Health and Safety Executive

HEALTH & SAFETY EXECUTIVE
NUCLEAR DIRECTORATE
ASSESSMENT REPORT

New Reactor Build

Westinghouse 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 Westinghouse AP1000 submission in accordance with the strategy outlined in Ref. 1. 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. 1) 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. 5).

2. REPORT

3. Westinghouse has provided a number of submissions relevant to C&I assessment. The main submission that describes the C&I is Ref. 3. 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 the Plant Protection and Monitoring System (PMS) which initiates reactor trip and also provides engineered safety features functions such as reactor core cooling via initiation of the passive residual heat removal system),
    - plant control and monitoring systems (e.g. the Plant Control System that performs functions such as reactor power control),
    - main control room with backup via the remote shutdown workstation, 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. Westinghouse provided a document (Ref. 2) that gives a specific response against each of the SAPs. The response either confirms compliance or notes that the SAP is addressed by some other argument such as it not being relevant to the AP1000 design (with a justification of such statements). The main "area" of C&I SAPs where a direct claim of compliance is not made is in the Essential Services Area (e.g. a number of the SAPs are claimed not to be relevant to the AP1000 design)

and the adequacy of claims in this area will be considered further during Step 3 (see Ref. 1).

6. The main body of the assessment is contained in the Annex of this report. Westinghouse claim compliance with all of the SAPs in the Annex except for ESS.21 complexity. Within the Annex there are a number of observations and these will need to be raised with Westinghouse 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 Westinghouse 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 Westinghouse approach to that defined by the IAEA, SAPs and BS IEC 1226:2005 will need to be determined. The Westinghouse 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. - 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 C&I equipment) (O4. - SAP ESS.21). For example, how is it ensured that component failures result in an appropriate system response. Typical protection system practice is to use some form of dynamic trip bus that fails to a safe state if not continuously stimulated.
- Clarification is required on the use of probabilistic criteria in the design of the AP1000 C&I systems (O5. - SAP EDR.2, O9 - SAP EDR.3, O6.2 - SAP ESS.7 and O9 - SAP EDR.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. Note the protection system reliability used in the PSA for software common mode failures is of the order 10-5 pfd (Ref. 7 section 26.5.4) and this is lower than the 10-4 pfd CCF cut-off figure applied to computer based safety systems (see Ref 8).
- Westinghouse should provide a demonstration that the primary protection system and diverse actuation 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 (O6. - 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 (as defined in Ref. 8) (O15.1. to O15.4. - SAP ESS.27 and O16 - SAP ESR.5).

7. The Westinghouse submissions on C&I mainly describe a conceptual design and Westinghouse explain that the "design certification" of the AP1000 focuses on the process used to design and implement the C&I rather than on the specific implementation (Ref. 3, section 7.1). Westinghouse also explain that the description of the protection system is based on the Common Q platform and it is noted that this platform has been generically approved by the USNRC. 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 UK implementation of the AP1000 conceptual design).

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. During the familiarisation presentation on 3 October 2007 Westinghouse provided further details of its current design implementation expectations (e.g. Diverse Actuation System based on Westinghouse 7300 hardware based product line) and this intent might be different to that described in the formal submissions (see O6.4 - SAP ESS.7).

O17. Westinghouse 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 AP1000 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. 6) which provided a consensus view on the safety case requirements for computer based systems. The USNRC were 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 Westinghouse 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 Westinghouse. 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 Westinghouse. It is noted that Ref. 3 contains a reference to "the

cyber security implementation for AP1000" (i.e. reference 22) but this has not been reviewed as part of this assessment.

O18. Westinghouse 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. 3 it was noted that some requirements are left for the "license applicant" to define e.g. protection system setpoints and response time testing (section 7.1.6). Also the licence applicant is required to perform an FMEA for the protection and safety monitoring system including software hazards analysis (section 7.2.3). The approach to be developed for the assessment of Steps 3, 4 and Phase 2 (see above) will need to address the satisfaction of the requirements placed on the "license applicant".

3. CONCLUSIONS

13. Westinghouse provide adequate claims of compliance for all of the fundamental C&I Step 2 SAPs (see Annex) except for ESS.21 complexity. It is considered that this is an acceptable position for the conclusion of the Step 2 assessment since clarification of the position on ESS.21 can be addressed during Step 3. The assessment has given rise to a number of observations and these will need to be raised with Westinghouse. These observations should be addressed during Step 3. The submissions largely describe a design concept (i.e. only limited information provided on the actual implementation details such as use of the common Q platform). 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 AP1000 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 Westinghouse from proceeding to Step 3. Therefore, Westinghouse should be allowed to proceed to Step 3.

R2. The "observations" identified throughout this assessment report by bold text will require a Westinghouse response prior to Step 3.

R3. NII should develop an approach (i.e. for Steps 3, 4 and Phase 2) for the assessment of the AP1000 C&I design implementation (i.e. covering the exact C&I systems, platforms, products and components etc. selected for the implementation of the AP1000 conceptual design within the UK).

5. REFERENCES

1. Step 2 C&I Assessment Strategy - NSD DIV 6 Assessment Report No. AR07002.
2. UK Compliance Document for AP1000 Design – Safety Assessment Principles Roadmap for AP1000 Design – UKP-GW-GL-710
3. UK AP 1000 Safety, Security and Environmental Report – Revision 1.
4. Nuclear Power Plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions – BS IEC 61226:2005
5. Nuclear Division – Division 6 Unit 6D Operating Plan 2 August 2007 – 31 March 2008
6. 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
7. UK AP1000 Probabilistic Risk Assessment – UKP-GW-GL-022-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	
Safety categorisation *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.* *Guidance - SAP paragraphs 149-152 .* *149 A safety categorisation scheme could be determined on the following basis:* *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.* *150 The method for categorising safety functions should take into account:* *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.* *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.* *152 The categorisation assigned to each safety function should be used to classify structures, systems and components required to deliver that function.*	ECS.1 - A claim is made in Ref. 2 page C-30 that Westinghouse comply with this SAP. The description outlines the classification of systems based on categorisation of functions. Westinghouse note that safety related classified items implement safety related functions and a brief description of such functions is provided within Ref. 2 (page C-31) where it is stated:- *"Safety-related is a classification applied to items relied upon to remain functional during or following a design basis event to provide a safety-related function. Safety-related also applies to documentation and services affecting a safety-related item.* *Safety-related function is a function that is relied upon during or following a design basis event to provide for the following:* *– Integrity of the reactor coolant pressure boundary* *– Capability to shut down the reactor and maintain it in a safe shutdown condition* *– Capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the guideline exposures of 10 CFR 100"* No other categories are described. The description of C&I systems in the UK AP 1000 Safety, Security and Environmental Report Ref. 3 (Chapter 7) identifies two classes of systems i.e. "safety-related" and "nonsafety-related" relevant to C&I. Ref. 3 Chapter 3 (section 3.2) provides a definition of the safety classes and explains how the "safety related" and "non-safety related" classes are further subdivided (e.g. safety related into classes A, B and C). However, it is unclear precisely how the functions to be implemented in the C&I systems (e.g. as described in Ref. 3 Chapter 7) were determined (i.e. definition of functions, category and allocation to appropriate class of system). It appears that the assignment might not be by precise functions (e.g. as determined by accident analysis) but by a general assignment in accordance with the broad definitions provided in Ref. 2 (see above). In addition it is not clear whether the C&I allocations would align with those shown in standards used internationally and in the UK such as BS IEC 61226:2005 Ref 4. **O1. Westinghouse 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 Westinghouse approach to that defined by the IAEA, SAPs and BS IEC 1226:2005 should be demonstrated.**
Safety classification of structures, systems and components *Principle ECS.2 - Structures, systems and components*	ECS.2 - A claim is made in Ref. 2 page C-32 that Westinghouse

that have to deliver safety functions should be identified and classified on the basis of those functions and their significance with regard to safety. *Guidance - SAP paragraphs 153-156 .*	comply with this SAP. However, the document refers to the description under ECS.1 which addresses both categorisation and classification (see comments above under ECS.1). P153 – see under ECS.1
153 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: *a) the category of safety function(s) to be performed by the item (see Principle ECS.1);* *b) the consequences of failure to perform its function;* *c) the probability that the item will be called upon to perform a safety function;* *d) the time following any initiating fault at which, or the period throughout which, it will be called upon to operate.*	
154 A safety classification scheme could be determined on the following basis: *a) Class 1 – any structure, system or component that forms a principal means of fulfilling a Category A safety function.* *b) 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.* *c) Class 3 – any other structure, system or component.*	P154 - For C&I, the classification system results in two categories, namely; safety-related and nonsafety-related. Note, for example, that the Plant Control System (PCS) would appear to be the equivalent of the Sizewell B Class 1 High Integrity Control System (HICS) but it is stated to be nonsafety-related. Reactor power control is performed by the PCS and this would be classified as safety-related according to IAEA criteria (Ref. 3 - page 7.1-4). Also the Diverse Actuation System is classified as nonsafety-related. Within Ref.3 (chapter 3) it is stated:- *"3.2.2.9 Electrical Classifications - Safety-related electrical equipment is equipment Class C, as outlined in subsection 3.2.2.5, and is constructed to IEEE standards for Class 1E. The nonsafety-related electrical equipment and instrumentation is constructed to standards including non-Class 1E IEEE standards and National Electrical Manufacturers Association (NEMA) standards. Safety-related electrical equipment and instrumentation is identified in Section 3.11."* Note that Ref. 3 section 3.11 deals with environmental qualification of electrical and mechanical equipment. **O2. Westinghouse 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.** Also see comments above under ECS.1.
155 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.	P155 - Ref. 3 (section 7.1.2.10) claims that "Isolation devices are used to maintain the electrical independence of divisions, and to prevent interaction between nonsafety-related systems and the safety-related system".
156 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	P156 - Step 3.

function.	
Standards *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.* *Guidance - SAP paragraphs 157-161*	ECS.3 - A claim is made in Ref. 2 page C-34 that Westinghouse comply with this SAP. Ref. 2 notes that "*the industry codes and standards that apply to the design and procurement of safety-related components are specified in the DCD*" (Ref. 3). From review of Ref. 3 it can be seen that the C&I standards base appears to be largely US (IEEE), some of which pre-date what would be considered "modern" for C&I. For example, one of the key standards (i.e. IEEE Std 603 IEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations) provides a reference to a 1991 version when a later version exists (i.e. 1998). There is a need to consider whether the selected standards are in agreement with modern UK national and international C&I nuclear standards. Note, also that, for example, Ref. 3 section 7.1.4.2 quotes "applicable portions" i.e. full compliance is not always claimed. **O3.1 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.** **O3.2 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.**
157 *The standards should reflect the functional reliability requirements of structures, systems and components and be commensurate with their safety classification.*	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 assumed normal practice). **O3.3 - Westinghouse should clarify how the standards reflect the functional reliability requirements.**
158 *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.*	P158 - See above
159 *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.*	P159 - See above
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,*	P160 - The AP1000 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

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. *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.*	related class is equivalent to SAP class 2. Hence the AP1000 nonsafety-related class appears to encompasses both SAP classes 2 and 3. **O3.4 – Westinghouse should clarify how SAP guidance paragraph 160 is met (e.g. claim of independence or standards appropriate to the highest class).** P161 – None identified.
Failure to safety	
Failure to safety *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.*	Westinghouse claim that the AP1000 design has addressed this principle (Ref. 2 page C 35). Westinghouse note that for the protection systems NRC Criterion 23 is relevant and compliance is claimed in Ref. 3, section 3.1 where it is stated:- *"AP1000 Compliance - The protection system is designed considering the most probable failure modes of the components under various perturbations of the environment and energy sources. Reactor trip channels are designed on the deenergize-to-trip principle so that a single event (that is, loss of power) that could affect many functions at the same time causes the channels to actuate to their tripped conditions."* Also, see below under ESS.21.
Reliability – fail-safe approach *Principle ESS.21 - The design of a safety system should avoid complexity,* ***apply a fail-safe approach and incorporate the means of revealing internal faults from the time of their occurrence.*** *Guidance - SAP paragraphs 356* *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.).*	Westinghouse claim that the AP100 design has addressed this SAP (Ref. 2). Within Ref. 2, in response to ESS.21, Westinghouse state "*AP1000 safety systems, fluid systems, instrumentation and control, and electrical power systems, incorporate self-monitoring features and are redundant. They are fail-safe to the extent practicable…. The instrumentation and control safety systems use self-diagnostics to reveal faults from the time of their occurrence*". Ref 3 section 7.2.2.1 claims that the protection system maintains safety functions "*during single point failures*". However, this is not necessarily equivalent to a fail-safe approach (e.g. use of dynamic trip bus to ensure system failures result in an appropriate response such as setting of a guardline "partial trip"). **O4. Westinghouse should clarify the basis of the fail-safe approach (e.g. how it is ensured that system failures result in an appropriate response).**
Defence in depth	
Redundancy, diversity and segregation *Principle EDR.2 - Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety*	EDR.2 – Westinghouse claim that the AP1000 design has adequately addressed this principle, for example, Ref. 2 states "*The AP1000 design has addressed EDR.2. … The AP1000 design, as documented in the DCD, has included redundancy, diversity, and segregation.* *The NRC has approved the AP1000 approach on redundancy, diversity, and segregation as part of the Design Certification process".* From Ref. 3 it can be seen that the AP1000 design does use redundancy and diversity, for example, through the provision of a Diverse Actuation System, as a backup to the protection system

Guidance - SAP paragraph 170 *170 It should be demonstrated that the required level of reliability for their intended safety function has been achieved.*	which utilises redundant logic systems. Note also, the provision of four reactor trip actuation divisions within the reactor protection system. Also, in response to NRC Criterion 24 (separation of Protection and control systems Westinghouse state. "*The protection system is separate and distinct from the control systems".* P170 - Two system classes have been identified (see above) but it is not clear how reliability figures are used in the design of AP1000 C&I systems nor how achievement is demonstrated (see O3.3 above). From discussion during the familiarisation presentation it was noted that the protection system reliability is of the order 10-5 pfd and the Diverse Actuation System reliability is 10-2 pfd. The reliability figure for the protection system is higher than the CCF limit for computerised safety systems stated in Ref. 8 (see EDR.3 below). **O5.1 Clarification is required on the use of probabilistic criteria in the design of the AP1000 C&I systems (e.g. definition and justification of the precise integrity targets assigned to C&I systems).** **O5.2 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.**
Determination of safety system requirements – Defence in depth *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.* *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.*	Westinghouse claim that "*The AP1000 design has addressed EDR.2*" (Ref. 2). For example, it is stated that "*In general, system design uses redundancy features to account for single failure criteria. Diversity is used to address shutdown requirements. Segregation is used to account for fire, flood, and seismic requirements".* In addition, Westinghouse state that the safety systems' design meets appropriate NRC 10 CFR 50 criteria, for example, Criterion 22, "Protection System Independence"; Criterion 23, "Protection System Failure Modes"; and Criterion 24, "Separation of Protection and Control Systems," (see Ref 3 section 3.1 for Westinghouse compliance statements). It is concluded that Westinghouse provide an adequate claim that the AP1000 design incorporates defence in depth. See also discussion above under EDR.2 and below against ESS.7 P337 - Step 3.
Diversity in the detection of fault sequences *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.* *Guidance - SAP paragraph 342* *342 This principle applies in particular to UK civil nuclear power reactor safety systems and in*	Westinghouse claim that the AP1000 design has addressed ESS.7. The following extract from Ref. 2 outlines the way in which it is claimed that the AP1000 design meets this SAP:- *"Diverse variables are generally provided to detect the approach to safety limits and ensure that required automatic or manual safety actions can be performed. The type of diversity used varies between safety functions depending on the variables available to*

particular to high integrity safety systems.	*monitor the conditions that might exist.* *Diversity in the initiation of safety functions is provided by the diverse actuation system that is provided. The diverse actuation system uses a diverse platform (hardware and software) from that used in the protection and safety monitoring system. The safety functions implemented in the diverse actuation system are based upon insights gained from the PRA study. Diverse actuation system functions are provided for event sequences that the PRA study indicated the potential for common mode failures within the protection and safety monitoring system to be substantial contributors to core damage frequency or large early release frequency."* Within Ref. 7 (chapter 27) it is stated that: *"Separate sensors are used for the protection and safety monitoring system and the diverse actuation system. These sensors may, however, be of the same type. Therefore, common cause failures of similar sensor types are applied across the protection and safety monitoring system, plant control system, and the diverse actuation system."* Further, it is noted that the analysis of the protection system contained in Ref.7 (chapter 26) is not based on the Common Q platform that is referenced in Ref. 3. From Ref. 7 it can be seen that the figure used for protection system software failure is of the order 1E-5 and the DAS has a 1E-2 pfd (also see below under EDR.3). **O6.1 Westinghouse should clarify why it is acceptable for the analysis of the protection system contained in UK AP1000 PRA (Ref. 7, chapter 26) not to be based on the Common Q platform that is referenced in the DCD (Ref. 3).** **O6.2 Westinghouse should provide a demonstration that the primary protection system and diverse actuation 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.** The approach to protection system diversity, as described, will require to be considered further during Step 3. 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), the adequacy of the diversity given the precise implementation details. Note that 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. During the familiarisation presentation on 3 October 2007 Westinghouse provided further details of its current design implementation expectations (e.g. Diverse Actuation System based on Westinghouse 7300 hardware based product line). However, statements in Ref. 3 indicate that software and computer equipment is used in the implementation of the DAS, for example:- *"7.7.1.11 Diverse Actuation System - ...* *Diversity is achieved by the use of different architectures, hardware implementations and any software from that of the protection and safety monitoring system.* *Diversity of any software is achieved by running different operating systems and programming in different languages. …* *The adequacy of the hardware and any software is demonstrated through the verification and validation program discussed in subsection 7.1.2.14. This program provides for the use of commercial off-the-shelf hardware and software."* It should be noted that 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). Note that the diversity required by this SAP is within the protection system not across independent systems such as the protection system and DAS. **O6.3 Westinghouse should clarify the extent of diversity in the detection of fault sequences within each "protection" system in addition to that claimed across systems.** **O6.4 With regard to the Diverse Actuation System (DAS) clarification will be required on:- i) justification of the use of the nonsafety-related DAS to initiate reactor trip ii) likelihood and acceptability of spurious trips, iii) DAS diversity analysis to substantiate its adequacy, iv) justification that the design meets appropriate (e.g. protection system) standards, v) scope of coverage of accident scenarios (e.g. compared to the protection system) and vi) technology used to implement the DAS.**
Failure independence *Principle ESS.18 - No fault, internal or external hazard should disable a safety system.* *Guidance - SAP paragraph 352* *Safety systems should be physically separate, independent, isolated from other systems, including safety-related systems, and share no equipment or services. There should be adequate segregation between independent parts of the safety system (including pipework and cabling) and also between a safety system and other facility equipment that, in the event of a fault, might jeopardise the safe working of the safety system.*	Westinghouse state that the AP1000 design has addressed ESS.18 and "*The AP1000 has been designed such that safety systems have adequate separation, redundancy/diversity, and protection so that required safety functions cannot be disabled by internal or external hazards*" (Ref. 2). NRC Criterion 23 and 24 are relevant to this SAP. "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*". Westinghouse's evaluation (Ref.3 section 3.1) against criterion 23 states "*AP1000 Compliance - The protection system is designed considering the most probable failure modes of the components under various perturbations of the environment and energy sources. Reactor trip channels are designed on the deenergize-to-trip principle so that a single event (that is, loss of power) that could affect many functions at the same time causes the channels to actuate to their tripped conditions".* P352 - NRC criterion 24 (Ref. 3 section 3.1) is relevant to this SAP, in particular, the guidance of SAP Paragraph 352. Criterion 24 states **"***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*." Westinghouse's' evaluation (Ref.3 section 3.1) against criterion 24 states: *"AP1000 Compliance - The protection system is separate and distinct from the control systems. Control systems are, in some cases, dependent on the protection system for control signals that are derived from protection system measurements, where*

	applicable. These signals are transferred to the control system by isolation devices classified as protection components. *The adequacy of the system isolation is verified by testing under conditions of postulated credible faults. The failure of a single control system component or channel, or the failure or removal from service of a single protection system component or channel common to the control and protection system, leaves intact a system that satisfies the requirements of the protection system. The removal of a protection division from service is allowed during testing of the division."* It is concluded that there is an adequate claim of compliance to this SAP through e.g. reference to NRC criterion. The acceptability of control systems depending upon protection system measurements will require further consideration during Step 3. **O7. 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).**
Shutdown systems *Principle ERC.2 - At least two diverse systems should be provided for shutting down a civil reactor.*	Westinghouse state that "*Two reactivity control systems are provided. These are RCCAs and GRCAs, and chemical shim (boric acid)*" (Ref 2). NRC criterion 26 "Reactivity Control System Redundancy and Capability" is also relevant to this SAP. Criterion 26 "*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 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*." Westinghouse's evaluation (Ref.3 section 3.1) against criterion 24 states: **"***AP1000 Compliance - Two reactivity control systems are provided. These are rod cluster control assemblies and gray rod assemblies, and chemical shim (boric acid). The rod cluster control and gray rod assemblies are inserted into the core by the force of gravity.* *During operation, the shutdown rod banks are fully withdrawn. The control rod system automatically maintains a programmed average reactor temperature compensating for reactivity effects associated with scheduled and transient load changes. See Section 4.3 for additional information.* *The shutdown and control rod banks are designed to provide reactivity margin to shut down the reactor during normal operating conditions and during anticipated operational occurrences, without exceeding specified fuel design limits. The safety analyses assume the most restrictive time in the core operating cycle and that the most reactive control rod cluster assembly is in the fully withdrawn position. See Chapter 15 for summaries of the analyses, assumptions, and results.* *The safety-related passive systems provide the required boration to establish and maintain safe shutdown condition for the reactor core. See Section 6.3 for additional information."*

	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. **O8. - Westinghouse should demonstrate that the C&I systems used for implementation of diverse shutdown are adequately independent and diverse.**
Common cause failure *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.* *Guidance - SAP paragraph 171 - 174* *171 CCF claims should be substantiated.* *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.* *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.*	Westinghouse claim that the potential for CCF has been addressed (Ref. 2). Within Ref. 2 it is stated "*The AP1000 PRA provides an analysis of common cause failures of structures, systems, and components."* Within the PRA (i.e. Ref. 7 chapter 29 Common Cause Analysis) it is stated: *"The common-cause basic events are defined in the system fault trees and are tabulated in each system chapter. The failure probabilities of these basic events are calculated and are given in Sections 29.4 and 29.5, except for instrumentation and control common-cause failures that are calculated in their respective system chapters."* The Ref. 7 Chapter on the Plant Protection and Monitoring System (i.e. chapter 26) was briefly reviewed and found to contain the following statement (i.e. section 26.5.4) *"The software common cause failure evaluations are based on a model that incorporates a number of factors that can affect the development and implementation of software modules.* *This model yields a resultant software common mode unavailability of 1.1E-05 failures/demand for any particular software module, and a software common mode unavailability of 1.2E-06 failures/demand for software failures that would manifest themselves across all types of software modules derived from the same basic design program in all applications.* These limits are significantly lower than those stated in the SAPs and Ref. 8 (see comments on SAP paragraph 172 below). It is noted that the C&I design includes a Diverse Actuation System (DAS) (Ref 3 section 7.7) which is required to meet NRC concerns on common mode failure of digital C&I. See also discussion under ESS.7. P171/172/173 - **O.9 Westinghouse should provide a justification for the CCF claim limits for computer based safety systems used in the PRA.** Note that for computer based safety systems the cut-off figure is 1 failure per 10,000 demands (Ref. 8) and the values used by Westinghouse are significantly lower than this value (see above).

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.	See under ESS.2.
Single failure criterion *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.* *Guidance - SAP paragraph 175* *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]	Westinghouse state "*The AP1000 design basis ensures that no single random failure will prevent a safety system from performing its safety function. … The NRC evaluated the single failure criteria and approved the AP1000 configuration in its Design Certification review.*" Ref. 2. NRC Criterion 21 is also relevant to this SAP as is satisfaction of IEEE std 603 clause 5.1. The NRC Criterion 21 Statement (from Ref.3) is as follows:- "*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)…..*". Westinghouse's evaluation (Ref.3 section 3.1) against criterion 21 states*: "AP1000 Compliance* **-** *The protection system is designed for functional reliability and in-service testability. The design employs redundant logic trains and measurement and equipment diversity."* Westinghouse's response to NRC Criterion 22 is also relevant and contains the following statement: *"Sufficient redundancy and independence are designed into the protection systems so that no single failure or removal from service of any component or channel of a system results in loss of the protection function. Functional diversity and location diversity are designed into the system."* Westinghouse also claim compliance with the single failure requirements of IEEE 603 1991 (e.g. see Ref. 3 section 7.2.2.2.2) (see comment above on modern standards). The response does not appear to explicitly address consequential failures. **O.10 - Westinghouse should clarify whether consequential failures resulting from the assumed single failure are considered as an integral part of the single failure.**
Safety systems	
Requirement for safety systems *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.*	Westinghouse claim that the AP1000 design has addressed ESS.1. The Westinghouse compliance document (Ref. 2) states that *"The AP1000 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" 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. The AP1000 safety systems reduce the*

Guidance - SAP paragraph 336 *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.*	*frequency of fault sequences that result in core damage or radiation release as summarized in Chapter 59, "PRA Insights and Results," of the AP1000 PRA summarized in Chapter 19 of the DCD".* From review of the Westinghouse documentation it is concluded that there is an adequate claim that ESS.1 is satisfied. P336 - See comments above and ERC.2
Determination of safety system requirements *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.***	Westinghouse claim that this SAP is addressed in the design of the AP1000 and Ref. 2 provides references to sections within Ref. 3 that cover this principle, for example:- "*The AP1000 DCD provides specifications, descriptions, analyses results for the safety systems and systems that perform "defense-in depth" functions. AP1000 DCD references include:* *• Volume 1, Section 2, "System Based Design Descriptions and ITAAC" (inspection, test, analyses, and acceptance criteria), specifies safety system provisions and functions that ensure that the as-built plant has been constructed in accordance with the bases used in the plant safety analysis and PRA.* *• Chapter 6, "Engineered Safety Systems," provides descriptions of these systems and specifications of their components, and contains the containment analysis.* *• Chapter 7, "Instrumentation and Controls," includes descriptions of the safety-related and defense-in-depth plant C&I features and specifications of their components.* *• Chapter 8, "Electrical Power," includes descriptions and equipment specifications for safety-related onsite power systems.* *• Chapter 9, "Auxiliary Systems," includes descriptions of the systems that perform defense-in-depth functions.* *• Chapter 15, "Accident Analysis," provides the results of the AP1000 safety analyses and shows the plant response to design basis events with minimum safety systems and conservative assumptions.* *The PRA, Chapters 8 through 28, provide a detailed reliability assessment for the safety systems as well as systems that perform defense-in-depth functions."* NRC criterion 20 is also relevant to this SAP (see Ref. 3). "*3.1.3 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 anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety*". Westinghouse's evaluation (Ref.3 section 3.1) against criterion 20 states*:" AP1000 Compliance - The protection system is a microprocessor-based system that trips the reactor and actuates engineered safety features when predetermined limits are exceeded or when manually initiated.*

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.*	*The reactor trip portion of the protection system includes four independent, redundant, physically separated, electrically-isolated divisions. The coincidence circuits guard against the loss of protection or the generation of false protection signals due to equipment failures through the use of a two-out-of-four logic and built-in operational bypasses.* *Independent, redundant, physically separated, electrically-isolated engineered safety features trains are provided. Signal conditioning for the plant sensors is provided. Control and status signals are transmitted between the protection system and the main control room and the remote shutdown workstation and between the distributed logic circuits by internally redundant fiber optic data links."* From review of the Westinghouse statements it is concluded that there is an adequate claim that this SAP is satisfied. P 337 - See comments above and under ESS.1. Satisfaction of SAP paragraph 337 will be considered during Step 3.
Monitoring of plant safety *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.*	Westinghouse claim that the AP1000 design satisfies this requirement. Westinghouse state (Ref. 2) that "*An analysis has been conducted to identify the appropriate variables and to establish the appropriate design bases and qualification criteria for instrumentation used by the operator for monitoring conditions in the reactor coolant system, the secondary heat removal system, the containment, and the systems used for attaining a safe shutdown condition. This selection of monitored variables is based on the guidance provided in Regulatory Guide 1.97. The variables and instrument design criterion selected for the AP1000 is described in DCD, Sections 7.5.2 and 7.5.3*." Two NRC criterion are relevant to this SAP, namely; *"Criterion 13 - 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.*" And *"Criterion 19 - 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."*

Guidance - SAP paragraph 338 *338 Monitoring provisions should be classified as safety or safety-related systems as appropriate and should be made:* *a) in a central control location; and* *b) at emergency locations (preferably a single point) that will remain habitable during foreseeable facility emergencies.*	Westinghouse claim that the AP1000 design is compliant with these criterion (Ref.3 chapter 3). For example, Westinghouse State in relation to Criterion 19:- *"AP1000 Compliance - The AP1000 main control room provides the man-machine interfaces required to operate the plant safely and efficiently under normal conditions and to maintain it in a safe manner under accident conditions, including LOCAs. … Operator action outside the main control room to mitigate the consequences of an accident is permitted. … In the event that the operators are forced to abandon the main control room, a workstation is provided with remote shutdown capability. A main control room evacuation is not assumed to occur simultaneously with design basis events. The remote shutdown workstation is described in Section 7.4."* P338 - The AP1000 design includes categorisation of the monitored variables see Ref. 3 (sections 7.5.2 and 7.5.3). Further assessment will be required during Step 3 to determine whether the allocation to AP1000 safety-related and nonsafety-related classes satisfies SAP paragraph 338 (see also comments under ECS.1). Ref. 3 (section 7.4.3) describes the arrangements for remote shutdown in the event the main control room is evacuated. It is claimed that "*The remote shutdown workstation has the same capabilities as the reactor operator's workstation in the main control room*". From review of the Westinghouse 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**.** **O11. Clarification will be required that the emergency locations remain habitable during foreseeable facility emergencies.**
Automatic initiation *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.*	Westinghouse claim that the AP1000 design meets this principle. For example, Westinghouse state (Ref.2) "*DCD Sections 6.2 through 6.5 provide a description of the engineered safety features that are all automatically actuated by the plant protection and safety monitoring system and/or the diverse actuation system. Once actuated, these safety systems do not normally require human intervention following the start of a requirement for protective action for as long as 3 days. The protection and safety monitoring system, diverse actuation system, and other instrumentation and control is described in Chapter 7 of the DCD." Electrical power for the safety systems is provided by the 1E on-site power systems described in Chapter 8 of the DCD."* Westinghouse provide compliance statements in relation to IEEE standard 603 in Ref. 3 (see section 7.2.2.27). Sections 5.2 of IEEE standard 603 is relevant to this SAP. Westinghouse's conformance statement says "*Once initiated, reactor trips proceed to completion. Return to operation requires deliberate operator action to reset the reactor trip circuit breakers that are opened by the reactor trip signal.* *The circuit breakers cannot be closed while the reactor trip signals are present from the respective protection and safety monitoring system division. A manual control is provided in the main control room for resetting the reactor trip signals following a reactor trip."* The following extracts from Ref.3 show that automatic initiation of

Guidance - SAP paragraph 343 *343 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.*	protective actions is addressed in the AP1000 design. "*7.2.1 … The reactor is tripped when two or more actuation divisions output a reactor trip signal. This automatic trip demand initiates the following two actions. It deenergizes the under-voltage trip attachments on the reactor trip breakers, and it energizes the shunt trip devices on the reactor trip breakers. Either action causes the breakers to trip. Opening the appropriate trip breakers removes power to the rod drive mechanism coils, allowing the rods to fall into the core."* *"7.2.1.1.2 Nuclear Overpower Trips -Power Range High Neutron Flux Trip (High Setpoint) Power range high neutron flux (high setpoint) trips the plant when two of the four power range channels exceed the trip setpoint."* From review of the Westinghouse statements it is concluded that there is an adequate claim that this SAP is satisfied. P343 - To be considered during Step 3.
Engineered safety features (Automatic initiation) *Principle ERL.3 - Where reliable and rapid protective action is required, automatically initiated engineered safety features should be provided.* *Guidance - SAP paragraph 180* *180 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.*	Westinghouse claim that the AP1000 design meets this principle. The compliance statement in Ref. 2 states: *The AP1000 design has addressed ERL.3. The instrumentation and control systems provide protection against unsafe reactor operation during steady-state and transient power operations. They initiate selected protective functions to mitigate the consequences of design basis events. The safety evaluations show that the systems can be designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power. DCD Chapter 7 discusses the engineered safety features actuation system.* The following extracts from Ref.3 show that automatic initiation of the engineered safety features is addressed in the AP1000 design. "*7.3.1 - …the measurements are compared against the setpoints for the engineered safety feature to be generated. When the measurement exceeds the setpoint, the output of the comparison results in a channel partial trip condition. The partial trip information is transmitted to the ESF coincidence logic to form the signals that result in an engineered safety features actuation.*" ***"**7.3.1.2.4 Automatic Depressurization System Actuation **-*** *A signal to actuate the first stage of the automatic depressurization system is generated from any of the following conditions:* *1. Core makeup tank injection alignment signal (subsection 7.3.1.2.3) coincident with core makeup tank level less than the Low-1 setpoint in either core makeup tank in two of the four divisions* *2. Extended loss of ac power sources (low Class 1E battery charger input voltage)* *3. Manual initiation* *Any actuation of the first stage of the automatic depressurization*

	system also trips the reactor and reactor coolant pumps, align the core makeup tanks for injection, and actuates the passive residual heat removal heat exchanger." Also see response above to ESS.8 From review of the Westinghouse statements it is concluded that there is an adequate claim that this SAP is satisfied.
Reliability – Avoidance of complexity *Principle ESS.21 - **The design of a safety system should avoid complexity**, apply a fail-safe approach and incorporate the means of revealing internal faults from the time of their occurrence.* *Guidance - SAP paragraphs 355* *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:* *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.*	Westinghouse do not appear to claim that the design avoids complexity. The use of two computer based systems to implement the reactor protection system (i.e. Reactor Protection System and DAS) could be seen as introducing complexity when compared to Sizewell B (e.g. use of a simple hardware based secondary protection system). However, during the Familiarisation Presentation Westinghouse stated that the DAS would be implemented by a hardware based system. The Familiarisation presentation also revealed that the Protection system has complex arrangements to facilitate on-line testing and repair. **O12.1. Westinghouse should either provide a justification that the design of the safety systems has avoided complexity (e.g. to facilitate on-line testing and repair) 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).** **O12.2. Clarification should be provided as to whether the C&I design uses any complex hardware such as ASICs/FPGAs etc.**
Allowance for unavailability of equipment *Principle ESS.23 - In determining the safety system provisions, allowance should be made for the unavailability of equipment* *Guidance - SAP paragraphs 357* *357 Sources of equipment unavailability will include:* *a) testing and maintenance;* *b) non-repairable equipment failures; and* *c) unrevealed failures.*	Westinghouse claim that the AP1000 design satisfies this principle (Ref. 2) and reference is made to the single failure criterion. Within Ref. 2 Westinghouse state: *"All safety systems are designed with redundant components in accordance with single-failure criteria. Chapters 6 and 15 of the DCD provide the containment and accident analyses performed assuming the worst single failure. The allowable unavailability of equipment is specified in the plant Technical Specification limiting conditions for operation, which are specified in Chapter 16 of the AP1000 DCD"* NRC criterion 21 is relevant to this SAP. Ref. 3 contains the following text: - "*Criterion 21 ... - 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.* Westinghouse's evaluation (Ref.3 section 3.1) against criterion 20

	states:*" AP1000 Compliance -The protection system is designed for functional reliability and in-service testability. The design employs redundant logic trains and measurement and equipment diversity. The protection system equipment includes integral testing circuits. System equipment, from input to output, in the protection cabinets and the engineered safety features cabinets, is tested. Simulated inputs replace the field signals. Outputs are monitored for validity. Manual and automatic testing is used to test the final stages of the reactor trip circuits and the reactor trip switchgear. Testing of cabinets and communications links verifies the functional operation of the equipment and the hardware. See Chapter 7 for further information concerning the test capabilities of the protection system.* However, review of Ref 3 (chapter 7) shows that Westinghouse state *"7.1.2.11 Test Subsystem -Reference 19, Section 6 describes the test subsystem"* (i.e. there is no information in ref. 3 Chapter 7 on this topic other than the quoted reference). Note that Reference 19 is a Westinghouse report entitled "*AP1000 Protection and Safety Monitoring System Architecture Technical Report," February 2007*". This reference has not been reviewed as part of this assessment. **O13. Further clarification will be required on specifically how the design addresses unavailability of safety systems due to test and maintenance.** From review of the Westinghouse statements it is concluded that there is an adequate claim that this SAP is satisfied. However, note that the scope of the systems classed as safety needs to be clarified (see ECS.1 above).
Functional testing *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.* *Guidance - SAP paragraphs 192 - 193* *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.* *193 Where complete functional testing is claimed not to be reasonably practicable, an equivalent means of functional proving should be demonstrated.*	Westinghouse claim that the AP1000 design satisfies this principle. Westinghouse state "*Each <u>safety system</u> has its own set of in service inspection/testing requirements. These are described within their respective sections of the DCD. In addition, DCD Chapter 16, "Technical Specifications," provides surveillances for assurance that systems important to safety are operable*". Within Ref. 2 it is stated that "*Reference 19 …Section 6 describes the maintenance, test, and bypass features of the protection and safety monitoring system*". NRC criterion 21 is relevant to the protection systems. See the comments above under ESS.23. **O14. Clarification will be required on whether other systems important to safety (i.e. safety related systems as defined by the IAEA) comply with this SAP.** P192 - See ESS.23. P193 - No claim identified.
Computer-based systems important to safety	
Computer-based safety systems *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*	Westinghouse claim (Ref. 2) that this SAP has been addressed. For example, Westinghouse state that "*Throughout the software development life-cycle, the AP1000 has demonstrated a high level*

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. *Guidance - SAP paragraphs 360 - 362* *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:* *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:* • *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.* *361 Independent 'confidence-building' should provide an independent and thorough assessment of a safety system's fitness for purpose. This comprises the following elements:* *a) Complete and preferably diverse checking of the finally validated production software by a team that is independent of the systems suppliers, including:* • *independent product checking providing a searching analysis of the product;* • *independent checking of the design and production process, including activities needed to confirm the realisation of the design intention; and* *b) Independent assessment of the test programme, covering the full scope of test activities.*	*of production excellence and confidence-building*". It is noted that the definition of V&V (Ref.3 section 7.1.16) appears to be based on dated IEEE standards and it is not obvious that key areas such as IV&V, third party assessments and Ref. 8 "Production Excellence and Confidence Building" are addressed. **O15.1. The arguments to support the claim of compliance to ESS.27 will need to be assessed during Step 3 and in particular the way in which each of SAP paragraphs 360 to 361 has been addressed. Westinghouse should clarify the activities that contribute to the independent confidence building (i.e. independent from the system's specifiers and producers) and production excellence legs. 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).** **O15.2. 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 Plant and Safety Monitoring System and Diverse Actuation System etc.). See also discussion above under ECS.1, ECS.2 and ECS.3.** **O15.3. The approach to instrumentation and actuators that contain programmable devices (e.g. SMART instruments) will need to be defined.** **O15.4. 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 for the protection and safety monitoring system Westinghouse state (Ref.3, section 7.1.2.14.2) that "WCAP-16097-P-A (Reference 8) provides for the use of commercial off-the-shelf hardware and software through a commercial dedication process". Reference 8 is entitled "*WCAP-16097-P-A (Proprietary) and WCAP-16097-NP-A (Non-Proprietary), Revision 0,"Common Qualified Platform," May 2003".*

362 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.	
Standards for computer based equipment *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.*	Westinghouse state "*The AP1000 design has addressed ESR.5."* and *"Reconciliation of U.S. and UK standards may be required, but in general, the instrumentation systems as described in DCD Chapter 7 and the human factors process described in Chapter 18 meet the outlined approach*". It is agreed that reconciliation of design standards will be required (see also ESS.27 and ECS.3). **O16. Westinghouse 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. 8) which means arguments of production excellence and independent confidence building will need to be presented.**
Control and instrumentation of safety-related systems	
Provision in control rooms and other locations *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.* *Guidance - SAP paragraphs 365 - 366* *365 Principle EHF.7 (paragraph 382 f.) on user interfaces is also relevant to this principle.* *366 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.*	Westinghouse state (Ref.2) that "*The AP1000 design has addressed SAP ESR.1*"and "*The AP1000 incorporates distributed plant computer systems with all information available to the main control room and emergency control room*". 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. 3 but note that the Westinghouse classification for many of the systems is nonsafety-related (see comments above under ECS 1, 2 and 3). From review of the Westinghouse documentation it is concluded that there is an adequate claim that this SAP is satisfied but see ECS.1, 2 and 3 above. P365/366 - See above and response to ESS.3. Extent of coverage will be considered during Step 3.
Provision of controls *Principle ESR.3 - Adequate and reliable controls should be provided to maintain variables within specified ranges*	Westinghouse state that the AP1000 design has addressed ESR.3. Also that this topic is covered by discussion in Ref. 3 Chapters 7 and 16, and in the PRA summarized in chapter 19. For example, Ref. 3 Chapter 7 (e.g. section 7.7) describes the significant controls (e.g. reactor power control system) provided within the AP1000 design and the introduction to section 7.7 notes "*The function of the AP1000 control systems is to establish and maintain the plant operating conditions within prescribed limits."*

	NRC Criterion 13 is quoted in Ref.3 (section 3.1) and this criterion has a similar requirement to SAP ESR.3 (i.e. "*Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges*"). In response Westinghouse state that:- "*Instrumentation and controls are provided to monitor and control neutron flux, control rod position, fluid temperatures, pressures, flows, and levels, as necessary, to maintain plant safety. Instrumentation is provided in the reactor coolant system, steam and power conversion system, containment, engineered safety systems, radioactive waste management systems, and other auxiliary systems.* *See Section 7.5 for a discussion of indications that are required for operator use under normal operating and accident conditions. Criteria regarding layout of the controls and displays are provided in Chapter 18.* *The quantity and types of process instrumentation used provide safe and orderly operation of systems over the design range of plant operations, including accident conditions."* It is concluded that there is an adequate claim that this SAP is addressed in the design of the AP1000.
Communications systems 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. Guidance - SAP paragraph 368 368 These communication systems should not have any adverse effect on safety systems, or safety-related systems.	Westinghouse state that the AP1000 design has addressed ESR.7. For example, within Ref. 2 it is stated that "*The communication system (EFS) provides effective intra-plant communications and effective plant-to-offsite communications during normal, maintenance, transient, fire, and accident conditions, including loss of offsite power*". The AP1000 communication system is described in Ref. 3 Section 9.5.2. where it is stated that "*9.5.2.1 Design Basis - The communication system serves no safety-related function and therefore has no nuclear safety design basis*". Note that the adequacy of the communications systems should be judged against the categorisation and classification scheme requirements (see ECS.1, 2 and 3 above). NB. BS IEC 61226:2005 Category C includes communications to warn of significant on or off-site releases for the purposes of implementing the emergency plan. In Ref. 3 (Chapter 9 section 9.5.2.1) Westinghouse explain that "*The communication subsystems are independent of one another; therefore, a failure in one subsystem does not degrade performance of the other subsystems."*

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