where they are ordered under assessment topics. These key Internal Hazard SAPs were used during the assessment.

2.3 ND Assessment

The definition of Internal Hazards is given in Ref 10, it states that, *“Internal hazards are those hazards to plant and structures such as fire, explosions, release of hazardous materials or gas, flooding etc, which originate within the site boundary, but external to the process in the case of nuclear chemical plant or primary circuit in the case of power reactors”*. This definition was used in the assessment.

The key Internal Hazard assessment topics addressed in the assessment, as identified in the process described above, were:

- **Internal Hazards**
 - Identification
 - Operating Conditions
 - Analysis
 - Sources of Harm
 - Fire Detection and Fighting
 - Use of Material
- **Defence in Depth**
- **Layout**
 - Effects of Incidents
- **Safety Systems**
 - Failure Independence

The overall objective of these principles is to minimise the effects of internal hazards, particularly to ensure that internal hazards do not adversely affect the reliability of safety systems designed to perform essential safety functions and that the potential common cause effects of internal hazards have been adequately addressed. Safety systems and

safety related systems should be either qualified to withstand the effects of internal hazards or protected against the hazards, i.e. appropriate use of equipment qualification, redundancy, diversity, separation or segregation.

In achieving this objective, the principles require that a comprehensive and systematic approach is used to identify the internal hazards and that the hazards are then appropriately combined with consequential and/or simultaneous hazards and/or faults and, where necessary, take into account plant out for maintenance. A “defence in depth” approach should also be applied to internal hazards, for internal hazards that cannot be eliminated the following approach is used:

- Prevent the hazard
- Limit the severity of the hazard should it occur
- Limit the consequence of the hazard should it occur and be severe

The Step 2 assessment considered whether AECL claimed that each key Internal Hazard SAP had been satisfied. The adequacy of any claim will be judged during Steps 3 & 4, where the arguments and supporting evidence will be assessed. The assessment findings against the key Internal Hazard SAPs are presented in tabular form in Appendix 1. A summary, highlighting a number of observations to be considered during Step 3, is given below and should be read in conjunction with Appendix 1.

2.3.1 Internal hazards

AECL claim that the ACR-1000 design has addressed these SAPs, Ref 5.

In the response, Ref 5, AECL claim that all internal hazards have been identified as part of the ACR design development and cross references to the SSER include the following internal hazards: internal flood, missiles, pipe break, fire and explosion. AECL provide limited information on the methodology used to identify the hazards. Consequently, in Step 2, it is not possible to confirm the completeness of the hazard listing.

AECL acknowledged that missiles could arise from rotating machinery. However, the disintegration of a turbine generator had been screened out on the basis of its low probability. This approach is not consistent with recent practice in the UK. Therefore, AECL will need to provide a justification for this approach.

AECL state that the release of toxic gases and corrosive chemicals will be addressed during the site evaluation stage (i.e. GDA Phase 2). This implies that AECL are addressing these hazards from an external hazards point of view which would be dependent on the siting of the power plant. However, there will be sources of these hazardous materials arising within the site boundary (an internal hazard) and they will need to be addressed during Phase 1 and not postponed until Phase 2.

Whilst AECL claim compliance with SAPs EHA.1 & 14, supporting arguments will be required, during Step 3, to justify their claim and in particular the completeness of the hazard listing. The adequacy of the hazard identification methodology used will also need

to be assessed during Step 3 and tested using the additional hazards listed in Appendix 1 – EHA.1 & 14.

O1. *Information will be required on the methodology used to identify internal hazards.*

O2. *Justification will be required for the completeness of the internal hazard listing.*

In claiming compliance with the SAP requirements for the hazard analysis to include appropriate combinations of consequential and independent hazards and/or faults, AECL refer to compliance with the CNSC Regulatory Standard S-310 “Safety Analysis for Nuclear Power Plants”. This standard requires events and event combinations to be identified and analysed for all operating modes of the plant. The standard also requires that the analysis takes account of consequential failures resulting from the events. The definition of events includes “common cause internally initiated events” which is interpreted by AECL to cover internal hazards.

It is noted that in the AECL Safety Design Guide “Fire Protection”, which establishes the fire protection design requirements, it is assumed that, *“Fires need not be postulated to occur concurrently with unlikely non-fire related failures in safety systems, unlikely plant accidents or natural phenomena that would not by themselves cause fires”*.

Whilst AECL claim compliance with EHA.5 & 6, supporting arguments will be required, during Step 3, to justify their claim and in particular that the ACR-1000 design has adequately addressed the hazard combination requirements in EHA.5 & 6.

O3. *Information will be required on the specific combinations of internal hazards and faults included in the internal hazards analysis.*

AECL claim to provide fire detection and fire suppression systems of appropriate capability and reliability. AECL state that, *“In general, the protection of fire safe shutdown systems is to be achieved by passive measures. However, fire suppression systems may be required as part of the defence-in-depth approach”*. It is noted that the design strategy outside the containment structure is to separate the systems important to safety with 3 hour fire barriers using the “Four Quadrant (4Q) Separation Philosophy”. In the containment structure, the design strategy is to use a combination of distance and elevation and make use of walls or partial fire barriers where possible. The AECL claim also referred to a fire hazards analysis which addressed fire prevention, provision of fire barriers and the separation of structures, systems and components important to safety.

It is noted that in the AECL Safety Design Guide “Fire Protection”, there is a statement that, *“The ACR fire protection design with respect to nuclear safety shall be consistent with the IAEA Safety Guide NS-G-1.7 Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants”*. This standard is accepted as a source of relevant good practice.

Whilst AECL claim compliance with SAP EHA.16, supporting arguments will be required, during Step 3, to justify their claim and in particular the adequacy of the fire barriers and any exceptions to the separation philosophy.

O4. Justification will be required for the adequacy of the fire barriers. This should include: a justification of the fire severity and the fire barrier resistance, the designation of an appropriate safety categorisation and safety classification which reflects the barriers role with regard to safety and the measures for the control (i.e. minimisation) and design of penetrations.

O5. Justification will be required for the adequacy of any fire protection systems that are claimed to maintain nuclear safety. This should include the designation of an appropriate safety categorisation and safety classification which reflects the systems role with regard to safety.

O6. Justification will be required for any exceptions to the “Four Quadrant (4Q) Separation Philosophy” of separating the redundant trains of safety-related equipment with fire/hazard barriers.

2.3.2 Defence in Depth

AECL claim that the ACR-1000 design is based on the principle of defence in depth and uses the following levels”:

- Prevention of abnormal operation and failures by design
- Control of abnormal operation and detection of failures
- Control of accidents within the design basis
- Control of severe plant conditions in which the design basis may be exceeded
- Mitigation of radiological consequences of significant releases of radioactive materials

It is noted that AECL statements covering a number of internal hazards imply that the defence in depth philosophy is also applied to the control and mitigation of internal hazards, most notably the fire hazard.

Whilst AECL claim compliance with SAP EKP.3, supporting arguments will be required, during Step 3, to justify their claim and in particular the application of the defence in depth philosophy to all of the internal hazards.

O7. Information will be required on the application of the defence in depth philosophy (prevention, limiting severity and limiting consequences) to internal hazards.

2.3.3 Layout

AECL claim that the effects of internal hazards are minimised and refer to the requirements in AECL Safety Design Guide (SDG) "Separation of Systems and Components", 108-03650-SDG-004-H, Rev 4, June 2006. The objective of the requirements is to ensure that common cause events (including internal hazards) do not impair the ability of structures, systems and components important to safety (SITS) from performing their safety function. The requirements primarily focus on the physical and functional separation of the SITS, employing the separation provisions referred to in 2.3.1 above. The scope of SAP ELO.4 also covers the provisions required to support access for any recovery actions following an event. There is limited discussion relating to any provisions required to support recovery actions following an event. If required, these actions may impose additional layout provisions not addressed in the SDG.

Whilst AECL claim compliance with SAP ELO.4, supporting arguments will be required, during Step 3, to justify the claim that the ACR-1000 design has adequately addressed all of the requirements in SAP ELO.4.

O8. Information will be required on the layout provisions required to facilitate access for any necessary recovery actions following an event.

2.3.4 Safety Systems

One of the requirements in SAP ESS.18 is to ensure that no internal hazard should disable a safety system. AECL claim that the ACR-1000 has been designed such that the safety systems have adequate separation, redundancy, diversity and protection so that following an internal hazard; the required safety functions are assured.

The separation and protection provisions claimed relate to the use of fire barriers and equipment qualification. The adequacy of these provisions is dependent upon the identification of all appropriate internal hazards. The reference to the term "fire barriers" is not fully descriptive as these passive barriers also act as a hazard barrier and will therefore have performance criteria based on the hazard challenge specific to their location, i.e. flood levels, missile impact, overpressure, fire severity, environmental effects etc.

Whilst AECL claim compliance with the internal hazard aspects of SAP ESS.18, supporting arguments will be required, during Step 3, to justify their claim and in particular the adequacy of the hazard barriers. This requirement is linked to the identification of hazards which has been discussed above, and the specification of the hazard challenge to each barrier or the equipment qualification.

O9. Justification will be required for the adequacy of the hazard barriers. This should include a justification of the hazard challenge to the barrier, a justification of the hazard barrier resistance, the designation of an appropriate safety categorisation and safety classification which reflects the barriers role with regard to safety and the measures for the control (i.e. minimisation) and design of penetrations.

2.3.5 General

The scope of the Step 2 assessment is limited to the key Internal Hazard SAPs. During Step 3 the full scope of the internal hazard and related SAPs will be assessed. Consequently, claims and supporting arguments will be required for the following SAPs:

O10. Claims and supporting arguments will be required for the remaining internal hazard and related SAPs, including:

EHA. 3, 4, 7, 10, 13 & 15

EHF.7

ESR.1 & 6

3. CONCLUSION

The Step 2 Internal Hazards assessment of the ACR-1000 was completed. The assessment in Step 2 considered the claims made by AECL against each of the key Internal Hazard SAPs.

It was concluded that AECL had made a claim against each key Internal Hazard SAP and as a consequence had met the assessment requirements of Step 2, Ref 2.

Whilst the claims were judged to be reasonable, supporting arguments and evidence will be required, during Steps 3 and 4, to confirm compliance with the claims and also to justify compliance, where reasonably practicable, with the full range of Internal Hazard SAPs. On that basis, I have no objection to the ACR-1000 proceeding to Step 3.

In preparation for Step 3, the assessment made a number of observations, which identified further information to be provided by AECL in support of the claims.

4. RECOMMENDATION

1. It is recommended that the observations identified throughout the assessment report should be raised with AECL during Step 3.

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 “GDA Phase 1 - Step 2 Internal Hazards Assessment Strategy”, Assessment Report No AR07010.
4. HSE ND – BMS G/AST/001, “Assessment Guidance – Assessment Process”, Issue 002, 28 February 2003.
5. AECL “Preliminary Review of ACR-1000 Compliance with 2006 UK Safety Assessment Principles”, 10820-01321-ASD-008-H, Revision 0, September 2007.
6. HSE Safety Assessment Principles for Nuclear Facilities, 2006 Edition.
7. HSE ND – BMS AST/001, “Assessment - Assessment Process”, Issue 002, 18 February 2003.
8. HSE ND – BMS AST/002, “Assessment - Assessment Activity management”, Issue 003, 16 April 2002.
9. HSE ND – BMS AST/003, “Assessment - Assessment Reporting”, Issue 002, 13 October 2003.
10. HSE ND – BMS, “Technical Assessment Guide – Internal Hazards”, T/AST/014, Issue 001, 24 June 1999.
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.

APPENDIX 1

Assessment of Internal Hazard SAPs Considered During Step 2

Assessment Topic/SAP	Assessment
<p>EXTERNAL AND INTERNAL HAZARDS</p> <p>Identification.</p> <p><i>Principle EHA.1 - External and internal hazards that could affect the safety of the facility should be identified and treated as events that can give rise to possible initiating faults.</i></p> <p><i>Guidance – SAP paragraphs 211-213.</i></p> <p><i>211 This identification should include consequential events and, as appropriate, combinations of consequential events from a common initiating event.</i></p> <p><i>212 Any generic type of hazard with a total frequency that is demonstrably below once in ten million years may be excluded. Any generic type of hazard, the impact of which has no effect on the safety of the facility, can also be excluded. This screening should retain all hazards for which the frequency of realisation and the potential impact might make a significant contribution to the overall risks from the facility.</i></p> <p><i>213 The potential of a hazard to affect the safety of a facility may take account of factors such as the source of the hazard in relation to the facility and the design characteristics of the facility.</i></p>	<p>AECL claim compliance with this principle.</p> <p>AECL state that all internal hazards are identified as part of the design development and included in the design basis assessment. AECL also state that Initiating Events (IEs), which include internal hazards, are identified in the “Systematic Review of the Plant Design” (SRPD) process.</p> <p>The AECL response acknowledges that internal hazards need to be identified and that they are to be treated in the analysis as an initiating event potentially leading to a Design Basis Event (DBE).</p> <p>The adequacy of the supporting argument and evidence in justifying compliance with EHA.1 will need to be assessed during Steps 3 & 4. This assessment will need to consider the adequacy of the internal hazard identification process in identifying all credible internal hazards and also include consideration of the following additional internal hazards:</p> <ul style="list-style-type: none"> • Spray effects from other than pipe failure, i.e. tanks, fire suppression systems, pump mechanical seals etc. • Hazards arising from TG disintegration. • Missile arising from pipe breaks. • Dropped loads. • On-site transport. • Toxic and hazardous substances. • Overpressure from fires.
<p>Operating conditions</p> <p><i>Principle EHA.5 - Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition.</i></p>	<p>AECL claim compliance with this principle.</p> <p>AECL state that compliance is ensured by adopting existing Canadian practice which assumes that the plant is being operated at the outer envelope of permitted operating states and with the minimum allowable plant availability.</p> <p>The adequacy of the supporting argument and evidence in justifying compliance with EHA.5 will need to be assessed during Steps 3 & 4 and also to ensure that the internal hazard analysis has adequately applied the assumptions given in the AECL claim.</p>
<p>Analysis</p> <p><i>Principle EHA.6 - Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects.</i></p> <p><i>Guidance – SAP paragraph 217.</i></p> <p><i>217 To achieve the above two principles the analysis should take into account that:</i></p> <p><i>a) certain internal or external hazards may not be independent of each other and may occur simultaneously or in a combination that it is</i></p>	<p>AECL claim compliance with this principle.</p> <p>AECL state that compliance is ensured by adopting existing Canadian practice and state that the safety analysis will take into account simultaneous effects, common cause failure, defence in depth and consequential effects.</p> <p>The adequacy of the supporting argument and evidence in justifying compliance with EHA.6 will need to be assessed during Steps 3 & 4 and to ensure that the internal hazard analysis has adequately applied the statements made in the AECL claim.</p>

Assessment Topic/SAP	Assessment
<p><i>reasonable to expect;</i></p> <p><i>b) an internal or external hazard may occur simultaneously with a facility fault, or when plant is out for maintenance;</i></p> <p><i>c) there is a significant potential for internal or external hazards to act as initiators of common cause failure, including loss of off-site power and other services;</i></p> <p><i>d) many internal and external hazards have the potential to threaten more than one level of defence in depth at once;</i></p> <p><i>e) internal hazards (e.g. fire) can arise as a consequence of faults internal or external to the site and should be included, therefore, in the relevant fault sequences; and</i></p> <p><i>f) the severity of the effects of the internal or external hazard experienced by the facility may be affected by facility layout, interaction, and building size and shape.</i></p>	
<p>Fire, explosion, missiles, toxic gases etc – sources of harm</p> <p><i>Principle EHA. 14 – Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.</i></p> <p><i>Guidance – SAP paragraph 230.</i></p> <p><i>230 This identification should take into account:</i></p> <p><i>a) projects and planned future developments on and off the site;</i></p> <p><i>b) the adequacy of protection of the nuclear facility from the effects of any incident in an installation, means of transport, pipeline, power supplies, water supplies etc either inside or outside the nuclear site.</i></p> <p><i>c) sources could be either on or off the site;</i></p>	<p>AECL claim compliance with this principle.</p> <p>AECL state that compliance will be ensured by following Canadian practice and refer to the following internal hazards, fire, explosion, missiles, toxic gas release, hydrogen release, pipe failure effects and internal flooding. AECL also refer to the “ACR-1000 Events” document that describes the methodology for identifying internal hazards and confirms the list previously stated. There is no reference to the dropped load hazard referred to in EHA.14.</p> <p>HSE guidance covering the application of EHA.14 is given in SAP paragraph 230. It is noted that this paragraph increases the scope of EHA.14 with reference to incidents arising from on-site transport, on-site pipelines and on-site power and water supplies. AECL’s statement does not make an explicit reference to these potential hazards.</p> <p>Consequently, the adequacy of the supporting argument and evidence in justifying compliance with EHA.14, including the guidance, will need to be assessed during Steps 3 & 4.</p>
<p>Fire, explosion, missiles, toxic gases etc – fire detection and fighting</p> <p><i>Principle EHA. 16 – Fire detection and fire-fighting systems of a capacity and capability commensurate with the credible worst-case scenarios should be provided.</i></p>	<p>AECL claim compliance with this principle.</p> <p>AECL state that compliance is ensured by satisfying the requirements of the ACR-1000 Fire Protection Safety Design Guide (SDG). One of the declared fire protection goals in the SDG is to “minimise the risk of radiological releases to the public, as a consequence of fire.” This is to be achieved by</p>

Assessment Topic/SAP	Assessment
<p><i>Guidance – SAP paragraphs 232-233.</i></p> <p><i>232 The systems should be designed and located so that any damage they may sustain or their spurious operation does not affect the safety of the facility.</i></p> <p><i>233 A fire hazard analysis should be made of the facility to:</i></p> <p><i>a) analyse the potential for fire initiation and growth and the possible consequences on safety systems and other structures, systems and components important to safety;</i></p> <p><i>b) determine the need for segregation of plant and the location and required fire resistance of boundaries to limit the spread of fire; and</i></p> <p><i>c) determine the capacity and capability of the detection and fire-fighting systems to be provided.</i></p>	<p>applying the defence in depth principles of:</p> <ul style="list-style-type: none"> • preventing fires occurring • rapidly detecting, controlling and extinguishing those fires that occur, and • providing design measures to limit the effects of fires on SSCs important to nuclear safety <p>The SDG provides requirements covering the assessment of fire hazards, the preparation of a fire hazards analysis, the provision of fire detection and fire fighting systems and the physical separation between redundant “Fire Safe Shutdown Systems.”</p> <p>The adequacy of the supporting argument and evidence in justifying compliance with EHA.16 will need to be assessed during Steps 3 & 4, with particular attention to the:</p> <ul style="list-style-type: none"> • Safety categorisation and classification of hazard barriers. • Single failure tolerance of active penetrations in the hazard barriers, where appropriate. • Justification of hazard barrier fire resistance. • Compliance with the relevant good practice established in the IAEA Safety Guide NS-G-1.7 “Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants.”
<p>Fire, explosion, missiles, toxic gases etc – use of material</p> <p><i>Principle EHA.17 - Non-combustible or fire-retardant and heat-resistant materials should be used throughout the facility.</i></p>	<p>AECL claim compliance with this principle.</p> <p>AECL state that compliance is ensured by satisfying the requirements of the ACR-1000 Fire Protection Safety Design Guide, which provides detailed requirements to limit the amount of combustibles. The scope of the requirements includes non-combustible materials to be used for structures and components and the use of flammable liquids and gases.</p> <p>The adequacy of the supporting argument and evidence in justifying compliance with EHA.17 will need to be assessed during Steps 3 & 4, with particular attention to the definition and standards used to determine non-combustibility.</p>
KEY PRINCIPLES	
<p>Defence in depth</p> <p><i>Principle EKP.3 - A nuclear facility should be so designed and operated that defence in depth against potentially significant faults or failures is achieved by the provision of several levels of protection.</i></p> <p><i>Guidance – SAP paragraphs 140-144 & Table 1 (not included)</i></p> <p><i>140 International consensus is that the appropriate strategy for achieving the overall safety objective is through the application of the concept of defence in depth. This should provide a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails.</i></p> <p><i>141 The levels of protection should prevent faults, or if prevention fails should ensure detection, limit the potential consequences and prevent escalation.</i></p>	<p>AECL claim compliance with this principle.</p> <p>AECL state that:</p> <p><i>The defence in depth principle is a basic approach to CANDU nuclear safety. Application of the concept of defence in depth in the design of a plant provides a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails. These levels are:</i></p> <ul style="list-style-type: none"> • <i>Prevention of abnormal operation and failures by design</i> • <i>Control of abnormal operation and detection of failures</i> • <i>Control of accidents within the design basis</i> • <i>Control of severe plant conditions in which the design basis may be exceeded</i> • <i>Mitigation of radiological consequences of significant releases of radioactive materials</i> <p>The defence in depth philosophy can also be applied to internal hazards, that is:</p> <ul style="list-style-type: none"> • Prevent the internal hazard. • Limit the severity of the internal hazard. • Limit the consequences of the internal hazard.

Assessment Topic/SAP	Assessment
<p>142 <i>The concept of defence in depth should be applied so that:</i></p> <p><i>a) deviations from normal operation and failures of structures, systems and components important to safety are prevented;</i></p> <p><i>b) any deviations from normal operation are allowed for by safety margins that enable detection and action that prevents escalation;</i></p> <p><i>c) inherent safety features of the facility, fail-safe design and safety measures are provided to prevent fault conditions that occur from progressing to accidents;</i></p> <p><i>d) additional measures are provided to mitigate the consequences of severe accidents.</i></p> <p>143 <i>Defence in depth is generally applied in five levels. The methodology ensures that if one level fails, it will be compensated for, or corrected by, the subsequent level. The aims for each level of protection are described in detail in IAEA Safety Standard NS-R-1, on which Table 1 is based. It should be noted that Table 1 deals with the application of defence in depth in the design of a facility, and does not deal with other important contributions such as human performance or equipment reliability. These topics are addressed in other sections of the SAPs.</i></p> <p>144 <i>An important aspect of the implementation of defence in depth is the provision of multiple, and as far as possible independent, barriers to the release of radioactive substances to the environment, and to ensure the confinement of radioactive substances at specified locations. The number of barriers will depend on the magnitude of the radiological hazard and the consequences of failure.</i></p>	<p>AECL statements in a number of internal hazard analyses apply this defence in depth philosophy to the control and mitigation of internal hazards, most notably the fire hazard.</p> <p>The adequacy of the supporting argument and evidence in justifying compliance with EKP.3 will need to be assessed during Steps 3 & 4.</p>
<p>LAYOUT</p>	
<p>Minimisation of the effects of incidents</p> <p><i>Principle ELO.4 - The design and layout of the site and its facilities, the plant within a facility and support facilities and services should be such that the effects of incidents are minimised.</i></p> <p><i>Guidance – SAP paragraphs 206-207.</i></p> <p>206 <i>For example, the design and layout should:</i></p> <p><i>a) minimise the direct effects of incidents, particularly internal and external hazards, on structures, systems or components;</i></p> <p><i>b) minimise any interactions between a failed structure, system or component and other</i></p>	<p>AECL claim compliance with this principle.</p> <p>The AECL Safety Design Guide (SDG) covering separation of systems and components describes the philosophy and safety objectives to be applied to the physical and functional separation of Structures Systems and Components Important to Safety (SITS). AECL claim that compliance with the SDG will address the requirements of the principle and its supporting guidance.</p> <p>The adequacy of the supporting argument and evidence in justifying compliance with EHA.ELO.4 will need to be assessed during Steps 3 & 4.</p>

Assessment Topic/SAP	Assessment
<p><i>safety-related structures, systems or components;</i></p> <p><i>c) ensure site personnel are physically protected from direct or indirect effects of incidents;</i></p> <p><i>d) facilitate access for necessary recovery actions following an event.</i></p> <p><i>207 Support facilities and services important to the safe operation of the nuclear facility should be designed and routed so that, in the event of incidents, sufficient capability to perform their emergency functions will remain. Support facilities and services include access roads, water supplies, fire mains and site communications.</i></p>	
SAFETY SYSTEMS	
<p>Failure Independence</p> <p><i>Principle ESS.18 - No fault, internal or external hazard should disable a safety system.</i></p> <p><i>Guidance – SAP paragraph 352.</i></p> <p><i>352 Safety systems should be physically separate, independent, isolated from other systems, including safety-related systems, and share no equipment or services. There should be adequate segregation between independent parts of the safety system (including pipework and cabling) and also between a safety system and other facility equipment that, in the event of a fault, might jeopardise the safe working of the safety system.</i></p>	<p>AECL claim compliance with this principle.</p> <p>AECL state that the safety systems are fully capable of mitigating all design basis events with due account taken of common cause failures. AECL also state that the safety systems are separated from each other and from the process systems [again] to minimise the possibility of common cause failures. Internal hazards are recognised as a potential common cause.</p> <p>Within the “Plant Design Philosophy” document, AECL state that the ACR 1000 safety systems will comply with CNSC requirements that require separation and independence from each other and from process systems.</p> <p>The adequacy of the supporting argument and evidence in justifying compliance with ESS.18 will need to be assessed during Steps 3 & 4.</p>