

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

New Reactor Build

AECL ACR 1000 STEP 2 C&I Assessment

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

1. INTRODUCTION

1. This assessment report records the Step 2 Control and Instrumentation (C&I) Assessment of the AECL ACR-1000 submission in accordance with the strategy outlined in Ref. 2. 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. With this in mind, a C&I Safety Assessment Principles (SAPs) subset, relevant to fundamental design aspects, was identified (see Ref. 2) and this selection forms the basis of the Step 2 C&I Assessment (see Annex). The main objective of the assessment is to determine whether an adequate claim of compliance exists for these “fundamental” C&I SAPs. The arguments and evidence supporting these SAPs will be assessed during Steps 3 and 4.
2. Within the Annex the assessment is recorded against each SAP and “observations” are identified by bold text. Observations cover further clarifications necessary for the start of Step 3 and technical matters that could develop into Regulatory Issues (RIs) (see Ref. 3).

2. REPORT

3. AECL provided a number of submissions relevant to C&I Assessment. The main submission that describes the C&I is Ref. 4. The C&I provisions described include those that would be expected of a modern nuclear reactor such as:-
 - safety systems (e.g. reactor shutdown systems such as Shutdown System 1 that actuates shut-off rods and Shutdown System 2 that injects a concentrated gadolinium nitrate solution, and reactor core cooling systems such as the Emergency Core Cooling system),
 - plant control and monitoring systems (e.g. the reactor regulating system that controls reactor power),
 - main control room with backup via a secondary control building, and
 - communications systems allowing information transfer both within and external to the plant.
4. An important aspect of the C&I safety demonstration is the classification of systems important to safety and the application of appropriate design standards. The normal practice is that the standards are more onerous for those systems that are more important to safety. In the UK the importance to safety is typically judged by a combination of deterministic (e.g. the function performed by the system such as to shut down the reactor) and probabilistic (the reliability required of the system) criteria.
5. AECL provided a document (Ref 1) that gives a specific response against the HSE SAPs. The response either confirms compliance to the SAP or provides a description of the ACR-1000 provisions. The main C&I SAPs where a direct claim of compliance is not made are ESS.1, 2, 3 and 27. The supporting text for these SAPs can, however, be seen to provide an implicit claim of compliance which will be considered further during Step 3 (see Ref. 2).

6. The main body of the assessment is contained in the Annex of this report. Within the Annex there are a number of observations and these will need to be raised with AECL and a response requested for Step 3 (see above). The main observations to emerge are briefly summarised below:-
- Clarification will be required as to how AECL address, for C&I, categorisation of functions and classification of structures, systems and components (O1. - SAP ECS.1). In particular, alignment of the AECL approach to that defined by the IAEA, SAPs and BS IEC 1226:2005 will need to be determined. Note the AECL approach which uses four categories (i.e. Category A, B, C and D) does not appear to align with UK and IAEA practice. During the familiarization presentations AECL explained that the approach to Programmable Electronic Systems (PESs) is different to the general scheme. From Ref. 5 it can be seen that the scheme for PES uses four function and system classes in accordance with IEC 61513 and IEC 61226. BSI raised reservations on the international version of IEC 61226 and has produced a BS version (i.e. BS IEC 61226:2005) which explains how the international standard should be interpreted in the UK context. Note that if the classification is incorrect, systems could be produced to an inappropriate standard.
 - Clarification should be provided that the selected C&I standards base provides adequate compliance with modern UK national and international C&I nuclear standards (O3. - SAP ECS.3). The standards base appears to be mainly Canadian and US (e.g. Canadian Standard Association (CSA) and US Institute of Electrical and Electronics Engineers (IEEE) standards) some of which might pre-date what would be considered "modern" for C&I. N.B. dates of applicable standards are not always stated by AECL in its Step 2 submissions.
 - Clarification will be required as to the basis of the fail-safe approach (i.e. for C&I equipment) (O4. - SAP ESS.21). For example, AECL will need to explain how it ensures that component failures result in an appropriate system response. Typical protection system practice is to use some form of dynamic trip bus that will fail to a safe state if not continuously stimulated.
 - Clarification is required on the use of probabilistic criteria in the design of the ACR 1000 C&I systems (O3.3 - SAP ECS.3, O5. - SAP EDR.2, O8. - SAP EDR.3 and O10 - SAP ESS.2). A sensitivity study should be carried out to assess whether there is any margin for a lower reliability figure to be adopted for the protection system(s). Note the protection system reliability appears to be 10^{-3} pfd for each of SDS 1 and SDS2 but how these two figures are combined in the PSA requires clarification.
 - Clarification is required that adequate diversity and independence exists both within and across the C&I safety systems (O5. - SAP EDR.2, O6. - SAP ESS.7 and O7. - SAP ERC.2). In particular, AECL should provide a demonstration that SDS 1 and SDS 2 are adequately diverse and independent. This should include a justification of the reliability figures used for each of the protection systems when claimed

independently and in combination. UK research on high reliability computer based C&I systems has shown that there are significant difficulties in justifying such systems.

- Clarification will be required on the approach to the demonstration of the adequacy of computer based systems important to safety. In particular, the identification of production excellence and independent confidence building activities (i.e. as defined in Ref. 8) (O15.1. to O15.4. - SAP ESS.27 and O16 - SAP ESR.5).
7. The design concept of the ACR-1000 C&I reflects Canadian custom and practice, and is largely based on Canadian and American C&I standards (e.g. Canadian Standard Association (CSA) and Institute of Electrical and Electronics Engineers (IEEE) standards) and regulatory requirements. As a result the observations in the Annex largely reflect the difference between UK and Canadian approaches.
 8. With regard to Canadian custom and practice, it is worth noting that, in 1997 HSE published a “four party” report (Ref. 6), which provided a consensus view on the safety case requirements for computer based systems. The Canadian AECB was a party to this report, which identified the common ground between the four regulatory authorities (i.e. from Canada, France, UK and USA). As a result it is expected that many of the issues (e.g. use of independent assessment and approach to commercial off-the shelf systems (COTS)) relevant to the safety demonstration of computer based system will have been addressed by AECL in its submissions to the Canadian Nuclear Safety Commission (i.e. the successor to AECB).
 9. The AECL submissions (Ref. 4) on C&I mainly describe a conceptual design (i.e. specific implementation detail for the C&I systems such as selected platforms is absent). As a result this assessment report is based on the C&I design concept and an approach (i.e. for Steps 3, 4 and Phase 2) will need to be developed for the assessment of the design implementation (i.e. covering the exact C&I systems, platforms, products and components etc. selected for the implementation of the ACR-1000 conceptual design within the UK).
 10. The approach to the design of the C&I systems will need to address computer security and a comprehensive computer security assessment (i.e. covering each of the systems singly and in combination taking into account any connectivity) will need to be submitted by AECL. While this requirement is contained in modern standards such as IEC 61513 (e.g. requirement for an overall security plan) it is raised here because of its importance to the design of modern digital C&I systems within nuclear plant. The production of a comprehensive computer security assessment is a complex task requiring competence in both computer security risk and safety assessment. As a result early production of a computer security assessment plan should ensure that the importance of this topic is fully recognised by AECL.

O18. AECL should submit a comprehensive computer security assessment plan (i.e. covering each of the computer based systems important to safety singly and in combination taking into account any connectivity).

11. This assessment is based on the documented Step 2 submissions and any changes to the document set will need to be subjected to strict configuration control.
12. The approach to be developed for the assessment of Steps 3, 4 and Phase 2 (see above) will need to address whether there are any requirements left for the licence applicant to define and the satisfaction of such requirements.

3. CONCLUSIONS

13. AECL provide adequate claims of compliance for all of the fundamental C&I Step 2 SAPs (see Annex). It is considered that this is an acceptable position for the conclusion of the Step 2 C&I Assessment. The assessment has given rise to a number of observations and these will need to be raised with AECL. These observations should be addressed during Step 3. The AECL submissions describe a C&I design concept (i.e. no information provided on the actual implementation details such as C&I platform). As well as completing the assessment of the C&I design concept during Steps 3 and 4, an approach to the assessment of the C&I design implementation will need to be developed.
14. The design concept of the ACR-1000 C&I reflects Canadian custom and practice, and is largely based on Canadian and American C&I standards (e.g. Canadian Standard Association (CSA) and Institute of Electrical and Electronics Engineers (IEEE) standards) and regulatory requirements. As a result the observations largely reflect the difference between UK and Canadian approaches, such as UK use of international standards (IEC and IAEA), three system classifications (i.e. safety system, safety related system and non-classified), and probabilistic criteria in the design of C&I systems important to safety.

4. RECOMMENDATIONS

- R1. The C&I assessment has not identified any fundamental issues that would prevent AECL from proceeding to Step 3. Therefore, AECL should be allowed to proceed to Step 3.
- R2. The “observations” identified throughout this assessment report by bold text will require an AECL response prior to Step 3.
- R3. Develop an approach (i.e. for Steps 3, 4 and Phase 2) to the assessment of the C&I design implementation (i.e. covering the exact C&I systems, platforms, products and components etc. selected for the implementation of the ACR-1000 conceptual design within the UK).

5. REFERENCES

1. Preliminary Review of ACR-1000 Compliance with 2006 U.K. Safety Assessment Principles - 10820-01321-ASD-008-H
2. Step 2 C&I Assessment Strategy - ND DIV 6 Assessment Report No. AR07002
3. Nuclear Division – Division 6 Unit 6D Operating Plan 2 August 2007 – 31 March 2008
4. AECL ACR-1000 Technical Description – 10820-01371-TED-001 revision 1
5. Categorization of Functions for the Classification of Programmable Electronic Systems (PES) in nuclear safety related applications – AECL Procedure 00-567.1 Rev. 0.
6. Safety Classification of Structures, Systems and Components - 108-03650-SDG-001-H rev. 5
7. List of Codes and Standards for ACR -108-03650-DG-004-H Rev. 0
8. HSE ND Technical Assessment Guide – Computer Based Safety Systems T/AST/046

Annex

Assessment Matrix of C&I SAPs to be considered during Step 2

Assessment Topic/SAP	Assessment
Safety classification and standards	
<p>Safety categorisation</p> <p><i>Principle ECS.1 - The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be categorised based on their significance with regard to safety.</i></p> <p><i>Guidance - SAP paragraphs 149-152 .</i></p> <p>149 A safety categorisation scheme could be determined on the following basis:</p> <ul style="list-style-type: none"> a) <i>Category A – any function that plays a principal role in ensuring nuclear safety.</i> b) <i>Category B – any function that makes a significant contribution to nuclear safety.</i> c) <i>Category C – any other safety function.</i> <p>150 The method for categorising safety functions should take into account:</p> <ul style="list-style-type: none"> a) <i>the consequence of failing to deliver the safety function;</i> b) <i>the extent to which the function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults;</i> c) <i>the potential for a functional failure to initiate a fault or exacerbate the consequences of an existing fault;</i> d) <i>the likelihood that the function will be called upon.</i> <p>151 The categorisation of safety functions should take no account of any redundancy, diversity or independence within the design – these aspects relate to the structures, systems and components required to deliver the safety function.</p> <p>152 The categorisation assigned to each safety function should be used to classify structures, systems and components required to deliver that function.</p>	<p>A claim is made in Ref. 1 section 8.1.2 that AECL comply with this SAP. The compliance statement is reproduced below:-</p> <p><i>“8.1.2 Compliance Statement - The SSCs important to safety (ITS) of the ACR-1000 are categorized based on their safety functions. Appropriate design requirements are then applied individually to the structures, systems, and components, based on the importance of the safety function. The requirements take into account the consequences of the potential failures and the failure frequency.”</i></p> <p>The approach based on the compliance statement in Ref.1 would appear not to categorise functions separately from the systems that implement the functions. Also, there would appear to be only two system categories, namely category A and B. The definition of the categories, as recorded in Ref.1 section 8.1.2, is shown below:-</p> <p><i>“Category A denotes systems and structures that perform a protective function during a DBA or a preventative safety function during the normal operation of the plant, where failure of the function results immediately (in the short term) in an accident with unacceptable consequences in the absence of further protective action by SSCs in this category.”</i></p> <p><i>“Category B denotes systems and structures which failure results in unacceptable consequences in the longer term, after stabilization of the initial transient, or the consequence of failure is less than that of Category A.”</i></p> <p>However, further details of the categorisation scheme can be found in Ref. 4 section 2.1.9.2. From this section it can be seen that four function categories and safety classes are used. The assignment of functions to categories does not appear to align with UK expectations (e.g. as stated in BS IEC 61226:2005 – see below). For example, it is stated that:-</p> <p><i>“Safety Function Category C: Failure of the function results in a DBA that is mitigated by a higher category system, or in a release of radioactive material that exceeds the AOO reference dose limits, or in the loss of the backup for an SSC in a higher category, or in the potential impairment of an SSC in a higher category. Functions of the following types are included in this safety function category:</i></p> <ul style="list-style-type: none"> <i>* Functions performed during AOOs and required to:</i> <ul style="list-style-type: none"> <i>- Control reactor power,</i> <i>- Shutdown the reactor,</i> <i>- Remove decay heat from the fuel,</i> <i>- Maintain a confinement boundary for radioactive materials whose failure would result in a minor release of radioactive materials or where a higher category protective safety function is provided.</i> <i>* Functions to monitor or test systems performing higher category functions during normal plant operation. ...”</i>

	<p>It appears that some of the above functions (e.g. removal of decay heat) would be assigned a higher category in the UK but this will require further clarification. Also, the use of “short term” and “long term” requires further clarification since this might lead to a different categorisation (e.g. moderator liquid poison system) to that used in the UK.</p> <p>It is also noted that in Ref. 4 section 2.1.9.2. it is stated that :-</p> <p><i>Safety requirements applied to SSCs important to safety are defined in terms of Safety Classes, which are assigned based on the Safety Function Category of the SSC:</i></p> <ul style="list-style-type: none"> • <i>Safety Class 1 requirements are applied to SSCs that perform Safety Function Category A functions,</i> • <i>Safety Class 2 requirements are applied to SSCs that perform Safety Function Category B functions,</i> • <i>Safety Class 3 requirements are applied to SSCs that perform Safety Function Category C functions,</i> • <i>Safety Class 4 requirements are applied to SSCs that perform Safety Function Category D functions.</i> <p>During the familiarisation presentations AECL explained that the approach to Programmable Electronic Systems (PESs) is different to the general scheme. From Ref. 5 it can be seen that the scheme for PES uses four function and system classes in accordance with IEC 61513 and IEC 61226. Note that the UK BSI raised reservations on the international version of IEC 61226 and has produced a BS version (i.e. BS IEC 61226:2005) which explains how the international standard should be interpreted in the UK context. Ref.6 table T1 shows the alignment of AECL functions and classes to IEC 61226 requirements.</p> <p>O1 - Clarification will be required as to how AECL address, for C&I, categorisation of functions and how the functional categorisation is used in the classification of structures, systems and components. In particular, AECL should demonstrate how its scheme aligns with the SAPs, IAEA scheme and BS IEC 61226:2005, and define the precise standards applied to each system class.</p>
<p>Safety classification of structures, systems and components</p> <p><i>Principle ECS.2 - Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance with regard to safety.</i></p> <p><i>Guidance - SAP paragraphs 153-156 .</i></p> <p>153 <i>The method for classifying the safety significance of a structure, system or component should primarily be based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgement, with account taken of factors such as:</i></p> <p>a) <i>the category of safety function(s) to be performed by the item (see Principle</i></p>	<p>ECS.2 - A claim is made in Ref. 1 section 8.2.3 that AECL comply with this SAP, namely:-</p> <p><i>“8.2.2 Compliance Statement - The SSCs of the ACR-1000 are categorized based on their safety functions. Appropriate design requirements are then applied individually to the structures, systems, and components, based on the importance of the safety function. This satisfies the intent of the above classification levels.”</i></p> <p>Note that AECL state that the approach satisfies the “intent” of the above classification levels. Also, see above under ECS.1.</p> <p>P153 – see above and under ECS.1.</p>

<p>ECS.1);</p> <ul style="list-style-type: none"> b) <i>the consequences of failure to perform its function;</i> c) <i>the probability that the item will be called upon to perform a safety function;</i> d) <i>the time following any initiating fault at which, or the period throughout which, it will be called upon to operate.</i> <p>154 <i>A safety classification scheme could be determined on the following basis:</i></p> <ul style="list-style-type: none"> a) <i>Class 1 – any structure, system or component that forms a principal means of fulfilling a Category A safety function.</i> b) <i>Class 2 – any structure, system or component that makes a significant contribution to fulfilling a Category A safety function, or forms a principal means of ensuring a Category B safety function.</i> c) <i>Class 3 – any other structure, system or component.</i> <p>155 <i>Appropriately designed interfaces should be provided between structures, systems and components of different classes to ensure that any failure in a lower class item will not propagate to an item of a higher class. Equipment providing the function to prevent the propagation of failures should be assigned to the higher class.</i></p> <p>156 <i>Auxiliary services that support components of a system important to safety should be considered part of that system and should be classified accordingly unless failure does not prejudice successful delivery of the safety function.</i></p>	<p>P154 - The alignment of the AECL scheme, which appears to have four Safety Classes (see above), to the three class scheme outlined in this SAP will need to be assessed during Step 3 (see O.1 above).</p> <p>P155 – Step 3.</p> <p>P156 - Within Ref.1 section 8.2.3 it is stated that :- <i>“Category B denotes systems and structures ... These functions are complementary to those of Category A and include functions that provide support services (power, air, water, lubrication).”</i> O2. - AECL should demonstrate that these complementary functions are implemented in systems of the appropriate class.</p>
<p>Standards</p> <p><i>Principle ECS.3 - Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate standards.</i></p>	<p>Within Ref.1 the compliance statement for ECS.3 includes the text shown below:-</p> <p><i>“8.3.2 Compliance Statement - The SSCs Important to Safety of the Advanced CANDU Reactor (ACR) are designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected according to the AECL formal design documents manual (FDDM), new build CANDU quality assurance manual (QAM), plant performance specifications (PPS), safety design guides (SDGs), analysis basis reports (AB), analysis reports (AR), design control documents (DCD), design descriptions (DD), design guides (DG), design danuals (DM), design requirements (DR), and technical specifications (TS) and examination, maintenance, inspection and testing schedules (EMITS).</i></p> <p><i>Those AECL documents refer to and comply with applicable Canadian nuclear standards set by the Canadian Standard Association (CSA) for the design, manufacturing, construction, installation, commissioning, quality assurance, maintenance, testing and inspection of the SSCs Important to Safety. In addition to the Canadian Standards Association (CSA) codes and standards, appropriate sections of other industrial standards, such as the Instrument Society of America (ISA) standards, Military Standards (MIL) and Institute of Electrical and Electronics Engineers (IEEE) standards are applied as</i></p>

<p>Guidance - SAP paragraphs 157-161</p> <p>157 <i>The standards should reflect the functional reliability requirements of structures, systems and components and be commensurate with their safety classification.</i></p>	<p><i>appropriate to the design of systems, structures, and components. The ACR design will also comply, to the extent applicable, with the requirements outlined in relevant International guides, such as those of the International Atomic Energy Agency (IAEA).</i></p> <p>Within Ref. 4 AECL state:-</p> <p><i>“2.1.9.3 Codes and Standards - The design of the ACR-1000 is compliant with the Canadian Standards Association’s standards for CANDU plants (see Table 2.1-4). International requirements are addressed where applicable. The codes and standards of other jurisdictions can be accommodated, as appropriate and where not in conflict with the codes and standards used in the design of the plant.”</i></p> <p>Table 2.1-4 of Ref. 4 contains a list of Canadian standards including those relevant to the C&I systems. Further, Ref. 7 provides a “List of Codes and standards for ACR” and within this document it is stated :-</p> <p><i>“ .. in addition to listing the mandatory Canadian codes and standards (i.e., required for licensing the plant in Canada), this document also includes a list of other national and international standards that are used in the design of NPPs. ...</i></p> <p><i>These standards can be applied in design, in their entirety or in part, as determined by the designers. This is a design guide and designers have some flexibility in applying its requirements, but overall it is intended to provide consistency in the design of the plant.”</i></p> <p>Within Ref. 7 Table 6.3 lists “Other National and International Codes and Standards” including those relevant to the C&I design (e.g. IEEE 603) but the applicable dates are not provided.</p> <p>In conclusion, it can be seen that the C&I standards base appears to be largely Canadian and US (e.g. IEEE standards and references to ISA requirements) with reference made to relevant IEC standards in Ref. 7. However, the precise set of applicable C&I standards and their dates of issue do not appear to be stated.</p> <p>O3.1. - AECL should clarify the precise set of applicable standards used for the C&I design and their issue date.</p> <p>It is considered that AECL provide a claim of compliance with appropriate standards. There is, however, a need to consider whether the precise set of selected standards are in agreement with modern UK national and international C&I nuclear standards.</p> <p>O3.2. - Clarification should be provided that the selected C&I standards base for C&I systems (e.g. those important to safety) provides adequate compliance with modern UK national and international C&I nuclear standards.</p> <p>P157 - The standards base will require further investigation to confirm the approach to inclusion of reliability requirements. Other than the higher safety class standards being more rigorous than those for lower safety classes there does not appear to be a link to the functional reliability requirements in the identified standards base.</p>
---	---

<p>158 <i>Appropriate national or international codes and standards should be adopted for Classes 1 and 2 of structures, systems and components. For Class 3, appropriate non-nuclear-specific codes and standards may be applied.</i></p> <p>159 <i>Codes and standards should be preferably nuclear-specific codes or standards leading to a conservative design commensurate with the importance of the safety function(s) being performed. The codes and standards should be evaluated to determine their applicability, adequacy and sufficiency and should be supplemented or modified as necessary to a level commensurate with the importance of the safety function(s) being performed.</i></p> <p>160 <i>Where a structure, system or component is required to deliver multiple safety functions, and these can be demonstrated to be delivered independently of one another, codes and standards should be used appropriate to the category of the safety function. Where independence cannot be demonstrated, codes and standards should be appropriate to the class of the structure, system or component (ie in accordance with the highest category of safety function to be delivered). Whenever different codes and standards are used for different aspects of the same structure, system or component, the compatibility between these should be demonstrated.</i></p> <p>161 <i>The combining of different codes and standards for a single aspect of a structure, system or component should be avoided or justified when used. Compatibility between these codes and standards should be demonstrated.</i></p>	<p>O3.3 - AECL should clarify how the standards reflect the functional reliability requirements.</p> <p>P158 - See above</p> <p>P159 - See above</p> <p>P160 - The ACR-1000 C&I systems encompass systems that in the UK and internationally would appear to fall into different classes (e.g. see IAEA Safety Standards Series – Instrumentation and control systems important to safety in nuclear power plants – safety guide NS-G-1.3). Whether or not the combination of safety functions in these system classes allows this SAP guidance to be met requires clarification.</p> <p>O3.4 Clarification is required as to how SAP guidance paragraph 160 is met (e.g. claim of independence or standards appropriate to the highest class).</p> <p>P161 – None identified by AECL. To be addressed in Step 3.</p>
<p>Failure to safety</p>	
<p>Failure to safety</p> <p><i>Principle EDR.1 - Due account should be taken of the need for structures, systems and components important to safety to be designed to be inherently safe or to fail in a safe manner and potential failure modes should be identified, using a formal analysis where appropriate.</i></p>	<p>AECL provide a compliance statement for this SAP within Ref.1 which states “10.1.2 Compliance Statement - The ACR-1000 design and the processes used to perform the design development comply with this Principle.”. AECL also provide a description of some of the fail safe features and an outline of the techniques used to identify failure modes. It is concluded that there is an adequate claim of compliance for this SAP.</p>
<p>Reliability – failsafe approach</p> <p><i>Principle ESS.21 - The design of a safety system should avoid complexity, <u>apply a fail-safe approach and incorporate the means of revealing internal faults from the time of their occurrence.</u></i> <i>Guidance - SAP paragraphs 356</i></p> <p>356 <i>The nature of some systems may be such that it is not possible to reveal all faults until the time of a test, eg in the case of fluid or mechanical systems. In such</i></p>	<p>AECL claim that a failsafe approach is used (see comments under EDR.1 above). Within Ref.1 the compliance statement for this SAP states:-</p> <p><i>“21.21.2 Compliance Statement - Fail-safe design principles are employed in the design wherever practicable. Safety System monitoring provisions are designed with a range of alarm and self-check features to ensure that faults within the safety system are revealed to the operator in a timely manner.”</i></p>

<p>cases, in-service or periodic testing will be the sole means available to support reliability claims for the equipment, see Principle EMT.6 (paragraph 189 f.).</p>	<p>Note that, while the above provides a reasonable claim of compliance, AECL qualify the response by the use of the phrases “wherever practicable” and in a “timely manner”. The impact of these qualifications will need to be assessed during Step 3. Within Ref. 4 there is very little information on this topic (e.g. for SDS1 and 2 a reference to a watchdog trip is made but a similar statement is not evident for other safety systems such as the ECC system).</p> <p>O4. - AECL should explain, for each safety system, the basis of the fail-safe approach (e.g. how it is ensured that safety system failures result in an appropriate response).</p>
<p style="text-align: center;">Defence in depth</p>	
<p>Redundancy, diversity and segregation</p> <p><i>Principle EDR.2 - Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety</i></p>	<p>In response to this SAP AECL state:- <i>10.2.2 Compliance Statement - In CANDU design ... principles of redundancy, diversity, separation, and independence are applied. These principles of diversity, redundancy, and independence are thus applied to the ACR-1000 design”.</i></p> <p>It should be noted that AECL refer to separation and independence as opposed to “segregation” (i.e. the physical separation of components and systems) used in the SAP. In addition to the above, AECL also provide the following statement:-</p> <p><i>10.2.3 AECL’s Interpretation/Compliance Support - In the ACR-1000 design as stated in Reference [16], the essential safety functions (Control, Cool, Contain and Monitor) are generally provided by at least two redundant systems or subsystems, and the trip signals to actuate these systems are provided by three or four redundant instrumentation channels that feed redundant actuation logic circuitry. Independence must be ensured between redundant systems and between redundant parts of a system. However, it should be noted that independence cannot be absolute, as many systems have to be in the same building, and they have to communicate with each other and with the operator. Basically any two systems or system divisions or redundant components within a division carrying out the same function and treated as being independent in safety analyses or Probabilistic Safety Assessments (PSA), need to be separated.</i></p> <p>While AECL provide a claim that this SAP is addressed in the design of the ACR-1000 the <u>approach to segregation will need particular consideration during the Step 3 assessment.</u></p> <p>From review of Ref. 4 it can be seen that AECL do employ redundancy and diversity in the design of the C&I systems, for example, through the provision of two diverse shutdown systems i.e. Shutdown System (SDS) 1 and 2 (the extent of this diversity will need investigation during Step 3 – see ERC.2 below).</p> <p>Also, within Ref.1 section 10.2.3 it is stated:- <i>One of the dependent failures that affect multiple system functions engineered for accident mitigation is the “cross-link” failure mechanism, propagated through system dependencies. There are other types of dependent failures that may appear in equipment design, manufacture, operation and maintenance practices.</i></p>

<p>Guidance - SAP paragraph 170</p> <p>170 <i>It should be demonstrated that the required level of reliability for their intended safety function has been achieved.</i></p>	<p>Assessment of the “cross-link” failure mechanisms will be required during Step 3 since this appears to be a means of defeating the measures put in place to satisfy this SAP.</p> <p>O5.1 - AECL should explain what has been done to analyse The potential for dependent failures such as “cross-link” failure.</p> <p>P170 - Four system classes have been identified (see above) but it is not clear how reliability figures are used in the design of the ACR 1000 C&I systems nor how achievement is demonstrated (see also O3.3 above). Note the protection system reliability appears to be 10-3 pfd for each of SDS 1 and SDS2 but how these two figures are combined in the PSA requires clarification</p> <p>O5.2 Clarification is required on the use of probabilistic criteria in the design of the ACR-1000 C&I systems and how achievement of such criteria is demonstrated.</p> <p>O5.3 A sensitivity study should be carried out to assess whether there is any margin for a lower reliability figure to be adopted for the protection system.</p>
<p>Determination of safety system requirements – Defence in depth</p> <p><i>Principle ESS.2 - The extent of safety system provisions, their functions, levels of protection necessary to achieve defence in depth and required reliabilities should be determined.</i></p> <p>Guidance - SAP paragraph 337</p> <p>337 <i>The design basis (Principles FA.4 (paragraph 512 f.) and FA.9 (paragraph 525 f.)) and probabilistic safety (Principle FA.14 (paragraph 540 f.)) analyses (or other suitable analyses) should determine the safety system provisions, functions and required reliabilities.</i></p>	<p>AECL’s response to this SAP in Ref.1 claims that a defence in depth approach has been taken in the design of the ACR-1000. AECL also explain that the systems provided which contribute to defence in depth include the Safety Systems (i.e. Shutdown System No. 1, Shutdown System No. 2, Emergency Core Cooling, Emergency Feed Water and Containment systems) and the Safety Support Systems. See also, comments under EDR.2 above.</p>
<p>Diversity in the detection of fault sequences</p> <p><i>Principle ESS.7 - The protection system should employ diversity in the detection of fault sequences, preferably by the use of different variables, and in the initiation of the safety system action to terminate the sequences.</i></p> <p>Guidance - SAP paragraph 342</p> <p>342 <i>This principle applies in particular to UK civil nuclear power reactor safety systems and in particular to high integrity safety systems.</i></p>	<p>AECL provide the following compliance statement within Ref.1:-</p> <p><i>“21.7.2 Compliance Statement - The shutdown systems of the Advanced CANDU Reactor (ACR) are designed such that there are diverse trip parameters for each design basis event (fault) sequence. The ECC system is initiated upon receipt of a LOCA signal, which occurs when heat transport system pressure falls below a specified setpoint. The containment isolation function automatically closes all penetrations open to the reactor building atmosphere when an increase in either containment pressure or radioactivity level is detected.”</i></p> <p>From the above it appears that the combination of the shutdown systems is claimed to meet this SAP. However, the precise means (e.g. use of diverse variables) by which the protection systems meet this SAP will require further clarification since it appears that different variables are not used within each protection system. Further, within Ref. 4 (section 7.2), it is stated that the actual parameters used for</p>

	<p>SDS1 and SDS 2 trips will be defined as detailed design progresses. Also, during the familiarisation presentation on 25/26 October 2007 AECL stated that it was not a requirement to have diverse parameters for the detection of each fault sequence.</p> <p>O6.1. - AECL should explain the precise means by which it is ensured that SAP ESS.7 is met (e.g. for each protection system, whether diversity is used in the detection of fault sequences (preferably by the use of different variables), and in the initiation of the safety system action to terminate the sequences).</p> <p>It is not claimed that the ECC system meets this SAP, rather it is explained that the system meets its reliability requirements (see Ref.1 section 21.7.3). Whether or not this function is required to be “high integrity” and falls under the requirements of this SAP (see SAP paragraph 342) will require assessment during Step 3.</p> <p>O6.2. - AECL should clarify the extent of diversity used in the ECC system (e.g. diversity in the detection of fault sequences preferably by the use of different variables – see SAP ESS.7).</p> <p>For the containment system it is noted that the containment pressure and radioactivity levels provide “<i>diverse and direct indications of the range of event sequences that may require containment isolation</i>”.</p> <p>Further assessment will be required during Step 3 to confirm whether the approach to compliance with this SAP is acceptable (e.g. given the integrity requirements of the individual systems).</p>
<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>352 <i>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 provide the following compliance statement in Ref.1:-</p> <p><i>“21.18.2 Compliance Statement - The ACR-1000 design complies fully with this principle. The safety systems in the ACR-1000 design are fully capable of mitigating all design basis events with due account taken of common cause failures.”</i></p> <p>Note also that AECL state (Ref. 1): <i>“21.1.2 Compliance Statement - As in the case of all CANDU designs, the Advanced CANDU Reactor (ACR) is provided with two fast acting, fully capable, diverse and separate shutdown systems which are physically and operationally independent of each other and from the reactor regulating system...”</i></p> <p>Hence, failures of the reactor regulating system (control) do not cause failure of the protection systems.</p> <p>AECL’s compliance statement is considered to provide an adequate claim of compliance for the purpose of the Step 2 assessment. However, see comments above under EDR.2.</p>
<p>Shutdown systems</p> <p><i>Principle ERC.2 - At least two diverse systems should be provided for shutting down a civil reactor.</i></p>	<p>AECL state in Ref.1 <i>“The ACR-1000 design incorporates two independent and diverse shutdown systems”</i>. It is considered</p>

	<p>that an adequate compliance statement is provided for this SAP.</p> <p>Note that AECL also state in Ref.1:-</p> <p><i>“27.2.3 AECL’s Interpretation/Compliance Support - The ACR-1000 incorporates two fast-acting, fully capable, diverse, and separate shutdown systems, which are physically and functionally independent of each other</i></p> <p><i>In both shutdown systems, the instrumentation to measure each of the parameters is quadrupled and trips the reactor automatically on a two-out-of-four logic basis via computerized shutdown.”.</i></p> <p>A description of the diverse shutdown (i.e. SDS 1, shut-off rods and 2, concentrated gadolinium nitrate solution injection) provisions can be found in Ref. 4. However, the description of the C&I systems does not provide adequate information to confirm or otherwise that they are likely to be adequately independent and diverse.</p> <p>07. - AECL should demonstrate that the C&I systems used for implementation of diverse shutdown are adequately independent and diverse.</p>
<p>Common cause failure</p> <p><i>Principle EDR.3 - Common cause failure (CCF) should be explicitly addressed where a structure, system or component important to safety employs redundant or diverse components, measurements or actions to provide high reliability.</i></p> <p>Guidance - SAP paragraph 171 - 174</p> <p>171 <i>CCF claims should be substantiated.</i></p> <p>172 <i>In general, claims for CCF should not be better than one failure per 100 000 demands. The figure of one failure per 100 000 demands represents a judgement by NII of the best limit that could reasonably be supported for a simple system by currently available data and methods of analysis. A worse figure may need to be used (say 1 per 10 000 or 1 per 1000) according to the complexity and novelty of the system, the nature of threat and the capability of the equipment.</i></p> <p>173 <i>Nevertheless, it is conceivable that the continuing accumulation of good data and</i></p>	<p>AECL’s compliance statement contained in Ref.1 section 10.3.2 states :-</p> <p><i>“10.3.2 Compliance Statement - The ACR-1000 is designed according to the safety design guide on ‘Separation of Systems and Components’ [16], which ensures that common cause failures are explicitly addressed, where a structure, system or component important to safety employs redundant or diverse components, measurements or actions to provide high reliability.”</i></p> <p>In addition AECL’s “Interpretation/Compliance support” statement provides further clarification on how this SAP is satisfied in the design of the ACR-1000. For example, of relevance to the C&I design, it is stated <i>“Diversity may also be needed to achieve the necessary protection against certain types of common cause events (e.g., design errors, software errors, manufacturing errors, maintenance errors), and is directly related to a need for increased reliability after redundancy and separation have been provided”.</i></p> <p>P171/172/173 - No information on the CCF limits (SAP paragraph 172) applied is provided and this will need to be clarified during Step 3. Note the protection system reliability appears to be 10-3 pfd for each of SDS 1 and SDS2.</p> <p>08. - AECL should clarify the CCF limits (SAP paragraph 172) applied to C&I systems.</p>

<p>advances in its analysis could lead, in exceptional circumstances, to a situation where a strong case could be made by the dutyholder for better figures. Such a case would not then be ruled out of consideration.</p> <p>174 Where required reliabilities cannot be achieved due to CCF considerations, the required safety function should be achieved taking account of the concepts of diversity and segregation, and by providing at least two independent safety measures.</p>	<p>See under ESS.2.</p> <p>It is concluded that an adequate compliance statement has been provided for this SAP for the purposes of the Step 2 assessment.</p>
<p>Single failure criterion</p> <p><i>Principle EDR.4 - During any normally permissible state of plant availability no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.</i></p> <p>Guidance - SAP paragraph 175</p> <p>175 Consequential failures resulting from the assumed single failure should be considered as an integral part of the single failure. Further discussion of the single failure criterion is given in IAEA Safety Standard NS-G-1.2.⁴</p>	<p>AECL provide an adequate statement of compliance to this SAP in Ref.1, namely:-</p> <p><i>“10.4.2 Compliance Statement - The ACR-1000 design complies with this principle since the design guide (DG) [26] specifically addresses the Single Failure Criterion (SFC) requirements. This DG covers the application of the SFC to both fluid and electrical portions of ACR-1000 systems important to safety by interpreting and providing guidance in the application of the SFC, discussing typical failures and presenting an acceptable method of single failure analysis.”</i></p> <p>Within Ref. 1 section 10.4.3 it is stated:- <i>“Any consequential and/or coincident failures specified by the required design basis analysis assumption are required to be considered in addition to the single failure.”</i></p>
<p>Safety systems</p>	
<p>Requirement for safety systems</p> <p><i>Principle ESS.1 - All nuclear facilities should be provided with safety systems that reduce the frequency or limit the consequences of fault sequences, and that achieve and maintain a defined safe state.</i></p>	<p>AECL do not provide an explicit statement of compliance for this SAP within Ref.1, rather they list the systems that they consider to be safety systems, see compliance statement below.</p> <p><i>“21.1.2 Compliance Statement - As in the case of all CANDU designs, the Advanced CANDU Reactor (ACR) is provided with two fast acting, fully capable, diverse and separate shutdown systems which are physically and operationally independent of each other and from the reactor regulating system. The other safety systems are the Emergency Core Cooling (ECC) System, the Emergency Feedwater (EFW) System and the Containment System. ECC system is designed to supply emergency coolant to the reactor in case of loss of coolant accident or rapid shrinkage of coolant. EFW system is designed to provide cooling water to the steam generators secondary side to enable the steam generators to transfer the decay heat to the ultimate heat sink. The containment system is designed to restrict the release of radioactivity to the environment within the maximum permissible dose limits in the event of a radioactivity release within the containment envelope.</i></p> <p>While the compliance statement does show that the ACR-1000 is provided with safety systems the extent and scope of such</p>

<p>Guidance - SAP paragraph 336</p> <p>336 <i>A reactor should be provided with safety systems that can shut it down safely in normal operating and fault conditions and maintain it in the shutdown condition. There should be a margin of reactivity that allows for systematic changes and uncertainties in nuclear characteristics, variations in plant state and other processes or mechanisms that might affect the reactivity of the core, even for the most reactive conditions of the core.</i></p>	<p>systems will require clarification (see ECS.1 above and comment below against SAP paragraph 336).</p> <p>Within Ref.1 section 21.1.3 the following statement is made “<i>SDS1, however, needs to be supplemented by the moderator liquid poison to keep the reactor in long-term safe shutdown.</i>” It would appear that the “moderator liquid poison” system should be classified as a safety system since it is required to “maintain ... the shutdown condition”. Note that this example might illustrate the difference between AECL’s categorization/classification approach and UK expectations (i.e. AECL approach of considering that it is acceptable for “long term” requirements to be fulfilled by systems in a lower safety class to those needed for the short term).</p> <p>O9. - AECL should clarify whether or not the “moderator liquid poison” system is classified as a safety system and if not provide a justification of its categorisation.</p> <p>P336 – See comments above and under ERC.2.</p>
<p>Determination of safety system requirements</p> <p><u>Principle ESS.2 - The extent of safety system provisions, their functions, levels of protection necessary to achieve defence in depth and required reliabilities should be determined.</u></p> <p>Guidance - SAP paragraph 337</p>	<p>AECL’s compliance statement for this SAP is contained in Ref.1 where it is stated:-</p> <p><i>“21.2.2 Compliance Statement -The adequacy of safety system design in achieving its specified function is verified through the performance of detailed safety assessments (consistent with Principle FP.6), which demonstrate that the plant design meets its safety objectives in response to postulated initiating events, and that radiation exposures to members of the public and operating staff are acceptable. Fault tree analysis is used to demonstrate achievement of reliability targets for the safety systems and safety support systems in the Advanced CANDU Reactor (ACR). Both deterministic and probabilistic analyses are performed as part of design-assist and licensing analysis.”</i></p> <p>In addition the text supporting this principle (Ref.1 section 21.2.3) outlines a number of techniques that are applied to demonstrate the adequacy of the safety system performance and reliability.</p> <p>O10. - AECL should explain how probabilistic criteria are used in the design of the C&I systems and the reliabilities assigned to the various C&I systems both individually and when these systems are required in combination to reduce accident frequencies to acceptable limits.</p> <p>It is considered that an adequate claim of compliance is made for Step 2 against this SAP but see ECS.1 and ESS.1 above (e.g. scope of safety systems).</p>

<p>337 <i>The design basis (Principles FA.4 (paragraph 512 f.) and FA.9 (paragraph 525 f.)) and probabilistic safety (Principle FA.14 (paragraph 540 f.)) analyses (or other suitable analyses) should determine the safety system provisions, functions and required reliabilities.</i></p>	<p>P 337 - See comments above and under ESS.1. Satisfaction of SAP paragraph 337 will be considered during Step 3.</p>
<p>Monitoring of plant safety</p> <p><i>Principle ESS.3 - Adequate provisions should be made to enable the monitoring of the plant state in relation to safety and to enable the taking of any necessary safety actions.</i></p> <p>Guidance - SAP paragraph 338</p> <p>338 <i>Monitoring provisions should be classified as safety or safety-related systems as appropriate and should be made:</i></p> <ul style="list-style-type: none"> a) <i>in a central control location; and</i> b) <i>at emergency locations (preferably a single point) that will remain habitable during foreseeable facility emergencies.</i> 	<p>While not providing a direct claim of compliance with this SAP AECL outline the monitoring provisions implemented in the ACR-1000 design in the compliance and supporting statements of Ref.1, for example:-</p> <p><i>“21.3.2 Compliance Statement - The Advanced CANDU Reactor (ACR) design has provisions (categorized as important to safety) for operating staff to perform the monitoring, control and operation of the plant in both normal and abnormal modes of plant operation in the main control room. Computerized Safety System displays are available at the main operator console and on the large displays in the main control room together with hardwired back-up information on back-up panels. A secondary control building is provided to carry out monitoring and control functions for events exceeding normal operation, including those in which the main control room becomes uninhabitable. The ACR, like other CANDU designs, fully meets the requirements of redundancy, independence and separation between the main control room and the secondary control building, and in the instrumentation and cabling that leads to these two locations.”</i></p> <p>The above statement is considered to provide an adequate claim of compliance against this SAP. However, clarification should be provided that the emergency locations remain habitable during foreseeable facility emergencies.</p> <p>Further details of the monitoring provisions can be found in Ref.4, for example, see section 7.6.4. which describes the “Safety Support Display Information”.</p> <p>O11. Clarification will be required that the emergency locations remain habitable during foreseeable facility emergencies.</p>
<p>Automatic initiation</p> <p><i>Principle ESS.8 - A safety system should be automatically initiated and normally no human intervention should be necessary following the start of a requirement for protective action.</i></p>	<p>Within Ref.1 section 21.8 AECL claim compliance with this SAP for all but a small number of unspecified events for which it is stated that operator action is required. It is also stated that such operator action is not required for a specific period of time (normally the first 30 minutes) following initiation of an event. AECL also note in Ref.1 section 21.9 that all human response times will be validated by human factors analysis. It is concluded that there is an adequate claim of compliance for this SAP. However, AECL will need to identify and justify those events for which operator action is required.</p> <p>The description of SDS 1 and 2 in Ref. 4 implies that their action is automatically initiated (e.g. section 6.2.1.4 “.. SDS1 is designed to promptly shut the reactor down for the entire spectrum of accident conditions. .. SDS1 uses at least one trip parameter to terminate any postulated events that require SDS1 action”). The only mention of manual actions in relation</p>

<p>Guidance - SAP paragraph 343</p> <p>343 <i>The design should be such that facility personnel cannot negate correct safety system action at any time, but they can initiate safety system functions and perform necessary actions to deal with circumstances that might prejudice safety.</i></p>	<p>to safety systems (i.e. SDS 1, SDS2, the Emergency Core Cooling (ECC) system, Emergency Feedwater (EFW) system and Containment System) in Ref. 4 was found in the section on the Containment System.</p> <p>O12. - AECL should identify those events for which operator action is claimed and demonstrate that such actions are fully justified (e.g. automatic initiation for these events is not reasonably practicable).</p> <p>P343 - To be considered during Step 3.</p>
<p>Engineered safety features (Automatic initiation)</p> <p><i>Principle ERL.3 - Where reliable and rapid protective action is required, automatically initiated engineered safety features should be provided.</i></p> <p>Guidance - SAP paragraph 180</p> <p>180 <i>For requirements that are less demanding or on a longer timescale, operator actions or administrative control may be acceptable to complement the engineered systems. The objective should be to minimise the dependence on human action to maintain a safe state.</i></p>	<p>See comments above under ESS.8.</p>
<p>Reliability – Avoidance of complexity</p> <p><i>Principle ESS.21 - <u>The design of a safety system should avoid complexity</u>, apply a fail-safe approach and incorporate the means of revealing internal faults from the time of their occurrence.</i></p> <p>Guidance - SAP paragraphs 355</p> <p>355 <i>Where this principle cannot be achieved because of the use of complex hardware, the elements of a safety demonstration should be determined. The demonstration should include:</i></p> <ol style="list-style-type: none"> a) <i>a comprehensive examination of all the relevant scientific and technical issues;</i> b) <i>a review of precedents set under comparable circumstances in the past;</i> c) <i>an independent third-party assessment in addition to the normal checks and conventional design;</i> d) <i>periodic review of further developments in technical information, precedent and best practice.</i> 	<p>With regard to this SAP AECL state in Ref.1:-</p> <p><i>“21.21.2 Compliance Statement -To the greatest practicable extent, the design of the safety systems for the ACR-1000 is based upon relatively simple, proven and robust design technologies that have been successfully applied in previous CANDU plant designs.”</i></p> <p>The description of the safety systems (see Ref. 4) includes reference to two computerised shutdown systems (i.e. SDS 1 and SDS 2). This arrangement can be seen as complex, requiring specific special case safety justification of each system and the diversity when both systems are required in combination to reduce accident frequencies to acceptable limits.</p> <p>O13.1 - AECL should provide a justification for the use of two complex computerised shutdown systems which should include consideration of diversity and probabilistic claims when these systems are required in combination to reduce accident frequencies to acceptable limits (see also ESS.2 above).</p> <p>O13.2 - AECL should identify and justify any other similar complex situations (e.g. where two safety systems are required in combination to reduce accident frequencies to acceptable limits).</p>

	<p>O13.3 - AECL will need to clarify whether any complex hardware such as ASICs/FPGAs etc. is used in the design of the ACR-1000 safety systems.</p>
<p>Allowance for unavailability of equipment</p> <p><i>Principle ESS.23 - In determining the safety system provisions, allowance should be made for the unavailability of equipment</i></p> <p><i>Guidance - SAP paragraphs 357</i></p> <p>357 Sources of equipment unavailability will include:</p> <ul style="list-style-type: none"> a) testing and maintenance; b) non-repairable equipment failures; and c) unrevealed failures. 	<p>With regard to this SAP AECL state in Ref.1:-</p> <p><i>“21.23.2 Compliance Statement - The ACR-1000 safety system designs incorporate redundancy to allow for unavailability of equipment due to testing and maintenance, and due to non-repairable equipment failures where applicable. ...Redundancy is designed into systems sufficient to ensure that no single active failure results in the loss of the ability of the system to perform its required safety function.”</i></p> <p>Further details of the arrangements that allow AECL to claim compliance with this SAP are provided in Ref. 1 section 21.23.3.</p> <p>Within Ref. 4 the descriptions of the safety system arrangements include specific mention of testing and maintenance. For example, for SDS1 and 2 it is stated (section 7.2) that <i>“The design of SDS 1 (2) allows maintenance to be done on any part of the system without jeopardizing(impairing) its availability target. ..”</i>.</p> <p>It is concluded that an adequate claim of compliance is made for this SAP.</p>
<p>Functional testing</p> <p><i>Principle EMT.7 - In-service functional testing of systems, structures and components important to safety should prove the complete system and the safety-related function of each component.</i></p> <p><i>Guidance - SAP paragraphs 192 - 193</i></p> <p>192 Maintenance, inspection and testing are a part of normal operation and it should be possible to carry out these tests without any loss of any safety function.</p> <p>193 Where complete functional testing is claimed not to be reasonably practicable, an equivalent means of functional proving should be demonstrated.</p>	<p>Within Ref.1 section 13.7.2 AECL claim that <i>“The Advanced CANDU Reactor (ACR) design complies fully with this principle”</i>. The text supporting this statement in Ref. 1 section 13.7.3 provides detail of the ACR-1000 in-service functional testing arrangements. It is noted that the compliance statement description addresses safety system testing.</p> <p>Ref. 4 contains descriptions of the safety system testing and maintenance arrangements. For example, for SDS1 and 2 it is stated (section 7.2) that <i>“For SDS 1 (2), parameter testing checks the operation of an individual channel. The trip logic reacts to simulated parameter measurements in the same manner as actual trip conditions. ..”</i>.</p> <p>It is concluded that an adequate compliance statement is provided for this SAP.</p> <p>O14. Clarification will be required as to whether other systems important to safety (e.g. safety related systems as defined by the IAEA) comply with this SAP.</p> <p>P192 - See ESS.23.</p> <p>P193 - No claim identified.</p>
<p>Computer-based systems important to</p>	

safety	
<p>Computer-based safety systems</p> <p><i>Principle ESS.27 - Where the system reliability is significantly dependent upon the performance of computer software, the establishment of and compliance with appropriate standards and practices throughout the software development life-cycle should be made, commensurate with the level of reliability required, by a demonstration of 'production excellence' and 'confidence-building' measures.</i></p> <p><i>Guidance - SAP paragraphs 360 - 362</i></p> <p>360 'Production excellence' requires a demonstration of excellence in all aspects of production, covering initial specification through to the finally commissioned system, comprising the following elements:</p> <ul style="list-style-type: none"> a) Thorough application of technical design practice consistent with current accepted standards for the development of software for computer-based safety systems. b) Implementation of an adequate quality assurance programme and plan in accordance with appropriate quality assurance standards. c) Application of a comprehensive testing programme formulated to check every system function, including: <ul style="list-style-type: none"> • prior to installation on site, the verification of all phases of the system production process and the validation of the integrated system against its requirements specification by persons not involved in the specification and design activities; • following installation on site, a demonstration that the safety system, in conjunction with the plant, performs to requirements, this demonstration being devised by persons other than the system specifiers, designers or manufacturers; and • a programme of dynamic testing, applied to the complete system, that is capable of demonstrating that the system meets its reliability requirements. <p>361 Independent 'confidence-building' should provide an independent and thorough assessment of a safety system's fitness for purpose. This comprises the following elements:</p> <ul style="list-style-type: none"> a) Complete and preferably diverse checking of the finally validated production software by a team that is independent of the systems suppliers, including: <ul style="list-style-type: none"> • independent product checking providing a searching analysis of the product; • independent checking of the 	<p>AECL do not provide a specific compliance statement against this SAP. Within Ref.1 section 21.27.2 AECL provide a description of the standard (i.e. CE-1001) applied to safety critical software used in real-time protective, control and monitoring systems employed in the Advanced CANDU Reactor (ACR) design. AECL note that the standard "owes much of its content to the experience and feedback gained in developing, licensing, and maintaining software for a range of CANDU designs". AECL explain that requirements are specified for "the process of development, verification, validation and support processes such as planning, configuration management and training. Specific requirements are defined for testing and independence". Further AECL claim that "A number of national and international standards were consulted in the preparation of CE-1001 with significant influence from IEC60880 ("Software for Computers in the Safety Systems of Nuclear Power Stations")". AECL also claim that "we also follow the IEC 61513 series of standards for category B and C systems which are also tied to reliability requirements."</p> <p>The description of the arrangements within Ref. 1 section 21.27.3 provides further detail on the requirements for independence (e.g. the development processes are executed by groups independent of the verification and validation processes). The validation and verification of safety critical software utilises formal methods (e.g. mathematical verification is done in two stages-from the requirements specification to the software design as well as from the software design to the code). Further it is stated that the "CANDU safety critical software development processes use a process called reliability demonstration testing in which the reliability of safety critical software is demonstrated using statistically valid, trajectory-based random testing".</p> <p>From the description of the arrangements it is concluded that the approach has many features that are consistent with SAP ESS.27 (e.g. use of formal methods and statistical testing). It is considered that the description provides an implicit claim that ESS.27 is met. However, further clarification will be required to ensure that the production excellence and confidence building legs are adequately defined.</p> <p>O15.1 - AECL should demonstrate the means by which its arrangements satisfy SAP ESS.27 and Ref. 8. In particular, the way in which each of SAP paragraphs 360 to 361 has been met should be clarified. The activities that contribute to the independent confidence building (i.e. independent of the system's specifiers and producers) as opposed to production excellence will need to be clearly identified. The confidence building leg is normally defined by a team within the licensee not the vendor. Note that the adequacy of the claimed standards base will require further consideration during Step 3 (see also comments under ECS.3).</p> <p>O15.2 - AECL should define the scope of application of this SAP and confirm it is applied to all safety systems (e.g. to cover all systems contributing to reactor protection). See also discussion above under ECS.1, ECS.2 and ECS.3.</p> <p>O15.3 - AECL should explain its approach to instrumentation and actuators that contain programmable devices (e.g. SMART instruments).</p>

<p><i>design and production process, including activities needed to confirm the realisation of the design intention; and</i></p> <p>b) <i>Independent assessment of the test programme, covering the full scope of test activities.</i></p> <p>362 <i>Should weaknesses be identified in the production process, compensating measures should be applied to address these. The type of compensating measures will depend on, and should be targeted at, the specific weaknesses found.</i></p>	<p>O15.4 - AECL should explain its approach to use of pre-developed hardware and software (e.g. compliance to appropriate standards such as IEC 60880).</p>
<p>Standards for computer based equipment</p> <p><i>Principle ESR.5 - Where computers or programmable devices are used in safety-related systems, evidence should be provided that the hardware and software are designed, manufactured and installed to appropriate standards.</i></p>	<p>For this SAP AECL claim within Ref.1 “22.5.2 Compliance Statement - Where computers or programmable devices are used in Advanced CANDU Reactor (ACR) systems important to safety, software and hardware are designed, manufactured and installed to appropriate standards”.</p> <p>Further details of the standards for computer based systems are provided in Ref.1 section 22.5.3 including categorisation into “four levels: level 1 for safety systems; level 2 for controls and displays important to safety having demanding reliability requirements (less than 10-2 failures per year); level 3 for controls important to safety having less demanding reliability requirements (greater than 10-2 failures per year); and level 4 for non-safety related controls”.</p> <p>It is also explained that “AECL uses a range of Canadian standards and guides to assure the appropriate quality in the hardware and software of programmable devices. These standards are broadly consistent with the corresponding IEC standards such as 61226 for categorization of systems, 61513 for system hardware and 62138 for software”. It is further stated that “Safety critical software used in real-time protective, control and monitoring systems employed in the Advanced CANDU Reactor (ACR) design will comply with the requirements of Standard CE-1001.”</p> <p>AECL also note that documentation includes “detailed guides for design, testing, verification, and documentation of new software, and for qualification of pre-developed software”.</p> <p>It is concluded that an adequate claim of compliance is made for this SAP but note comments below in bold. See also SAP ESS.27 and ESC.3 above.</p> <p>O16. - AECL should demonstrate that appropriate design standards are used for this class of system (see also ESS.27 and ECS.3). The concept of ESS.27 is applicable to computers used in safety-related systems (see Ref. 8) which means arguments of production excellence and independent confidence building will need to be presented. See also comments under ESS.27 above.</p>
<p>Control and instrumentation of safety-related systems</p>	
<p>Provision in control rooms and other locations</p>	

	<p><i>occurrences, the normal process and control systems will allow safe operation or shutdown, if necessary, without the necessity of invoking safety systems.”</i></p> <p>This is considered to provide an adequate statement of compliance for the purposes of Step 2 assessment. Note that the supporting text to AECL's compliance statement in Ref. 1 section 22.3.3 includes a fuller description of the arrangements. Also, see Ref.4 which provides a fuller description of the controls (e.g. section 7.5 Process Control System and 7.6.3 Control Computers).</p>
<p>Communications systems</p> <p>Principle ESR.7 - Adequate communications systems should be provided to enable information and instructions to be transmitted between locations and to provide external communications with auxiliary services and such other organisations as may be required.</p> <p>Guidance - SAP paragraph 368</p> <p>368 These communication systems should not have any adverse effect on safety systems, or safety-related systems.</p>	<p>AECL confirm that it complies with this SAP in Ref.1 where it is stated (section 22.7.2):- <i>“22.7.2 Compliance Statement - The Advanced CANDU Reactor (ACR) complies with this principle, and provides communication both within the plant and between the plant staff and outside organizations as required.”</i></p> <p>This is considered to provide an adequate statement of compliance for the purposes of Step 2 assessment. Note that the supporting text to AECL's compliance statement in Ref. 1 section 22.7.3 includes a fuller description of the arrangements. For example, it is stated that “.. <i>The communications systems provide facilities for communicating between predefined locations where personnel involved with safety functions are located. These locations are the Main Control Room, Secondary Control Building, Work Control Area, Technical Support Centre (for site technical support in emergency), Emergency Operations Centre (for coordination with offsite personnel such as a fire department; the centre will have a dedicated set of telephone lines, fax and data communications systems consistent with local site needs), and various plant locations. ...The radios and cell phones are designed to not interfere with safety systems or other instrumentation systems important to safety”</i>. See also Ref.4 section 7 (e.g. 7.6.4.1 which provides an outline of the facilities provided in the Technical Support Centre).</p>

NB. SAP Guidance in the above table is considered when it is relevant to C&I assessment.