Health and Safety Executive

HEALTH & SAFETY EXECUTIVE
NUCLEAR DIRECTORATE
ASSESSMENT REPORT

New Reactor Build

AREVA/EDF EPR 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 EDF/AREVA UK-EPR submission in accordance with the strategy outlined in Ref. 6. 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. 6) 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. 7).

2. REPORT

3. EDF/AREVA has provided a number of submissions relevant to C&I assessment. The main submission that describes the C&I is Ref. 1. 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 Protection System (PS) that initiates insertion of neutron absorbing rods),
    - plant control and monitoring systems (e.g. the Process Automation System (PAS) and Process Information and Control System (PICS)),
    - main control room with backup via the Remote Shutdown Station, 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. EDF/AREVA 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. 5 section 4. "Status with Respect to the UK Regulations, Rules and Guidelines" EDF/AREVA explain "... *For this Fundamental Safety Overview submitted for Step 2 of pre-licensing, a systematic review of EPR safety features against UK requirements is not available. However, a limited review has been undertaken which indicates that the EPR design already meets the majority of UK*

requirements. Detailed analyses of the EPR status with respect to UK regulations will be performed and documented in subsequent pre-licensing steps...". Technical Query (TQ) - EPR000003 was raised requesting an explanation of how the EPR 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. EDF/AREVA's response to TQ EPR000003 (Ref. 9) shows that EDF/AREVA claim compliance with all of the "fundamental" C&I SAPs. However, within the Annex there are a number of observations that will need to be raised with EDF/AREVA 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 EDF/AREVA address, for C&I, categorisation of functions and classification of structures, systems and components (O1. - SAP ECS.1 and SAP ECS.2). In particular, alignment of the EDF/AREVA approach to that defined by the IAEA, SAPs and BS IEC 1226:2005 will need to be determined. Note that the EDF/AREVA approach which uses four functional classes (i.e. F1A, F1B, F2 and NC) does not appear to 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 F1A, F1B, F2 and NC systems, and E1A, E1B, E2 and NC equipment provides adequate compliance with modern UK national and international C&I nuclear standards (O2. - SAP ECS.3). The standards base appears to be mainly French national (e.g. RCC-E codes) some of which might 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) (O3. - 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 (O4.1 and O4.2 - 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 that adequate diversity and independence exists both within and across the C&I safety systems (O5 - SAP EDR.2, O6. - SAP ESS.7, O7. - SAP ERC.2, O8.1 - SAP EDR3 and O13.1 - SAP ESS.21). In particular, EDF/AREVA should provide a demonstration that the 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. UK research on high reliability computer based C&I systems has shown that there are significant difficulties in justifying such systems.
- Clarification is required into the use of probabilistic criteria in the design of the EDF/AREVA ESBWR C&I systems (O2.2 - SAP ECS.3, O5. – SAP EDR.2, O8.2 – SAP EDR.3 and O10. - SAP ESS.2). A sensitivity

study should be carried out to assess whether there is any margin for a lower reliability figure to be adopted for the protection system.

- 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. 10) (O15.1. to O15.4. - SAP ESS.27 and O16 - SAP ESR.5).

7. The EDF/AREVA submissions on C&I mainly describe a conceptual design. It is noted that only limited information is provided on the actual implementation details in Ref.1 (e.g. such as reference to the TELEPERM XS platform in the description of the Reactor Protection System in Ref. 1 subchapter G.3 section 1.6 and statement in Ref. 1 subchapter G.3 section 2.6 "Technology section" for the Safety Automation System which states "*This sub-section will be provided after the standard C&I equipment has been chosen*"). Note also, for example, that during the familiarisation presentation on 17 October 2007 it was stated that the PACS would be implemented using relay technology whilst Ref.1 states that "*The PACS technology is defined by the equipment which processes the functions*". As a result this assessment report is based on the C&I design concept and an approach (i.e. for Steps 3, 4 and Phase 2) will need to be developed for the assessment of the design implementation (i.e. covering the exact C&I systems, platforms, products and components etc. selected for the implementation of the UK-EPR 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 (PACS based on relay technology – see above) is different to that described in the formal submissions then a modification to the documentation will be required.

O17. EDF/AREVA 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 EDF/AREVA design concept reflects French custom and practice, and is largely based on French standards (e.g. RCC-E) and French regulatory requirements. As a result the observations in the Annex largely reflect the difference between French and UK approaches.

10. With regard to French custom and practice it is worth noting that in 1997 HSE published a "four party" report (Ref. 8) which provided a consensus view on the safety case requirements for computer based systems. France 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 EDF/AREVA in its submissions to the French regulator.

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 EDF/AREVA. 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 EDF/AREVA.

O18. EDF/AREVA 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. The approach to be developed for NII C&I assessment of Steps 3, 4 and Phase 2 (see above) will need to address whether there are any requirements left for the licence applicant to define and the satisfaction of such requirements.

3. CONCLUSIONS

13. EDF/AREVA provide adequate claims of compliance with all of the fundamental Step 2 SAPs (see Annex). It is considered that this is an acceptable position for the conclusion of the Step 2 assessment. The assessment has given rise to a number of observations and these will need to be raised with EDF/AREVA. 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 reference to the TELEPERM XS 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 EDF/AREVA UK-EPR reflects French custom and practice, and is largely based on French standards and regulatory requirements. As a result the observations largely reflect the difference between French 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 EDF/AREVA from proceeding to Step 3. Therefore, EDF/AREVA should be allowed to proceed to Step 3.

R2. The “observations” identified throughout this assessment report by bold text will require an EDF/AREVA response prior to Step 3.

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

5. REFERENCES

1. UK EPR FUNDAMENTAL SAFETY OVERVIEW VOLUME 2: DESIGN AND SAFETY CHAPTER G: INSTRUMENTATION AND CONTROL SYSTEM
2. UK EPR FUNDAMENTAL SAFETY OVERVIEW VOLUME 2: DESIGN AND SAFETY CHAPTER C: DESIGN BASIS AND GENERAL LAYOUT
3. UK EPR FUNDAMENTAL SAFETY OVERVIEW VOLUME 2: DESIGN AND SAFETY - CHAPTER B: INTRODUCTION AND GENERAL DESCRIPTION OF THE PLANT
4. UK EPR FUNDAMENTAL SAFETY OVERVIEW VOLUME 2: DESIGN AND SAFETY - CHAPTER I: AUXILIARY SYSTEMS
5. UK EPR FUNDAMENTAL SAFETY OVERVIEW VOLUME 1: HEAD DOCUMENT CHAPTER E: SAFETY PRINCIPLES AND CRITERIA
6. Step 2 C&I Assessment Strategy - ND DIV 6 Assessment Report No. 2007/02
7. Nuclear Division – Division 6 Unit 6D Operating Plan 2 August 2007 – 31 March 2008
8. 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
9. Full response to TQ EPR000003 raised 2 October 2007 - Compliance with HSE Safety Assessment Principles for Nuclear Installations (2006 Edition).
10. 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.*	EDF/AREVA claim compliance with this SAP in Ref. 9. In particular EDF/AREVA state: *"EPR compliance with ECS.1 and ECS.2 is confirmed in SSER 1.E.5.3, (especially paragraph 5.3.1). The detailed implementation of those principles is reported in SSER 2.C.2."* NB. The references to the SSER are to Ref. 5 and Ref. 2 respectively of this report. The UK-EPR design approach does include categorisation of safety functions and an explanation of the approach is provided in Ref. 2. For example, within Ref. 2 (subchapter C.2) it is stated:- *"1.4. FUNCTIONAL CLASSIFICATION* *The definition of safety classes is linked to three physical states corresponding to shutdown conditions to be attained in PCC and RRC safety analyses. They make it possible to establish a hierarchy of the functions used to attain shutdown conditions.* *1.4.1. Definition of physical states* *Physical states are the controlled state, safe shutdown state and final state for RRC-A analysis.* *They are defined as follows:* *Controlled state: the core is subcritical (a return to short-term criticality before operator actions leading simply to low nuclear power could be acceptable on a case by case basis for a few events), heat removal is assured on a short-term basis, for example via steam generators, core water inventory is stable and radioactive discharges remain acceptable.* *Safe shutdown state: the core is subcritical, residual heat removal is assured on a long-term basis and radioactive discharges remain acceptable.* *Final state: the core is subcritical, residual heat removal is assured via primary or secondary systems and radioactive discharges remain acceptable.* *1.4.2. Definition of functional classification* *Functions are classified in accordance with the three states identified above. Consequently, these three states lead to three functional safety classes, designated by F1A, F1B and F2."* However, it will need to be shown that the EDF/AREVA system as outlined above is in general agreement with that of the SAPs, IAEA and BS IEC 61226:2005. **O1. - Clarification will be required as to how EDF/AREVA address, for C&I, categorisation of functions and classification of structures, systems and components. In particular, alignment of the EDF/AREVA approach to that defined by the IAEA, SAPs and BS IEC 61226:2005 will need to be determined.** It is concluded that there is an acceptable claim that ECS.1 has been addressed.

Safety classification of structures, systems and components

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.

EDF/AREVA claim compliance with this SAP in Ref. 9. In particular EDF/AREVA state:-
"EPR compliance with ECS.1 and ECS.2 is confirmed in SSER 1.E.5.3, (especially paragraph 5.3.1). The detailed implementation of those principles is reported in SSER 2.C.2."
NB. The references to the SSER are to Ref. 5 and Ref. 2 respectively of this report.

The UK-EPR approach to classification is addressed in Ref. 2 (subchapter 2) where it is stated:-

***"**1.5.1. Classification principles - System classification is defined in accordance with the required safety functions, and includes the following categories:*
F1A systems,
F1B systems,
F2 systems.

Systems that are not F1- or F2-classified are designated as non-classified (NC)."

Also in Ref. 2 (subchapter C.2):-

"1.9.1. Principles of C&I equipment classification - C&I classification takes into account C&I safety function categorisation (classes of associated C&I systems and equipment) in accordance with the safety functional classification (F1A, F1B, F2) as previously defined…

C&I equipment safety classes are defined as follows:

E1A: C&I equipment necessary to ensure F1A safety functions,

E1B: C&I equipment necessary to ensure F1B safety functions,

E2 : C&I equipment necessary to ensure F2 safety functions,

NC : Non-classified."

The above classification scheme leads to the definition of C&I system classes as shown in Ref. 2 subchapter C.2 Table 6 "*CLASSIFICATION OF C&I SYSTEMS AND EQUIPMENT***"** i.e. :-

C&I systems	*Functional classification*	*Seismic classification*
PS – Protection system	*F1A*	*Yes*
PAS – Plant unit C&I system	*F2/NC*	*No*
SAS – Safety C&I system	*F1B*	*Yes*
MCS – Safety operation facilities	*F1B*	*Yes*
MCP(PICS) – Main operation facilities	*F2/NC*	*No*
PACS – Priority and actuation control management	*F1A**	*Yes*

From the above it can be seen that C&I systems (F1A, F1B and F2) and equipment (E1A, E1B and E2) are classified on the

Guidance - SAP paragraphs 153-156 . *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.* *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.* *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 function.*	basis of functions and their significance with regard to safety. <u>However, the comments under ECS.1 (see O.1) above will need to be addressed.</u> P153 – See above and under ECS.1. P154 - The alignment of the EDF/AREVA scheme, which appears to have four Safety Classes (see above), to the three class scheme outlined in this SAP will need to be assessed during Step 3 (see O.1 above). P155 - Step 3 - However it does appear that this principle is addressed. For example, within Ref. 1 section 1.3.1.2 "independence" it is stated that: - "*1.3.1.2.2 Independence between equipment of different safety classes - According to RCC-E requirements, equipment of different safety classes within the Protection System must be independent in such a way that a failure occurring in lower class equipment does not impair the functions of the higher class equipment. …* *the use of common components must be avoided as far as possible. If not, the common equipment used must be assigned, classified and designed according to the requirements of the higher class"* P156 - Step 3
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.*	EDF/AREVA claim compliance with this SAP in Ref. 9. In particular EDF/AREVA state: *"EPR design is considered to comply with the SAP* *The objective of EPR safety classification is precisely to achieve through design, manufacturing and operating requirements, an acceptable quality of systems, components and civil structures involved in the plant safety. The safety classified systems, components and structures are arranged in*

	classes, with corresponding requirements dependent on the safety functions to be performed. The most stringent requirements correspond to the most important safety functions." NB. The compliance statement Ref. 9 also provides a reference to the SSER 2.C.2 which is Ref. 2 of this report. The allocation of requirements to C&I systems is addressed in Ref. 2 (e.g. see Table 1) where it is stated, for example, that for F1A and F1B the equipment requirements are "as defined by the RCC-E" and for F2 "As defined by the design and construction code". Also in Ref. 3 it is stated that: - "*EPR TECHNICAL CODES* *The design of the EPR reactor is based on a scalable approach and reinforced safety requirements. The codes and standards corresponding to industrial practice implemented in the design, construction and commissioning of the EPR reactor are of three types:* − *technical codes referred to as RCC (Rules for Design and Construction) which describe industry practice for PWR reactors currently in operation. The following RCC codes are applicable to EPR: …. RCC-E "Design and Construction Rules for electrical components of PWR nuclear islands*". Clarification will be required as to the precise standards that result from this requirement. **O2.1 - EDF/AREVA should demonstrate the adequacy of the C&I system and "equipment requirements". In particular, it should be demonstrated that the selected C&I standards base for F1A, F1B, F2 and NC systems, and E1A, E1B, E2 and NC equipment provides adequate compliance with modern UK national and international C&I nuclear standards.**
Guidance - SAP paragraphs 157-161	
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. It is assumed that the higher safety class standards are more rigorous than those for lower safety classes (i.e. the assumed normal practice). **O2.2 – EDF/AREVA 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, 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.*	P160 - The EPR systems encompass systems that in the UK and internationally would appear to fall into different classes (e.g. see IAEA Safety Standards Series – Instrumentation and control systems important to safety in nuclear power plants – safety guide NS-G-1.3). Whether or not the combination of safety functions in these system classes allows this SAP guidance to be met requires clarification. **O2.3 Clarification is required as to how SAP guidance paragraph 160 is met (e.g. claim of independence or standards appropriate to the highest class).** P161 – None identified by EDF/AREVA. To be addressed in Step 3.
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.*	EDF/AREVA claim compliance with this SAP in Ref. 9. In particular, EDF/AREVA state:- *"EPR design is considered to comply with the SAP* *The structures, systems and components (SSCs) important to safety are designed according to the general design requirements indicated in SSER 2.E. Safety classification of the SSCs is carried out using complementary approaches, and is extensively described in SSER 1.H: it results in stringent requirements expressed in terms of design and reliability."* NB. The references to the SSER are to the UK EPR Fundamental Safety Overview Volume 2 Design and safety Chapter E and Volume 1 Head Document Chapter H. Within "SSER 2.E" it is stated that "*Technical Guidelines - Requirements specific to the RCP RCS are given in Chapter C.1.2.*", where C.1.2 is Ref. 2 of this report. While no direct equivalent of this principle was found the following "Technical Directive" contained in Ref. 2 is relevant:- "*G3.7. Instrumentation and control failures must be systematically considered for the design of and demonstration of safety for next generation nuclear power plants. In particular, the designer must consider all reasonable initiating event generation possibilities resulting from inappropriate instrumentation and control system actions and check if these initiating events are covered by analysing the reference transients, incidents and accidents and the operating conditions with multiple failures. (FSO ref G.3, G.4)* *On the other hand, such inappropriate instrumentation and control system actions must also be considered as single aggravating factors when analysing reference transients, incidents and accidents. Only unscheduled actions (single or multiple) that may result from a single failure in the instrumentation and control sub-systems or support systems are to be considered. (FSO ref P)* *In all cases, adequate techniques must be implemented when*

	designing equipment, software and functional applications to reduce the possibilities of inappropriate actions. Specific attention should be paid at the design stage to the simultaneous control actions that are sensitive to design errors or operator errors. (FSO ref G.6)" The above requirement is the nearest equivalent to EDR.1 and "reducing the possibilities of inappropriate actions" can be compared with the SAP requirement to fail in a safe manner. The reference to Ref. 1 sub-chapter G.6 was reviewed and found to address C&I procedures and tools. However, the section does not appear to address this SAP (e.g. fail in a safe manner or identification of potential failure modes). However, for the protection system it is stated (Ref. 1 subchapter G3) :- *"1.3.1.3. Detection of degraded states - Appropriate measures should be taken to detect and identify occurrence of failures. This is to avoid long periods of operation with a degraded C&I configuration which might lead to lose a function due to an accumulation of failures.* *For this reason, self tests and periodic tests of the equipment performing the F1 functions must be implemented to detect any failure that could prevent the F1 function from operating."* **O3. - EDF/AREVA should explain how the UK-EPR C&I design addresses SAP EDR.1 for all systems important to safety.**
Reliability – failsafe 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.).*	EDF/AREVA claim compliance with this SAP in Ref. 9. In particular, EDF/AREVA state: *"EPR design is considered to comply with the SAP* *The EPR safety systems incorporate means of revealing internal malfunction and a part of Protection System is designed to withstand single failure even during maintenance or periodic testing. Self tests and periodic tests are implemented to detect any component failures, and tests frequencies are calculated from the reliability expected of the tested function."* A reference is also made to "SSER 2.F.5" which "*describes in service inspection performed*". However, there does not appear to be a specific requirement for the design of a safety system to apply a failsafe approach but see comments above under EDR.1 With regard to revealing internal faults the following extracts from Ref.1 subchapter G.3 are relevant:– *"1.0.4.2. Periodic tests and in-service inspection - Long periods of operation with a potential degraded C&I configuration (accumulation of failures) which might lead to lose a safety function are shortened by periodic testing. Self tests and periodic tests must be implemented in F1 functions to detect failures. Tests frequencies are calculated from the reliability expected of the tested function. ….* *1.3.1.3. Detection of degraded states - Appropriate measures should be taken to detect and identify occurrence of failures. This is to avoid long periods of operation with a degraded C&I configuration which might lead to lose a function due to an accumulation of failures.*

	For this reason, self tests and periodic tests of the equipment performing the F1 functions must be implemented to detect any failure that could prevent the F1 function from operating." These extracts relate to the section on the Reactor Protection System and can be seen as an implicit claim that the SAP principle on revealing internal faults from the time of their occurrence is met. However, equivalent statements where not found for other F1 systems. **O4.1 - EDF/AREVA should explain how it is ensured that all safety systems (e.g. such as F1 systems) reveal internal faults from the times of their occurrence.** **O4.2. - Further clarification will be required as to 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*	Within Ref. 9 EDF/AREVA claim compliance with this SAP and provide various references to sections of the Step 2 submission (e.g. Ref. 2 and Ref. 5). Ref. 9 also provides a high level overview of the system design principles. Of particular note are the following statements:- *"Redundancy: the EPR design requires application of the single failure criterion at the system level to F1A classified systems; rules for PCC studies insure functional redundancy for F1B functions, corresponding to IAEA requirement for functional redundancy. At a third level, redundancy is implemented as necessary through PSA analyses and corresponding RRC scenarios to achieve EPR probabilistic safety objectives.* *Diversity: there is no a priori design rule applicable to diversity. Diversity is implemented as required to protect against common cause failures of F1 systems, when it is possible to achieve diversity without lowering safety performance. This is the case, in particular, for RRC complex sequences: examples are requirement for diverse Station Black-Out diesels, or diverse reactor trip function for ATWS scenarios.* *Segregation: a number of layout rules are applied to implement the principle of segregation, albeit highly simplified as a result of the overall 4 division layout concept. The design ensures that the occurrence of a failure, internal or hazard-made, that affects a safety train must not result in the loss of another train."* From review of Ref. 2 it was found that two "technical guides" are relevant to this SAP, namely G3.4 and A.2.2, and these in turn refer to Ref.1 The introduction to the section on Technical guidelines notes that "*This section describes how the basic safety requirements set down in the Technical Guidelines for the design and construction of the next generation of nuclear pressurized water reactors, are taken into account in design of the EPR (Chapter B.7)".* The introduction to chapter B.7 notes that it is based on the Flamanville safety case and it is considered that the chapter is not relevant to the GDA process. However, within Ref. 1 there are sections relevant to this principle. In particular, subchapter G.1 section 0.3.2.2 "Technical Guides" notes that "technical Guides" A.2.2 and G.3

Guidance - SAP paragraph 170 *170 It should be demonstrated that the required level of reliability for their intended safety function has been achieved.*	are applicable to the design of C&I systems. Within Ref.1 subchapter G.1 section 0.3.1.2 it is stated that "*The single failure criterion (SFC) must be taken into account in the design of F1 systems by ensuring a sufficient degree of redundancy, adequate structures and arrangements (independence, physical and electrical separation)*". It is also claimed (subchapter G.1 section 2.1) that "*The overall C&I design approach to achieve the safety goals is based on:* - *the organization of C&I in levels,* - *functional classification (cf. Chapter C.2)* - *the application of the single failure criterion to C&I,* - *the defence in depth concept,* - *priority requirements between different C&I functions,* - *categorisation of the C&I functions, .."* It is concluded that there is an acceptable claim that SAP EDR.2 is met for C&I systems. However, the adequacy of the arguments supporting this claim will need to be considered further during Step 3. P170 - Four system classes have been identified (see above) but it is not clear how reliability figures are used in the design of the EPR C&I systems nor how achievement is demonstrated (see also O2.2 above). Note the protection system reliability will need to be defined and confirmed through sensitivity study. **O5.1 Clarification is required on the use of probabilistic criteria in the design of the EPR C&I systems and how achievement of such criteria is demonstrated.** **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.*	Within Ref. 9 EDF/AREVA claim compliance with this SAP and provide various references to sections of the Step 2 submission (e.g. Ref. 2). Ref. 9 also provides a high level overview of the defence in depth concept. Also, see comments under EDR.2 above. P337 - Step 3. See below under ESS.2. Note that Ref. 9 contains references to the safety analyses and PSA.
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 particular to high integrity safety*	Within Ref. 9 EDF/AREVA state "*EPR design is considered to comply with the SAP*". The supporting text covers distribution of C&I functions and functional/equipment diversity rather than diversity within the protection system. Within Ref.1 subchapter G3 section 1.0.3.2.3 "technical Guidelines there is a reference to Technical Guideline A.2.2 (redundancy and diversity in the safety system). Technical Guideline A.2.2 requires the "*reliability to be obtained via an adequate combination of redundancy and diversity*". Furthermore, within Ref.1 Subchapter G3 it is stated that**:-** **"***1.3.1.2.3 Independence between diverse functions* **-** *When*

systems.	*functional diversity is required, a sufficient degree of independence must be achieved. This requirement involves the implementation of the following design measures:* *- instrumentation, process units and cabling for each of the diverse function must be separated.* *- equipment diversity for instrumentation may be implemented when diverse functions use of the same process parameter (decision made on case by case basis)."* The above extracts reveal that there is a requirement to consider diversity in the design of the protection system. However, the precise means (e.g. use of diverse variables) by which this is addressed in the UK-EPR design is unclear (e.g. "*<u>When</u> functional diversity is required …diverse functions use of same process parameter (decision made on a case by case basis*") and will require clarification. **O6. - EDF/AREVA should explain the precise means by which it is ensured that, for the protection system, diversity is used in the detection of fault sequences (e.g. preferably by the use of different variables), and in the initiation of the safety system action to terminate the sequences.**
Failure independence *Principle ESS.18 - No fault, internal or external hazard should disable a safety system.*	Within Ref. 9 EDF/AREVA state:- *"EPR design is considered to comply with the SAP* *The EPR safety systems (extensively described in SSER 2.F) are physically separate, independent and isolated from other systems. SSER 2.C.3 and 4 explain how safety systems are protected against external and internal hazards. In addition, safety studies demonstrate that in case of one protection system failure, safety function can be ensured with other safety systems allowing the reactor to reach a safe state."* Within Ref. 1 Subchapter G3 section 1.3 on Design Basis there are a number of clauses which are relevant to this SAP (e.g. addressing redundancy, single failure and independence). For example, with regard to the F1A protection system subchapter G3 section 1.3.1.2 states:- "*In accordance with RCCE, three kinds of independence are considered in one C&I system.* *- independence between redundancies of the C&I system.* *- independence between equipment of different safety classes.* *- independence between diverse functions.* *In addition to requirements applying to independence within the Protection System, the independence between the Protection System and the other C&I systems must is also necessary*". Also within Ref. 1 Subchapter G3 section 1.0.3.1.6 "Seismic classification" it is stated:- *"The Protection System must be seismic classified, according to the classification principles presented in chapter C.2.* *The objective of the dimensioning provisions is to ensure that the safety functions of the systems and components necessary for plant return to safe shutdown state will not be affected by an Increased Safety Earthquake."* It is considered that there is an implicit claim of compliance

Guidance - SAP paragraph 352 *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.*	against this SAP for the F1A protection system. For the F1A PACS system Subchapter G.3 section 4.0.2 contains a number of relevant requirements such as :- *" 4.0.2.1.2 Single failure criterion (active and passive)* *The single failure criterion is applicable to the PACS, to ensure an adequate degree of redundancy.* *If periodic tests of the PACS functions are possible and are undertaken (in accordance with the principles defined in sub-chapter C.1 and applied in section G.3.4.8), then the PACS must be provided with sufficient redundancy to ensure that it can continue to process F1A safety functions even if some of the equipment is unavailable due to testing and further equipment is assumed to fail as a result of the application of the single failure criterion.* *Independence and physical separation: the PACS is subject to these requirements, which lead to the physical and electrical independence of the equipment of the four C&I divisions on which it depends. Each PACS actuator must be independent of the other PACS: there is no exchange between them. Provision must be made to isolate different equipment items to ensure the PACS functions and avoid common cause failures. Thus, links between the PS [RPS], PAS, SAS and electrical cubicle are hardwired"*. *"4.0.2.1.6 Seismic classification - The cubicle must be: at seismic class 1 (SC1), when managing F1 or F2E functions …"* It is considered that there is an implicit claim of compliance against this SAP for the F1A PACS. It is noted that the extent of application of this SAP is to safety systems and hence the scope of application (i.e. to only F1A systems) is dependent upon the adequacy of the classification scheme (see ECS.1). P352 - The approach to segregation will be assessed during Step 3.
Shutdown systems *Principle ERC.2 - At least two diverse systems should be provided for shutting down a civil reactor.*	Within Ref. 9 EDF/AREVA state:- *"EPR design is considered to comply with the SAP* *Core reactivity can be controlled by adjusting either the control rod insertion in the core or the soluble boron (boric acid) concentration in the primary coolant."* and "*Soluble boron injection comes in addition to or as a back-up of*

	insertion of the control rods. Soluble boron injection can be achieved either by the Extra Boration System (EBS) see SSER 2.F.7, or by the Safety Injection System (SIS) see SSER 2.F.6: both systems are safety classified, and are designed, manufactured and tested accordingly. Analysis of Design Extension Conditions (RRC) events involving failure of the control rods to insert shows that the EBS system is functionally capable of safely shutting down the reactor to achieve a final safe state (see SSER 2.S.1.2) independently of the control rods." In addition to the Reactor Protection System described in Ref. 1, which operates to insert the rods, there is also an Extra Boration System (EBS) which has the following safety role as defined in Volume 2 subchapter F.7:- *"0.1. SAFETY FUNCTIONS* *0.1.1. Reactivity control* *In the event of PCC-2 to PCC-4 conditions, the safety boration system (RBS) [EBS] must ensure boration of the primary cooling system, irrespective of the primary coolant pressure, in order to:* *- attain a controlled state (when necessary),* *- compensate for the reactivity insertion caused by the RCP [RCS] cooldown in reaching a safe shutdown state (RIS/RRA [SIS/RHR] connected) from the controlled state. Boration is terminated when the boron concentration required for the safe shutdown state is obtained. …* *In the event of ATWS (RRC-A condition), the RBS [EBS] ensures automatic boration of the RCP [RCS].* *0.2. FUNCTIONAL CRITERIA* *0.2.1. Reactivity control* *In PCC-2 to PCC-4 and RRC-A accident conditions and events, the negative-reactivity provided by the RBS [EBS] has to enable the core to be brought to a subcritical state (controlled state) or to RIS/RRA [SIS/RHR] connection conditions (safe shutdown state), in order to comply with fuel limits."* *"4.3. SAFETY BORATION* *The safety boration carried out by the RBS [EBS] is activated manually by the operator from the control room with two separate on/off controls that belong to each train (except in the event of ATWS where the RBS [EBS] is started automatically)."* From the above it can be seen that there are requirements for manual and automatic C&I equipment in the fulfilment of the diverse (boration) shutdown function. While there appears to be two means of shutdown the diversity of the C&I equipment for implementation of the Safety Injection System (SIS) and RBS[EBS] (boration) function requires further investigation. **O7. - EDF/AREVA should demonstrate that the C&I equipment for implementation of the SIS and RBS[EBS] (boration) function is adequately diverse from that used in other reactor shutdown equipment such as the reactor protection system.**
Common cause failure *Principle EDR.3 - Common cause failure (CCF)*	Within Ref. 9 EDF/AREVA state:-

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.	*"EPR design is considered to comply with the SAP Common cause failure is addressed for structures, systems and components important to safety."* and *"Diversity is implemented as required to protect against common cause failures of F1 systems, when it is possible to achieve diversity without lowering safety performance. This is the case, in particular, for RRC complex sequences where F1 systems are backed by F2 systems to mitigate accident consequences: examples are requirement for diverse Station Black-Out diesels, or diverse reactor trip function for ATWS scenarios (SSER 2.S.1)"* **O8.1 EDF/AREVA should explain why it is considered acceptable for F1 systems to be backed by F2 systems.** Within Ref.1 subchapter G.3 for the protection systems there are a number of relevant statements, for example, it is stated:- *"1.0.3.1.2 Single failure criterion (active and passive))* *The single failure must be applied at the system level. As a consequence, the PS [RPS] must be made of redundant trains able to perform the safety functions after the loss of one train. The redundant protection channels must be implemented in separate divisions to prevent common cause failure in case of internal or external hazard affecting one division. …."* *1.0.3.2.3 Technical Guidelines* *In addition to the general requirements given in chapter A.1 (General safety approach), requirements applicable to the PS [RPS] are presented in sections A.2.2 (Redundancy and diversity in the safety systems), B.2.2.2 (Computerized safety systems) and G3 (Design of Instrumentation and Control)* *1.3.1.1. Redundancy - …The F1 part of the Protection System is designed to withstand single failure even during maintenance or periodic testing. In order to achieve tolerance to single failure and maintenance, while minimizing the occurrence of spurious actuation, a four-fold redundancy is necessary. In addition, the four redundant protection channels must be implemented in separated divisions to prevent common cause failure in case of an internal hazard in one division (a single failure must be tolerated in addition to an internal hazard)."* Of particular note is rule A2.2 which includes the following text *"A.2.2 - Redundancy and diversity in the safety systems …. This reliability must be obtained via an adequate combination of redundancy and diversity. Adequate attention must be paid to the fact that the possibilities of common modes of failure limit the possibilities for reducing unavailability by adding identical trains (on this point, it is highlighted that it is probably not possible to demonstrate that the unavailability of a redundant safety system consisting of identical trains is less than 10-4 per demand), and due to the fact that diversity may result in more complex systems and maintenance difficulties; in addition, due attention must be paid to the support systems when the benefits linked to implementing diverse equipment and systems are evaluated.* *Special attention must be paid to reducing the possibility of common cause failures .."*

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.* *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.*	The above extracts demonstrate that there is a requirement to address CCF for the F1A safety systems (e.g. 10-4 limit quoted above) such as the protection system. Note that similar statements to those above exist for the PACS (e.g. see Ref. 1 subchapter 3 section 4.0.2.3 There is evidence of this SAP being addressed for the non F1A systems that employ redundancy (e.g. SAS – Ref. 1 subchapter G.3 section 2.0.2.3) but the approach to these systems will be considered during Step 3 (i.e. once the issue of categorisation, classification and standards has been clarified – see ECS.1). Note that the F1B SAS contributes to residual heat removal and might be a categorised F1A within the UK. P171/172/173 - **O8.2 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 (Ref. 10) and this aligns with Rule A2.2 (see above). However, it is not clear how this value is used in the design of the protection system. P174 - See under ESS.2. It is considered that there is a claim of compliance to SAP EDR.3.
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.*	EDF/AREVA claim compliance with this SAP in Ref. 9. The approach to single failure is outlined in Ref. 2 subchapter C.2 (e.g. section 1.5.2), and includes application of the single failure criterion to systems (F1A) and functions (F1B). There is, therefore, a claim that the design of the UK-EPR addresses the single failure criterion. Note that Ref.2 subchapter C.2 section 1.5.2 provides the following description of system/function single failure:- *"The criterion of (active or passive) single failure is taken into account in the design of F1A systems. This means that such systems are necessarily redundant. For F1B systems, the (active or passive) single failure criterion is taken into account at the function level. This means that such systems are not necessarily redundant and that, when they are not, another existing train (functional diversity, F1A or F1B) has to be*

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]	*assessed against a single failure. In this case, the requirement for physical separation is applied to the diverse trains."* P175 - Within Ref. 9 it is stated that "*Consequential failures resulting from the postulated single failure are also considered when applying the single failure principle (when means are not available to detect the occurrence of a failure and restore the function of the affected system or component in a short time period)."* The acceptability of the qualification (means are not available .. in the short term) will be considered further during Step 3. **O9. - EDF/AREVA should clarify why it is considered acceptable to only consider consequential failures "*when means are not available to detect the occurrence of a failure and restore the function of the affected system or component in a short time period"*.**
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.* *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.*	EDF/AREVA claim compliance with this SAP in Ref. 9. The UK EPR is provided with safety systems and these are described in Ref. 1 (e.g. Reactor Protection system and PACS). These systems are classified as F1A. There are other systems (F1B) that contribute to the maintenance of a safe state such as the SAS and clarification that these systems are appropriately classified is required (see above under ECS.1, ECS.2 and ECS.3). P336 – See comments above and under 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.***	Within Ref. 9 EDF/AREVA claim compliance with this SAP and provide various references to sections of the Step 2 submission (e.g. Ref. 2). Also, see comments under ESS.2 and EDR.2 above. Within Ref. 2 Subchapter C.1 there is the following Technical Guideline:- *"G.3 - DESIGN OF THE INSTRUMENTATION AND CONTROL 1. The requirements that apply to safety classified instrumentation and control must be described by the designer in a specification; compliance of these requirements with the demonstration of safety relating to the reference transients, incidents and accidents and to operating conditions with multiple failures must be justified."* There is a reference from this Technical Guideline into Ref.1 (i.e. G.1.0, G.3, G.4 and G.5). These references do provide an outline of safety system provisions and their functions.

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.*	Within Ref.1 Subchapter G.2 it is stated that " *1.2.2. Availability requirements - The availability objectives for typical C&I functions are defined in Chapter R.1 (C&I failure model). …"* However, note the following extracts from Chapter R which provide an insight into reliability figures assigned to the C&I systems: - *"Page 8 Note: for the F2 and NC systems used in the safety evaluation, an **unavailability of 10-3/demand** is used for the specific processing parts, provided design provisions (redundancy, independence in terms of process interruptions caused by the accident) are sufficient. Otherwise, a higher value is adopted."* ***"**2.2.3.3. Non-specific processing part **-** The numerical values used for the unavailability are global values, which dependent essentially on the class of C&I controllers. The global unavailability values allow for:* *- common cause failures due to errors in the operating software and data exchanges on networks,* *- internal common points in the hardware or software, (data buses, communication protocols common to all boards, etc.),* *- common cause failures due to use of the same technology (design, manufacture, etc.).* *The proposed values are **ten times lower** than those used for the specific parts of systems."* The above suggest a figure in the order of 10-2/demand for F2 and NC systems. Note also, the CCF limitation of 10-4 pfd for F1A safety systems (see EDR.3). The above is considered to show that there is an implicit claim that this SAP is met. However, clarification is required into the use of probabilistic criteria in the design of the EDF/AREVA ESBWR C&I systems. **O10. - EDF/AREVA should explain how probabilistic criteria are used in the design of the C&I systems and the reliabilities assigned to the various F1A, F1B, F2 and NC systems, and E1A, E1B, E2 and NC equipment.** P 337 - See comments above and under ESS.1. Satisfaction of SAP paragraph 337 will be considered during Step 3. Note that Ref. 9 contains references to the safety analyses and PSA.
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.* *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*	Within Ref. 9 EDF/AREVA claim compliance with this SAP and provide various references to sections of the Step 2 submission. In particular, it is stated:- *"The EPR safety systems are monitored as described in SSER 2.G. Also refer to SSER 1.A.7.2 presenting the C&I functions* *In the **Main Control Room**, all the means necessary to control and monitor the plant in operation (within specified operating limits and conditions) are available to operators.*

single point) that will remain habitable during foreseeable facility emergencies.	*If the Main Control Room is unavailable (e.g. due to fire), the operators are able to carry out monitoring and control of the plant from a **Remote Shutdown Station**, to allow a safe shutdown state to be reached and maintained."* The Technical Directives also contain requirements relevant to this SAP. Within Ref.2 Technical Directive G.3 (6) states *"6. In addition to the main control room, an Emergency Control Centre must be installed in case the main control room becomes unavailable. The designer must specify the situations for which the main control room would be unavailable, the consequences of such situations and the tasks to be performed accordingly from the Emergency Control Centre and the associated means."* The Technical Directive provides a compliance reference to Ref. 1 Subchapter G.2. Within Ref.1 Subchapter G.2 the provisions for monitoring the plant are described (e.g. safety information and control system). The requirement for a Main Control Room and Remote Shutdown Station is also stated. It is concluded that there is an acceptable 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.*	Within Ref. 9 EDF/AREVA claim compliance with this SAP and provide various references to sections of the Step 2 submission. In particular, it is stated:- *"As a general design rule, automation is adopted when it improves significantly safety, availability or cost and applies more particularly to tasks that otherwise would likely represent a source of human errors (e.g. those requiring a short response time or the assimilation of a large amount of information).* *In the event of a design basis event, all functions necessary to reach the controlled state[1] (namely "F1A" functions, as described in SSER 2.C.1) are initiated by the Protection System (PS). The functions to reach the safe state[2] (namely "F1B" functions) are either automatically generated in the Safety Automation System (SAS) or manually initiated."* **O12. – EDF/AREVA should identify those events for which operator action is claimed and demonstrate that such actions are fully justified (e.g. automatic initiation for these events is not reasonably practicable).** The Technical Directives also contain requirements relevant to this SAP. Within Ref.2 there is a Technical directive which states:- *"G3.2. The instrumentation and control functions may be F1A,*

[1] The **controlled state** is defined as a state where the fast transient resulting from a PCC-1 to PCC-4 event is finished. The plant is stabilized and where the core is sub critical, the heat removal is ensured in the short term, the core coolant inventory is stable and activity releases remain tolerable.

[2] The s**afe shutdown state** is defined as a state following a PCC-1 to PCC-4 event where the core is sub critical, the decay heat is removed durably and activity releases remain tolerable.

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.*	*F1B or F2 classified according to the general safety function classification (see section B.2.1). The effectiveness of automatic actions in these classes must guarantee the grace period defined for manual countermeasures in the event of an incident."* There is a reference to Ref.1 Subchapter G.1 (Design Principles of the C&I system) in response to this Technical Directive and this section contains the following statement:- *"0.2. FUNCTIONAL CRITERIA …C&I must ensure the execution of automatic actions identified in the safety case, according to the class of the incident or event."* The Protection System section of Ref. 1 Subchapter G.3 (F1 Classified C&I Systems) contains the following statement:- *"1.0.2. FUNCTIONAL CRITERIA - The Protection System must implement the necessary short-term automatic actuation of safety systems which are used to mitigate the consequences of PCC-2, 3 or 4 events….* *This system is required to accomplish similar actions in case of RCC-A accidents."* The section of subchapter G.3 on the F1A Priority and Actuation Control system (PACS) explains that the PACS must support "automation functions". From review of the various documents referenced above it appears that there is evidence that this SAP is addressed In the design of the UK-EPR. Further clarification will be required, during Step 3, as to the extent of application of this SAP, once the scope of safety systems has been confirmed (see also ECS.1 above). 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.*	Within Ref. 9 EDF/AREVA claim compliance with this SAP and provide a reference to Ref. 1. In particular, it is stated:- *"As a general design rule, automation is adopted when it improves significantly safety, availability or cost and applies more particularly to tasks that otherwise would likely represent a source of human errors (e.g. those requiring a short response time or the assimilation of a large amount of information).* *As a consequence, and in accordance with the Design Basis Faults analysis rules, all actions required within 30 minutes of an accident to reach a controlled or safe shutdown state are automated."* Also, see response above to ESS.8
Reliability – Avoidance of complexity *Principle ESS.21 - **The design of a safety system should avoid complexity**, apply a fail-safe*	Within Ref. 9 EDF/AREVA claim compliance with this SAP and

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.*	provide a reference to the "SSER 2.F.5" for in-service inspection. In particular, it is stated:- *"EPR design is considered to comply with the SAP* *The EPR safety systems incorporate means of revealing internal malfunction and a part of Protection System is designed to withstand single failure even during maintenance or periodic testing. Self tests and periodic tests are implemented to detect any component failures, and tests frequencies are calculated from the reliability expected of the tested function."* EDF/AREVA do not appear to specifically claim that the design avoids complexity. However, from the descriptions of the C&I systems within Ref.1 it can be seen that the systems (e.g. digital C&I) are typical of those used in modern nuclear plants. However, clarification will be required as to whether any complex features are employed such as combination of computer based systems to mitigate the consequences of postulated initiating events and ASICs/FPGAs etc. **O13.1 - EDF/AREVA should 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).** **O13.2 - EDF/AREVA should clarify 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.*	Within Ref. 9 EDF/AREVA claim compliance with this SAP and provide various references to sections of the Step 2 submission. In particular, it is stated:- *"EPR design is considered to comply with the SAP* *Redundant trains of the main safety systems (one per Safeguard Building) are strictly separated into four divisions. The four divisions of safety systems are consistent with the N+2 safety concept. With four divisions, one division can be out-of-service for maintenance and one division can fail to operate, while the remaining two divisions are available to perform the necessary safety functions even if one is ineffective due to the initiating event* *Moreover, self tests and periodic tests are implemented to detect any component failures. They consist of periodically checking the systems carrying out safety functions. In case of unavailability of equipment, maintenance (followed by re-qualification tests after maintenance work) can be performed. The maintenance is preventive or corrective, depending on the safety system state (in operation or not).* *Testing and maintenance of equipments are described in SSER 2.F.5 and G.6."* There is no specific requirement that matches this SAP (e.g. within Ref.1 Subchapter G.1 "Design Principles of the C&I System). However, within Ref.1 subchapter G.1 it is stated that:- **"***0.3.1.7. PERIODIC TESTING - F1 C&I systems, and F2 C&I systems not in continuous operation, must be designed to permit periodic tests to be performed in order to verify their ability to perform their functions*"

	With regard to the Protection System it is stated in Ref.1 subchapter G.3 :- ***"****1.0.4.2. Periodic tests and in-service inspection -* *…. Self tests and periodic tests must be implemented in F1 functions to detect failures. …* *The PS [RPS] is designed to allow the implementation of the periodic tests.* *Layout and design of the Protection System equipment must provide easy access to enable performance of in-service inspections and periodic tests. Suitable techniques have to be applied to reduce the possibilities of inappropriate actions during tests."* Also, see EDR.4 above on single failure criterion. Note the following text contained within Ref.1 subchapter G.3 "*1.3.1.1. Redundancy - …The F1 part of the Protection System is designed to withstand single failure even during maintenance or periodic testing. In order to achieve tolerance to single failure and maintenance, while minimizing the occurrence of spurious actuation, a four-fold redundancy is necessary."* It is concluded that there is an acceptable claim that unavailability of equipment is required to be addressed in the design of the safety systems. Note, however, issues exist regarding the classification of systems (see above under ECS.1) that could impact satisfaction of this SAP (e.g. expand the scope of those systems classified as safety to systems such as the SAS which is involved in decay heat removal).
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.*	Within Ref. 9 EDF/AREVA claim compliance with this SAP and provide various references to sections of the Step 2 submission. In particular, it is stated:- *"EPR design is considered to comply with the SAP* *EPR design development has fully acknowledged this general principle and the requirement for periodic testing is considered as the most basic requirement for safety classified components."* Within Ref. 1 subchapter G.1 "Design Principles of the C&I System) it is stated that:- *"0.3.1.7. PERIODIC TESTING - F1 C&I systems, and F2 C&I systems not in continuous operation, must be designed to permit periodic tests to be performed in order to verify their ability to perform their functions."* With regard to the F1A Protection System it is stated in Ref.1 subchapter G.3 :- *"1.0.4.2. Periodic tests and in-service inspection - ... Long periods of operation with a potential degraded C&I configuration (accumulation of failures) which might lead to lose a safety function are shortened by periodic testing.* *Self tests and periodic tests must be implemented in F1 functions to detect failures. Tests frequencies are calculated from the reliability expected of the tested function.* *The PS [RPS] is designed to allow the implementation of the periodic tests."*

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.*	Also for the F1A PACS it is stated :- *"4.0.2.1.7 Periodic testing - The F1A C&I functions managed by PACS must be subject to periodic testing (as defined in section C.2.1) and hence the PACS must be designed to allow periodic testing."* From the above it is concluded that there is a requirement for in-service functional testing of systems important to safety. However, clarification will be required on how this SAP is satisfied for non F1 systems. For, example, what is meant by "F2 C&I not in continuous operation". See also the response above to ESS.23. **O14. - EDF/AREVA should clarify the approach to in-service functional testing of non F1 systems. The response should include a description of how SAP EMT.7 is satisfied for "F2 C&I not in continuous operation".** 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 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*	Within Ref. 9 EDF/AREVA claim compliance with this SAP and provide references to the SSER (i.e. Ref. 1). The information within the compliance statement provides an overview of the intended processes but does not demonstrate compliance to the production excellence and confidence building elements of ESS.27. Within Ref. 2 it is stated: "*table 1 -Technical Directives (Technical Guidelines) for the design and construction of the next generation of pressurized water nuclear power plants - B.2.2.2 - Computerised safety systems - To obtain the high reliability required for the instrumentation and control systems, the designer must, when computerised systems are used, implement specific safety requirements, for the qualification of such computerised systems for each safety category, including design rules for the software.* *The three main principles for the design of computers for safety systems are to avoid faults, to eliminate faults and to tolerate faults. Avoiding faults may be implemented in a approach to construction via strict directives and rules that are applicable during the entire life cycle of a system, including system specification (hardware, software and integration), production (design, software coding and installation of hardware, tests), operation and maintenance.* *Avoiding faults must be completed by an analytical approach to eliminate faults. This includes informal procedures such as inspections, re-readings, audits, reviews and formal procedures such as accuracy tests, statistical analyses and various integration tests.* *In order to deal with residual faults which would persist in spite of all of the measures taken to avoid and eliminate faults, fault tolerance must be introduced into the design. For the hardware,*

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.* *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.*	*this may be obtained via redundancy and diversity The diversity must be examined to obtain tolerance to the software faults*" Within Ref. 1 there are sections (e.g. 3.6) in subchapter G.2 that address qualification of the C&I system and require evaluation and assessment. For example, with regard to "system software" (section 3.6.2) it is stated that "*the evaluation of confidence ... is particularly important*" and "*The evaluation and assessment of the confidence in system software components depends on the equipment class. Gradation criteria for the individual equipment classes follow the different requirements of the system requirements specifications as expressed in rules and standards."* Also, in Ref.1 subchapter G.2 section 3.6.1 it is stated that *"3.6.1. Properties of Components and intended Configurations - …The degree of evaluation and assessment depends on the equipment class of the C&I system: … safety and integrity properties are related to the reliability of the C&I system. This depends on: … the safety integrity of software that can be evaluated by qualitative analysis of the development process in order to assess a sufficient degree of confidence in the software."* It is concluded that the issue of demonstrating the adequacy of computer software is considered in the UK-EPR submission. However, precisely how the approach aligns with SAP ESS.27 (e.g. extent of independent confidence building) will need to be demonstrated. **O15.1 - EDF/AREVA should demonstrate the means by which its arrangements satisfy this SAP. 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 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). 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).**
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.*	Within Ref. 9 EDF/AREVA claim compliance with this SAP. In particular, it is stated:- *"EPR design is considered to comply with the SAP* *Description in SSER 2.G.1 table G1 addresses this question (see also SSER 2.B.6 referenced in this table)."*

	The referenced table G1 provides very brief details of the requirements for the different classes of C&I systems. Also, "SSER 2.B.6" only provides a brief overview of EPR technical codes. Also see response above to ESS.27 (e.g. approach based on equipment class and gradation of requirements). **O16. - EDF/AREVA 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. 10) 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.*	Within Ref. 9 EDF/AREVA claim compliance with this SAP. In particular, it is stated:- *"EPR design is considered to comply with the SAP* *As described in SSER 2.Q.4.1.2, a remote shutdown station (RSS) is provided as a back-up to the Main Control Room, for use in the event that the latter becomes uninhabitable due to fire, gas, smoke, etc. The function of the RSS is to allow control of the Unit when the MCR is unavailable, but when there is no other failure or accident, apart from a possible loss of the external power supply. The RSS enables the Unit to be monitored and managed during all PCC-1 (normal operational) situations and includes the instrumentation and controls required to bring the reactor to, and maintain it in, a safe state.* *The EPR design assumes that when operations are managed from the RSS the external electrical supply may not be available so power may only be obtainable from the diesel generators supplying the emergency switchboards.* *Note that the design assumes the RSS will not be required to be available in incident and accident conditions (PCC 2-4 and RRC) as the MCR is qualified to remain available under such conditions."* There are requirements relevant to this SAP within Ref.1 Subchapter G.1 "Design Principles of the C&I System, for example: - *"0.2. FUNCTIONAL CRITERIA - In the Main Control Room, all the means necessary to control and monitor the plant in operation (within specified operating limits and conditions) must be available to operators.* *In addition, in the Main Control Room, the operators must have at their disposal all the operating facilities required to carry out all actions identified in the safety case.* *If the Main Control Room is unavailable (due to a fire for example), the operators must be able to carry out monitoring and control of the plant from a Remote Shutdown Station, to allow a safe shutdown state to be reached and maintained."* Further, within other sections of Ref. 1 the various C&I systems that are to be provided to implement the above requirement are

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.*	described. For example, Ref.1 subchapter G.3 states:- *"3.5. OPERATING MODES - The MCP[PICS] , in the Main Control Room, is the preferred means of operating the plant. The operating team operates from the MCS[SICS] when no sufficient operator workstations in the Main Control Room are available or if the MCP[PICS] is completely unavailable.* *In case of the loss of the Main Control Room due to an internal hazard (such as fire), operation by the MCS[SICS] and the MCP[PICS] in the Main Control Room is no longer possible. In that situation, the operating team uses the MCP[PICS] control facilities in the Remote Shutdown Station."* It is concluded that there is an acceptable claim that this SAP is addressed in the design of the UK-EPR. P365/366 - See above and response to ESS.3 (e.g. O10). 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*	Within Ref. 9 EDF/AREVA claim compliance with this SAP. In particular, it is stated:- " *EPR design is considered to comply with the SAP* *Three systems are involved in process control, all of which use digital C&I architecture:* • *The Process Automation System (PAS). The main role PAS is the monitoring and automation of the plant in all normal operating conditions. Additionally the system performs some monitoring and control of sub-functions related to risk reduction (mitigation of RRC design extension condition). It is therefore F2 classified.* • *The Reactor Control, Surveillance and Limitation System (RCSL). The role of the RCSL is to process F2 and NC C&I classified functions related to core control and monitoring, including automatic LCO (limiting conditions of operation) functions, and limitation functions for core and reactor coolant circuit parameters requiring control rod actuation.* • *The Process Information and Control System (PICS). This system is used by the operators to monitor and control the plant in all plant conditions. It is classified to perform F2 and NC operating and monitoring functions. It accesses information from control systems and presents the information to the operating personnel at workstations in the Main Control Room, Remote Shutdown Station and Technical Support Centre or at local to plant workstations during commissioning or maintenance activities. It generates alarms in case of process or system anomalies and provides the operators with guidance for*

	implementing appropriate measures. *SSER 1.A.7.2, presents the C&I functions and SSER 2.G.3 and 4 the C&I systems.* Within Ref. 1 there are descriptions of the various control systems provided within the UK-EPR design to maintain variables within there range such as the Safety Automation System (subchapter G.3 section 2) and the Process Information and Control System (subchapter G.4 section 1). It is concluded that there is an adequate claim that this SAP is addressed in the design of the UK-EPR.
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.	Within Ref. 9 EDF/AREVA claim compliance with this SAP. In particular, it is stated:- *"EPR design is considered to comply with the SAP* *However, as stated in SSER 2.Q.2.2.3, the design of systems to communicate outside the main control room (MCR) has not been finalised at the current stage of the FA3 EPR design. This is because, given the rapid pace of technological development in this area, it is considered more effective to defer the choice of communication systems until as near as possible to the Unit's set-to-work date. For similar reasons, detailed specification of the plant communication systems in the UK EPR is likely to take place after the conclusion of the GDA process."* The reference to SSER 2.Q.2.2.3 does not appear correct (2.Q.2.3.2 appears to contain the referenced text). However, the requirement for communications systems is addressed in Ref.4 subchapter 5 section 4. For example, section 4.1 states **"***This section covers requirements relating to the plant communication systems, including the alarm systems, paging and internal and external telephone communication systems. The communication systems are designed to provide safe communications within the plant. They play an important role regarding safety since certain functions are linked to the PUI (Internal Emergency Plan).* *The communication systems are designed for the normal operational needs of the plant as well as for incidents and accidents."* It is considered that there is an adequate claim that this SAP is addressed by the UK-EPR design. <u>However, note that aspects of the communication system may not have been finalised.</u> During Step 3 confirmation will be required that paragraph 368 is met.

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