Health and Safety Executive

NUCLEAR DIRECTORATE

GENERIC DESIGN ASSESSMENT – NEW CIVIL REACTOR BUILD

STEP 3 CONTROL AND INSTRUMENTATION ASSESSMENT OF THE EDF AND AREVA UK EPR

DIVISION 6 ASSESSMENT REPORT NO. AR 09/038-P

HSE Nuclear Directorate
Redgrave Court
Merton Road
Bootle
Merseyside L20 7HS

EXECUTIVE SUMMARY

This reports presents the findings of the Control and Instrumentation (C&I) assessment of the EDF and AREVA UK EPR Pre-Construction Safety Report (PCSR) (Ref. 1) undertaken as part of Step 3 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process.

Scope of Assessment carried out

The report provides an overview of the safety case presented in the PCSR and the standards and criteria adopted in the assessment. The report presents the results of Nuclear Directorate's (ND) assessment, on a sampling basis, primarily directed at the C&I system level and an initial analysis of the Requesting Party's (RP) supporting arguments. The assessment was undertaken in accordance with HSE guidance (e.g. Safety Assessment Principles (SAPs) and technical assessment guides etc).

EDF and AREVA's safety arguments are set out in the PCSR. These include compliance to French C&I standards and guidance, and C&I provisions that would be expected of a modern nuclear reactor such as:

- safety systems (e.g. reactor shutdown systems such as the Protection System (PS));
- 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 (RSS) and communication systems for information transfer within and external to the plant.

ND's C&I assessment sample covered topics of particular relevance to C&I system level design including review of C&I system architecture, diversity of systems implementing reactor protection functionality and a subset of SAPs considered to be relevant at the system level. To assist with the C&I Step 3 assessment a Technical Support Contractor (TSC) was engaged to undertake technical reviews of SAP argumentation, system architecture and diversity. Points requiring clarification and technical review observations were raised by Technical Queries (TQs). Points of significant safety concern are covered by Regulatory Issues (RI) and one such issue (RI-UKEPR-002) was raised during Step 3.

Conclusion

As a result of the Step 3 C&I assessment I conclude that:

a) A number of significant concerns (raised in RI-UKEPR-002) were identified in relation to the adequacy of the UK EPR architecture, namely:

   i) substantiation of the reliability claims for the computer based Systems Important to Safety (SIS) that use the Teleperm XS and SPPA T2000 platforms;

   ii) complexity and interconnectivity of the architecture, and independence of systems;

   iii) absence of Class 1 displays and manual controls.

b) The PCSR and supporting documentation cover the main C&I systems expected in a modern nuclear reactor but the safety case argumentation needs improvement.

I have been encouraged by the positive response of EDF and AREVA to the concerns raised in RI-UKEPR-002. EDF and AREVA have proposed a way forward in relation to RI-UKEPR-002 that provides a basis for proceeding to Step 4 of the GDA which includes provision of a non-computer based backup system, one way communication from the Protection System (PS) to lower classified systems, Class 1 displays and manual controls, and reduction of reliability claims for the computer based Systems Important to Safety (SIS). Overall, I see no reason, on C&I grounds, why the UK EPR should not proceed to Step 4 of the GDA process.

LIST OF ABBREVIATIONS

BMS	(Nuclear Directorate) Business Management System
C&I	Control and Instrumentation
CAE	Claims-Argument-Evidence
CCF	Common Cause Failure
CINIF	Control and Instrumentation Nuclear Industry Forum
EDF and AREVA	Electricité de France SA and AREVA NP SAS
GDA	Generic Design Assessment
HSE	The Health and Safety Executive
IAEA	The International Atomic Energy Agency
NARPS	Next generation Analysis of Reactor Protection Systems
ND	The (HSE) Nuclear Directorate
NRC	Nuclear Regulatory Commission
OL3	Olkiluoto 3
PAS	Process Automation System
PCSR	Pre-construction Safety Report
PICS	Process Information and Control System
PPS	Primary Protection System
PS	Protection System
PSA	Probabilistic Safety Assessment
TAG	(Nuclear Directorate) Technical Assessment Guide
TQ	Technical Query
TSC	Technical Support Contractor
RCSL	Reactor Control, Surveillance and Limitation
RI	Regulatory Issue
RP	Requesting Party
RSS	Remote Shutdown Station
SAP	Safety Assessment Principle
SAS	Safety Automation System
SPS	Secondary Protection System
SIS	Systems Important to Safety

TABLE OF CONTENTS

1 INTRODUCTION

1 This reports presents the findings of the Control and Instrumentation (C&I) assessment of the EDF and AREVA Pre-Construction Safety Report (PCSR) (Ref. 1) undertaken as part of Step 3 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process. This assessment has been undertaken in line with the requirements of the Business Management System (BMS) document AST/001 (Ref. 2) and its associated guidance document G/AST/001 (Ref. 3). AST/001 sets down the process of assessment within the Nuclear Directorate (ND) and explains the process associated with sampling of safety case documentation. The Safety Assessment Principles (SAPs) (Ref. 4) have been used as the basis for the assessment of the C&I associated with the UK EPR design. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

2 The report provides an overview of the safety case presented in the PCSR and the standards and criteria adopted in the assessment. The report presents the results of ND's C&I system level assessment and initial analysis of the Requesting Party's (RP) supporting arguments. NB. An 'argument' is defined as "the set of evidence components that support a claim, together with a specification of the relationship between these evidence components and the claim" (Ref. 5).

3 The assessment was undertaken in accordance with the Step 3 Project Initiation Document (PID) (Ref. 6) and HSE guidance (e.g. on a sampling basis). Points requiring clarification and technical review observations have been raised by Technical Queries (TQs) (Ref. 7). Points of significant safety concern are covered by Regulatory Issues (RI) and one such issue (RI-UKEPR-002, Ref. 8) was raised during Step 3 (see below).

2 NUCLEAR DIRECTORATE'S ASSESSMENT

2.1 Requesting Party's Safety Case

4 EDF and AREVA provided a number of documents setting out its C&I safety case and a submission outlining where the various SAPs are addressed in the documents. The main submission that describes the C&I is Ref. 1. The C&I provisions claimed 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));
- 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 (RSS);
- communication systems for information transfer within and external to the plant.

5 The EDF and AREVA Step 2 submission on C&I mainly describes a conceptual design. During Step 3 EDF and AREVA confirmed its wish to have the HSE GDA C&I assessment based on the Flamanville 3 (FA3) design and documentation. Therefore, the architecture and technology of the UK EPR C&I submitted for GDA is identical to the architecture and technology of FA3. The UK EPR makes use of two main C&I platforms, Teleperm XS (e.g. PS and Reactor Control, Surveillance and Limitation (RCSL) system) and Siemens SPPA T2000 (e.g. PAS, PICS and Safety Automation System (SAS)).

6 An important aspect of the safety demonstration is the classification of Systems Important to Safety (SIS) 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. The UK EPR C&I design concept reflects French custom and practice, and is largely based on French standards (e.g. RCC-E) and French regulatory requirements. EDF and AREVA have stated that RCC-E is largely based on IEC nuclear standards. Four function (i.e. F1A, F1B, F2 and NC) categories and equipment (i.e. E1A, E1B, E2 and NC) classes are used.

2.2 Standards and Criteria

7 The standards and criteria used for the C&I Step 3 assessment include:

- a subset of SAPs considered to be relevant at the system level (Table 1);
- relevant sections of HSE Technical Assessment Guides (TAGs) (e.g. Ref. 9 and Ref. 10) and regulatory guidance (Ref. 5);
- relevant nuclear sector standards related to C&I system level design, system architecture and diversity of systems (e.g. Ref. 11 and 12 etc.).

2.3 Nuclear Directorate Assessment

8 During Step 3 EDF and AREVA's safety case argumentation was assessed using a subset of SAPs considered to be relevant at the C&I system level (Table 1). Aspects of particular relevance to C&I system level design were also assessed, namely:

- C&I system architecture;
- diversity of systems implementing reactor protection functionality.

9 To assist with the C&I Step 3 assessment a Technical Support Contractor (TSC) was engaged to undertake technical reviews of SAP argumentation, system architecture and diversity. The TSC's reports (Refs 13, 14 and 15) provide the technical opinion of the TSC. I specified and undertook reviews of the TSC's work. Following review, all areas requiring further clarification were raised with EDF and AREVA by TQ. Assessment of EDF and AREVA's TQ responses will continue during Step 4.

2.3.1 Step 3 SAP Assessment

10 A list of the SAPs used to assess the adequacy of EDF and AREVA's safety case argumentation during Step 3 can be found in Table 1. In selecting the SAPs for Step 3 particular attention was given to those SAPs considered to have particular relevance to system and architectural design. A detailed report on the adequacy of EDF and AREVA's safety case argumentation was produced by the TSC (Ref. 13). Annex 3 contains a table of the TSC's main findings and observations. As a result of the SAP argumentation assessment it is concluded that:

- While EDF and AREVA claim compliance to the SAPs further argumentation and evidence will need to be provided to substantiate the claims.
- The PCSR content does not provide adequate reference to the evidence that supports the claims.
- Safety Categorisation and Classification - The UK EPR 4 levels of categorisation (F1A, F1B, F2 and NC) and classification (E1A, E1B, E2 and NC) do not align with HSE's SAPs (Ref. 4) or BS IEC 61226:2005 (Ref. 19).
- Standards – Further clarification is required in relation to the standards used by EDF and AREVA.

- Defence-in-Depth - The allocation of safety functions to C&I systems conforms to the defence-in-depth concept, aligning with the 5 levels referred to in IAEA Safety Standard NS-R-1 (Ref. 28). However, use is made of only two digital platforms (i.e. Teleperm TXS and SPPA-T2000). A failure of one digital platform due to Common Cause Failure (CCF) may result in the loss of more than one level of defence.
- Redundancy - The level of equipment redundancy within the PAS and SAS requires further clarification.
- Diversity - Functional and equipment diversity is used across the two digital platforms Teleperm XS and SPPA-T2000.
- PS Independence - It should be demonstrated that faults in other systems will not impact on the PS safety function and that the communications are outwards from the PS.
- Reliability - The PCSR PSA gives 1×10^{-5} pfd and 1×10^{-4} pfd for the common 'Processing (non-specific)' parts of the E1A (Teleperm XS) and non-E1A (SPPA-T2000) systems respectively. These reliability claims are either beyond or at the normal limits for computer based safety systems (Ref. 10) and insufficient justification of these claims is provided.
- Failure to Safety - The fail-safe principle as applied to C&I systems is not well covered in the PCSR.
- Computer Based SIS - Further clarification is required as to how the independent confidence building and production excellence legs (Ref. 10) are addressed.

11 The majority of SAP assessments resulted in TQs being raised. The responses to the TQs will continue to be assessed during Step 4.

12 The TSC report (Ref. 13) was based on the PCSR submitted for the start of GDA Step 3 which was dated April 2008 (Ref. 16). A revision of the PCSR was submitted in June 2009 (Ref. 1) and the TSC assessed the impact of the revisions to the PCSR on its report conclusions (Ref. 17) and determined that the June 2009 Issue 2 of the PCSR (Ref. 1) did not introduce significant improvements to the safety argumentation presented in the April 2008 PCSR (Ref. 16). A major change was the introduction of References at the end of each sub-chapter. The TSC concluded that "the use of '[Ref]' at the end of a paragraph in a Section within a sub-chapter is not very specific when several references are listed under this Section. The system of referencing is, therefore, inefficient but does provide some link to supporting evidence. However, this may not tie in well with a particular argument against a specific SAP".

13 EDF and AREVA is to provide further information on the production excellence and confidence building activities applied to computer based SIS in response to RI-UKEPR-002 (submission planned for November 2009). Discussions are ongoing with regard to the use of statistical testing to support the PS reliability claim.

14 Overall, as a result of the SAP argumentation assessment it is concluded that there is currently insufficient Claims-Argument-Evidence (CAE) structure in the PCSR to clearly demonstrate how the C&I SAPs are addressed. The PCSR rarely makes any direct reference out to evidence to support the claims and arguments.

2.3.2 C&I System Level Architecture

15 At the start of Step 3 an initial assessment of the UK EPR C&I architecture was undertaken. The assessment revealed that the C&I architecture is overly complex with reliance on two computer based systems (originally developed by the same Company) and a high degree of connectivity between systems. Independence between the safety

(Class 1) and safety related systems (Class 2/3) appears to be significantly compromised.

16 A particular concern is that lower safety class systems appear to have write access (permissives etc.) to higher safety class systems (i.e. the usual UK practice of only allowing one-way online communication from a safety system to systems of a lower safety class is not applied in the UK EPR design).

17 Other significant concerns identified include:

- substantiation of the reliability claims for the computer based SIS that use the Teleperm XS and SPPA-T2000 platforms (e.g. PS, Safety Automation System (SAS) and PAS);
- the absence of a safety Class 1 display system;
- no Class 1 manual controls or indications either in the Main Control Room or Remote Shutdown Station;
- EPR function categories / equipment class assignments do not appear to align with UK expectations as defined in BS IEC 61226:2005 (Ref. 19).

18 It is considered that the PCSR PSA reliability claims for C&I systems (i.e. 10^{-5} pfd for the common 'Processing (non-specific)' parts of the Teleperm XS Protection System (PS) and 10^{-4} pfd for the Siemens SPPA -T2000 platform that provides reactor protection) will prove very difficult if not impossible to substantiate. The claim on the PS system is beyond the normal limit for reliability claims (i.e. 10^{-4} pfd) as stated in nuclear sector standards and guidance (Ref. 5, 10, 18, 19, 20 and 21) including that of the safety advisory group to France's regulatory body (ASN) (Ref. 22), and the claim for the Siemens SPPA-T2000 platform is at the limit.

19 EDF and AREVA undertook a sensitivity study that looked at the potential for using less demanding reliability values for the computer based C&I platforms. The sensitivity study revealed that there is unlikely to be any margin for reducing the claimed C&I system reliabilities to more credible values without significantly increasing EDF and AREVA's risk estimates to levels which are close to or in excess of the Basic Safety Levels (see Ref. 4). By way of comparison it should be noted that the claim on the Sizewell B computerised Primary Protection System (PPS) when standing alone was 10^{-4} pfd and for the most frequent faults the claim for the combination of the PPS and hardware (laddic) based Class 1 Secondary Protection System (SPS) was 10^{-7} pfd. From this it can be seen that EDF and AREVA are claiming two orders of magnitude better reliability for the combination of two computer based systems (i.e. 10^{-9} pfd) one of which (i.e. the Siemens SPPA-T2000 platform) was (to our knowledge) not developed to nuclear sector protection system standards such as IEC 60880 (Ref. 23) or IEC 60987 (Ref. 24).

20 Regulatory Issue RI-UKEPR-002 was raised in relation to the concerns on the C&I architecture and this was communicated to EDF and AREVA in letter EPR70085R dated 16 April 2009 (Ref. 8). The Regulatory Issue Actions raised in Ref. 8 are reproduced in Annex 2. EDF and AREVA were advised that the provision of a hardware back up protection system (as employed in Olkiluoto 3 (OL3)) might be a possible way forward on some of the concerns identified above. The provision of a hardware backup system on OL3 and Class 1 display system (e.g. US EPR) suggests that the implementation of such systems is reasonably practicable and necessary for a plant designed to meet modern international safety standards.

21 In addition to our initial UK EPR architecture review, the TSC undertook a detailed review of the UK EPR C&I architecture (Ref. 14). The main objective of the work was to consider the overall system architecture (C&I systems) looking at safety design features in the EDF and AREVA UK EPR submission, namely:

- Defence-in-depth and failure mode management including CCF.
- Independence and diversity.
- Provision for automatic and manual safety actuation.
- Appropriateness of equipment type / class.

22 The TSC work involved defining a list of reactor-independent essential / desirable system architecture characteristics needed to comply with relevant standards and guidance. In selecting the characteristics consideration was given to HSE SAPs (Ref. 4), TAGs (Ref. 9 and 10) and nuclear sector C&I standards (i.e. Ref. 11, 12 and 24).

23 The main conclusion of the TSC report (Ref. 14) on the C&I architecture of the UK EPR is that "the submission made by EDF and AREVA for the overall C&I architecture of the UK EPR reactor does not demonstrate that the UK EPR C&I architecture is in accordance with many of the relevant principles, standards and guidance." A full list of the TSC's main observations can be found in Annex 4. The main concerns and observations arising from the TSC's review include:

- overall specification of the C&I architecture design including the interface requirements between different systems;
- complexity and inter-connectivity of the C&I architecture;
- classification of certain safety systems and safety-related systems;
- reliability and diversity claims for the C&I systems;
- write access to Class 1 systems from lower class systems;
- absence of key information in the PCSR.

24 It is important that the C&I architecture is based on an overall consideration of the safety functions that need to be performed, including the category and reliability of the functions. In assigning the functions to systems, consideration needs to be given to the maintenance of independence (so that a failure in a lower safety class system does not frustrate the correct operation of systems of a higher safety class) and communication of information to other systems (e.g. communication of important safety display information to the main control room). The rigourous definition of the overall system architecture including assignment of functions to systems and definition of interface and independence requirements assists with the demonstration that there are no safety deficiencies in the overall system architecture.

25 The work described in Ref. 14 was carried out on the basis of the April 2008 PCSR (Ref. 16). The TSC assessed the impact of the June 2009 UK EPR PCSR revision (Ref. 1) on its report conclusions and determined that the revision has not introduced significant changes to the C&I architecture compared to that described in Ref. 16. In particular, the major concerns remain over, for example, inputs into the Class 1 system from non-Class 1 sources and absence of architectural requirements.

26 The most significant change in Ref. 1, in relation to the C&I architecture, is the introduction of the RRC-B SAS and the provision of more information on the RRC-B Severe Accident C&I; the former using the SPPA-T2000 platform and the latter using Teleperm XS. The SAS has been renamed the Plant SAS and a dedicated SAS communications bus has been introduced.

27 The TSC's work confirmed the initial concerns in relation to the C&I architecture as raised under RI-UKEPR-002.

28 In response to RI-UKEPR-002, EDF and AREVA provided further substantiation of the UK EPR C&I design and a commitment (Ref. 25) to undertake a number of modifications

to the UK EPR C&I architecture (i.e. as currently submitted in Ref. 1) to address the main areas of concern. The main commitments are summarised below (further details are contained in the attachment to Ref. 25):

- One way communication will be implemented from the PS to the lower classified systems (should any exceptions be identified then they will be justified on a case-by–case basis).
- All signals transmitted between the Safety Information and Control System (SICS) and the PS will use a F1A (Class 1) path.
- A non-computerised backup system (1×10^{-3} pfd) will be implemented in order to provide protection and controls in case of total loss of C&I functions from the Teleperm XS and SPPA-T2000 platforms.
- Reduction of the reliability claims for the Teleperm XS (1×10^{-5} pfd to 1×10^{-4} pfd) and SPPA-T2000 (1×10^{-4} pfd to 1×10^{-2} pfd) platforms.

29 The detailed list of information transmitted from the PS to the SICS and necessary to operate the plant using EDF's State Oriented Approach will be submitted during GDA Step 4. The technology used for the SICS control and display system will be fixed and justified during GDA Step 4. If non-F1A (Class 1) SICS indicators are required to be connected to the PS then the connection will be implemented via one-way electrically decoupled links.

30 The non-computerised backup system will include the implementation of automatic functions and facilitate operator actions (after 30 minutes) as necessary to achieve a controlled state of the plant and to maintain it in a safe state for the long term. The functions of the system will be defined through a functional analysis based on PSA studies to ensure that HSE SAP (Ref. 4) risk targets are met. The automatic functions will be implemented in the four C&I divisions using a 2 out of 4 voting logic. The manual controls will be directly hardwired to the switchgear of the actuators. Actuation will either be initiated from the main control room (from SICS) or at the switchgear level (i.e. depending on time available as justified by human factor's analysis).

31 The impact of the architectural changes on the design and operation of the plant will be considered and reported in the last update of the PCSR at the end of GDA Step 4.

32 I have been encouraged by the positive response of EDF and AREVA to the concerns raised in RI-UKEPR-002 on the UK EPR C&I architecture. EDF and AREVA have proposed a way forward (Ref. 25) in relation to RI-UKEPR-002, that provides a basis for proceeding to Step 4 of the GDA. In particular, the provision of a non-computer based backup system, one way communication from the PS to lower classified systems, Class 1 information and manual controls, and reduction of reliability claims for the computer based systems address, in principle, our major concerns. Assessment of the details of EDF and AREVA's proposals will be undertaken during Step 4 of the GDA.

2.3.3 Diversity of Systems Implementing Reactor Protection Functionality

33 A review of the diversity of those systems implementing reactor protection functionality was undertaken by the TSC. The systems included in the diversity review were the PS (Teleperm XS) and SAS / PAS (Siemens SPPA-T2000). These systems were selected because they perform the UK EPR protection functions.

34 The approach adopted by the TSC included consideration of various forms of diversity, including:

- Functional and equipment diversity (including diversity of platform).
- Diversity of Verification and Validation.

- Diversity of physical location (segregation).
- Software diversity.
- Data diversity / signal diversity.
- Diversity of design / development.
- Diversity of specification.

35 The work required the definition of a list of reactor-independent diversity characteristics derived from relevant standards and guidance. In selecting the characteristics consideration was given to SAPs, TAGs, nuclear sector C&I standards (i.e. 11 and 12), regulatory guidance (Ref. 5) and relevant research (Ref. 26).

36 The main finding of the TSC's report (Ref. 15) on the diversity of systems implementing reactor protection functionality is that the submission made by EDF and AREVA for adequacy of the diversity between the primary (PS) and secondary (SAS/PAS) protection systems, does not demonstrate accordance with many of the relevant principles, standards and guidance used in the review. A full list of the TSC's main observations can be found in Annex 5. The main concerns arising from the review are:

- excessive reliability claim for the diverse protection systems taken together;
- lack of evidence of platform diversity;
- lack of evidence of diversity within systems in the same safety group when high reliability is needed;
- absence of key information in the PCSR.

37 In responding to RI-UKEPR-002, EDF and AREVA have provided further substantiation of the diversity between the Teleperm XS and SPPA T2000 platforms. In addition, the changes proposed to the UK EPR architecture and reliability claims will have a significant impact on the conclusions of the TSC's diversity review. During Step 4 the adequacy of the diversity of those systems implementing Category A functions will be considered further, in particular, taking into account the modifications proposed in response to RI-UKEPR-002.

2.3.4 Step 2 Observations

38 Regular progress meetings have been held with EDF and AREVA to progress close out of ND's Step 2 assessment observations (Ref. 27). EDF and AREVA have produced an action tracking matrix to capture the work required to close out the observations. So far reasonable progress has been made in closing out the observations and the work will extend into Step 4 which, given the progress made, is not considered unreasonable. In closing out the Step 2 observations consideration will need to be given to the impact of the architectural changes proposed to address RI-UKEPR-002. In carrying out its work the TSC has included consideration of the Step 2 observations and responses received from EDF and AREVA.

2.3.5 Use of Overseas Regulators Information

39 The United States Nuclear Regulatory Commission (US NRC) has completed a safety evaluation of the Teleperm XS platform and the safety evaluation report will be considered during our Step 4 assessment.

2.3.6 GDA Related C&I Research

40 Research into the means of justifying graphical based auto-code generators (as used for the implementation of systems based on the Teleperm XS) is being undertaken as part of the Control and Instrumentation Nuclear Industry Forum (CINIF) Next generation Analysis of Reactor Protection Systems (NARPS) project. The results of the research, where considered appropriate, will be used to inform ND's assessment.

3 CONCLUSIONS AND RECOMMENDATIONS

41 As a result of the Step 3 C&I assessment I conclude that:

- A number of significant concerns (raised in RI-UKEPR-002) were identified in relation to the adequacy of the UK EPR architecture, namely:
  - i) substantiation of the reliability claims for the computer based Systems Important to Safety (SIS) that use the Teleperm XS and SPPA T2000 platforms;
  - ii) complexity and interconnectivity of the architecture, and independence of systems;
  - iii) absence of Class 1 displays and manual controls.
- The PCSR and supporting documentation cover the main C&I systems and provisions that would be expected in a modern nuclear reactor but the safety case argumentation and identification of evidence needs improvement.

42 I have been encouraged by the positive response of EDF and AREVA to the concerns raised in RI-UKEPR-002. EDF and AREVA have proposed a way forward (Ref. 25) in relation to RI-UKEPR-002, that provides a basis for proceeding to Step 4 of the GDA, which includes provision of a non-computer based backup system, one way communication from the protection system to lower classified systems, Class 1 information and manual controls, and reduction of reliability claims for the computer based SIS. Overall, I see no reason, on C&I grounds, why the UK EPR should not proceed to Step 4 of the GDA process.

4 REFERENCES

1 *UK EPR Pre-Construction Safety Report.* UK EPR-0002-132 Issue 02, EDF and AREVA, June 2009.

2 *ND BMS, Assessment Process.* AST/001, Issue 2, HSE, February 2003.

3 ND BMS, Guide: Assessment Process. G/AST/001, Issue 2, HSE, February 2003.

4 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition, Revision 1, HSE, January 2008.

5 *Seven Party task force on safety critical software report on "Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorized technical support organizations".* Available via the HSE website.

6 *New Reactor Build. Step 3 C&I Assessment Strategy.* ND Division 6 AR 08/018, TRIM Ref. 2008/164681.

7 *EDF and AREVA UK EPR - Schedule of Technical Queries Raised during Step 3*. HSE-ND, TRIM Ref. 2009/358252.

8 *UK EPR Control and Instrumentation (C&I) Architecture Regulatory Issue RI-UKEPR-002.* HSE letter Unique Number EPR70085R, 16th April 2009. Available on the HSE website.

9 *ND BMS, Technical Assessment Guide. Safety Systems.* T/AST/003, Issue 4, HSE, 10 June 2009.

10 *ND BMS, Technical Assessment Guide. Computer Based Safety Systems.* T/AST/046, Issue 2, HSE, 16 June 2008.

11 *BS IEC 61513:2001 Nuclear power plants - Instrumentation and control for systems important to safety – General requirements for systems.* International Electrotechnical Commission (IEC), 2001

12 *BS IEC 62340:2007 Nuclear power plants - Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF).* International Electrotechnical Commission (IEC), 2007.

13 *NII GDA Technical Review – C&I SAP Compliance Assessment for EDF / AREVA UKEPR* – 36331/35856R, Issue 1.7.

14 *NII GDA Technical Review – C&I System Architecture Safety Assessment for UK EPR* – S.P1440.57.11, Issue 2.0.

15 *NII GDA Technical Review – C&I Diversity Aspects of C&I Category A Functional Systems Design Assessment for UK EPR* - S.P1440.57.12, Issue 2.0.

16 *UK EPR Pre-Construction Safety Report.* UK EPR-0002-011 Issue 00, EDF and AREVA, April 2008.

17 *NII GDA Technical Review - C&I UK EPR - PCSR Impact Assessment* – 36331/3593R, Issue 1.0. June 2009

18 *Software for Computer Based Systems Important to Safety in Nuclear Power Plants. I*AEA Safety Standards Series No. NS-G-1.1. International Atomic Energy Agency (IAEA) Vienna 2000.

19 *BS IEC 61226:2005 Nuclear power plants - Instrumentation and control systems important to safety – Classification of instrumentation and control functions.* International Electrotechnical Commission (IEC), 2005.

20 *The Tolerability of Risk From Nuclear Power Stations.* (HSE 1992) ISBN 0-11-886368-1.

21 *The use of computers in safety-critical applications – Final report of the study group on the safety of operational computers* – (HSC 1998) ISBN 0 7176 1620 7.

22 *Technical Guidelines for the design and construction of the next generation of nuclear pressurized water plant units* - adopted during plenary meetings of the GPR and German experts on the 19 and 26 October 2000.

23 *BS IEC 60880:2006 Nuclear power plants - Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions.* International Electrotechnical Commission (IEC), 2006.

24 *BS IEC 60987:2007 Nuclear power plants - Instrumentation and control important to safety – Hardware design requirements for computer-based systems.* International Electrotechnical Commission (IEC), 2007.

25 *EDF and AREVA Letter EPR00180R "RI-UKEPR-002 – C&I architecture issues".* TRIM Ref. 2009/386051.

26 *Guidance on means to achieve system diversity: DISPO6 view.* Littlewood B, Popov P, Strigini L, Version V1.0 PP_DISPO6_01, 27th October 2008.

27 *New Reactor Build. EDF and AREVA Step 2 C&I Assessment.* HSE-ND, March 2008. TRIM Ref. 2008/135496.

28 *Safety of Nuclear Power Plants: Design – Requirements.* IAEA Safety Standards Series – No. NS-R-1. International Atomic Energy Agency (IAEA) Vienna 2000.

Table 1

Control & Instrumentation Safety Assessment Principles Considered During Step 3 Assessment

SAP No.	Assessment topic / SAP title
EKP - Key Principles	
EKP.3*	Defence in depth
EKP.5*	Safety Measures
ECS - Safety classification and standards	
ECS.1	Safety categorisation
ECS.2	Safety classification of structures, systems and components
ECS.3	Standards
EQU - Equipment Qualification	
EQU.1*	Qualification procedures
ERL - Reliability Claims	
ERL.2*	Measures to achieve reliability
ERL.4*	Margins of Conservatism
EMT - Maintenance, inspection and testing	
EMT.1*	Identification of requirements
EMT.3*	Type testing
EMT.6*	Reliability claims
EMT.7	Functional testing
ELO –Layout	
ELO.1*	Access
EHA - External and internal hazards	
EHA.10*	Electromagnetic interference
EDR, ESS - Failure to safety	
EDR.1	Failure to safety
ESS.21(part)	Reliability – failsafe approach
EKP, EDR, ESS, ERC - Defence in depth	
EKP.3*	Defence in depth
EDR.2	Redundancy, diversity and segregation
ESS.2(part)	Determination of safety system requirements – Defence in depth
ESS.7	Diversity in the detection of fault sequences

SAP No.	Assessment topic / SAP title
ESS.18	Failure independence
ERC.2	Shutdown systems
EDR.3	Common cause failure
EDR.4	Single failure criterion
EKP, ESS, ERL - Safety systems	
EKP.5*	Safety Measures
ESS.1	Requirement for safety systems
ESS.2(part)	Determination of safety system requirements
ESS.3	Monitoring of plant safety
ESS.8	Automatic initiation
ERL.3	Engineered safety features (Automatic initiation)
ESS.9*	Time for human intervention
ESS.10*	Definition of capability
ESS.11*	Demonstration of adequacy
ESS.12*	Prevention of service infringement
ESS.15*	Alteration of configuration, operational logic or associated data
ESS.16*	No dependency on external sources of energy
ESS.19*	Dedication to a single task
ESS.20*	Avoidance of connections to other systems
ESS.21(part)	Reliability – Avoidance of complexity
ESS.23	Allowance for unavailability of equipment
ESS.24*	Minimum operational equipment requirements
ESS, ESR - Computer-based systems important to safety	
ESS.27	Computer-based safety systems
ESR.5	Standards for computer based equipment
ESR - Control and instrumentation of safety-related systems	
ESR.1	Provision in control rooms and other locations
ESR.3	Provision of controls
ESR.4*	Minimum operational equipment
ESR.7	Communications systems
EES - Essential services	
EES.1*	Provision
EES.2*	Sources external to the site
EES.8*	Sources external to the site – only source
EES.9*	Loss of service

SAP No.	Assessment topic / SAP title
EHF - Human Factors	
EHF.7*	User interfaces

SAPs identified with an asterisk, e.g. EES.1*, are new for Step 3 (i.e. they were not considered during Step 2).

Annex 1 – Control and Instrumentation – Status of Regulatory Issues and Observations

RI / RO Identifier	Date Raised	Title	Status	Required timescale (GDA Step 4 / Phase 2)
Regulatory Issues				
RI-UKEPR-001	16 Apr 2009	UK EPR Control and Instrumentation (C&I) – Architecture. C&I assessment work completed to date has identified the adequacy of the UK EPR C&I architecture as a matter of sufficient importance to raise this as a RI at this stage that may, if not resolved, prevent the successful outcome of GDA.	EDF and AREVA have proposed a way forward that provides a basis for proceeding to Step 4 of the GDA.	Step 4
Regulatory Observations				
None.				

Annex 2 – Regulatory Issue RI-UKEPR-002 – Regulatory Issue Actions

This annex reproduces the Regulatory Issue Actions raised with EDF and AREVA in HSE letter Unique Number EPR70085R, *UK EPR Control and Instrumentation (C&I) Architecture Regulatory Issue RI-UKEPR-002,* dated 16 April 2009 (Ref. 8), available from the HSE web-site.

"*RI-UKEPR-002.A1 – Adequacy of Reactor Protection System Arrangements*

Discussion - See letter for discussion related to this action. EDF and AREVA have not demonstrated that the UK EPR C&I design satisfies the following HSE Safety Assessment Principles (SAPs); ECS.3 (O2), EDR.2 (O5), EDR.3 (O8), ERL.4, ESS.1, ESS.2 (O10), ESS.7 (O6), ESS.21 (O13), ESS.27 (O15) and ESR.5 (O16).*

Action A1.1: EDF/Areva to review the UK EPR C&I systems' architecture to identify and implement measures to reduce the reliability claims placed on the Teleperm TXS and Siemens SPPA T2000 systems.

Action A1.3: EDF/Areva to review the UK EPR C&I systems' architecture to determine the reasonable practicability of providing a hardware based back up protection system (i.e. as provided on OL3, AP1000 and Sizewell B).

Action A1.3: EDF/Areva to demonstrate that the protection System PS (Teleperm XS) and back up/secondary protection system are adequately diverse and independent (ERC.2 (O7), ESS.18 and ESS.27/Ref. 4 Appendix 4).

Action A1.4: EDF/Areva to justify the reliability figures used for each of the protection systems when claimed independently and in combination. EDF/Areva to ensure its response includes consideration of appropriate guidance and standards (e.g. Refs 1 to 7) and explains how its standards reflect the functional reliability requirements. NB. UK research on high reliability computer based systems has shown that there are significant difficulties in justifying such systems.

Action A1.5: EDF/Areva to explain its approach to the demonstration of the adequacy of computer based systems important to safety (CBSIS) including the identification of production excellence and independent confidence building activities (Ref. 4) for each of the CBSIS.

RI-UKEPR-2.A2 – Failure Independence between Safety (Class 1) and Other Systems Including Safety Related Systems (Class 2/3).

Discussion - See letter (paragraph 2) for discussion related to this action. EDF/Areva has not demonstrated that the UK EPR C&I design satisfies the following HSE SAPs; ERC.2 (O7), ESS.15, ESS.18 and ESS.20.

Action A2.1: EDF/Areva to review and explain the extent of information transmitted to the Teleperm TXS Protection System from non F1A systems (e.g. permissives, vetoes and resets of automatically initiated F1 functions etc.).

Action A2.2:EDF/Areva to review and implement measures to ensure the C&I systems' design meets HSE SAP ESS 15, 18 and 20, and the security principle that there should be no communication to safety systems from safety related systems.

Action A2.3: EDF/Areva to demonstrate that electrical and functional isolation exists for interfaces to systems of different safety class.

Discussion – The Reactor Control, Surveillance and Limitation System

(RCSL) and the protection system (PS) are both based on the Teleperm XS system and as such there exists the potential for a common mode failure of both systems.

Action A2.4: EDF/Areva to explain why the potential for common mode failure of the RCSL and PS is not a concern (SAP ESS 18).

RI-UKEPR-2.A3 – Provision of Class 1 Manual Controls and Indications in the MCR and RSS.

Discussion – There are no Class 1 manual controls or indications either in the MCR or RSS (c.f. AP1000 and Sizewell B which do have significant Class 1 manual controls and indications including hardwired reactor trip). Note that the SICS is Class 2 (F1B/E1B) and the interface to the Class 1 (F1A/E1A) protection system is via a communications bus (i.e. not hardwired). Manual operation of RT/ESFAS appears to be via the Class 3 (F2/E2) PAS. EDF/Areva has not demonstrated that the UK EPR C&I design satisfies the following HSE SAPs; ESS.3, ESS.8 and ESS.13.

Action A3: EDF/Areva to review the C&I architecture design to determine the reasonable practicability of providing Class 1 manual control and indication systems (e.g. as for the OL3 and US EPRs that have the TXS (QDS) which is not present in FA3 or UK EPR) in the MCR and RSS.

RI-UKEPR-2.A4 - EPR Function Categories and Equipment Classes

Discussion - EPR function categories do not appear to align with UK interpretation of IEC 61226 (see Table 1 below). The only agreement is for the PS and PACS (Category A) all others appear to be one category lower. EDF/Areva has not demonstrated that the UK EPR C&I design satisfies the following HSE SAPs; ECS.1, ECS.2 and ECS.3.

Action: EDF/Areva to review Table 1 and provide the requested clarifications (see comments column of Table 1), namely;-

Action A4.1: EDF/Areva to clarify why the functional safety category of the SICS is not F1A.

Action A4.2: EDF/Areva to clarify the SICS operational state when the PICS is operational.

Action A4.3: EDF/Areva to review and explain the reasonable practicability of providing plant operation with indications and controls appropriate to the function (e.g. NSSS controls are normally Class 1/2 as per Sizewell B and AP1000) which are normally in operation as opposed to relying on changeover to a backup of correct class upon failure of the PICS.

Action A4.4: EDF/Areva to explain why the functions implemented in the SAS are not Category A (e.g. given implementation of reactor trip via the SAS).

Action A4.5: EDF/Areva to explain why the functions implemented in the RCSL are not Category B (e.g. given implementation of main reactor controls).

Action A4.6: EDF/Areva to explain whether the PAS implements any of the main reactor controls (e.g. reactor coolant temperature, pressuriser pressure/level, steam generator level, feed water and steam dump controls) and if so why Category B (F1B) is not the appropriate categorisation.

Action A4.7: EDF/Areva to explain how it determined that the SA I&C is Category C (F2).

RI-UKEPR-2.A5 - Network Determinism and Response Times

Discussion - Given the complexity of the architecture it appears that network determinism and response times may be an issue, for example to ensure that:-

the time to acquire and display sensor information meets the required response times, and

actuators can be operated within the required actuation times (i.e. including detection of the event requiring the actuation, subsequent information communication and signal and logic processing etc.).

EDF/Areva has not demonstrated that the UK EPR C&I design satisfies the following HSE SAPs; ESS.2 (FA9), ESS.5, ESR.2, ESR.3 and ESR.9.

Action A5: EDF/Areva to demonstrate that safety/safety related network communications are deterministic and the required response times are achievable (see examples in discussion above).

** NB. The references in brackets following identification of the SAPs in the above text are to Observations in HSE's Step 2 Report on EPR C&I."*

Letter Table 1

System	Technology	Functional Safety Category EDF and AREVA	Safety Category ND – Based on BS IEC 61226	Comments
Safety Information and Control System (SICS)	Mostly Hardwired but interface to PS is via PI/MSI/PS datalink.	F1B (B)	A	Requires clarification. - Need for Manual reactor trip/ESFAS actuation implies SICS should be Category A. SICS required to achieve and maintain safe state. SICS required to cover failure of PICS. to clarify why the SICS is not F1A. EDF/Areva to clarify SICS operational state when PICS is operational.
Process Information and Control System (PICS)	SPPA-T2000	F2 (C)	B	Requires clarification. - PICS is the main control and operator station in the MCR and RSS, and is required to monitor and control plant in all plant conditions. Normal plant operation is with PICS Class 3 (F2) indications and controls. Changeover to the F1B SICs is required on failure of the PICS. EDF/AREVA argument for C is that B functions are backed up in the SICS. NII believes that Cat B functions should be delivered by operational equipment of the appropriate class NOT by changeover to a backup of correct class. EDF/Areva to review and explain the reasonable practicability of providing plant operation with indications and controls appropriate to the function (e.g. NSSS controls are normally class 1/2 as per Sizewell B and AP1000) which are normally in operation as opposed to relying on changeover to a backup of correct class upon failure of the PICS.
Protection System (PS)	TELEPERM XS	F1A (A)	A	Categorisation agreed.
Priority and Actuator Control System (PACS)	Mostly hardwired	F1A (A)	A	Categorisation agreed.
Safety Automation System (SAS)	SPPA-T2000	F1B (B)	A	Requires clarification. Implementation of diverse reactor trip function leads to Category A categorisation. EDF/Areva to explain why the functions implemented in the SAS are not category A (e.g. given implementation of reactor trip via the SAS).

System	Technology	Functional Safety Category EDF and AREVA	Safety Category ND – Based on BS IEC 61226	Comments
Reactor Control, Surveillance and Limitation System (RCSL)	TELEPERM XS	F2 (C)	B	Requires clarification. - Main Reactor Controls, hence Category B function. EDF/Areva to explain why the functions implemented in the RCSL are not Category B (e.g. given implementation of main reactor controls).
Process Automation System (PAS)	SPPA-T2000	F2 (C)	B/C	Requires clarification. EDF/Areva to explain whether the PAS implements any of the main reactor controls and if so why Category B (F1B) is not the appropriate categorisation.
Severe Accident I&C (SA I&C)	TELEPERM XS	F2 (C)	B/C	Requires clarification. EDF/Areva to explain how it determined that the SA I&C is F2.

Letter References

1. IAEA safety guide NS-G-1.1 IAEA Safety Standards Series, Safety Guide No.NS-G-1.1 - Software for Computer Based Systems Important to Safety in Nuclear Power Plants. (2000).

2. IEC 61226:2005. Nuclear power plants - Instrumentation and control systems important to safety – Classification of instrumentation and control functions.

3. Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorised technical support organisations. Revision 2007

4. HSE T/TAST/046 Computer based safety systems.

5. Technical Guidelines for the design and construction of the next generation of nuclear pressurized water plant units" adopted during plenary meetings of the GPR and German experts on the 19 and 26 October 2000.

6. The Tolerability of Risk From Nuclear Power Stations (HSE 1992) ISBN 0-11-886368-1.

7. The use of computers in safety-critical applications – Final report of the study group on the safety of operational computers – (HSC 1998) ISBN 0 7176 1620 7.

Annex 3 – Safety Assessment Principle Argumentation Review - TSC's Main Findings and SAP Summary Review

This annex reproduces below the main findings and SAP summary review from the TSC report "NII GDA Technical Review – C&I SAP Compliance Assessment for EDF / AREVA UKEPR – 36331/35856R, Issue 1.6", Ref. 13.

Main findings

"*The majority of SAP assessments resulted in Technical Queries (TQs) being raised. A total of 103 questions were raised in 50 TQs. The key issues identified are listed below, by topic area:*

Safety Categorisation, Classification and Standards

- *The UKEPR 4 levels of Categorisation and Classification (F1A, F1B, F2 and NC) does not readily align with SAP or IEC61226 requirements (A, B, C/1, 2, 3).*
- *EDF/Areva only claim to apply 11 of the 51 IEC Standards listed in BS NCE8 without justification for the omissions.*

Defence in Depth

- *The C&I Systems Safety Function allocation conforms to the defence in depth concept, aligning with the 5 levels referred to in IAEA Safety Standard NS-R-1. However, the levels of Defence-in-Depth within the C&I system functional allocation relies on two digital platforms TXS and SPPA-T2000, therefore a failure of one digital platform due to CCF may result in the loss of more than one level of defence.*
- *C&I systems in 4 trains, in 4 separate divisions and 4 Safeguard Buildings provides redundancy and segregation, particularly for PS, but the level of redundancy within the PAS and SAS is not as clearly demonstrated, apart from redundant component within the SPPA-T2000 Automation System AS620B.*
- *Diversity, both functional and equipment, has been addressed between the two digital C&I platforms Teleperm XS (used for the PS, PACS and RCSL) and SPPA-T2000 (used for PICS, PAS and SAS) at a high level but assessment of SAP ESS.18, Failure Independence, highlights that there is insufficient clarity about communication between PS and other C&I systems. It is necessary to demonstrate that faults in these other systems will not impact on the PS safety function and that the flow is only outwards from the PS.*

Reliability Claims/Maintenance, Inspection and Testing

- *Reliability claims for C&I systems are not well addressed within the PCSR although use of a Compact Failure Model in the Probabilistic Safety Assessment (PSA) Chapter 15 of the PCSR gives 1E-05 pfd and 1E-04 pfd for the common 'Processing (non-specific)' parts of the F1A and non-F1A systems respectively. This level of reliability is beyond the TAG046 limit for computer based safety systems and insufficient justification is provided in the PCSR.*
- *F2 systems in continuous operation are considered proven without need for functional testing but justification of acceptability of this is not provided.*

Failure to Safety

- *Incorporation of defences to meet the Single Failure Criterion (SFC) and Common Cause Failure (CCF) through redundancy and segregation is well addressed but a fail-safe approach is not well covered.*

Safety Systems

- *Only the PS and PACS are F1A classified systems; the safety systems for each fault initiator, automatic and manual initiation and required reliabilities needs clarification.*

Computer Based Systems Important to Safety

- *There is a shortfall in independent 'confidence-building' regarding independent and diverse checking of validated software, and no claim to testing the 'design and production' process nor independent assessment of the test programme.*

General

- *There are no references within the PCSR to documents that support SAP compliance.*

Based on the SAPs assessed it is considered that overall there is currently insufficient CAE structure in the PCSR to clearly demonstrate how C&I systems address the SAPs. Of particular note, the PCSR PSA gives 1E-05 pfd and 1E-04 pfd for the common 'Processing (non-specific)' parts of the F1A and non-F1A systems respectively. These reliability claims are beyond the TAG046 limits for computer based safety systems and insufficient justification of these levels is provided in the PCSR.

In addition, it was found that the PCSR rarely made any direct reference out to supporting evidence to back up any claim or argument presented. Although much detail was provided in the PCSR this was sometimes duplicated and disjointed making Claim, Argument, Evidence assessment difficult."

SAP Summary Review

The table below is a reproduction of Table 1 "Findings and Observations Summary" from the TSC report Ref. 13.

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
General	*The PCSR does not reference out to any supporting documentation to provide Evidence in support of the Claims and Arguments made.* *<u>Response to TQ-EPR-313</u>* *The response simply states that the references to supporting documentation have been added to the June 2009 PCSR. The adequacy of this change will be assessed during future assessments against the June 2009 PCSR.*	*TQ-EPR-313*	*General comment – not an assessment of argument.*
ECS.1 *Safety Categorisation*	*A methodology for the categorisation (classification) of functions based on significance regards to safety exists but it is still unclear how the 4 levels of categorisation and classification (F1A, F1B, F2 and NF/NC) align with the Cat A, B and C and Class 1, 2 and 3.* *The PCSR does not readily demonstrate how the Categorisation methodology for C&I systems takes into account the requirements of ECS.1 paragraph 150 a) to d).*	*TQ-EPR-331*	***P***
ECS.2 *Safety Classification of SSC*	*It is concluded that:* *There is a scheme for the classification of C&I systems and equipment that is linked to the functional classification but other elements required to be addressed by this SAP are less obviously covered.* *The extent of Auxiliary services supporting C&I systems that can be considered as part of that system are not clearly addressed neither is their classification.*	*TQ-EPR-342*	***P***
ECS.3 *Standards*	*A review of the list of IEC standards applied to the UK EPR, supplied by EDF/AREVA June 2009 in response to 2-C&I-3 (Ref ND(NII) EPR00111N), against the BS NCE 8 document 'Nuclear Power Plants - I&C Systems, A Guide to Applicable IEC Standards' identified a significant amount of omissions. From the TATS action list, action 7-I&C-11states: 'EDF/AREVA to review the list provided through action 2-I&C-3 with the list of International standard and to indicate reasons for omission (if any)'; the status of this is reported as 'in progress' with no visibility of this review and reasons for omission. Clarification has been requested by TQ.* *C&I systems are required to perform multiple safety functions, as in the protection system where PCSR Appendix 7B Section 2.2 lists the F1A, F2B, F2 and NC functions at Sections 2.2.1, 2.2.2, 2.2.3 and 2.2.4 respectively. It is not*	*TQ-EPR-365* *TQ-EPR-372*	***I***

[1] *Status is: A - Adequate, P- Partially Adequate or I - Inadequate.*

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	clearly demonstrated whether these are delivered independently and although appropriate codes and standards have been claimed, whether these codes and standards have been used appropriately in relation to the safety function category. TQ raised. *There are no instances of combination of different codes or standards for a single aspect identified within the PCSR. TQ raised.*		
EDR.1 *Failure to Safety*	*The PCSR implies an FMEA study has yet to be carried out and reported.* *It is considered that failure modes have been addressed within the PCSR and mitigation has been presented for CCF and SFC in the design of C&I systems and these have been copiously discussed in the Design Basis Assessment and the Probabilistic Safety Assessment.* *However, 'inherent safety' or 'fail in a safe manner' does not appear to have been specifically addressed within the PCSR.* *<u>Response to TQ-EPR-310</u>* *The response highlights that FMEAs are to be provided to HSE and have been provided for SPPA-T2000 based systems. These need to be referenced in the PCSR at update. The documents themselves will form evidence for future assessment during Step 4.* *In relation to fail-safe approach, the response points to letter ND(NII) EPR00150N that refers to document 'NLE-F DC 33 Protection System – Concept for I&C Failure Handling' and 'NLTC-G/2008/en/0079, Teleperm XS Self-Monitoring and Fail-Safe Behaviour'. The latter describes the self-monitoring features implemented in the TXS and the exception-handler that ensures fail-safe behaviour of the TXS computers. As none of this is referenced or discussed in the PCSR there is no change to the current assessment. The documents quoted are noted and shall be used as evidence in future assessment.*	*TQ-EPR-310*	***P***
EDR.2 *Redundancy, Diversity and Segregation*	*<u>Redundancy</u>* *It has been concluded that:* *Strengths:* *The design of the Protection System has led to a 4 division architecture and it is considered that the principle of Redundancy has been addressed for the Protection Systems.* *Redundancy in the design of the PICS has been well covered within the PCSR and it is considered that the PICS has been sufficiently designed to take account of the requirements for*	*TQ-EPR-311*	***A***

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	Redundancy. *The correct level of redundancy for the RCSL System has been demonstrated to fulfil its F2 and NC functions.*		
	Areas for Improvement: *Redundancy with respect to the SAS and PAS appears to be weakly addressed within the PCSR and as such it is considered that the PCSR does not provide a strong demonstration of Redundancy for the SAS and PAS.* *Although implicit claims are made there does not appear to be any argument within the PCSR discussing how redundancy or SFC has been applied to the SICS or to the PACS to enable testing.*		***P***
	<u>Diversity</u> *It has been concluded that:* *The incorporation of diversity (both Functional and Equipment) appears to be addressed at a high level within the PCSR and much claim is made on the full diversity of the two platforms; TELEPERM XS and SPPA-T2000. The detailed analysis of the architecture and components used should identify if these high level arguments on diversity can be sufficiently demonstrated.* *<u>Segregation</u>* *It has been concluded that:* *The PCSR provides a sufficient level of argument to demonstrate that the EPR C&I design takes full account of the need for Segregation/Separation and this is provided in the four separate divisions in dedicated rooms around the MCR. It is considered that adequate argumentation on the Segregation requirements of EDR.2 has been provided.*		
	<u>Demonstration that Required Reliability Levels have been Achieved</u> *It has been concluded that:* *The reliability goals for the protection action stated above are beyond the limits specified in TAG 046 as applied in the UK and are, therefore, unlikely to be acceptable. Apart from the above, the PCSR does not appear to provide any substantiation of required level of reliability and hence it has not been possible to find demonstration within the PCSR that this reliability target has been achieved. It is believed that the document promised in response to Step 2 Observation O5.1 has yet to be received. It is considered that compliance with the requirements of para 170 to SAP*		

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	EDR.2 has not been adequately demonstrated. *<u>Response to TQ-EPR-311</u>* *D01. The response points to PCSR Appendix 7C Section 3.3.4 which has been assessed and refers specifically to the AS620 system associated with the SPPA-T2000 platform used by the SAS and PAS. Following a review of this and accepting that this is the basic building blocks of the SAS and PAS, and closer scrutiny of the applicable figures; 17, 19, 22 and 20, it is considered that this issue has been addressed.* *D02. The response point to PCSR Chapter 7.3 Section 3.0.2.1.2 and quotes 'insert the contents'. This section was addressed during the assessment and found to provide a claim that does not appear to have any substantiation; hence the TQ raised. The response has pointed back to a claim already found but does not provided any reference to demonstrate how this claim is met. This TQ has not been satisfied.* *D03. The response refers to the reliability claims presented in the PSA and detailed reliability analysis, and PCSR Chapter 15. Chapter 15 has 8 sub-chapters, so this reference is not very specific. Reference out to the PSA and 'detailed analysis' should be made in the PCSR; the PSA is already listed as an expected evidence document for detailed assessment. Table 2 in Chapter 15.1 does give reliability data for equipment and Section 3.4 gives 'unavailability' values for the C&I systems. It is still considered that the PCSR does not provide sufficient demonstration, or reference to appropriate demonstration, that required reliabilities of structures, systems or components important to safety have been achieved.*		
EDR.3 *Common Cause Failure*	*<u>Addressing Common Cause Failure</u>* *Many of the arguments for how CCF has been addressed are covered under EDR.2 relating to Diversity and Segregation. The conclusion of this assessment was that these elements of the design had been addressed at a high level in relation to the SAP requirements. In addressing Common Cause Failure, the use of diversity (Functional and Equipment) and segregation has been sufficiently argumented in support of SAP EDR.3.* *<u>Common Cause Failure Reliability Claims</u>* *The RP's response to Observation O8.2 from Step 2 was:* *The basis for the functional reliability claims of the 2*	*TQ-EPR-314*	***P***

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	independent processing systems used in EPR will be presented in a further document which will be provided to NII in November 2008. *It is not clear what this document is or whether it has been received.* *The most current comment in the TATS is:* *EDF/AREVA to provide an action plan to justify the claims on reliability by July 2009.* *Note that EDF/AREVA position regarding standard IEC 61508 was sent by letter UKEPR000083R on 20/02/2009.* *It is considered that the CCF claims have been presented within the PSA discussion at Chapter 15 of the PCSR but the detailed substantiation has not been presented or referenced to as evidence.* *Analysis of PCSR Chapter 15.7 Table 6 shows that the majority of events have a pfd of 1E-04 with only the highest ranking RIF event with a 1E-05 pfd. There are, however, a number of events with a pfd of the order of 1E-06. All of these relate to CCF between groups of sensors of 4 SGs. These all relate to an equipment class of E1A.* *CCF claims presented in the PCSR at Chapter 15 for the computer based systems TXS and SPPA-T2000 are 1E-05 and 1E-04 respectively for the Processing (Non-specific), the former being beyond the TAG046 limit and the latter unrealistically on the limit where this is standard commercial equipment. Additionally, the reliability claims for combined failure of C&I systems have not been addressed within the PCSR, but a combined pfd of 1E-09 by multiplication is considered an unrealistic target.* *Non-achievement of required reliabilities does not appear to be presented in the PCSR, and therefore the existence or not of such non-achievement is non-determinable. A TQ has been raised requesting clarification of any reliabilities that cannot be achieved and the associated 2 independent safety measures applied.* *<u>Response to TQ-EPR-314</u>* *In relation to substantiation of CCF reliability claims, the response cites the response under letter ND(NII) 00108R and lists:* • *ECECC050092 – "Justification of diversity between SPPA T2000 and TXS"* • *HP1A 2007 03 803 AN 1.0 – "CCF Analysis of FA3 C&I architecture"* • *ECECC08669B "Defence in depth principle"*		

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	• *ECEEE08586 "Justification of the independence of C&I systems based on SPPA T2000 platforms"* ***The first 2 sent under EPR00127N, the last 2 sent under EPR00145N. The TQ asked where this was covered within the PCSR. From the response it clearly is not. The documents quoted are noted.*** ***In relation to reliabilities that cannot be achieved, the response refers to substantiation of claims on reliability provided in framework of RI02 and list:*** • *TXS FMEA* • *QU633 v5.0 Self coverage test analysis* • *NLTC-G 2008 en 0079 revB – "TXS Self-monitoring and fall-safe behaviour"* *(above sent with letter EPR00127N on 30 June 2009)* • *SIE QU626 "Module reliability - FMEA SPPA / T2000"* • *SIE QU627 " PICS, SAS, and PAS system reliability"* *(above sent with letter EPR00145N on 31 July 2009)* ***This does not identify where/if any required reliabilities cannot be achieved and does not refer to this being addressed within the PCSR or any reference from the PCSR to the documents quoted. The quoted references are noted for future assessment of evidence. The current assessment is unchanged.***		
EDR.4 *Single Failure Criterion*	***<u>Application of the Single Failure Criterion</u>*** ***With the previous assessment of redundancy in design for SAP EDR.2 and the accident analysis of active and passive Single Failures captured within the PCSR at Chapter 14 and associated Sub-Chapters, it is considered that the application of the Single Failure Criterion has been adequately demonstrated and this requirement of SAP EDR.4 has been well argumented.*** ***<u>Consideration of Consequential Failures in Applying SFC</u>*** ***With no apparent discussion on Consequential Failures within the PCSR it is hard to identify how or where Consequential Failures have been considered when applying the Single Failure Criterion. Despite EDF/Areva response to Step 2 stating that clarification would be given in the Step 3 PCSR submission, this does not appear to have happened.***	*TQ-EPR-315*	***P***
EES.1 *Provision (of Essential Services)*	***The claims are not clear from the PCSR, there is little obvious interpretation in relation to the I&C systems. It is suggested that the EPR essential services relevant to I&C safety and safety related systems are listed and a summary is provided of how these are supported during normal and fault conditions. Furthermore the tolerance of I&C systems***	*TQ-EPR-328*	***P***

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	to power interruptions and transients should be covered. *The use of relevant IAEA, IEC or any other standards during the design needs to be demonstrated. Evidence is also required to support the intent of the SAP i.e. the documents providing evidence of I&C design in relation to essential services (e.g. I&C system / design specification).*		
EES.2 *Sources External to the Site*	*The claim made by the RP generally supports the SAP intent i.e. that there is a back-up source of electrical power on-site following loss of off-site power to support the I&C Safety Systems. However, clarification is required regarding the extent of coverage by the Diesel Generators, i.e. are Safety Related Systems also included in the stand-by power arrangements. The continuity of power during switch-over from grid to DGs is ensured by an uninterruptible power supply that uses battery power for up to 2 hours.* *It is concluded that evidence is required to support the RP claims, e.g. relevant industry standards and/or an I&C system requirements specification / design documentation.*	*TQ-EPR-363*	***P***
EES.8 *Sources External to the Site*	*From a review of the PCSR, an external grid power supply is available, however, it is found that the EPR I&C does not rely on this for electrical essential services (i.e. back-up on-site power is available).* *The RP should provide supporting documentation e.g. I&C system requirements specification / design documents that demonstrates that the EPR I&C systems do not rely on an external electrical source of power.*	*TQ-EPR-329*	***P***
EES.9 *Loss of Services*	*The claim made by the RP appears to be adequate with respect to the SAP, although it is assumed that the SBO/ultimate emergency diesel generators will be available and that they can be manually started within 1.5 hours, although, there is no specific wording in the claim for the reliance on the SBO/ultimate emergency diesel generators.* *It is recommended that the RP should provide as evidence;* *1) 'Emergency Operating Procedures' and 'additional mitigation features' relevant to the I&C systems.* *2) The I&C system requirements specification to demonstrate that in the event of LOOP and EDGs, that the provision of UPS and ultimate diesels allows the Safety Systems and Safety-Related Systems to function adequately.*	*TQ-EPR-376*	***P***
EHA.10 *Electromagnetic Interference*	*There does not appear to be any claims or arguments in the PCSR of an assessment of on or off site sources of EMI. The only detailed assessment made is in relation to lightening strike covered in detail in PCSR Chapter 13.1 Section 7.* *The only link to design standards for EMI is given in PCSR Appendix 7A Section 3.3.1 that states:*	*TQ-EPR-316*	***P***

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	The hardware equipment has to be qualified following standard IEC 60780 for the general qualification process, applicable parts of IEC 60068 for applicable climatic and mechanical tests, ***applicable parts of IEC 61000 for the Electro Magnetic Compatibility (EMC)*** *and IEC 60980 for earthquake specific qualification process.* *A detailed discussion on the design requirements to protect against lightening strike is provided at Chapter 13.1 Section 7 and addresses such issues as earthing, civil structure meshing, grounding and screening etc.* *From assessment of the C&I System sections of the PCSR it is considered that the design of the EPR C&I equipment cabinets, cabinet rooms and cabling has taken account of protection requirements against electromagnetic interference.* *Response to TQ-EPR-316* *The response provided is:* *'The electromagnetic interference is taken into account into the qualification programs of the Teleperm XS and SPPA-T2000. The documents NLZ-F DC 3 (for the TXS) and NLF-F DC 14 (for SPPA-T2000) describe all the qualification requirements applicable including EMI. These two documents have been sent to HSE on 12 January 2009 by letter EPR00057N.'* *There is no reference to this being addressed in the PCSR specifically. Ideally, reference to NLZ-F DC 3 and NLF-F DC 14 should be made in the PCSR; this may be the case in the June 2009 issue. These two documents are noted and will be assessed as evidence during future assessment. Current assessment remains unchanged.*		
EHF.7 *User Interfaces*	*It is concluded that there is sufficient Claim and Argument that the PICS and SICS are considered to provide the controls, indications, recording instrumentation and alarms required to operate and control the plant in all normal and accident situations, including severe accidents. Provision is also made local-to-plant for maintenance activities as required.*	*NONE*	***A***
EKP.3 *Defence in Depth*	*At the Key Principle level it is considered that the C&I systems have safety function allocation that conforms to the Defence in Depth concept and that the EPR design appears to align with the 5 levels referred to in IAEA Safety Standard NS-R-1. However, the role of C&I in Emergency response is not clearly identified within the PCSR.* *The levels of Defence-in-Depth within the C&I system functional allocation relies on only two digital platforms TXS and SPPA-T2000, therefore a failure of one digital platform*	*TQ-EPR-317*	***P***

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	due to CCF may result in the loss of more than one level.		
EKP.5 *Safety Measures*	*At the Key Principle level, the safety functions of the Protection System and the safeguard systems it initiates have been identified within the PCSR.* *'Manual activation of certain engineered safeguards' is not adequately explained within the PCSR. However, it is implied within the PCSR that manual activation of safeguards is a post accident F1B function that takes place following automatic activation.* *The reliability and availability of safety actions has not been determined within the PCSR to meet the PSA targets. Hence, demonstration that they are commensurate with the significance of the radiological hazard to be controlled has not been provided in the PCSR.*	*TQ-EPR-323*	***P***
ELO.1 *Access*	*Four different levels of lighting support, combined with the access and habitability claims, ensure that adequate argument is provided to address sub paragraph 205a.* *Despite the lack of claims in relation to C&I Systems, PCSR Chapter 12.3 provides discussion on radiation monitoring of controlled areas where certain items of equipment (sensors, actuators, valves etc.) that may require access are situated. Clarification of C&I system design to minimise/remove radiation dose during operation and maintenance of these systems has been requested by TQ.* *Space requirements relating to electronic equipment making up the cabinet assemblies ensure that there would be sufficient access to preclude adverse interaction with other systems or components.* *Access to alternative means of controlling functions essential to safety is provided by alternate locations (RSS, Local Control Stations etc.) and alternative control systems (PICS for normal control, SICS for alternative control). Access to these alternative locations appears to be separate from each other such that loss of access to the MCR does not prevent access to the RSS. It is considered that sub paragraph 205d is met in principle.* *It is considered that suitable and sufficient means of normal and emergency lighting to enable safe escape has been considered in the EPR design in relation to control rooms associated with C&I.*	*TQ-EPR-370*	***P***
ELO.2 *Unauthorised Access*	*Although EDF/Areva make no claim that the UKEPR complies with this SAP in UKEPR-0005-001 Issue 00, from assessment of relevant sections of the PCSR it is concluded that adequate controls are in place to prevent unauthorised access to or interference with C&I systems important to safety.*	*NONE*	***A***

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
EMT.1 *Identification of Requirements*	*It is concluded that the safety requirement is implicitly identified for testing as fault detection and assurance of continued safety function provision. The required frequencies for such testing and maintenance activity do not appear to have been specifically identified within the PCSR as required by the SAP.*	*TQ-EPR-324*	***P***
EMT.3 *Type-testing*	*It is concluded that:* *The requirement for Type Testing as part of the qualification process is identified within the PCSR.* *There is no further detail within the PCSR as to the extent of the type testing on the C&I systems to assess whether they meet the 'conditions equal to, at least, the most severe expected in all modes of normal operational service' required by this SAP.*	*TQ-EPR-325*	***P***
EMT.6 *Reliability Claims*	*There is sufficient argument that provision has been made within the design of the C&I systems for Periodic Testing, Maintenance and monitoring with little mention of Inspection, which is probably not as relevant to C&I systems, but at a relatively high level. However, it has not been clearly demonstrated within the PCSR why it is acceptable not to test F2 systems that are in continuous operation to ensure they continue to operate within specification and meet the design intent. [see also EMT.7]* *It has not been possible to identify any claim that testing/maintenance requirements cannot be provided where required for C&I systems commensurate with their reliability and classification. (para 190)* *The PCSR makes no real claim to the test equipment, or other means, utilised in the testing, maintenance, monitoring and inspection of C&I systems and equipment. The only item identified was the Service Unit within the PS as part of the Teleperm XS platform; there is no discussion on specifically what the SU does to detect faults and therefore there is no justification as to the extent to which it reveals failures affecting safety functions. (para 191)* *There are no claims or discussion in relation to the testing of the SU or the test intervals that could be assessed against the PS reliability claims. (para 191)* *The PCSR makes no reference to external documentation where the detail of specific tests and maintenance, test equipment justification or test equipment testing intervals may be found.* *<u>Response to TQ-EPR-307</u>* *The response to this TQ highlights that no external test equipment is used with the C&I systems and testing is internal self testing and periodic testing; this being covered*	*TQ-EPR-307* *TQ-EPR-371*	***P***

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	within the PCSR. The response also refers to 3 reference documents to support arguments on self and periodic testing that should be referenced from within the PCSR but currently are not. Therefore, although the references exist, there is still no auditable trail to demonstrate SAP compliance through the PCSR. Existence of these documents is noted.		
EMT.7 Functional Testing	It is concluded that the PCSR provides adequate discussion on the requirement for periodic testing of the safety functions of F1A and F1B C&I systems and F2 C&I systems not in continuous operation, from sensor through to actuator. However, for F2 C&I systems in continuous operation it is claimed that no testing is required but there is no justification as to why this is acceptable, to which systems this applies and how it is demonstrated that such systems continue to operate within specification and to design intent The requirement for conduct of maintenance and testing during operation is addressed by either use of continuous self test/monitoring or a 4 train redundant architecture allowing reduction to 2 out of 3 logic for maintenance activity.	TQ-EPR-466	**P**
EQU.1 Qualification Procedures	There is no discussion on the existence of 'Qualification Procedures' that implement the process/requirements discussed in Chapter 7.2 and Appendix 7A of the PCSR. However, the detailed discussion on the Qualification Plan and Qualification Programme provides sufficient argumentation of the existence of a detailed process that could constitute a 'Procedure' Although the general process and requirements are covered and illustrated in Chapter 7.2 Figures 9 and 10, there is no reference to Qualification Procedures, what they are and what they include. However, from the generic process and requirements discussed in Section 3 it is assessed that the required safety function performance should be confirmed for the operational life if implemented through procedure. <u>Response to TQ-EPR-308</u> The response refers to references now included in the June 2009 PCSR and the Technical Sheets. They are essentially System Quality Plans, V&V Quality Plans and TXS Cabinet Qualification Programme. It is considered that these would form suitable evidence to check the qualification process is correctly implemented during the Step 4 work package. On the basis of this the argumentation is amended to 'Adequate'.	TQ-EPR-308	**P** Amended to **A** following TQ response

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
ERC.2 Shutdown Systems	It is considered that the F1A trip function (RT, SIS, EBS) actuation by the PS and the RRC-A accident mitigation F2 trip functions provided by the SAS/PAS provides for at least two diverse (Functional and Equipment) C&I systems to shutdown the reactor. It is considered that C&I system provision for the initiation of RT, SIS and EBS to shut down the reactor via the PS and SAS/PAS provides sufficient argument to suggest C&I systems contribute to the maintenance of a suitable and sufficient shutdown margin.		A
ERL.2 Measures to Achieve Reliability	The claimed reliabilities of C&I systems based on a Compact Failure Model are presented in the PCSR at Chapter 15. However, the measures to achieve claimed reliabilities in practice are not clearly stated in the PCSR as required by this SAP, although the use of redundancy and segregation can be seen as general methods of achieving this. There is also no evidence of the existence of a reliability analysis of random and systematic failures of C&I systems.	TQ-EPR-326	I
ERL.3 Engineered Safety Measures	The claims identified in PCSR Chapter 7 partially satisfy the SAP requirement in that the Protection System provides the automatic initiation that is rapid (within 30 minutes of an IEF) and reliable. However there is found to be no supporting argumentation in the PCSR, i.e. an explanation of what responses require reliable and rapid protective actions and how the PS supports these criteria and any reference to evidence documentation. Although automatic initiation of engineered safety features is preferable the PCSR does not appear to provide justification of operator actions where deemed acceptable	TQ-EPR-476	P
ERL.4 Margins of Conservatism	There does not appear to be any claims within the PCSR that multiple safety-related systems and/or other means are used to reduce fault sequence frequency. It therefore follows that there is no identified demonstration that any reduction in fault sequence frequency that might exist has a margin of conservatism or how this is achieved. The PCSR does not readily differentiate between C&I Safety Systems and C&I Safety-Related Systems. Without an understanding of which safety-related systems reduce which fault sequence frequencies it is not possible to assess the use of the four issues, in paragraph 181 to SAP ERL.4, in ensuring conservatism. It is acknowledged that common cause failure has been considered in the design of C&I systems and has been assessed under SAPs EDR2, EDR3 and EDR4, but was not in relation to fault sequence frequency reduction. <u>Response to TQ-EPR-309</u> The response provides detail on the use of RRC-A multiple fault sequence mitigation features addressed in the PSA	TQ-EPR-309	I Amended to P following TQ response

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	and covered in the PCSR in Chapter 16.1. A table is provided detailing the core damage frequency reduction with the RRC-A feature; this being generally a factor of 100. This could be considered to be a conservative margin, particularly as frequencies are in the 10E-6 to 10E-9 range. Despite this, claims and arguments relating to ERL.4 are not clearly brought out. On the basis of this the argumentation is amended to 'Partially Adequate'.		
ESR.1 Provision in Control Rooms and Other Locations (C&I)	It is concluded that the claims found in the PCSR partially address the SAP intent. The PICS is identified as providing I&C in the MCR and RSS, the SICS is in the MCR. However, the PCSR needs to include, or refer to, any I&C safety-related systems used at other locations. The PCSR needs to explain why the identified systems are 'suitable and sufficient'. There is also no claim regarding 'indicating and recording instrumentation'. It is also concluded that evidence of design compliance with appropriate international standards is required to support the RP claims.	TQ-EPR-364	P
ESR.3 Provision of Controls	The claims found in the PCSR only partly address the SAP requirements. No explicit claim regarding the adequacy, reliability or ability of the I&C systems to control variables within a specified range has been identified. It is concluded that argumentation and supporting evidence is also required to demonstrate that the I&C systems are able to reliably control the plant, for example an I&C requirements specification document for the plant control. Supporting documents could also include reliability/availability considerations.	TQ-EPR-330	P
ESR.4 Minimum Operational Equipment	There is a lack of a credible claim in the PCSR that relates to the documentation of the minimum I&C equipment. The RP response refers to Technical Specifications for Operation (TSO) documents and a TSO justification document, however, these, or other equivalent documents, are not claimed in the PCSR and are not currently available. It is concluded that evidence of compliance is provided, for example the TSOs and TSO justification documentation, or equivalent documentation, is required.	TQ-EPR-377	I
ESR.5 Standards for Computer Based Equipment	The response made by EDF/AREVA in UKEPR-0005-001 (Issue 00) is unhelpful and does not address the SAP intent. Following a review of the PCSR (including chapters not referred to by EDF/AREVA response) acceptable claims relating to the use of standards were identified. The use of French RFS standards, which are claimed to sometimes extend the current scope of IEC standards, should be explained, and their use for the PS and PACS (PCSR Chapter 7.3) and for PICS and PAS (PCSR Chapter 7.4) should be clarified. Generally it is found that the	TQ-EPR-382	P

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	supporting information is adequate since relevant IEC standards are claimed to be used. *It is concluded that specific evidence (e.g. I&C design documentation) is required to support the RP response that the relevant hardware and software international standards have been used.*		
ESR.7 *Communications Systems*	*The response made by EDF/AREVA does not attempt to demonstrate compliance with the SAP because it is stated that the details of the communications systems will be deferred until the in-service date is nearer, although an explanation of the design principles would be useful. It is concluded that there is no acceptable claim made in the PCSR.* *Providing evidence of the design principles is recommended, for example, an I&C system specification that describes the I&C requirements of the planned communications systems including how they will avoid adverse effects on safety systems and safety-related systems.*	*TQ-EPR-360*	***I***
ESS.1 *Requirement for Safety Systems*	*The RP claims found within the PCSR only partially satisfies the SAP intent, further information needs to be supplied to address the SAP intent, and the step 2 observation (SAP ECS.1) regarding classification of the F1B systems has yet to be resolved. There is found to be no claim in the PCSR relating to the capability of safety systems to shutdown the reactor during normal operations (PCC-1) although the SICS is able to.* *There is a need for evidence relating to I&C systems to support the RP claims e.g. a Safety Schedule or Fault schedule.*	*TQ-EPR-475*	***P***
ESS.2 *Determination of Safety System Requirements*	*It cannot be seen from the PCSR that a distinction has been made between Safety Systems and Safety-Related Systems in relation to C&I. The discussion, therefore, has looked at all classifications across the required functions for Defence in Depth.* *From analysis of the PCSR, it is considered that the C&I system provision to meet required levels of Defence in Depth has been clearly determined and their functions and protection against CCF and SFC through Redundancy, Diversity and Segregation has been supported by adequate argument.* *It is considered that the C&I Safety System required reliabilities have been alluded to as 'unavailability' in Chapter 15. If 'unavailability' is taken as 'failure' then it can be seen from the tables above that for the non-specific processing the PS is claiming 10-5 pfd which is outside the limit required by TAG 046 where 10-4 pfd is stated as the best that can be justifiably claimed for computer based*	*TQ-EPR-312*	***P***

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	safety systems. Clarification of Safety System reliability determination has been requested by TQ (TQ-EPR-312) *<u>Response to TQ-EPR-312</u>* *This response refers to substantiation of claims of reliability for TXS and T2000 being provided under cover of letter ND(NII) 00108R and the detailed UK EPR PSA 'NEPS-F DC 355 B FIN' that provides insights into the modelling of C&I reliability. This is still not covered within the PCSR for C&I systems (Chapter 7) nor are the documents referenced from the PCSR. Assessment of the detailed PSA is out with the scope of Tasks 1 to 3. No change to current assessment.*		
ESS.3 *Monitoring of Plant Safety*	*The RP response in UKEPR-0005-001 (Issue 00) is very high level and does not state the PCSR chapters that provide the claims and supporting argumentation nor to the specific I&C systems intended to support the SAP intent.* *A review of the PCSR has revealed information that there is broad support for the provision of monitoring of plant state. The functional specification in EDF/AREVA documentation supports the argument that operators will be able to take the necessary safety actions.* *The PCSR has been found to contain information supporting claims for compliance with para 338, the PICS and SICS are safety classified and are located to support the MCR. The PICS is available in the RSS as well.* *However, EDF/AREVA need to provide information that provides evidence of the capability of the MCR and RSS, for example design specification documents.*	*TQ-EPR-361*	***P***
ESS.7 *Diversity in the Detection of Fault Sequences*	*It is considered that diversity in the detection of faults has been addressed within the PCSR for the Protection System design, but there is some suggestion that the diverse detection of fault sequences is not always possible, contrary to the requirements of ESS.7. There is no further information to explain this and a TQ has been raised requesting clarification.* *It is considered that diverse initiation of safety systems within the PS, as required by ESS.7, has been addressed within the PCSR for RT (use of Breakers and Contactors) and has been demonstrated within the Protection System for the provision of diverse initiation signals from subsections A and B for the other Engineered Safety Feature Actuation Systems.* *The PCSR, Appendix 7D, discusses diverse ESFAS functions implemented in the PAS and SAS and diverse RT functions*	*TQ-EPR-383* *TQ-EPR-465*	***P***

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	implemented in the PAS (diverse from those implemented in the PS) but it is not clear whether there is diversity in detection of fault sequences and initiation of safety systems within each of these systems. The PSA and SAS, based on AS620B of the SPPA-T2000, have 2 Automation Processors (AP) but these are claimed for redundancy and not diversity as each address the same parameter. TQ raised requesting clarification.		
ESS.8 *Automatic Initiation*	*The SAP requires that all safety system actuations should normally be automatic. The PCSR includes a claim that the Protection System includes automatic and manual functions, it is not clearly stated what these manual functions are or what they achieve. Clarification is required regarding the possible use of manual actions.* *There is judged to be insufficient argumentation relating to the use of automatic and manual actions.* *For SAP guidance paragraph 343:* *'Priority rules' (see PCSR Chapter 7.1) are claimed to be implemented in the I&C design but it is not clear that these satisfy the SAP guidance paragraph 343. More claims are required to address para 343, for example, the provision of interlocks and manual over-rides for the claimed Safety Systems.* *To support the assessment, the following information / evidence is suggested;* *1) Schedule of Safety Systems - to provide information on what systems are initiated via manual and automatic means.* *2) Details of how the choice between Manual / Automatic functions were decided.* *3) Details of any interlocks preventing personnel from overriding Safety Systems.* *4) Details of the operator actions allowed to initiate, override or repair automatic systems.*	*TQ-EPR-357*	***P***
ESS.9 *Time for Human Intervention*	*The information contained in the PCSR is generally consistent with the general requirements of SAP ESS.9, although there are no claims related to I&C aspects (alarms and indications that are necessary).* *Some clarification is required so that the I&C aspects are considered as follows;* • *It would be useful to list all the events requiring manual intervention, including what alarms / indications are provided and what operator actuation needs to be taken and where (e.g. MCR or other locations).* • *Have all the operator actions for Safety System*	*TQ-EPR-384*	***P***

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	operation been justified as not appropriate for automatic initiation (this is covered by the Step 2 assessment). EDF/AREVA provides documented support to the intent of para 344, i.e. that there is at least a 30 minute period before human intervention is necessary, although this is not directly related to I&C assessment. The provision of evidence should include documentation relating to the required human interventions in response to safety system demands that are claimed within the design basis (e.g. details of initiation alarm / signal, where operator action taken, claimed grace period before manual action is required to bring plant into a safe state).		
ESS.10 Definition of Capability	There are no clear claims identified that address the I&C safety system capability (including any sub-systems and components). The PCSR chapters referred to are not directly relevant to I&C although it has been found that PCSR Chapter 7 does provide some information regarding I&C system general functional performance. There is no claim for the requirements for guidance paragraph 345. There needs to be claims and supporting information relating to the provision of defined capabilities for each I&C safety system (e.g. that satisfy the requirements of T/AST/003 Section 6.3.5 ii), the provision of clear design margins for the I&C safety systems including allowance for uncertainties in plant characteristics in accordance with SAP guidance paragraph 345. It is also concluded that there is no evidence that the capability of I&C safety systems has been documented, that the I&C design exceeds the maximum service requirement(s) by a clear margin or that the I&C design performance makes due allowance for uncertainties in plant characteristics including the effects of foreseeable degradation mechanisms.	TQ-EPR-359	P
ESS.11 Demonstration of Adequacy	The RP response relies on conclusions from a DBA and a PSA that the overall consequences of identified fault sequences are within target limits. There is no identified claim that each EPR I&C system achieves the specified function as required by the SAP and safety system reliabilities are not presented. Chapter 14.0 indicates hazards are not included in the DBA and thus does not comply with SAP guidance paragraph 346. It is also concluded that EDF/AREVA needs to provide evidence, in particular a Safety Schedule or Fault and Protection Schedule, evidence that the EPR I&C Safety systems are substantiated as adequate for the faults they are claimed against, and evidence of compliance with the	TQ-EPR-358	P

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	relevant international standards.		
ESS.12 *Prevention of Service Infringement*	*There are no identified claims that directly address the I&C systems and how infringement of any supporting services is prevented. There is a lack of claimed analysis of how there may be infringement of the services, and if there is, if there is a fail-safe outcome.* *There should be an explanation of the means used to prevent infringement of services supporting the I&C safety systems and justification as to the adequacy. EDF/AREVA should also provide an explanation with supporting information that SAP guidance para 348 is satisfied by the EPR design.* *There should be supporting evidence that the prevention of infringement of I&C services has been considered and is demonstrated as adequate and/or that either the possibility of infringement of services is low, or that a fail-safe capability has been considered and is adequate.*	*TQ-EPR-378*	***P***
ESS.15 *Alteration of Configuration, Operational Logic or Associated Data*	*There are no claims that address the SAP intent, no assurance is provided that the I&C safety systems software or hardware configuration is protected from erroneous alteration. For alteration of software there is a claim for the provision of off-line programming, although it is not clear if this is the only method to alter software.* *Supporting evidence should be provided that alteration of the EPR I&C safety system software/hardware settings is adequately prevented through engineered means and/or controlled by strict administrative controls.*	*TQ-EPR-362*	***P***
ESS.16 *No Dependency on External Sources of Energy*	*The PCSR contains adequate claims that the F1 classified I&C systems have an emergency / back-up power source such that during loss of external power the local diesel generators and UPS can provide adequate power for continued operation of the safety classified systems.* *The response provided in the EDF/AREVA comparison document (ref. UKEPR-0005-001, Issue 00) is limited to electrical power sources, also, the EPR PCSR does not include information relating to other sources of energy (e.g. compressed air) that might be required by safety systems following safety system actuation.*	*TQ-EPR-477*	***P***
ESS.18 *Failure Independence*	*It is considered that the protection of C&I Systems (PS, PACS, PAS and SAS) from Internal and External hazards is provided by the 4 redundant trains housed in separate Safeguard and Electrical Buildings and that protection from internal faults is provided by incorporation of the Common Mode Failure and Single Failure Criterion principles.* *The PCSR does not provide sufficient argumentation as to*	*TQ-EPR-327*	***P***

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	the communication flow between the PS and other C&I systems in order to demonstrate that faults in these systems will not impact on the safety function of other systems. There is sufficient argument that physical separation within a safeguard building and provision of 4 diverse divisions within separate safeguard buildings provides protection for the PS, PAS, SAS and PACS from any fault that might jeopardise their safe working. However, it is believed that there is not complete independence of power supplies and other supporting services within a division; i.e. all cabinets fed from the same supply, although separate supplies for separate divisions.		
ESS.19 Dedication to a Single Task	The PCSR does not provide a clear claim for the SAP requirements (including guidance para 353) it is not clear if all the safety systems are claimed to perform a single function. From PCSR Chapter 7.3, the I&C safety systems generally perform several functions and the whole system is safety classified at the level of the highest safety function. The safety systems have functions that are classified at lower levels (e.g. although the PS is F1A, it also implements F1B and F2 functions). No explicit claim can be found regarding other functions jeopardising the safety function. The PCSR does not identify in detail the functions (if any) that are not in support of the safety functions, it is suggested that a more detailed specification of the 'other' functions and evidence of a justification that they do not jeopardise the safety function as required by guidance para 353.	TQ-EPR-379	**P**
ESS.20 Avoidance of Connections to Other Systems	The PCSR contains no clear claim relating to the connection to systems external to plant. Clarification is therefore required that Safety Systems are not connected to other systems external to plant. The PCSR does not contain information that relates to connections between safety systems and other systems external to plant and thus no argumentation was found that provides substantiation that they are limited to monitoring and contain appropriate isolation features. EDF/AREVA do not provide references to the supporting documentation (i.e. the PCSR), examination of the PCSR suggests there are no obvious references to design documents that detail the I&C connections between Safety Systems and other external to plant systems.	TQ-EPR-374	**P**
ESS.21 Reliability	It is so far concluded that the provision of Self and Periodic testing to identify internal faults is addressed. However, there are no apparent claims or argumentation to support	TQ-EPR-405	**P**

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	avoidance of complexity or addressing fail-safe approach in relation to the Protection System.		
ESS.23 Allowance for Unavailability of Equipment	Claims have been identified in the PCSR that cover aspects of unavailability due to testing and maintenance and that the redundancy present in F1 systems assures the required availability. However, the claims need to be clarified in areas relating to availability due to 'non-repairable' or 'unrevealed' failures faults. The PCSR shows argumentation that redundancy in F1 systems allows availability requirements to be met, however, there needs to be reference to the applicable design documents that support this. EDF/AREVA should provide reference to evidence that the EPR documentation adequately controls maintenance and testing, i.e. that plant availability is managed and maintained.	TQ-EPR-375	P
ESS.24 Minimum Operational Equipment Requirements	The EDF/AREVA response that the Technical Specifications (TSOs) provide documentation of the minimum amount of operational safety system equipment is not supported by a claim in the PCSR. EDF/AREVA support the SAP intent by stating in the PCSR that the PS, PACS, SICS and SAS are designed with sufficient redundancy to meet the single failure criterion even during testing/maintenance which is supported by 'accident analyses' in PCSR Chapter 14. However, it is concluded that EDF/AREVA should provide documentation that shows how the I&C availability requirements are satisfied. Observations have been raised to clarify the identified shortfalls.	TQ-EPR-474	A
ESS.27 Computer-based Safety Systems	PCSR section 7 deals with aspects of the I&C computer based life cycle including design, coding, integration/installation/commissioning, validation, operation/maintenance and modifications. Although 'production excellence' and 'confidence-building' measures are not referred to directly it can be seen that most of the elements of 'production excellence' are contained in Chapter 7 of the PCSR, although observations have been raised where clarification is required. For 'confidence building' there are however some identified shortfalls. Guidance para 361 part a) requires independent, preferably diverse, checking of the final production software, it is not clear from the PCSR if this checking will be diverse. Guidance para 361 part b requires the test programme to be independently assessed, however, it is not clear from the PCSR if this is specified. Guidance para 362 requires the understanding and mitigation of weaknesses relating to production excellence / confidence-building' during the production process, no reference to this can be found in the EPR PCSR. The PCSR	TQ-EPR-479	P

SAP	Main Findings / Observations	TQ Reference	Status of Argument[1]
	does not provide references to the supporting documents that demonstrate evidence of compliance.		

Annex 4 – Main Observations of the TSC's Architecture Review

This annex reproduces below the main observations from the "TSC report NII GDA Technical Review – C&I System Architecture Safety Assessment for UK EPR – S.P1440.57.11, Issue 2.0.", Ref. 14. and the relevant results of the June 2009 PCSR impact assessment "NII GDA Technical Review - C&I UK EPR - June 2009 PCSR Impact Assessment – 36331/3593R, Issue 0.3" Ref.17.

C&I System Architecture Safety Assessment for UK EPR, Ref. 14:-

"*The main observations are listed below:*

EPR.7.1. The lack of depth and completeness of the C&I design in the PCSR, and the difficulty in locating information in chapter 7 of the PCSR, has constrained the review to consideration of only the highest priority (priority 'A' in the Compliance Matrix) SAP, TAG and standards clauses. For example, there is an absence of external references to supporting material in the body of PCSR chapter 7.

EPR.7.2. The reliability claims for the Teleperm platform, and for the primary protection system, exceed the claim limit for computer-based systems as defined by nuclear standards and guidelines.

EPR.7.3. The reliability claim for the SPPA-T2000 platform is at the limit for class 1 computer-based systems as defined by nuclear standards and guidelines, but there is no evidence that the platform has been developed to the requisite nuclear safety standards.

EPR.7.4. Nuclear guidance recommends that where diverse safety systems are required, and one is computer based, the second one should be provided using a non-computer based system. This is not the case for the primary and secondary protection systems (PS, SAS/PAS).

EPR.7.5. There are examples of data communication into a class 1 system (especially the primary protection system) from lower classified systems. This does not meet nuclear safety assessment principles and security guidelines.

EPR.7.6. There are examples of systems of different classification that share common resources, such as platform, cabinets, or network. The sufficiency of segregation of such systems (eg. electrical and functional isolation as required), to ensure non-interference with a higher class system by a lower class system, has not been demonstrated.

EPR.7.7. It has not been possible to establish exact alignment of the classification system used within the EPR (F1A, F1B, F2, E1A, E1B, E2) with that defined by IEC 61226 (category A, B and C, and class 1, 2 and 3).

EPR.7.8. There is no clear list in the PCSR of C&I safety requirements and corresponding functions with their categorisation, and their apportionment to the safety systems of the associated safety group. (The PCSR instead lists the C&I systems and the functions they perform). Hence the sufficiency of the classification of several C&I systems could not be determined, (in particular the classification of PICS, SICS, SAS, RCSL, PAS and SA I&C were questioned).

EPR.7.9. Manual and automatic indications and controls that are part of category A safety functions need to be executed by class 1 systems, but this is not the case, eg. SICS and SAS are class F1B, and the RSS plant shutdown equipment is class E2/NC.

EPR.7.10. SICS MMI category A and B controls appear to be required to achieve and maintain the safe state, but these controls are disabled whilst the PICS is operational (although the displays are active). However the PICS is only class F2 and so does not have sufficient classification to carry out these functions instead of the SICS.

EPR.7.11. The classification of networks involved in the execution of category A and B functions could not be found.

EPR.7.12. The use of networks in the execution of category A functions introduces a risk of non-deterministic performance. The adequacy of worst-case performance times for end-to-end category A functions could not be found.

EPR.7.13. There is a risk of a cascaded fault sequence when a single C&I system executes functions at different levels in the defence-in-depth strategy, eg. PAS. Hence system failure would affect multiple defence-in-depth functions.

EPR.7.14. There is a risk of a cascaded fault sequence when a common platform hosts multiple systems that execute functions at different levels in the defence-in-depth strategy, eg. Teleperm XS. Hence platform failure would affect multiple defence-in-depth functions.

EPR.7.15. A common cause failure analysis at the level of the C&I systems that are members of the same safety group could not be found in the PCSR.

EPR.7.16. The analysis of the application of the single failure criterion to each member of each safety group could not be found in the PCSR. Consequently the identification of failure modes and consequences for each C&I safety system could not be established.

EPR.7.17. The rationale for the choice of each manual safety action in preference to an automatic action could not be found.

EPR.7.18. The architecture is overly complex. The systems are highly inter-connected, with complex information flow. Hence independence requirements are difficult to assure, for example absence of communication between the primary and secondary protection systems (whose platforms are connected via gateways)."

The TSC findings described above were raised on the basis of the April 2008 PCSR. Following submission of the June 2009 PCSR an impact assessment Ref. 17 was undertaken and the table below shows the impact of the June 2009 PCSR revision on the above findings.

Impact Assessment of June 2009 PCSR Revision on Architecture Assessment Findings

Identifier	Review Comment	Impact of PCSR Changes
EPR.7.1.	The lack of depth and completeness of the C&I design in the PCSR, and the difficulty in locating information in chapter 7 of the PCSR, has constrained the review to consideration of only the highest priority SAP, TAG and standards clauses. In particular, there is absence of clear argumentation to back up a set of claims that demonstrate an adequate level of safety in the C&I systems, via compliance with the SAPs.	Although lists of references to supporting documents are provided in many of the chapter 7 sub-chapters, the new cross-referencing style of using the anonymous text "[Ref]" is unhelpful in linking the referenced documents to specific sentences in the PCSR. Furthermore, many of the references are at the level of the individual C&I system, rather than at the higher level of C&I requirements, safety functions, and safety groups, covering aspects such as common cause failure and application of the single failure criterion in a systematic way. Finally, the PCSR still does not contain clear argumentation to back up a set of claims that demonstrate an adequate level of safety in the C&I systems.
EPR.7.2.	The reliability claims for the Teleperm platform, and for the primary protection system, exceed the claim limit for computer-based systems as defined by nuclear standards and guidelines.	No change
EPR.7.3.	The reliability claim for the SPPA-T2000 platform is at the limit for class 1 computer-based systems as defined by nuclear standards and guidelines, but there is no evidence that the platform has been developed to the requisite nuclear safety standards.	No change
EPR.7.4.	Nuclear guidance recommends that where diverse safety systems are required, and one is computer based, the second one should be provided using a non-computer based system. This is not the case for the primary and secondary protection systems (PS, SAS/PAS)	No change
EPR.7.5.	There are examples of data communication into a class 1 system (especially the primary protection system) from lower classified systems. This does not meet nuclear safety assessment principles and security guidelines.	No change

Identifier	Review Comment	Impact of PCSR Changes
EPR.7.6.	There are examples of systems of different classification that share common resources, such as platform, cabinets, or network. The sufficiency of segregation of such systems (eg. electrical and functional isolation as required), to ensure non-interference with a higher class system by a lower class system, has not been demonstrated.	No change
EPR.7.7.	It has not been possible to establish exact alignment of the classification system used within the EPR (F1A, F1B, F2, E1A, E1B, E2) with that defined by IEC 61226 (category A, B and C, and class 1, 2 and 3)	No change.
EPR.7.8.	The PCSR does not reference an overall Architecture Requirements Specification for the C&I systems that defines all functional, performance, capacity, safety, security and interfacing requirements that the design of the C&I architecture must meet.	No change. References to system specifications have been added, but no references to requirements specifications could be found.
EPR.7.9.	The PCSR does not contain a list of all C&I safety functions that are each traceable to one or more C&I requirements, together with the justification of their categorisation, and their apportionment to the safety systems of the associated safety groups. (The PCSR instead lists the C&I systems and the functions they perform). Hence the sufficiency of the classification of several C&I systems could not be determined, (in particular the classification of PICS, SICS, SAS, RCSL, PAS and SA I&C were questioned).	No change. References to system specifications have been added, but no list of C&I safety functions traced to requirements, plus apportioned to their safety groups, could be found.
EPR.7.10.	Manual and automatic indications and controls that are part of category A safety functions need to be executed by class 1 systems, but this is not the case, eg. SICS and SAS are class F1B, and the RSS plant shutdown equipment is class E2/NC.	No change.
EPR.7.11	SICS MMI category A and B controls appear to be required to achieve and maintain the safe state, but these controls are disabled whilst the PICS is operational (although the displays are active). However the PICS is only class F2 and so does not have sufficient classification to carry out these functions instead of the SICS.	The dedicated SA I&C panel is located in the SICS. PCSR chapter 7.3 section 3.1 implies that whilst the PICS system is available in the MCR, the SICS is active only for periodic testing and safety monitoring. Therefore the concern remains that the SA I&C panel might not be able to control a severe accident condition without prior explicit activation via the PICS-SICS transfer controls (see section 3.0.2.1.2 of 7.3)

Identifier	Review Comment	Impact of PCSR Changes
EPR.7.12.	The classification of networks involved in the execution of category A and B functions could not be determined.	The classification of the plant network has been downgraded to E2 with the introduction of the SAS Bus. The concern remains that E2 classification may be insufficient, especially if the Protection System for example uses this network for input and/or output of category A or B information from/to the PICS (see section 7.3.1 Tables 1 and 2).
EPR.7.13.	The use of networks in the execution of category A functions introduces a risk of non-deterministic performance. The adequacy of worst-case performance times for end-to-end category A functions could not be determined.	No substantive change, except that the SAS Bus network is used for F1B information transfer between divisions, instead of the Plant Bus.
EPR.7.14.	There is a risk of a cascaded fault sequence when a single C&I system executes functions at different levels in the defence-in-depth strategy, eg. PAS. Hence system failure would affect multiple defence-in-depth functions.	No change in the involvement of PAS both in normal control operation, and in RRC-A mitigation functions. However the split of SAS into two systems that embody the RRC-A and RRC-B functions is an improvement in the architectural structure that strengthens the modularity of the defence-in-depth layers.
EPR.7.15.	There is a risk of a cascaded fault sequence when a common platform hosts multiple systems that execute functions at different levels in the defence-in-depth strategy, eg. Teleperm XS. Hence platform failure would affect multiple defence-in-depth functions.	No change in allocation of functions to platforms.
EPR.7.16	A common cause failure analysis at the level of the C&I systems that are members of the same safety group could not be found in the PCSR.	No change.
EPR.7.17	The analysis of the application of the single failure criterion to each member of each safety group could not be found in the PCSR. Consequently the identification of failure modes and consequences for each C&I safety system could not be established.	No change.
EPR.7.18.	The rationale for the choice of each manual safety action in preference to an automatic action could not be found.	No change.

Identifier	Review Comment	Impact of PCSR Changes
EPR.7.19.	The architecture is overly complex. The systems are highly inter-connected, with complex information flow. Hence independence requirements are difficult to assure, for example absence of communication between the primary and secondary protection systems (whose platforms are connected via gateways).	Small change. The split of SAS into two systems that embody the RRC-A and RRC-B functions, coupled with the definition of the SAS bus for inter-division communication of SAS RRC-A information, is a minor improvement in architectural modularity. However, communication from the SAS into the PS via the inter-platform gateway remains, and is confirmed by section 7.3.1 Table 1 for example.

Annex 5 - Main Observations of the TSC's Diversity Review

This annex reproduces below the main observations from the "NII GDA Technical Review – C&I Diversity Aspects of C&I Category A Functional Systems Design Assessment for UK EPR - S.P1440.57.12, Issue 2.0.", Ref. 15.

"*The main observations are listed below … :*

EPR.8.1 Diversity-related information in PCSR chapter 7 is not captured together in one section, which makes it difficult to analyse all aspects of diversity for the primary and secondary protection systems (including program development, verification, execution platform, functional, equipment usage, physical separation, and maintenance). The inability to find key supporting evidence has hindered the provision of a positive assessment of sufficient diversity.

EPR.8.2 Nuclear guidance recommends that dependence on reliability claims of 1E-8 or lower should be avoided due to the difficulty in demonstration. This guidance is also supported by the findings of the scientific community, eg. [8,15]. The reliability claim for the primary and secondary protection systems taken together (within the same safety group) may be required to have a pfd of 1E-8 or lower for some Postulated Initiating Events, using the product of the PS reliability claim (1E-5 pfd) and the SAS/PAS reliability claim (1E-4 pfd). Furthermore, these reliability claims exceed the claim limits for class 1&2 computer-based systems as defined by nuclear standards and guidelines and show no margin of conservatism. Finally, the Sensitivity Study carried out by EDF/Areva [13] has shown that it is unlikely that there is any scope for adjusting the claimed reliabilities to more demonstrable values without significantly increasing risk estimates to levels which are close to, or in excess of, the Basic Safety Objectives.

EPR.8.3. Nuclear guidance recommends that where diverse safety systems are required, and one is computer based, the second one should be provided using a non-computer based system. This is not the case for the primary and secondary protection systems.

EPR.8.4. The two platforms Teleperm XS and SPPA-T2000 (previously known as Teleperm XP) appear to have potential common ancestry within the Siemens organisation. Their program development and execution models are also similar, based on the use of auto code-generation from function block diagrams, and supported by a library of runtime functions. Therefore the sufficiency of the claim of full diversity between these platforms (both in terms of development and in terms of execution) could not be established.

EPR.8.5. The determination of absence of common cause failure between diverse members of the same safety group, across the entire lifecycle, could not be established, since no common cause failure analysis at the level of the C&I systems could be found. This determination includes CCF between the following pairs: (a) part A and part B of PS; (b) SAS and PAS; (c) PS (as a whole system) and SAS/PAS (considered as a whole system). This also includes any CCF within the entire function execution paths (from sensing the plant status to the actuation of the plant safety systems). Finally, this also includes any CCFs from the use of a common platform to develop or execute these systems.

EPR.8.6. Absence of communication between the primary and secondary protection systems (which are connected via gateway-linked networks) could not be established. Any such communication (intended or unintended) could defeat the independence claim between these systems.

EPR.8.7. The precise mechanism used for activating the secondary protection system as a backup for the case of primary protection system failure could not be found. In particular, the independence of any such mechanism from the (failed) primary protection system would need to be established.

EPR.8.8. Whilst PS is claimed to incorporate internal functional diversity between parts A and B, it could not be established whether there exists any internal functional diversity within the backup safety functions carried out by SAS and PAS. Such diversity would be required to meet the reliability claim of 1E-4 pfd for the secondary protection system.

EPR.8.9 The classification of both SAS and PAS systems is not class 1, but they provide backup for category A PS functions.

EPR.8.10 The Postulated Initiating Event (PIE) that each safety function mitigates, its probability, and the apportionment of the safety function to the safety group of C&I systems, could not be found. It was therefore not possible to check that diversity in the protection system exists within the safety group whenever the PIE probability is less than 1E-4 pfd.

EPR.8.11. It has been clarified by letter [16] that both PS and SAS/PAS have the functionality to initiate each of the diverse shutdown systems (the reactor shutdown equipment (RT) and the extra boration equipment (SIS and EBS)). However it was not possible to establish whether diverse input signals and diverse actuation are used by the corresponding PS and SAS functions, nor whether all Postulated Initiating Events are covered by diverse initiation functions.

EPR.8.12 It was not possible to locate the specifications of the Teleperm XS and the SPPA-T2000 platform, nor to locate any detailed description of the SPPA development platform tools and methods."