

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

**New Reactor Build
GE ESBWR 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 GEH ESBWR submission in accordance with the strategy outlined in Ref. 8. 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. 8) 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. 9).

2. REPORT

3. GEH provided a number of submissions relevant to assessment of the ESBWR C&I design. The main submission that describes the C&I is Ref. 1. The C&I provisions outlined in the submissions include those that would be expected of a modern nuclear reactor such as:-
 - safety systems (e.g. reactor shutdown systems such as the Reactor Protection System (RPS) that initiates insertion of neutron absorbing rods and the Standby Liquid Control System that injects a neutron absorbing sodium pentaborate solution),
 - plant control and monitoring systems (e.g. the Nonsafety-related Distributed Control and Information System, and the Rod Control and Information System that controls reactor power),
 - main control room with backup via the Remote Shutdown System panels, 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 accepted 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. GEH did not provide a document that directly addresses compliance with each of the SAPs (e.g. a route map indicating the section(s) of the submissions that address each SAP). Within Ref. 4 section 2.14.1 “Comparison with Safety

Assessment Principles” GEH explain “ .. *A high level comparison has been undertaken between the HSE’s Safety Assessment Principles (SAPs, reference 2.14-1) and the NRC General Design Criteria. ... Further work will be required to address UK regulatory requirements ...*”. Technical Query (TQ) ESBWR-000001 was raised requesting an explanation of how the ESBWR design complies with each of the SAPs including a request for an early response on the “fundamental” C&I SAPs.

6. The main body of the assessment is contained in the Annex of this report. The assessment in the Annex has included consideration of GEH’s response to TQ ESBWR-000001 (i.e. Ref. 10) on the fundamental C&I SAPs. GEH claim compliance with all of the SAPs in the Annex. However, within the Annex there are a number of observations that will need to be raised with GEH 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 GEH address, for C&I, categorisation of functions and classification of structures, systems and components (O1. - SAP ECS.1 and O.2 - SAP ECS.2). In particular, alignment of the GEH approach to that defined by the IAEA, SAPs and BS IEC 1226:2005 will need to be determined. The GEH practice of using only two classes (i.e. safety-related and nonsafety-related) does not align with UK or IAEA practice. 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 for safety-related and nonsafety-related C&I systems provides adequate compliance with modern UK national and international C&I nuclear standards (O3.1, O3.2 and O3.3 - SAP ECS.3). The standards base appears to be mainly US (e.g. IEEE standards) some of which pre-date what would be considered “modern” for C&I.
- Clarification will be required as to the basis of the fail-safe approach (i.e. for all C&I equipment) (O4. - SAP EDR.1). Also, for the safety systems, clarification is required on how it is ensured that component failures result in an appropriate system response (O5.1 and O5.2 – SAP ESS.21). 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 GEH ESBWR C&I systems (O3.4 - SAP ECS.3, O6. - SAP EDR.2, O7.2 - SAP ESS.7, O10 - SAP EDR.3 and O12. - 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. Note the protection system software common cause failure figure used in the PSA appears to be 10⁻⁵ pfd but this requires clarification (Ref. 11 Table 4.5-7). A 10⁻⁴ pfd CCF cut-off figure is usually applied to computer based safety systems (see Ref. 12).
- GEH should provide a demonstration that the primary protection system (e.g. the safety system logic and control system, and reactor protection system) and diverse protection system 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 (O7. - SAP ESS.7). 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. 12) (O17.1. to O17.4. - SAP ESS.27 and O18 - SAP ESR.5).

7. The GEH submissions on C&I mainly describe a conceptual design and GEH explained during the familiarisation presentation on 9 October 2007 that the Design Control Document (of which Ref. 1 is a part) is intended to be “platform” independent. GEH further explained that aspects of the C&I design are specifically excluded from the design certification by the NRC but are dealt with through the Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC process) (see Ref. 6). It is noted that only limited information is provided on the actual implementation details in Ref.1 (e.g. such as reference to the NUMAC platform in the description of the Reactor Protection System). Therefore, this assessment report only addresses 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 ESBWR conceptual design within the UK).
8. 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. For example, if the current design intent as explained during the familiarisation presentation is different to that described in the formal submissions, (see O7.3 - SAP ESS.7) then a modification to the documentation will be required.
O19. GEH should confirm that the submissions accurately reflect the current C&I design (e.g. as described during the familiarisation meetings) and explain how changes to the documentation and C&I systems are controlled.
9. The GEH ESBWR C&I design concept reflects US custom and practice, and is largely based on US C&I standards (e.g. IEEE) and NRC regulatory requirements. As a result the observations in the Annex largely reflect the difference between US and UK approaches.
10. With regard to US custom and practice, it is worth noting that in 1997, HSE published a “four party” report (Ref. 7) which provided a consensus view on the safety case requirements for computer based systems. The USNRC 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 GEH in its submissions to the USNRC.
11. 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 GEH. 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 GEH.

O20. GEH 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).

12. From Ref. 1 it was noted that, unlike the Westinghouse submission, there does not appear to be any C&I requirements left for the “license applicant” to define. 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 license applicant to define and the satisfaction of such requirements.

3. CONCLUSIONS

13. GEH 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 GEH. The response to these observations should be addressed during Step 3. The GEH submissions largely describe a design concept (i.e. only limited information is provided on the actual implementation details such as reference to the NUMAC platform in the description of the RPS in Ref.1). As well as completing the assessment of the 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 GEH ESBWR C&I reflects US custom and practice, and is largely based on US C&I standards (e.g. IEEE) and NRC regulatory requirements. As a result the observations largely reflect the difference between US and UK 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 GEH from proceeding to Step 3. Therefore, GEH should be allowed to proceed to Step 3.
- R2. The “observations” identified throughout this assessment report by bold text will require a GEH response prior to Step 3.

- R3. Develop an approach (i.e. for Steps 3, 4 and Phase 2) for the assessment of the ESBWR C&I design implementation (i.e. covering the exact C&I systems, platforms, products and components etc. selected for the implementation of the ESBWR C&I conceptual design within the UK).

5. REFERENCES

1. ESBWR Design Control Document Tier 2, Chapter 7 Instrumentation and Control – GE Energy Nuclear 26A6642AW Revision 3 February 2007.
2. ESBWR Design Control Document Tier 2, Chapter 3 Design of Structures Components, Equipment, and Systems Sections 3.1 – 3.8 – GE Energy Nuclear 26A6642AJ Revision 3 February 2007.
3. ESBWR Design Control Document Tier 2, Chapter 1 Introduction and General description of Plant 1.1 – 1.11 – GE Energy Nuclear 26A6642AD Revision 3 February 2007.
4. ESBWR – UK Preliminary Safety Report Step 2 Sections 1.0 – 2.18 - GE-Hitachi Nuclear Energy 26A7403AA Revision 0 August 2007.
5. ESBWR Design Control Document Tier 2, Chapter 9 Auxiliary Systems – GE Energy Nuclear 26A6642AY Revision 3 February 2007.
6. USNRC Standard Review Plan NUREG-0800.
7. Health and Safety Executive - Four Party Regulatory Consensus Report on the Safety Case for Computer-Based Systems in Nuclear Power Plants; AECB - Canada, DSIN/IPSN - France, NII- UK, USNRC – USA
8. Step 2 C&I Assessment Strategy - ND DIV 6 Assessment Report No. AR07002
9. Nuclear Division – Division 6 Unit 6D Operating Plan 2 August 2007 – 31 March 2008
10. Full response to TQ ESBWR-000001 raised 1 October 2007 – Compliance with HSE Safety Assessment Principles for Nuclear Installations (2006 Edition)
11. ESBWR Certification Probabilistic Risk Assessment Licensing Topical Report - NEDO 33201 Rev 2.
12. 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) Category A – any function that plays a principal role in ensuring nuclear safety. b) Category B – any function that makes a significant contribution to nuclear safety. c) Category C – any other safety function. <p>150 The method for categorising safety functions should take into account:</p> <ul style="list-style-type: none"> a) the consequence of failing to deliver the safety function; b) the extent to which the function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults; c) the potential for a functional failure to initiate a fault or exacerbate the consequences of an existing fault; d) the likelihood that the function will be called upon. <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>ECS.1 – Ref. 10 provides a claim that the ESBWR complies with ECS.1. In particular, GEH state:</p> <p><i>“The historical determination of safety function importance suggested by the text following ECS.1 was not used. Instead a classification scheme is developed leading to the broad categories “safety-related” or “nonsafety-related”. See DCD Section 3.2.”</i></p> <p>Note that GEH describe a system (Ref. 2) where safety related classified items would appear to implement safety related functions (this is explicitly stated by Westinghouse for the AP1000) but no explicit description of these functions or their categorisation is provided. See also comments below under ECS.2.</p> <p>O1. GEH should clarify how it addresses, for C&I, categorisation of functions and how the functional categorisation is used in the classification of structures, systems and components. In particular, alignment of the GEH approach to that defined by the IAEA, SAPs and BS IEC 1226:2005 should be demonstrated.</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>Ref. 10 provides a claim that the ESBWR complies with this SAP. GEH's response provides references to sections within Ref. 2.</p> <p>Within Ref. 2 it is stated that the <i>“ESBWR structures, systems and components (SSCs) are categorized as safety-related (as defined in 10 CFR 50.2) or Nonsafety-Related. The safety-related structures, systems and components are those relied upon to remain functional during and following design basis events to ensure:</i></p> <ul style="list-style-type: none"> • <i>The integrity of the reactor coolant pressure boundary (RCPB);</i> • <i>The capability to shut down the reactor and maintain it in a</i>

<p>Guidance - SAP paragraphs 153-156 .</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 ECS.1);</i></p> <p> b) <i>the consequences of failure to perform its function;</i></p> <p> c) <i>the probability that the item will be called upon to perform a safety function;</i></p> <p> d) <i>the time following any initiating fault at which, or the period throughout which, it will be called upon to operate.</i></p> <p>154 <i>A safety classification scheme could be determined on the following basis:</i></p> <p> a) <i>Class 1 – any structure, system or component that forms a principal means of fulfilling a Category A safety function.</i></p> <p> 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></p> <p> c) <i>Class 3 – any other structure, system or component.</i></p> <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</i></p>	<p><i>safe condition; or</i></p> <ul style="list-style-type: none"> <i>• The capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the applicable guidelines exposures set forth in 10 CFR 50.34(a)(1)".</i> <p>Note that the classification does not appear to be explicitly based on categorisation of functions although it is implicit that the safety related systems implement safety related functions. The safety related category is further divided into one of three Classes (i.e. Class 1, 2, 3). Table 3.2-1 in Ref. 2 outlines the safety class of the C&I systems (e.g. the reactor protection system is Safety Class 3).</p> <p>The categorization of functions, classification of systems and allocation of design standards does not align with UK (SAPS) or international expectations. In particular, it appears that some of the systems classed as nonsafety-related might fall in a safety related category (IAEA) and therefore, they might require more rigorous standards.</p> <p>P153 - See above.</p> <p>P154 - Two categories have been identified i.e. safety-related and nonsafety-related. The safety-related category is subdivided into three safety classes. Note that SAP class 3 would appear to align with the non-safety related class. Some of the C&I systems defined as nonsafety-related in Ref. 1 (e.g. Rod Control and Information System) would appear to fall in SAP class 2 and IAEA safety related class. Also note that the Diverse Protection System is classified as nonsafety-related.</p> <p>O2. GEH should clarify how its safety classification scheme for C&I aligns with international standards and NII's SAPs, and demonstrate that the design standards for each class (see ECS.3 below) are appropriate.</p> <p>P155 - Step 3 – However, note that it does appear that this requirement is considered in the design (e.g. see description of Q-DCIS to N-DCIS interface in Ref.1 section 7.1.3.3)</p> <p>P156 - Step 3</p>
---	---

<p>function.</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><i>Guidance - SAP paragraphs 157-161</i></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>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</i></p>	<p>Ref. 10 provides a claim that the ESBWR complies with this SAP. Within Ref. 10 GEH state: “<i>Structural and electrical design codes are provided for the safety-related SSCs and many non-safety related SSCs throughout DCD Chapters 3-11. For example, the use of ASME Code safety classifications is described in DCD Sub-section 3.2.3, and are listed on a system major component basis in DCD Table 3.2-1</i>”.</p> <p>The GEH “safety related” C&I equipment is defined to be Safety Class 3. GEH state (Ref. 2) that “<i>All Safety Class 3 SSCs are subject to 10 CFR 50 Appendix B quality assurance requirements</i>”. While for nonsafety-related equipment it is stated that “<i>Generally, design requirements for Nonsafety-related equipment are based on applicable industry codes and standards as summarized in Table 3.2-3. Where these are not available, accepted industry or engineering practice is followed</i>”.</p> <p>O3.1 Since some of the C&I systems within the nonsafety-related categorisation (see above) would appear to fall in SAP Class 2 further clarification will be required as to the appropriateness of the selected codes and standards.</p> <p>It can be seen from Ref. 1 that the C&I standards base appears to be largely US (e.g. IEEE standards and references to NRC requirements).</p> <p>O3.2 The dates of the standards are not quoted so clarification of the applicable set will be required.</p> <p>There is a need to consider whether the selected standards are in agreement with modern UK national and international C&I nuclear standards.</p> <p>O3.3 Clarification should be provided that the selected C&I standards base for safety-related and nonsafety-related C&I systems 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 (see above). It is assumed that the higher safety class standards are more rigorous than those for lower safety classes (i.e. the normal practice).</p> <p>O3.4 - GEH should clarify how the standards reflect the functional reliability requirements.</p> <p>P158 - See above</p> <p>P159 - See above.</p>

<p>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.</p> <p>160 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.</p> <p>161 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.</p>	<p>P160 - The ESBWR nonsafety-related systems encompass systems that in the UK and internationally would fall into a safety related class (e.g. see IAEA Safety Standards Series – Instrumentation and control systems important to safety in nuclear power plants – safety guide NS-G-1.3). Note that the safety related class is equivalent to SAP class 2. Hence the ESBWR nonsafety-related class appears to encompass both SAP classes 2 and 3. However, it is noted that separation of the safety-related and nonsafety-related systems functions appears to be addressed (e.g. separation of the Q-DCIS and N-DCIS Ref. 1).</p> <p>O3.5 GEH should clarify 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 GEH. To be addressed in Step 3.</p>
Failure to safety	
<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>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response in Ref.10 specifically refers to safety systems and does not explain the approach for other systems. For safety systems see comments below under ESS.21.</p> <p>O4. GEH should clarify the “failure to safety” approach for systems other than the safety systems.</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></p> <p>Guidance - SAP paragraphs 356</p> <p>356 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 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>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response in Ref.10 specifically refers to safety systems and states:</p> <p><i>“For all safety systems a full analysis has been undertaken to determine the best fail safe state of components. As an example for the reactor protection system, DCD Sections 3.1 and 7.2 discuss the design philosophy for failures and self-testing to reveal failures in the RPS. The acceptability of these failure states has been undertaken in the PSA as described in DCD Chapter 19 and Reference 3.”</i></p> <p>NRC criterion 23 (Ref. 2) is also relevant to this SAP.</p> <p><i>“Criterion 23 Statement - The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.”</i></p>

	<p>Within Ref 2 'Evaluation Against Criterion 23' GEH State :- <u>"The Reactor Protection (trip) System is designed to fail into a safe state. Use of independent channels allows the system to sustain any logic channel failure without preventing other sensors monitoring the same variable from initiating a scram. With a two-out-of-four logic design, the trip of any two channels initiates a scram. Intentional bypass for maintenance or testing causes the scram logic to revert to two-out-of-three. A failure of any one reactor protection input or subsystem component produces a trip in one channel. This condition is insufficient to produce a reactor scram, and the system performs its protective function upon trip of another channel. Failure of inputs or subsystem components in two channels produces a reactor scram. The fail-safe design of the Reactor Protection (trip) System meets the requirements of Criterion 23"</u>.</p> <p>GEH claim that the protection system is designed to fail into a safe state. However, it is not clear how this fail safe behaviour is ensured (e.g. use of dynamic trip bus to ensure system failures result in an appropriate response such as setting of a guardline "partial trip").</p> <p>O5.1 GEH should clarify the basis of the fail-safe approach (e.g. how it is ensured that system failures result in an appropriate response).</p> <p>O5.2 GEH should clarify whether internal faults are revealed from the time of their occurrence.</p>
Defence in depth	
<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>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response in Ref.10 states:</p> <p><i>"The redundancy, diversity and segregation associated with the C&I systems are described in DCD Chapter 7 and for the Electrical Power systems is covered in DCD Chapter 8. The reliability analysis of the Electrical and C&I systems is presented in DCD Chapter 19. The Reactor Building is divided into four quadrants which are kept separate to meet fire protection (DCD Sub-section 9.5.1 and Appendix 9A) and flood (DCD Section 3.4) requirements."</i></p> <p>From a review of Ref. 1 it can be seen that the ESBWR design does include redundancy, diversity, and segregation. For example, this is described in Ref.1 sections that address compliance with standard IEEE 603 such as sections 7.1.6.6.1.7 "Independence" and 7.1.6.6.1.2 "single failure criterion".</p> <p>Note that Ref. 1 section 7.1.6.6.1.2 'Single Failure Criterion (IEEE std .603, 5.1)' states <i>"The ESBWR safety-related control systems include sufficient redundancy, diversity, and independence to meet system performance requirements even if the system is degraded by any single credible failure.Licensing Topical Report (LTR), "ESBWR C&I Defense-In-Depth and Diversity Report," NEDO-33251, (See Reference 7.1-4) describes the type of diversity that exists among the four echelons of defense-in-depth for the ESBWR and identifies the dependencies, redundancy and independence among the echelons."</i></p>

<p>Guidance - SAP paragraph 170</p> <p>170 It should be demonstrated that the required level of reliability for their intended safety function has been achieved.</p>	<p>In addition, there are numbers of NRC criterion that are relevant and for which GEH claim compliance in Ref. 2 i.e. Criterion 22, "Protection System Independence"; Criterion 23, "Protection System Failure Modes"; and Criterion 24, "Separation of Protection and Control Systems,".</p> <p>It is concluded that GEH provide an adequate claim that the ESBWR design incorporates redundancy, diversity and segregation. The adequacy of the arguments will need to be considered further during Step 3 and it should be noted that this is linked to clarification of which systems are important to safety and their class (see ECS 1, 2 and 3 above).</p> <p>P170 - Two system classes have been identified (see above) but it is not clear how reliability figures are used in the design of the ESBWR C&I systems nor how achievement is demonstrated. Note the protection system software common cause failure figure used in the PSA appears to be 10-5 pfd but this requires clarification (Ref. 11 Table 4.5-7).</p> <p>O6.1 Clarification is required on the use of probabilistic criteria in the design of the ESBWR C&I systems and how achievement of such criteria is demonstrated.</p> <p>O6.2 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.</p>
<p>Determination of safety system requirements – Defence in depth</p> <p>Principle ESS.2 - The extent of safety system provisions, their functions, <u>levels of protection necessary to achieve defence in depth</u> and required reliabilities should be determined.</p> <p>Guidance - SAP paragraph 337</p> <p>337 The design basis (Principles FA.4 (paragraph 512 f.) and FA.9 (paragraph 525 f.)) and probabilistic safety (Principle FA.14</p>	<p>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response in Ref.10 states:</p> <p><i>"In DCD Section 15.1, Nuclear Safety Operational Analysis (NSOA) shows for each safety analysis the system level requirements and function that ensure the plant can be brought to a stable safe condition. As a minimum, all safety-related functions can be accomplished assuming the occurrence of the most limiting single failure.</i></p> <p><i>The timings and sequences of events for all DBEs are addressed in DCD Sections 15.2 through 15.4.</i></p> <p><i>The timings and sequences of events for all beyond DBEs (Special Events), which involve common mode failures and/or multiple failures beyond the single failure criterion, are addressed in DCD Section 15.5."</i></p> <p>Examples of levels of protection within the C&I systems' architecture include the separation of control and protection (see comments on NRC criterion 24 below under ESS.18), and the provision of a Diverse Protection System.</p> <p>It is concluded that GEH provide an adequate claim that the ESBWR design incorporates defence in depth. See also discussion above under EDR.2 and below against ESS.7.</p> <p>P337 - Step 3</p>

<p>(paragraph 540 f.)) analyses (or other suitable analyses) should determine the safety system provisions, functions and required reliabilities.</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><i>Guidance - SAP paragraph 342</i></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>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response in Ref.10 states:</p> <p><i>“Diverse parameters are used to detect fault sequences and initiate safety systems - both ‘event’ based and symptom based. DCD Chapter 7 provides the detail. The Diverse Protection System (DPS) provides diverse detection and initiation of key safety functions, (Reference DCD Section 7.8).”</i></p> <p>Clarification is required as to how the protection system satisfies this SAP. <u>Note that the diversity required by this SAP is within the protection system not across independent systems such as the RPS and DPS.</u></p> <p>07.1 - GEH 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>The design does employ diversity in the totality of the protection arrangements. For example, GEH state Ref. 1 (section 7.2.1.2.1) <i>“The RPS sensors, hardware and logic are diverse from both ECCS logic and from the Diverse Protection System (DPS).”</i></p> <p><u>The approach to protection system diversity, as described, will be considered further during Step 3.</u> The adequacy of the arguments used to justify the chosen architecture will need to be considered, for example, use of Common Cause failure limits (see SAP EDR 3) and adequacy of the diversity given the technology used. NB. The use of two computer based systems would be novel in the UK context (Sizewell B used a hardware based secondary protection system that was accepted on the basis of e.g. the simplicity of the hardware design) and the risk reduction required singly and in combination. GEH stated during the 8/9 October 2007 familiarisation presentation that the DPS is hardware based. However, statements in Ref. 1 indicate that software and computer equipment is used in the implementation of the DPS, for example:-</p> <p><i>“7.8.1 System Description ... Diverse reactor trip initiation logic which is different from the safety-related RPS using separate and independent hardware with diverse software. ...</i></p> <p><i>7.8.1.2.1 Diverse Reactor Trip Functions ... This diverse set of scram logics resides in independent and separate hardware and software equipment from the RPS. ... The trip logic is based on two-out-of-four coincidence logic processed by two-out-of-three triplicate redundant processors and sent via three isolated fiber optic cables to the scram timing panel.”</i></p> <p>This assessment is based on the documented submissions and any changes to the document set will need to be subjected to strict configuration control (e.g. if the current design intent as explained during the familiarisation presentation is different to that described in the formal submission).</p>

	<p>07.2 GEH should provide a demonstration that the RPS and DPS 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.</p> <p>07.3 With regard to the Diverse Protection System (DPS) clarification will be required on:- i) justification of the use of the nonsafety-related DPS to initiate reactor trip ii) likelihood and acceptability of spurious trips, iii) DPS diversity analysis to substantiate its adequacy, iv) justification that the design meets appropriate (e.g. protection system) standards, v) technology used to implement the DPS and vi) scope of coverage of accident scenarios (e.g. compared to the protection system)</p>
<p>Failure independence</p> <p><i>Principle ESS.18 - No fault, internal or external hazard should disable a safety system.</i></p>	<p>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response in Ref.10 (see under internal hazards section) states:</p> <p><i>“Segregation associated with the C&I systems are described in DCD Chapter 7 and for the Electrical Power systems is covered in DCD Chapter 8. The reliability analysis of the C&I systems is presented in DCD Chapter 19. The Reactor Building is divided into four quadrants which are kept separate to meet fire protection (DCD Sub-section 9.5.1 and Appendix 9A) and flood (DCD Section 3.4) requirements, thus limiting the consequences of threats to one of four divisions of safety equipment.”</i></p> <p>NRC Criterion 23 and 24 are relevant to this SAP.</p> <p><i>“Criterion 23 – “The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as is connection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced”.</i></p> <p>GEH's evaluation against criterion 23 states <i>“The Reactor Protection (trip) System is designed to fail into a safe state. Use of independent channels allows the system to sustain any logic channel failure without preventing other sensors monitoring the same variable from initiating a scram. With a two-out-of-four logic design, the trip of any two channels initiates a scram. Intentional bypass for maintenance or testing causes the scram logic to revert to two-out-of-three. A failure of any one reactor protection input or subsystem component produces a trip in one channel. This condition is insufficient to produce a reactor scram, and the system performs its protective function upon trip of another channel. Failure of inputs or subsystem components in two channels produces a reactor scram. The environmental conditions in which the instrumentation and equipment of the reactor protection must operate were considered in establishing the component specifications. Instrumentation specifications are based on the worst expected ambient conditions in which the instruments must operate. The fail-safe design of the Reactor Protection (trip) System meets the requirements of Criterion 23”.</i></p>

Guidance - SAP paragraph 352

<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>P352 - NRC criterion 24 (Ref. 2) is relevant to this SAP, in particular, the guidance of SAP Paragraph 352.</p> <p>Criterion 24 states “<i>The protection system shall be separated from control systems to the extent that failure of any single control system component or channel or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited to assure that safety is not significantly impaired.</i>”</p> <p>GEH's evaluation against criterion 24 states “<i>Evaluation Against Criterion 24 - There is separation between the Reactor Protection System and the process control systems. Logic channel and actuator logics of the Reactor Protection System are not used directly for automatic control of process systems. Sensor outputs may be shared, but each signal is optically isolated before entering a redundant or Nonsafety-Related channel interface. Therefore, failure in the controls and instrumentation of process systems cannot induce failure of any portion of the protective system. Scram reliability is designed into the Reactor Protection System and hydraulic control unit for the control rod drive. The scram signal and mode of operation override all other signals. The systems that isolate containment and the reactor pressure vessel are designed so that any one failure, maintenance operation, calibration operation, or test to verify operational availability does not impair the functional ability of the isolation systems to respond to safety-related variables. The protection system is separated from control systems as required in Criterion 24.</i>”</p> <p>It is concluded that there is an adequate claim of compliance to this SAP through e.g. reference to NRC criterion. <u>The acceptability of control systems depending upon protection system measurements will require further consideration during Step 3.</u></p> <p>O8. Further clarification will be required as to the justification for control systems depending upon protection system measurements (e.g. how it is ensured that common cause failure of the sensors results in an appropriate response).</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>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response in Ref.10 (see under reactor core section) states:</p> <p><i>“Reactivity control is addressed in DCD Section 4.6 (FMCRD) and control rod shutdown margin is addressed in DCD Sub-section 4.3.3. No single failure or malfunction of any type can cause an inserted control rod to withdraw.</i></p> <p><i>The Standby Liquid Control system design is addressed in DCD Sub-section 9.3.5, its shutdown capability is demonstrated in DCD Sub-sections 9.3.5.3 and 15.5.4.”</i></p> <p>NRC criterion 26 “Reactivity Control System Redundancy and Capability” is also relevant to this SAP.</p> <p>Criterion 26 “<i>Two independent reactivity control systems of different design principles shall be provided. One of these systems shall use control rods, preferably including a positive means for inserting the rods, and shall be capable of reliably controlling</i></p>

	<p><i>reactivity changes to assure that under conditions of normal operation, including anticipated operational occurrences, and with appropriate margin for malfunctions such as stuck rods, specified acceptable fuel design limits are not exceeded. The second reactivity control system shall be capable of reliably controlling the rate of reactivity changes resulting from planned, normal power changes (including xenon burnout) to assure acceptable fuel design limits are not exceeded. One of the systems shall be capable of holding the reactor core subcritical under cold conditions."</i></p> <p>GEH's Evaluation Against Criterion 26 contained in Ref. 2 includes the following statements "<i>Two independent reactivity control systems utilizing different design principles are provided. The normal method of reactivity control employs control rod assemblies, which contain boron carbide (B4C), hafnium or other approved material. A Standby Liquid Control (SLC) system is also provided.</i></p> <p><i>..... Because of the carefully planned and regulated rod withdrawal sequence, prompt shutdown of the reactor can be achieved with the insertion of a small number of the many independent control rods.</i></p> <p><i>A Standby Liquid Control system containing a neutron-absorbing sodium pentaborate solution is the independent backup system. This system has the capability to shut the reactor down from full power and maintain it in subcritical condition at any time during the core life.The redundancy and capabilities of the reactivity control systems for the ESBWR satisfy the requirements of Criterion 26".</i></p> <p>Also note that Ref. 1 (section 7.8.1) states "<i>The ATWS/Standby Liquid Control (SLC) mitigation logic provides a diverse means of emergency shutdown using the SLC for soluble boron injection.</i>"</p> <p>It is concluded that there is an adequate claim that this SAP is met. However, clarification is required that the C&I systems used for implementation of diverse shutdown are adequately independent and diverse.</p> <p>O9. - GEH 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><i>Guidance - SAP paragraph 171 - 174</i></p>	<p>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response in Ref.10 states:</p> <p><i>"The design addresses CCF, by providing diverse means of delivering safety functions. PSR Section 2.12 and DCD Section 6.3 for example describe diversity and removal of common causes in initiation of the GDCS and initiation of DPVs to allow GDCS initiation. CCF is assessed in the PRA described in PSR Section 2.6, DCD Chapter 19 and Reference 3. The safety analyses of the beyond DBE (Special Events), which involve common mode failures and/or multiple failures beyond the single failure criterion, are addressed in DCD Section 15.5."</i></p> <p>it is noted that the C&I design includes a Diverse Protection System (DPS) (Ref 1 section 7.8) which is required to meet NRC concerns on common mode failure of digital C&I.</p> <p>See also discussion under ESS.7.</p>

<p>171 CCF claims should be substantiated.</p> <p>172 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.</p> <p>173 Nevertheless, it is conceivable that the continuing accumulation of good data and 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>P171/172/173 - O.10 Clarification is required on the use and justification of claim limits for software common cause failures. Note that for computer based safety systems the cut-off figure is 1 failure per 10,000 demands. The protection system software common cause failure figure used in the PSA is quoted as 10-4 pfd in Ref. 11 section 4.5.9.4. and in Ref. 11 table 4.5-7 a figure of 10-5 pfd is quoted as follows: “Table 4.5-7 -C&I System – Basic Events C63-CCFSOFTWARE 1.00E-05 Common cause failure of software”.</p> <p>P174 - See under ESS.2.</p> <p>It is concluded that an adequate compliance claim is made for this SAP.</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>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response to this SAP in Ref.10 states:</p> <p><i>“As a minimum, all safety-related functions can be accomplished assuming the most limiting single failure. Where appropriate, the plant safety analyses (DCD Chapter 15) include the effects of single failures. Compliance against single failure criteria is addressed in the General Design Criteria in DCD Section 3.1. All ECCS (DCD Section 6.3) and reactor shutdown (DCD Section 4.6) functions can be accomplished assuming more than just a single failure”.</i></p> <p>NRC Criterion 21 is also relevant to this SAP as is satisfaction of IEEE std 603 clause 5.1</p> <p>Criterion 21 Statement (from Ref. 2):- <i>“The protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2).....”.</i></p> <p>GEH state in Ref. 2 that <i>“Evaluation Against Criterion 21 - Reactor Protection System design provides assurance that, through redundancy, each channel has sufficient reliability to fulfill the single-failure criterion. No single component failure, intentional bypass maintenance operation, calibration operation, or test to verify operational availability, impairs the ability of the system to perform its intended safety function. The high functional reliability, redundancy, and in-service testability of the protection system satisfy the requirements</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>specified in Criterion 21.”</p> <p>Also in Ref. 1 (section 7.1.6.6.1.2 – Single Failure Criterion (IEEE std, 603, 5.1) GEH state “The ESBWR safety-related control systems include sufficient redundancy, diversity, and independence to meet system performance requirements even if the system is degraded by any single credible failure. ...”</p> <p>It is concluded that GEH claim compliance with this SAP.</p> <p>The response does not appear to explicitly address consequential failures.</p> <p>O.11 – GEH should clarify whether consequential failures resulting from the assumed single failure are considered as an integral part of the single failure.</p>
Safety systems	
<p>Requirement for safety systems</p> <p>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.</p>	<p>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response to this SAP in Ref.10 states:</p> <p>“ESBWR safety systems are described in DCD Chapter 6, “Engineered Safety Features,” Chapter 7, “Instrumentation and Controls,” and Chapter 8, “Electrical Power.” DCD Section 6.2, “Containment Systems”, DCD Section 6.3, “ECCS” and Chapter 15, “Accident Analysis,” provide the results of analyses demonstrating the ability of the safety systems to limit the consequences of design basis accidents and to achieve and maintain a safe state. Specifically, the ESBWR is designed to shutdown the reactor by a single safety system, e.g. the main control drive system alone even for most reactive conditions, e.g. cold shutdown, see DCD Chapter 4.”</p> <p>The full range of C&I safety systems (e.g. reactor protection system) are described in Ref. 1. See also the response to ERC.2.</p> <p>Within Ref. 4 (section 2.5) it is stated:- “A systematic approach to plant safety consistent with the GEH Boiling Water Reactor (BWR) technology base is applied to ESBWR for deterministic safety analyses. The key to the approach to plant safety is a Nuclear Safety Operational Analysis (NSOA). NSOA is a system level qualitative Failure Modes and Effects Analysis (FMEA) that shows which protective functions and systems are required to show compliance with regulatory criteria for events addressed in safety analyses. NSOA considers the entire duration of each event from the spectrum of possible initial conditions and aftermath until either some mode of planned operation is resumed or the plant is in a stable shutdown condition. The NSOA process uses operational criteria and required actions to identify the required systems, automatic instrument trips, monitored parameters (associated with required operator actions), and auxiliary systems to bring the plant to a stable shutdown condition for each event. The system-level requirements identified as required in the NSOA reflect the licensing basis of the plant and constitute the minimum required actions to bring the plant to a stable shutdown condition. Safety analyses are performed to demonstrate compliance with appropriate event acceptance criteria that focus on event consequences for limiting event paths. For a given event, the safety analysis limiting event path is selected to pose the most significant challenge to the applicable event acceptance criteria. Therefore, the safety analysis is consequences oriented, focusing on the limiting response to the event, while the</p>

<p>Guidance - SAP paragraph 336</p> <p>336 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.</p>	<p>NSOA is system oriented, focusing on the system-level required actions necessary to bring the plant to a stable configuration.”</p> <p>Also in Ref. 4 section 2.6 :-</p> <p>“ 2.6.1 Introduction - The ESBWR Probabilistic Safety Analysis (PSA) is a comprehensive study of the risks of severe accidents from the ESBWR. This section demonstrates that the design features of the ESBWR are sufficiently robust such that the risks of severe accidents and personnel exposure to radioactive nuclides due to the ESBWR plant are significantly lower than regulatory limits.”</p> <p>“2.6.4.3 Risk Reduction Initiatives Directed By the PSA Insights from the ESBWR PSA have already been used to implement several design enhancements. The following is a summary of several PSA-based changes that have been incorporated into the ESBWR design, and consequently have contributed to a significant improvement in nuclear safety: ...</p> <ul style="list-style-type: none"> • Determined the loads to be served by the Diverse Protection System, which supplies diverse control signals to safety functions. • Improved the design of digital controls to reduce the likelihood of inadvertent actuation of specified systems.” <p>Also from Ref.4 Table 2.6-1 ‘ESBWR Design Features That Reduce Core Damage Frequency and Severe Accident Risk’:- <i>“Instrumentation and Control - Multiple diverse systems to minimise common cause failures.”</i></p> <p>From review of the GEH documentation it is concluded that there is an adequate claim that ESS.1 is satisfied.</p> <p>P336 - See comments above and 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>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response to this SAP in Ref.10 states:</p> <p><i>“DCD Chapter 15 demonstrates safety by analyses against deterministic requirements; DCD Chapter 19 demonstrates probabilistic safety including levels of protection necessary to achieve defence in depth and required reliabilities. Also see response to “Defence in Depth” above.”</i></p> <p>NRC criterion 20 is also relevant to this SAP (see Ref. 2). <i>“3.1.3.1 Criterion 20 — Protection System Functions Criterion 20 Statement - The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of</i></p>

anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety”.

GEH's evaluation against criterion 20 states “The Reactor Protection System (RPS) is designed to provide timely protection against the onset and consequences of conditions that threaten the integrity of the fuel barrier and reactor coolant pressure boundary barrier. Fuel damage is prevented by initiation of an automatic reactor shutdown if monitored variables of nuclear steam supply systems (Section 7.2) exceed preestablished limits of anticipated operational occurrences. Response by the Reactor Protection System is prompt and the total scram time is short. In addition to the Reactor Protection System, which provides for automatic shutdown of the reactor to prevent fuel damage, protection systems are provided to sense accident conditions and to initiate automatically the operation of other systems and components important to safety. Other systems automatically isolate the reactor vessel or the containment to prevent the release of significant amounts of radioactive materials from the fuel and the reactor coolant pressure boundary. The controls and instrumentation for the ECCS and the isolation systems are initiated automatically when monitored variables exceed pre-selected operational limits. The design of the protection system satisfies the functional requirements as specified in Criterion 20”.

With regard to the determination of required reliabilities GEH's compliance statement to IEEE 603 standard (Ref. 1) is relevant:-

“7.1.6.6.1.16 Reliability (IEEE Std. 603, Section 5.15)-
The degree of redundancy, diversity, testability, and quality of the ESBWR safety-related C&I design is adequate to achieve the functional reliability necessary to perform its function. Safety related equipment is provided under GEH's Appendix B quality program. BTP-14 will be followed for software development processes to achieve reliable software design and implementation. To achieve defense against common mode failure, the design includes many defense-in-depth and diversity measures including the incorporation of the DPS described in Section 7.8. LTR, “ESBWR C&I Defense-in-Depth and Diversity Report,” NEDO-33251 (Reference 7.1-4), provides specific information on the redundancy and diversity used in ESBWR safety-related C&I systems. Q-DCIS is included in the consideration of the ESBWR PRA. (See Chapter 19)”

The description of reliability appears to address this topic in a qualitative manner without definition of the quantitative reliability targets for each system.

O12. GEH should clarify how the safety system quantitative reliabilities were determined.

Also see above under ESS.7.

From review of the GEH statements it is concluded that there is an adequate claim that this SAP is satisfied.

Guidance - SAP paragraph 337

337 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.

P 337 - See comments above and under ESS.1. Satisfaction of SAP paragraph 337 will be considered during Step 3.

<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><i>Guidance - SAP paragraph 338</i></p> <p>338 <i>Monitoring provisions should be classified as safety or safety-related systems as appropriate and should be made:</i></p> <p>a) <i>in a central control location; and</i></p> <p>b) <i>at emergency locations (preferably a single point) that will remain habitable during foreseeable facility emergencies.</i></p>	<p>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response to this SAP in Ref.10 states: <i>“The monitoring provisions of the plant are described in DCD Chapter 7 and include remote shutdown stations.”</i></p> <p>Two NRC criterion (Ref. 2) are relevant to this SAP</p> <p><i>“Criterion 13 Statement - Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the RCPB, and the containment and its associated systems.”</i></p> <p>And</p> <p><i>“Criterion 19 Statement -A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident. Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrument action and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of procedures.”</i></p> <p>GEH claim that the ESBWR design is compliant with these criterion (Ref.2). For example, GEH State (Ref. 2):- <i>“ In the unlikely event that the control room must be vacated and access is restricted, instrumentation and controls are provided by two divisional Remote Shutdown System (RSS) panels located outside the control room in the Reactor Building. Either or both of the RSS panels can be utilized to safely perform a hot shutdown and a subsequent cold shutdown of the reactor.</i></p> <p><i>The control room design meets the requirements of Criterion 19”.</i></p> <p>From review of the GEH statements it is concluded that there is an adequate claim that this SAP is satisfied. However clarification should be provided that the emergency locations remain habitable during foreseeable facility emergencies.</p> <p>O13. 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>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response to this SAP in Ref.10 states:</p> <p><i>“SCRAM, ECCS and depressurisation are all automatically initiated and require no operator intervention for 72 hours. Once started these operations cannot be reversed by the operator. Details are provided in DCD Sections 6.2, 6.3 and Chapter 7.”</i></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>GEH provide compliance statements in relation to IEEE standard 603. Sections 5.2 and 7.3 of IEEE standard 603 are relevant to this SAP.</p> <p>In Ref. 1 section (7.1.6.6.1.3) GEH state "<i>Completion of Protective Action (IEEE Std. 603, Sections 5.2 and 7.3) - After initiation by either automatic or manual means, the protective actions go to completion in conformance with IEEE Std. 603, Section 5.2, either by the use of seal-in logic, non-resettable squib valves, manually reset valves, diverse functions, or a combination of logic, valves and functions. Deliberate operator action is required to return the safety-related systems to normal.</i>"</p> <p>The following extracts from Ref.1 show that automatic initiation of protective actions is addressed in the ESBWR design. :-</p> <p><i>"7.2.1.2.4.1 Arrangement - The RPS-related equipment is divided into four redundant divisions of sensor (instrument) channels, trip logics and trip actuators, and two divisions of manual scram controls and scram logic circuitry. The sensor channels, divisions of trip logic, divisions of trip actuators, and associated portions of the divisions of scram logic circuitry together constitute the RPS automatic scram and air header dump (backup scram) initiation logic. The divisions of manual scram controls and associated portions of the divisions of scram logic circuitry together constitute the RPS manual scram and air header dump initiation logic. The automatic and manual scram initiation logics are independent of each other and use diverse methods and equipment to initiate a reactor scram.</i></p> <p><i>7.1.3.2.2.1 Emergency Core Cooling System (ECCS)</i> <i>The safety-related ECCS is an engineered safety feature that provides automatic initiation of the Isolation Condenser System, Automatic Depressurization System, Gravity Driven Cooling System and Standby Liquid Control system to mitigate loss of coolant accidents. Refer to Subsection 7.3.1 for additional information."</i></p> <p>It is concluded that there is an adequate claim against this SAP. Further investigation will be required during Step 3 to ensure adequate automatic initiation of all safety system (protective) functions (see claim below made in response to ERL.3).</p> <p>P343 - To be considered during Step 3, however, it is noted that In Ref. 1 GEH state "<i>7.1.6.6.1.18 Manual Control (IEEE Std. 603, Sections 6.2 and 7.2) - The ESBWR design provides for manual initiation of each protective action at the system level in conformance with RG 1.62, and at the division level in conformance with IEEE Std. 603, Sections 6.2 and 7.2. After manual initiation, the protective actions go to completion in conformance with IEEE Std. 603, Section 5.2 as described in Subsection 7.1.6.6.1.3. The manual initiation of a protective action performs all actions carried out by automatic initiation.</i></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</i></p>	<p>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response to this SAP in Ref.10 states:</p> <p><i>"All protective actions for safety functions are automatic in the Design Basis and no credit is taken for operator actions. Further detail is in DCD Chapter 6 and 15 for the analysis, whilst Chapter 7 describes the associated C&I."</i></p> <p>Also, see response above to ESS.8.</p>

<p>safe state.</p>	<p>From review of the GEH statements it is concluded that there is an adequate claim that this SAP is satisfied.</p>
<p>Reliability – Avoidance of complexity</p> <p>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.</p> <p>Guidance - SAP paragraphs 355</p> <p>355 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:</p> <ul style="list-style-type: none"> a) a comprehensive examination of all the relevant scientific and technical issues; b) a review of precedents set under comparable circumstances in the past; c) an independent third-party assessment in addition to the normal checks and conventional design; d) periodic review of further developments in technical information, precedent and best practice. 	<p>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response to this SAP in Ref.10 states:</p> <p><i>“Safety systems are simplified by use of passive operation principles. The ESBWR has immediate reporting of failures within the digital RPS and significant control systems. DCD Chapters 5 (ICS), 6 (Containment, ECCS, Control Room habitability), 7 (C&I), 8 (Electrical) and 9 (SLCS) provide discussions of the safety-related systems design and fail safe philosophy. See also response to “Failure to Safety” above.”</i></p> <p>GEH do not appear to address whether the design avoids complexity within the safety systems.</p> <p>O14.1 - GEH should either provide a justification that the design of the safety systems has avoided complexity or identify and justify any complex situations. For example, where two computer-based systems important to safety are required in combination to mitigate the consequence of a postulated initiating event (e.g. to reduce accident frequencies to acceptable limits).</p> <p>O14.2 Clarification should be provided as to whether the C&I design uses any complex hardware such as ASICs/FPGAs etc.</p>
<p>Allowance for unavailability of equipment</p> <p>Principle ESS.23 - In determining the safety system provisions, allowance should be made for the unavailability of equipment</p> <p>Guidance - SAP paragraphs 357</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>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response to this SAP in Ref.10 states:</p> <p><i>“Protection systems are all 4 channels (2/4 logic) with allowance for one channel to be out for maintenance at which time the system defaults to 2/3 logic as described in DCD Chapter 7 (C&I). DCD Chapter 16 defines allowable plant states and durations with unavailable equipment through the definition of Technical Specifications.”</i></p> <p>NRC criterion 21 is relevant to this SAP. Ref. 2 contains the following text:- <i>“Criterion 21 Statement - “The protection system shall be designed for high functional reliability and in service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that(2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.</i></p> <p>GEH’s Evaluation Against Criterion 21 states - <i>“Reactor Protection System design provides assurance that, No single component failure, intentional bypass maintenance operation, calibration operation, or test to verify operational availability, impairs the ability of the system to perform its intended safety function. ... The Reactor Protection System includes design features that permit in-service testing. This ensures the functional reliability of</i></p>

	<p><i>the system should the reactor variable exceed the corrective action setpoint. The Reactor Protection System can be tested during reactor operation. ...The high functional reliability, redundancy, and in-service testability of the protection system satisfy the requirements specified in Criterion 21."</i></p> <p>The above statements are judged to provide an adequate claim that SAP ESS.23 is addressed for the reactor protection system.</p> <p>O15. Clarification will be required as to whether other safety systems (i.e. in addition to the protection system) comply with SAP ESS.23.</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 <i>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.</i></p> <p>193 <i>Where complete functional testing is claimed not to be reasonably practicable, an equivalent means of functional proving should be demonstrated.</i></p>	<p>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response to this SAP in Ref.10 states:</p> <p><i>"Safety system surveillance testing, unavailabilities, and maintenance intervals are presented within the Technical Specifications, as presented in DCD Chapter 16."</i></p> <p>NRC criterion 21 is relevant to the protection systems. See the comments above under ESS.23.</p> <p>O16. 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 safety</p>	
<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 <i>'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:</i></p> <p>a) <i>Thorough application of technical design practice consistent with current accepted standards for the development of software for computer-based safety systems.</i></p> <p>b) <i>Implementation of an adequate quality assurance programme and plan in accordance with appropriate quality</i></p>	<p>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response to this SAP in Ref.10 states: <i>"Software safety management arrangements, software QA plan and standards, and testing (Verification & Validation) are described DCD Chapter 7 and Appendix 7B."</i></p> <p>GEH state that the Q-DCIS (i.e. the safety related portion of the Distributed Control and Instrumentation System - DCIS) conforms to various regulations and standards some of which are relevant to the performance of computer software (e.g. see Ref. 1 sections 7.1.2.4 and 7.1.6). One of the key standards quoted is IEEE 7-4.3.2 "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" and in section 7.1.6.4 of Ref. 1 NRC endorsement (or otherwise) of sections of this standard is described. It is also stated that the software development process of the Q-DCIS will follow the guidelines of NRC BTP HICB-14.</p> <p>From review of the GEH documentation (e.g. discussion in Ref. 1) it is concluded that there is a claim that there are adequate arrangements for the development of computer-based safety systems.</p>

<p>assurance standards.</p> <p>c) <i>Application of a comprehensive testing programme formulated to check every system function, including:</i></p> <ul style="list-style-type: none"> • <i>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;</i> • <i>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</i> • <i>a programme of dynamic testing, applied to the complete system, that is capable of demonstrating that the system meets its reliability requirements.</i> <p>361 <i>Independent ‘confidence-building’ should provide an independent and thorough assessment of a safety system’s fitness for purpose. This comprises the following elements:</i></p> <p>a) <i>Complete and preferably diverse checking of the finally validated production software by a team that is independent of the systems suppliers, including:</i></p> <ul style="list-style-type: none"> • <i>independent product checking providing a searching analysis of the product;</i> • <i>independent checking of the design and production process, including activities needed to confirm the realisation of the design intention; and</i> <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>O17.1 The arguments to support the claim that adequate arrangements are in place for the development of computer-based safety systems will need to be assessed during Step 3 and in particular the way in which each of SAP paragraphs 360 to 361 has been met. 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 (which is largely US IEEE standards or NRC regulatory guides will require further consideration during Step 3 (see also comments under ECS.3).</p> <p>O17.2 The scope of application of this SAP will need to be clarified as applying to all safety systems (e.g. to cover all systems contributing to reactor protection such as Q-DCIS and Diverse Protection System etc.). See also discussion above under ECS.1, ECS.2 and ECS.3.</p> <p>O17.3 The approach to instrumentation and actuators that contain programmable devices (e.g. SMART instruments) will need to be defined.</p> <p>O17.4 Clarification will also be required on the approach to use of pre-developed hardware and software (e.g. compliance to appropriate standards such as IEC 60880). For example, it is noted that in Ref. 1 section 7.1.6.4 “Conformance with Regulatory Guides” it is stated that “<i>The following sections are noted in IEEE Std. 7-4.3.2 as specifically addressed by the NRC in RG 1.152:.... - Annex C ‘Dedication of existing commercial computers’: This is similar to the 1993 version. The NRC refers to Reference 7.1-11 as a replacement for Annex C’.</i> Note reference 7.1-11 is to the Electric Power Research Institute (EPRI) TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications”.</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>The GEH response to this SAP in Ref.10 states: “<i>The ESBWR complies with ESS.27. Hardware and software standards are defined in DCD Chapter 7 and Appendix 7B.</i>”</p> <p>See discussion under ESS.27.</p> <p>O18. GEH should demonstrate that appropriate design standards are used for this class of system (see also ESS.27 and ECS.3). In addition, the general concept of ESS.27 is applicable to computers used in safety-related systems (see Ref. 12) which means arguments of production excellence and</p>

	independent confidence building will need to be presented.
Control and instrumentation of safety-related systems	
<p>Provision in control rooms and other locations</p> <p><i>Principle ESR.1 - Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate locations on the facility.</i></p> <p><i>Guidance - SAP paragraphs 365 - 366</i></p> <p>365 <i>Principle EHF.7 (paragraph 382 f.) on user interfaces is also relevant to this principle.</i></p> <p>366 <i>The provisions should encompass normal operation, abnormal operation and postulated fault conditions including, where reasonably practicable, severe accidents. The equipment should include indicating and recording instrumentation and controls as appropriate.</i></p>	<p>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response to this SAP in Ref.10 states: <i>“The Main Control Room is discussed in DCD Chapter 7 and includes descriptions of the Remote Shutdown Stations where the operator can affect safe shutdown outside of the Main Control Room.”</i></p> <p>NRC criterion 13 and 19 are relevant to this SAP (see above under ESS.3). Details of the safety related controls is provided in Ref.1 but note that the GEH classification for many of the systems is nonsafety-related (see comments above under ECS 1, 2 and 3).</p> <p>From review of the GEH documentation it is concluded that there is an adequate claim that this SAP is satisfied but see ECS.1, 2 and 3 above.</p> <p>P365/366 - See above and response to ESS.3. Within Ref.3 it is stated that <i>“The main control room (MCR) is comprised of an integrated set of operator interface panels (e.g., main control console, large display panel). The main control room panels and other MCR operator interfaces are designed to provide the operator with information and controls needed to safely operate the plant in all operating modes (as denoted in the Chapter 16 Table 1.1-1, MODES) and maintain the plant in a safe shutdown condition. Human factors engineering principles have been incorporated into all aspects of the MCR design”</i>. Extent of coverage will be considered during Step 3.</p>
<p>Provision of controls</p> <p><i>Principle ESR.3 - Adequate and reliable controls should be provided to maintain variables within specified ranges</i></p>	<p>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response to this SAP in Ref.10 states:</p> <p><i>“DCD Chapter 7 describes both protection system controls and operational controls. DCD Chapter 18 describes the process employed to implement Human Factors Engineering and develop the Man-Machine Interface Systems.”</i></p> <p>NRC Criterion 13 is quoted in Ref.2 and this criterion has a similar requirement to SAP ESR.3 (i.e. <i>“Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges”</i>). In response GEH state that <i>“Appropriate controls have been provided to maintain the variables in the operating range and to initiate the necessary corrective action in the event of abnormal operational occurrence or accident”</i>. The controls provided for the ESBWR are described in Ref.1. There is, therefore, an adequate claim that this SAP is addressed in the design of the ESBWR.</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><i>Guidance - SAP paragraph 368</i></p>	<p>Ref. 10 provides a claim that the ESBWR complies with this SAP. The GEH response to this SAP in Ref.10 states: <i>“Communications systems are described in DCD Sub-section 9.5.2.”</i></p> <p>The ESBWR communication system is described in Ref. 5 Section 9.5.2. where it is stated that <i>“9.5.2 Communications System - The communication system provides the means to conveniently and</i></p>

368	<p>These communication systems should not have any adverse effect on safety systems, or safety-related systems.</p>	<p><i>effectively communicate between various plant locations and with off-site locations during normal, maintenance, transient, fire, and accident conditions under maximum potential noise levels”.</i></p> <p>Within Ref. 5 it is stated that: “9.5.2.1 Design Bases - Safety (10 CFR 50.2) Design Bases - The communication system serves no safety-related function and thus has no safety design basis”.</p> <p><i>Power Generation Design Bases</i></p> <p><i>The communication system power generation design bases are as follows:</i></p> <ul style="list-style-type: none"> • <i>Communication subsystems are independent of one another, therefore, a failure in one subsystem does not degrade the performance of the other subsystems;</i> • <i>The communication system is in accordance with applicable codes and standards and the equipment is shielded as necessary, from the adverse effects of electromagnetic interference (EMI) and radio frequency interference (RFI); and</i> • <i>The communication subsystems are operable during a loss of off-site power.</i> <p>It is concluded that an adequate claim exists against this SAP.</p>
-----	---	--

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