Office for Nuclear Regulation

An agency of HSE

Generic Design Assessment – New Civil Reactor Build

GDA Step 4 and Close-out for Control and Instrumentation Assessment of the EDF and AREVA UK EPR™ Reactor

Assessment Report: ONR-GDA-AR-11-022
Revision 1
March 2013

COPYRIGHT

PREFACE

The Office for Nuclear Regulation (ONR) was created on 1st April 2011 as an Agency of the Health and Safety Executive (HSE). It was formed from HSE's Nuclear Directorate (ND) and has the same role. Any references in this document to the Nuclear Director ate (ND) or the Nucle ar Installations Inspectorate (NII) should be taken as references to ONR.

EXECUTIVE SUMMARY

My report presents the findings of the Control and Instrumentation (C&I) assessment of the UK EPR™ reactor undertaken as part of Step 4 and close-out of the Office for Nuclear Regulation's (an agency of HSE) Generic Design Assessment (GDA) process. I carried out my assessment using the Pre-Construction Safety Report (PCSR) and supporting documentation submitted by EDF and AREVA during GDA Step 4 and close-out of the GDA Issues.

My assessment has followed a step-wise-approach in a claims-argument-evidence hierarchy. In GDA Step 2, the claims made by EDF and AREVA (the Requesting Party (RP)) were examined; in GDA Step 3 the arguments that underpin those claims were examined.

The scope of the GDA Step 4 assessment was to review the safety aspects of the UK EPR™ reactor in greater detail, by examining the evidence, supporting arguments and claims made in the safety documentation. The GDA Step 4 assessment builds on the assessments already carried out for GDA Steps 2 and 3, and provides a judgement on the adequacy of the C&I information contained within the PCSR and supporting documentation. The GDA close-out phase assessment addressed resolution of the GDA Issues raised during Step 4.

It is seldom possible, or necessary, to assess a safety case in its entirety; therefore, sampling is used to limit the areas scrutinised, and to improve the overall efficiency of the assessment process. Sampling is performed in a focused, targeted and structured manner with a view to revealing any topic-specific or generic weaknesses in the safety case. To identify the sampling for the C&I, assessment plans for GDA Step 4 and close-out were set-out in advance.

My assessment has focussed on the:

- arguments and evidence presented for conformance to the HSE C&I Safety Assessment Principles (SAPs);
- principal design and implementation standards for all C&I safety and safety related systems (i.e. the Systems Important to Safety (SIS));
- RP's safety case for selected key C&I SIS and platforms used to implement the systems (e.g. covering the safety Class 1 Protection System (PS), Class 2 Safety Automation System (SAS) and Class 3 Process Automation System (PAS));
- C&I architecture including provision for defence-in-depth, independence and diversity (including review of EDF and AREVA's responses to Regulatory Issue (RI) **RI-UKEPR-002** raised on the adequacy of the UK EPR™ C&I architecture);
- diversity of those systems contributing to implementation of the highest category safety functions (e.g. PS and SAS / PAS): and
- GDA Issue Resolution Plan submissions provided by the RP.

A number of items have been agreed with EDF and AREVA as being outside the scope of the GDA process and hence have not been included in my assessment.

From my assessment, I have concluded that the:

- PCSR and supporting documentation cover the main C&I SIS expected in a modern nuclear reactor;
- principal design and implementation standards used by EDF and AREVA for all C&I SIS are broadly in accordance with those expected in the nuclear sector;

- RP's safety case for the sampled key C&I SIS and platforms used to implement the SIS is broadly in line with expectations; and
- significant C&I architecture concerns raised in **RI-UKEPR-002** have been addressed by i) the reduction of reliability claims for the computer-based SIS, and ii) introduction of a safety Class 2 Non-Computerised Safety System (NCSS), one way network communication from the PS to lower classified systems, and Class 1 displays and manual controls.

However, some of the observations identified during Step 4 were of particular significance and required resolution before HSE would agree to the commencement of nuclear safety related construction of a UK EPR™ reactor in the UK. These are identified in this report as GDA Issues and the C&I GDA Issues are listed in Annex 2. In summary, these relate to:

- revision of the safety case to address the introduction of the NCSS, including the demonstration of its diversity from the computer-based safety systems;
- revision of the safety case to address PS changes to ensure there are only outward network communications to other systems from the PS, and justification of the small number of hardwired links to the PS;
- justification of the revised reliability figures used for the protection systems (PS, SAS / PAS and NCSS) when claimed independently and in combination;
- provision of detailed substantiation of the Class 1 control and display facilities, including justification of functional coverage;
- revision of the safety case to classify the C&I systems (e.g. PAS and SAS) in accordance with international standards and commitments provided by EDF and AREVA;
- finalisation of the PS independent confidence building activities' scope (covering statistical testing, static analysis and compiler validation), and definition of production excellence and independent confidence building measures for other SIS;
- enhancements to the safety case, in particular, to the presentation of the claims-arguments-evidence trail (i.e. covering key safety case claims and SAP conformance);
- fully defining the approach to the justification of smart devices (based on computer technology) used in SIS, including provision of a programme showing when implementation evidence will be available; and
- revision of the SAS / PAS safety case to address obsolescence of the SPPA-T2000 (Siemens S5 based) platform.

In response to the GDA Issues, the RP published Resolution Plans for each GDA Issue. My GDA Issue close-out assessment focussed on the submissions identified within the Resolution Plans. The submissions have included the provision of additional safety case information (e.g. Basis of Safety Case (BSC) documents for the NCSS, SPPA-T2000 platform version change and Protection System Operating Terminal (PSOT) Class 1 display system), methodologies to be implemented during the Site Specific Phase (SSP) (e.g. approach to smart device qualification and diversity assessment methodology) and proposals for plant modifications (e.g. provision of diverse sensor conditioning and Priority Actuation Control System (PACS) actuator modules). I conclude that the submissions are satisfactory and sufficient for closing out the C&I GDA Issues.

In some areas of the GDA Step 4 and close-out there has been a lack of detailed information, which has limited the extent of my assessment. This lack of detailed information is due to the fact that for the UK EPR™ the detailed design has not yet been undertaken. As a result I will need additional information to underpin my conclusions, and these are identified as Assessment Findings to be carried forward as normal regulatory business. Assessment Findings have been raised to cover items such as standards' compliance demonstration, and implementation of process improvements (e.g. relating to PS requirements traceability and production of method statements). Assessment Findings are listed in Annex 1.

Overall, based on the sample undertaken in accordance with ND procedures, I am broadly satisfied that the claims, arguments and evidence laid down within the PCSR and supporting documentation submitted as part of the GDA process present an adequate safety case for the C&I of the generic UK EPR™ reactor design. The UK EPR™ reactor is therefore suitable for construction in the UK with respect to the adequacy of C&I, subject to assessment of additional information that becomes available as the GDA Design Reference is supplemented with additional details on a site-by-site basis.

LIST OF ABBREVIATIONS

2oo4	2 out of 4 (voting logic)
ALARP	As Low As Reasonably Practicable
AP	Automation Processor
ASIC	Application Specific Integrated Circuits
ASN	Autorité Sûreté Nucléaire – French Nuclear Safety Authority
BMS	(Nuclear Directorate) Business Management System
BS	British Standards
BSC/BoSC	Basis of Safety Case
C&I	Control and Instrumentation
CAE	Claims-Argument-Evidence
CASSIS	Functional test coverage tool
CBSIS	Computer Based Systems Important to Safety
CCF	Common Cause Failure
CINIF	Control and Instrumentation Nuclear Industry Forum
CMF	Change Management Form
COTS	Commercial Off The Shelf
COW	Computerised Operator Workstation
CPLD	Complex Programmable Logic Devices
CPU	Central Processing Unit
CSCT	Conditions for Standard I&C Systems
DA	Design Authority
DAC	Design Acceptance Confirmation
DI	Data Interface
DNBR	Departure from Nucleate Boiling Ratio
EDF and AREVA	Electricité de France SA and AREVA
EDG	Emergency Diesel Generator
EFWP	Emergency Feedwater Pump
EFWS	Emergency Feedwater System
EMIT	Examination, Maintenance, Inspection, and Test
EN	European Standards / Euro Norme
ERBUS	Computer assisted test system for TXS
ESFAS	Engineered Safety Features Actuation System
FA3	Flamanville 3 Nuclear Power Plant
FPGA	Field Programmable Gate Array
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis

LIST OF ABBREVIATIONS

FUM	Function Module
GDA	Generic Design Assessment
HMI	Human Machine Interface
HSE	Health and Safety Executive
HVAC	Heating, Ventilation, and Air Conditioning
ICBM	Independent Confidence Building Measures
iDAC	Interim Design Acceptance Confirmation
IEC	International Electrotechnical Commission
IAEA	International Atomic Energy Agency
MALPAS	Malvern Program Analysis Suite
MCP	Main Coolant Pump
MCR	Main Control Room
MDEP	Multinational Design Evaluation Programme
MSI	Monitoring and Service Interface
NC	Non-Categorised
NCSS	Non-Computerised Safety System
ND	The (HSE) Nuclear Directorate
NEA	Nuclear Energy Agency
NNB	Nuclear New Build
NP	Nuclear Plant
NSL	Nuclear Site Licensing
OECD	Organisation for Economic Co-operation and Development
OLMAS	Optical Link Module Application Specific integrated circuit
PACS	Priority Actuation Control System
PAS	Process Automation System
PCEC	Programmable Complex Electronic Components
PCSR	Pre-Construction Safety Report
PE	Production Excellence
pdfy	Probability of Dangerous Failure per Year
pfd	Probability of Failure on Demand
PICS	Process Information and Control System
PIE	Postulated Initiating Event
PIPO	Pupitre Inter Poste Opérateur – Inter-workstation console
PIPS	Process Instrumentation Pre-processing System
PS	Protection System
PSA	Probabilistic Safety Analysis
PSOT	Protection System Operating Terminal

LIST OF ABBREVIATIONS

PWR	Pressurised Water Reactor
QA	Quality Assurance
QDS	Qualified Display System
QMS	Quality Management System
RAMS	Reliability, Availability and Maintainability Study
RCS	Reactor Coolant System
RCSL	Reactor Control, Surveillance and Limitation system
RI	Regulatory Issue
RIF	Requirements Identification File
RO	Regulatory Observation
RP	Requesting Party
RPMS	Rod Position and Monitoring System
RPR	Reactor Protection System
RRC-A	Risk Reduction Category - A
RRC-B	Risk Reduction Category - B
RSS	Remote Shutdown Station
RTE	Run Time Environment
RT-SIM	Run Time Simulator
SA I&C	Severe Accident Instrumentation and Control
SAP	HSE Nuclear Directorate Safety Assessment Principle
SAS	Safety Automation System
SCC	Source to Code Comparison
SDM	System Design Manual
SFC	Single Failure Criterion
SICS	Safety Information and Control System
SIL	Safety Integrity Level
SIS	Systems Important to Safety
SIVAT	Simulation Based Validation Tool
SOUP	Software of Unknown Pedigree
SRS	Safety Related Systems / Safety Requirements Specification
SS	Safety Systems
SSP	Site Specific Phase
STUK	Sateilyturvakeskus, the Finnish nuclear safety regulator
TAG	(Nuclear Directorate) Technical Assessment Guide
TO	TSC Technical Observation
TQ	Technical Query
TSC	Technical Support Contractor

LIST OF ABBREVIATIONS

TXS	Teleperm XS
US	United States
US NRC	US Nuclear Regulatory Commission

TABLE OF CONTENTS

1 INTRODUCTION 1
2 NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR C&I 2
2.1 GDA Step 4 and Close-out Assessment Plans 2
2.2 Standards and Criteria 3
2.3 Assessment Scope 3
2.3.1 GDA Step 4 Assessment Scope 3
2.3.2 GDA Close-out Assessment Scope 4
2.3.3 Findings from GDA Step 3 4
2.3.4 Additional Areas for Step 4 C&I Assessment 5
2.3.5 Use of Technical Support Contractors 5
2.3.6 Cross-cutting Topics 6
2.3.7 Out of Scope Items 7
3 REQUESTING PARTY'S SAFETY CASE 10
4 GDA STEP 4 AND GDA ISSUE CLOSE-OUT ASSESSMENT FOR C&I 11
4.1 C&I SAP and Safety Case Claims-Arguments-Evidence, and Consolidated Final GDA Submission Assessment 11
4.1.1 Step 4 Assessment 11
4.1.2 Step 4 Findings 14
4.1.3 GDA Issue Close-out Assessment 14
4.1.4 GDA Close-out findings 21
4.2 C&I Systems' Classification and Standards 21
4.2.1 Step 4 Assessment 21
4.2.2 GDA Step 4 Findings 26
4.3 C&I SIS Platforms and Pre-Developed Equipment 26
4.3.1 GDA Step 4 Assessment 26
4.3.2 GDA Step 4 Findings 36
4.3.3 GDA Close-out Assessment 36
4.3.4 GDA Close-out Findings 41
4.4 C&I Systems Important to Safety 41
4.4.1 GDA Step 4 Assessment 41
4.4.2 GDA Step 4 Findings 52
4.4.3 GDA Close-out Assessment 52
4.4.4 GDA Close-out Findings 55
4.5 C&I System Level Architecture 55
4.5.1 GDA Step 4 Assessment 55
4.5.2 GDA Step 4 Findings 61
4.5.3 GDA Close-out Assessment 61
4.5.4 GDA Close-out findings 93
4.6 Diversity of Systems Implementing Reactor Protection Functionality 93
4.6.1 GDA Step 4 Assessment 93
4.6.2 GDA Step 4 Findings 95

4.7 Overseas Regulatory Interface ... 95
4.7.1 Bilateral Collaboration ... 95
4.7.2 Multilateral Collaboration ... 96
5 CONCLUSIONS ... 97
5.1 Key Findings from the GDA Step 4 and Close-out Assessment ... 97
5.1.1 Assessment Findings ... 98
5.1.2 GDA Issues ... 98
6 REFERENCES ... 99

Tables

Table 1: C&I Scope: C&I Automation Systems

Table 2: C&I Scope: Instrumentation

Table 3: C&I Scope: C&I Platform Development

Table 4: C&I Scope: HMI Systems

Table 5: Relevant Safety Assessment Principles for Control & Instrumentation Considered During Step 4

Annexes

Annex 1: Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business – Control & Instrumentation – UK EPR™

Annex 2: GDA Issues – Control & Instrumentation – UK EPR™

Annex 3: TSC Task Summary – C&I SAP Conformance and Adequacy of PCSR Review for UK EPR™

Annex 4: TSC Task Summary - Review of EDF and AREVA QMS Processes Against Principal Design and Implementation Standards

Annex 5: TSC Task Summary - Review of Class 1 and 2 System Platforms and Pre-Developed Complex Components

Annex 6: TSC Task Summary - Review of C&I Safety and Safety-Related Systems

Annex 7: TSC Task Summary - Review of the C&I Architecture for Safety Capability

Annex 8: TSC Task Summary - Review of the Diversity of those Systems Contributing to the Implementation of Category A Functions

Annex 9: TSC Task Summary - Review of Responses to Regulatory Issue **RI-UKEPR-002**

Annex 10: EDF and AREVA Final Deliverables in Response to the C&I GDA Issues

Annex 11: TSC task summary - GDA Issue **GI-UKEPR-CI-01** – Design Information for the Non-Computerised Safety System (NCSS) Required

Annex 12: TSC task summary - GDA Issue **GI-UKEPR-CI-02** – Protection System Independent Confidence Building Measures

Annex 13: TSC task summary - GDA Issue **GI-UKEPR-CI-03** – Claims, Arguments, Evidence Trail

Annex 14: TSC task summary - GDA Issue **GI-UKEPR-CI-04** – Smart Devices

Annex 15: TSC task summary - GDA Issue **GI-UKEPR-CI-05** – Obsolescence of the SPPA T2000 Platform

Annex 16: TSC task summary - GDA Issue **GI-UKEPR-CI-06** – Issues arising from Regulatory Issue RI02

Annex 17: TSC task summary - GDA Issue **GI-UKEPR-CC-01 ACTION 6** - Categorisation and Classification of Systems, Structures and Components

Annex 18: TSC task summary - GDA Issue **GI-UKEPR-CC-02 ACTION 1** - Consolidated Final GDA Submission Including Agreed Design Change For The UK EPR™

1 INTRODUCTION

1 My report presents the findings of the GDA Step 4 and GDA Issue close-out Control and Instrumentation (C&I) assessment of the UK EPR™ reactor Pre-Construction Safety Report (PCSR) (Ref. 22) and supporting documentation provided by EDF and AREVA under the Office for Nuclear Regulation's (an agency of HSE) Generic Design Assessment (GDA) process. Assessment was undertaken of the PCSR and the supporting evidentiary information derived from the Master Submission List (Ref. 23). The approach taken was to assess the main submission, i.e. the PCSR, and then undertake assessment of the relevant documentation sourced from the Master Submission List on a sampling basis in accordance with the requirements of ND Business Management System (BMS) procedure AST/001 (Ref. 2). I used the Safety Assessment Principles (SAPs) (Ref. 4) as the basis for this assessment. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

2 During the assessment a number of Technical Queries (TQs), topic meeting actions, Regulatory Observations (ROs), one Regulatory Issue (RI) and six Step 4 C&I GDA Issues were issued and the responses made by EDF and AREVA assessed. Where relevant, detailed design information from specific projects for this reactor type has been assessed to build confidence and assist in forming a view as to whether the design intent proposed within the GDA process can be realised.

3 It is not the purpose of this report to provide a detailed description of the C&I architecture; such description may be found in "PCSR – Sub-Chapter 7.2 – General architecture of the Instrumentation & Control systems" (Ref. 22).

4 A number of items have been agreed with EDF and AREVA as being outside the scope of the GDA process and hence have not been included in this assessment. These are identified in Section 2.3.7 of this report.

2 NUCLEAR DIRECTORATE’S ASSESSMENT STRATEGY FOR C&I

5 My GDA Step 4 and GDA Issue close-out assessment strategy for the C&I topic area was set out in assessment plans (Refs 1 and 67) that identified the intended scope of the assessment and the standards and criteria that would be applied. This is summarised below.

2.1 GDA Step 4 and Close-out Assessment Plans

6 The objective of the GDA Step 4 C&I assessment was to review the safety aspects of the proposed C&I design by examining the evidence supporting the claims and arguments made in EDF and AREVA’s safety documentation. The GDA Step 4 assessment builds on the GDA Steps 2 and 3 work, and provides a judgement on the adequacy of the C&I safety demonstration contained within the PCSR and supporting documentation.

7 My GDA Step 4 assessment examined the remaining claims not previously assessed (e.g. addressing relevant HSE SAPs not previously considered) and the underpinning arguments. However, the scope of this assessment was primarily concerned with examination of samples of the ‘evidence’ to support claims for all HSE SAPs within the scope of assessment. For C&I ‘evidence’ was broadly interpreted as including:

- the detailed documentation showing conformance with the relevant HSE SAPs (i.e. how the HSE SAP goals are met);
- the detailed documentation showing compliance with the standards for the equipment, production processes and safety justification;
- information substantiating the C&I functionality and reliability claims; and
- information supporting Production Excellence (PE) for the pre-existing platforms.

8 My GDA Step 4 assessment included a review of the processes to be used to produce and justify the application specific software and hardware for the Safety Systems (SS) and Safety Related Systems (SRS) (i.e. the Systems Important to Safety (SIS)). Samples of the application software (using examples from the Flamanville 3 (FA3) plant) were reviewed.

9 My GDA Step 4 assessment commenced with consideration of the relevant chapters of the PCSR and supporting references available at that time, and these are referred to as appropriate in this report. As the GDA submission developed during Step 4, in response to my regulatory questions, amendments were made as appropriate to the PCSR and its supporting references.

10 During Step 4 I reviewed the updates to the C&I GDA submission and determined that the updates to or information included in the GDA submission and/or supporting references were not as expected. Further work was required to address these shortfalls. This was be progressed in GDA through a C&I GDA Issue **GI-UKEPR-CI-03** and cross-cutting GDA Issue **GI-UKEPR-CC-02**. In the C&I topic area my assessment was therefore limited to the versions of the GDA submission documents referred to in my Assessment Report. Although the consolidated PCSR (Ref. 62) and its supporting references were therefore acceptable as the reference point for an Interim Design Acceptance Confirmation (iDAC) the outstanding GDA Issues required acceptable resolution before a final Design Acceptance Confirmation (DAC) could be issued.

11 The objective of the C&I GDA Issue close-out assessment was to assess submissions made by EDF and AREVA in response to the Step 4 GDA Issues (see Annex 2 for the

C&I GDA Issues) and design changes requested by EDF and AREVA, and if judged acceptable, clear the GDA Issues. The overall bases for the assessment of the GDA Issues are the C&I elements of the submissions outlined below.

- Submissions made in accordance with the published Resolution Plans.
- Update to the submissions, PCSR and supporting documentation.
- The Design Reference that relates to the PCSR and submissions as set out in UK EPR™ GDA Project Instruction UKEPR/I/002, as updated through GDA Issue resolution. This includes Change Management Forms (CMF).
- Design change submissions as proposed by EDF and AREVA and submitted in accordance with the UK EPR™ GDA Project Instruction UK-EPR-I-003.

2.2 Standards and Criteria

12 The standards and criteria that were used to judge the adequacy of the UK EPR™ C&I were HSE SAPs (Ref. 4), Technical Assessment Guides (TAGs) and relevant international standards and guidance (e.g. Ref. 5). Unless stated otherwise, these standards and criteria set the expectations mentioned throughout this assessment report. Table 5 identifies the HSE C&I SAPs considered during my assessment.

13 Nuclear Directorate's (ND's) C&I TAGs provide further guidance for some of the HSE C&I SAPs. The key TAGs are T/AST/003 (Ref. 8) for SS and T/AST/046 (Ref. 9) for systems containing computer / complex te chnology. The majority of the SIS deployed on the UK EPR™ contain such technology.

14 The standards and criteria used for the C&I GDA assessment included relevant nuclear sector standards related to SIS design (e.g. BS IEC 61513:2001 (Ref. 10) and BS IEC 62340:2007 (Ref. 11)). Other significant guidance includes the report of the seven party task force on safety critical software (Ref. 5).

2.3 Assessment Scope

15 This section outlines the:

- assessment scope for both GDA Step 4 and close-out;
- way GDA Step 3 matters were taken forward during Step 4;
- scope of the Technical Support Contractor's (TSC's) work;
- cross cutting issues; and
- out-of-scope items.

2.3.1 GDA Step 4 Assessment Scope

16 The C&I GDA Step 4 assessment included the specific elements shown below.

- Completion of the technical review of EDF and AREVA's responses to regulatory issue **RI-UKEPR-002** and resolution of ND GDA Step 3 Assessment Report observations (Ref. 6). For example, covering topics such as categorisation of functions, classification of systems, compliance to International Electrotechnical Commission (IEC) C&I SIS standards and the special case procedure for computer-based systems (Ref. 9).

- Review of the "arguments" and "evidence" made for conformance to the HSE C&I SAPs (Ref. 4) (i.e. completion of the claims-arguments-evidence (CAE) based review against the SAPs).
- Review of the principal design and implementation standards for C&I SIS (Class 1, 2 and 3) equipment. Sampling of detailed evidence during GDA Step 4 (e.g. to demonstrate the standards have been adequately applied) predominately focused on the Class 1 systems (e.g. reactor protection) and the key Class 2 SIS.
- Review of EDF and AREVA's safety case for the Class 1 (e.g. Teleperm XS (TXS)) and key Class 2 SIS platforms and pre-developed components using appropriate guidance and standards.
- Review of the safety case for the implementation of the Class 1 and key Class 2 SIS (e.g. development of application code, independent verification and validation, and Independent Confidence Building Measures (ICBMs)) using the platforms and pre-developed equipment selected by EDF and AREVA.
- Further review of the C&I architecture including provisions for defence-in-depth, independence and diversity, automatic and manual safety actuations, and appropriateness of equipment class.
- Further review of the diversity of those systems contributing to implementation of Category A functions (e.g. Protection System (PS) and Safety Automation System (SAS)).
- Review of the impact of PCSR revisions.

2.3.2 GDA Close-out Assessment Scope

17 The C&I GDA Issue close-out scope includes assessment of EDF and AREVA's responses to the GDA Issues undertaken in accordance with the milestone programmes provided in the Resolution Plans. The information provided by EDF and AREVA in response to the GDA Issues, as detailed within their Resolution Plans (Refs 68 to 73), was broken down into the component GDA Issue Actions and then further detailed by reference to specific deliverables. A table listing the final version of every deliverable submitted in response to each of the C&I GDA Issue Actions is presented in Annex 10.

18 The scope of my C&I GDA Issue close-out assessment includes review of the EDF and AREVA Resolution Plan submissions against the expectations detailed in the relevant GDA Issues (i.e. **GI-UKEPR-CI-01 to 06**, **GI-UKEPR-CC-01** and **GI-UKEPR-CC-02**) and the associated GDA Issue Actions. The C&I GDA Issues are detailed within Annex 2 of this report. My review of Resolution Plan programme submissions made appropriate use of the standards and criteria outlined in Section 2.2. The results of my assessment are detailed in Section 4 below.

19 The scope of the GDA close-out assessment was not to undertake further assessment of the PCSR nor was it to extend this assessment beyond the expectations stated within the GDA Issue Actions.

2.3.3 Findings from GDA Step 3

20 The findings of my GDA Step 3 Assessment Report (Ref. 6) are summarised below.

- 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 SIS (CBSIS) that use the TXS 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 needed improvement.

21 EDF and AREVA proposed a way forward in relation to **RI-UKEPR-002** that provided a basis for proceeding to GDA Step 4, which included:

- provision of a backup safety system that is not based on computer technology and is known as the Non-Computerised Safety System (NCSS);
- one-way network communication from the Protection System (PS) to lower classified systems; and
- the provision of a Class 1 display facility and manual controls.

In addition to changes in the technology and C&I architecture, EDF and AREVA also agreed to a reduction of the CBSIS reliability claims. Assessment of these proposals and EDF and AREVA's response to concerns raised in the GDA Step 3 Assessment Report (Ref. 6) is provided in Section 4.

2.3.4 Additional Areas for Step 4 C&I Assessment

22 My GDA Step 4 assessment includes completion of the review of HSE C&I SAPs considered appropriate for sampling during assessment of a new reactor design. Therefore, there is an increase in the number of HSE SAPs reviewed during GDA Step 4 compared to that assessed during GDA Step 3. In addition, GDA Step 4 included sampling of the detailed evidence used to substantiate safety case claims.

23 During GDA Step 4 the assessment scope was widened to include coverage of the C&I standards for Class 1, 2 and 3 SIS, a review of key C&I platforms (e.g. TXS and SPPA-T2000) and a review of the processes used to develop applications for systems using these platforms.

2.3.5 Use of Technical Support Contractors

24 A Technical Support Contractor (TSC) was engaged to assist with the C&I assessment work in GDA Step 3. The same contractor assisted during GDA Step 4 and GDA Issue close-out. The scope of work undertaken by the TSC included:

- sample-based review of the evidence used to demonstrate conformance to HSE C&I SAPs;
- sample-based review of the main design and implementation standards used for C&I SIS related equipment (i.e. for architecture, platforms (TXS and SPPA-T2000), applications, and also smart devices);

- sampling of the detailed design and implementation evidence of the Class 1 platform (TXS) and the Class 2 platform (SPPA-T2000);
- sampling of the detailed evidence of the implementation methods for Class 1 systems (e.g. PS), Class 2 systems (e.g. SAS) and Class 3 systems (e.g. PAS);
- sampling of the detailed evidence of C&I architecture safety capability, including a review of the overall system integration; and
- sampling of the detailed evidence of the diversity of the designs of platforms and systems contributing to implementation of Category A functions, and assessment of the possible contribution of platforms / systems to Common Cause Failure (CCF) of the Category A functions.
- review of submissions made by EDF and AREVA in response to the Step 4 GDA Issues in accordance with the Resolution Plan programme.

25 The TSC undertook detailed technical reviews under the close direction and supervision of ND. The regulatory judgment on the adequacy or otherwise of the UK EPR™ C&I was made exclusively by ND. A ll TQs, ROs, the one RI and the six GDA Issues were raised by ND.

26 The TSC has provided GDA Step 4 and GDA Issue close-out reports that address the scope of work listed above. The TSC also reviewed responses to ROs, TQs and Level 3 meeting Actions placed on EDF and AREVA. The TSC reports include a summary statement of the results of its work and findings (i.e. Technical Observations (TOs)). The summary statements including all TOs ar e reproduced in Annexes 3 to 9 (GDA Step 4) and Annexes 11 to 18 (GDA Issue close-out). I reviewed the TSC's TOs arising from GDA Step 4 and, as considered appropriate, took them forward under GDA Issues (see Annex 2 for the C&I GDA Issues) or Assessment Findings (see Annex 1). As appropriate, TSC TOs arising from GDA close-out reviews are taken forward under Assessment Findings (Annex 1). The TSC TOs provide further guidance on the GDA Issues or Assessment Findings and their means of resolution. Within this report, references to the TSC TOs are provided using the unique TO identifiers (e.g. T17.TO1.01).

2.3.6 Cross-cutting Topics

27 I address the following Cross-cutting Topics in this report: Safety Categorisation and Classification, and Smart Devices.

28 Safety Categorisation and Classification - The four levels of functional categorisation (F1A, F1B, F2 and Non-Categorised (NC)) and C&I system classification (E1A, E1B, E2 and NC) proposed b y EDF and AREVA do not align wit h HSE's SAPs (Ref. 4) o r relevant British issue of international C&I standards (i.e. BS IEC 61513:2001 (Ref. 10) and BS IEC 61226:2005 (Ref. 13)). This con cern was initially raised with EDF and AREVA as part of **RI-UKEPR-002** (Ref. 26) and then progressed as a transverse issue (i.e. affecting more than one topic a rea) as part of **RO-UKEPR-43**. EDF and AREVA have stated that categorisation and classification will be in accordance with BS IEC 61226:2009 (Ref. 44). A cross-cutting GDA Issue has been raised to cover submission of the outcome of EDF and AREVA's classification of C&I SIS in accor dance with the defined guidance and standards (see Section 4.5 for further details).

29 Smart Devices - EDF and AREVA needs to fully define the approach to be used for the justification of smart devices (i.e. devices based on computer technology) used in SIS. This type of device can be found in many types of modern equipment such as sensors,

actuators, electrical protection relays and mechanical packaged plant. It is my expectation that EDF and AREVA will have arrangements that ensure such devices are identified wherever they are used in SIS and they are appropriately qualified for their intended use. In relation to smart devices used in C&I SIS, a submission that fully defines an acceptable approach to the justification of smart devices including provision of a programme showing when implementation evidence will be available is required. I have raised a GDA Issue to cover the submission of the justification approach for smart devices and evidence of the implementation of the approach (see Section 4.3). Another concern associated with smart devices is the potential for their use, for a given Postulated Initiating Event (PIE), in multiple lines of defence. This concern is addressed by GDA Issue Action **GI-UKEPR-CI-06.A9** (see Section 4.5).

2.3.7 Out of Scope Items

30 The following items have been agreed with EDF and AREVA as being outside the scope of GDA (i.e. as identified in letter ND (NII) EPR00686N, Ref. 25 and Ref. 108).

- Turbine C&I.
- Fire protection and detection C&I.
- Waste Treatment Building C&I.
- Seismic Monitoring System.
- Fatigue, Leakage, Loose parts or Vibration Monitoring C&I.
- Radiation Monitoring C&I.
- Qualification of Excore sensors, Incore sensors and the Rod Position and Monitoring System (RPMS).
- Detailed design of the RPMS.
- Commissioning and site manuals for all C&I systems.
- NCSS detailed design, and verification and validation activities.

31 Where UK EPR™ information is not yet available to support the safety case, EDF and AREVA have offered equivalent FA3 information, if this has been available, as this project is at a more advanced stage than the UK EPR™. For example, the PS application code was not available for GDA, however, samples of FA3 application code and lifecycle documents were provided. The FA3 documents were provided so that a better understanding of the design processes could be obtained. In Ref. 25 the following categories of scope were defined.

- Scope Category A: C&I design is defined in terms of quality plan, process, structure, function, sizing and specification for detailed design. Supporting documents associated with this category are either: specific UK EPR™ documents or FA3 documents with an impact analysis for changes in the C&I architecture implemented to address the issues of **RI-UKEPR-002**.
- Scope Category B: Definition of methodology to be adopted for specific C&I design aspects of the UK EPR™. Applies to any development steps. Supporting documents associated with this category are methodology documents applicable to the UK EPR™. The application of the methods was illustrated by samples from other projects, when available.

- Scope Category C: Out of GDA scope.

32 The following list, provided in Ref. 25, defines how these categories were applied to plant C&I architecture (with A / B denoting Scope Category):

- Plant I&C - Quality plan – Scope Category A;
- Plant I&C - Requirement Specification – Scope Category A;
- Plant I&C - Architecture description – Scope Category A;
- Plant I&C - Allocation of I&C functions – Scope Category A;
- Plant I&C - Test plan – Scope Category A; and
- Plant I&C - Security plan – Scope Category B.

33 Tables 1, 2, 3 and 4 below define how the principle of scope categorisation was applied. Table 1 covers the following automation systems:

- Plant Automation System (PAS);
- Safety Automation System (SAS);
- Reactor Control, Surveillance and Limitation (RCSL) System;
- Protection System (PS);
- Severe Accident (SA) I&C system;
- Non-Computerised Safety System (NCSS); and
- Priority and Actuation Control System (PACS).

34 Table 2 covers instrumentation, including the Process Instrumentation Pre-processing System (PIPS). Table 3 covers platform development and Table 4 covers Huma n Machine Interface (HMI) systems, including the Process Information and Contr ol System (PICS) and the Safety Information and Control System (SICS).

Table 1: C&I Scope: C&I Automation Systems

	PAS	SAS	RCSL	PS	SA I&C[1]	NCSS	PACS
Quality plans	A	A	A	A	A	A	A
System specification	A	A	A	A	A	A	A
Detailed Design	B	B	B	B	B	C	C
Verification & Validation Activities	B	B	B	B	B	C	C
Commissioning & Site manuals	C	C	C	C	C	C	C

[1] ONR note: SA I&C is an abbreviation of Severe Accident Instrumentation and Control.

Table 2: C&I Scope: Instrumentation

	Process Sensors	PIPS (sensor conditioning)	Ex-core Sensors	In-core Sensors	RPMS
Specification	A	A	A	A	A
Detailed Design	C	A	B	B	C
Qualification	B	B	C	C	C

Table 3: C&I Scope: C&I Platform Development

Set of Documentation	GDA Step 4 Scope
TELEPERM XS – Description	A
TELEPERM XS – Qualification	A
SPPA-T2000 – Description	A
SPPA-T2000 – Qualification	A
NCSS platform – Description	B
NCSS platform – Qualification	B

Table 4: C&I Scope: HMI Systems

Set of documentation	GDA Step 4 scope
PICS – Specification	B
PICS – Qualification	A
SICS – Specification	B
SICS – Qualification	A

35 Insufficient information was made available during Step 4 to allow some nominally in-scope aspects of the UK EPR™ design to be assessed under GDA (e.g. the design of the Class 1 displays facility to be provided in the main control room). These items were not included within the Step 4 assessment. However, appropriate GDA Issue Actions were raised (see Section 4) to cover items that needed to be addressed prior to issue of a DAC.

3 REQUESTING PARTY'S SAFETY CASE

36 EDF and AREVA provided a number of documents setting out the UK EPR™ C&I safety case and also a submission outlining where the HSE SAPs are addressed in the documents. The main submission that describes the C&I is the PCSR (Ref. 22). The C&I provisions claimed include those that would be expected of a modern nuclear reactor such as:

- SSs (e.g. reactor shutdown systems such as the Protection System (PS));
- plant control and monitoring systems(e.g. the SAS, PAS and PICS);
- Main Control Room (MCR) facilities with backup via the Remote Shutdown Station (RSS); and
- communication systems for information transfer within and external to the plant.

37 EDF and AREVA's GDA Step 2 C&I submission described a conceptual design. During GDA Step 3 EDF and AREVA stated that the HSE GDA C&I assessment should be based on the FA3 design and documentation, and this concept was refined in GDA Step 4 as described in Section 2.3.6. The UK EPR™ makes use of two main computer-based C&I platforms, Teleperm XS (e.g. PS and RCSL system) and Siemens SPPA T2000 (e.g. PAS and SAS). At the time of the assessment the PCSR had not been updated to reflect the impact of design changes agreed under **RI-UKEPR-002** (see Section 2.1 for information concerning the PCSR update).

38 An important aspect of the safety demonstration is the classification of 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 (i.e. Class 1 systems are implemented using higher safety standards). 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 (see Section 4.2 for further discussion on this topic). Four function categories (i.e. F1A, F1B, F2 and NC) and equipment classes (i.e. E1A, E1B, E2 and NC) are used (see comments in Section 2.3.4).

39 The safety case assessed under GDA Step 4 consisted of the PCSR (Ref. 22), Requesting Party (RP) responses to the RI, ROs and TQs, and submissions provided by EDF and AREVA under cover of formal correspondence as listed in the Master Submission List (Ref. 23).

40 During the GDA Issue close-out phase of the work I sampled the deliverables submitted in response to each of the C&I GDA Issue Actions (see Annex 10). It is important to note that this information is supplementary to the information provided within the November 2009 PCSR (Ref. 22), which has already been subject to assessment during earlier stages of GDA. In addition, it is important to note that the deliverables are not intended to provide the complete safety case for C&I. Rather they form further detailed arguments and evidence to supplement those already provided during earlier Steps within the GDA Process.

4 GDA STEP 4 AND GDA ISSUE CLOSE-OUT ASSESSMENT FOR C&I

41 This section documents the results of my GDA Step 4 and GDA Issue close-out C&I assessment and details the GDA Issues and Assessment Findings that I have raised. GDA Issues require resolution before nuclear island safety-related construction of the reactor could be considered. Assessment Findings are important to safety but are not considered critical to the decision to start nuclear island safety related construction of the reactor (see Guidance to HSE and Environment Agency Inspectors on the content of; GDA Issues, Assessment Findings, Resolution Plans, GDA Issue Metrics (Ref. 55 and see also Ref. 49)). In order to close the GDA Issues and Assessment Findings the related TSC TOs that provide further guidance need to be resolved. A unique TSC TO reference is used to identify the TSC's TOs (see the Annexes for the TO detail).

42 The complete C&I GDA Issues and associated actions are formally defined in Annex 2 of this report.

4.1 C&I SAP and Safety Case Claims-Arguments-Evidence, and Consolidated Final GDA Submission Assessment

4.1.1 Step 4 Assessment

43 This section provides the results of the assessment of the UK EPR™'s conformance to the HSE C&I SAPs and the adequacy of the safety case "Claims-Argument-Evidence" (CAE) trail. This section also describes the resolution of the GDA Step 3 assessment observations.

44 A list of the HSE SAPs used to assess the adequacy of EDF and AREVA's safety case argumentation during GDA Step 3 can be found in my GDA Step 3 C&I Assessment Report (Ref. 6). In selecting the HSE SAPs for GDA Step 3 assessment, I paid particular attention to those HSE SAPs considered to have particular relevance to system and architectural design.

45 The GDA Step 3 HSE SAP argumentation assessment raised a number of observations related to adequacy of the CAE trail and HSE SAP conformance. Those addressed in this section are:

- "while EDF and AREVA claim conformance 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".

46 The GDA Step 3 Assessment Report HSE SAP assessment observations addressed elsewhere in this report (relating to architecture, platforms and / or applications) are shown below.

- 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 SAPs (Ref. 4) or BS IEC 61226:2005 (Ref. 13) (see Sections 2.3.4 and 4.2).
- Standards - Further clarification was required in relation to the standards used by EDF and AREVA (see Section 4.2).
- Defence-in-Depth - The allocation of safety functions to C&I systems conforms to the defence-in-depth concept, aligning with the five levels referred to in the International Atomic Energy Agency (IAEA) Safety Standard NS-R-1 (Ref. 27).

However, use was made of only two computer-based platforms (i.e. Teleperm XS and SPPA-T2000). It was noted that a failure of one computer-based platform due to CCF may result in the loss of more than one level of defence (see Section 4.5).

- Redundancy - The level of equipment redundancy within the PAS and SAS required further clarification (see Section 4.4).
- Diversity - Functional and equipment diversity is used across the two computer-based platforms Teleperm XS and SPPA-T2000 but the extent required clarification (see Section 4.6).
- 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 (see Section 4.5).
- Reliability - The PCSR Probabilistic Safety Analysis (PSA) gives 1 x 10^{-5} probability of failure on demand (pfd) and 1 x 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 SS (Ref. 9) and insufficient justification of these claims was provided (see Section 4.5).
- Failure to Safety - The fail-safe principle as applied to C&I systems was not well covered in the PCSR (see Section 4.2).
- Computer-Based SIS - Further clarification was required as to how the independent confidence building and PE legs (for further guidance see also T/AST/046, Ref. 9) were addressed (see Section 4.2).

47 During GDA Step 4, a review of the "arguments" and "evidence" made for conformance to the HSE C&I SAPs (Ref. 4) (i.e. completion of the CAE based review against the SAPs) was completed. A list of the HSE SAPs considered during the assessment of the adequacy of EDF and AREVA's safety case argumentation during GDA Step 4 can be found in Table 5.

48 The TSC reviews performed during GDA Step 3 were based on the PCSR submitted for the start of GDA Step 3 which was dated April 2008 (Ref. 46). A revision of the PCSR was submitted in June 2009 (Ref. 47) and the TSC reviewed (see Ref. 48) the impact of the revisions to the PCSR on the conclusions to its report. The TSC determined that the June 2009 Issue 2 of the PCSR (Ref. 47) did not introduce significant improvements to the safety ar gumentation. A major change in PCSR Issue 2 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".

49 The ND GDA Step 3 Assessment Report determined that the safety case argumentation and identification of ev idence needed improvement (Ref. 6). **RO-UKEPR-62** was raised on EDF and AREVA with two actions, namely:

- to review and revise the UK EPR™ PCSR C&I sections so that a clear CAE trail exists within the document for all claims (Action 1);
- identify the evidence and related argument which demonstrates satisfaction of each of the HSE C&I SAPs (Action 2).

It was subsequently agreed that Action 1 could be addressed by the provision of a document referenced from the PCSR.

50 The results of the TSC's GDA Step 4 review of EDF and AREVA's HSE C&I SAP conformance demonstration and the adequacy of the safety case CAE trail is reported in the TSC GDA Step 4 report (Ref. 28). The TSC review also considered EDF and AREVA's responses to relevant Step 3 TQs and the TSC's GDA Step 3 observations, as recorded in the ND C&I Step 3 report (Ref. 6). In addition, the observations raised in the ND GDA Step 2 report have been progressed by the TSC. Those matters that remain open are recorded as TOs in the TSC's Step 4 report (Ref. 28). Annex 3 contains a summary of the TSC HSE SAP conformance and safety case CAE review, including identification of the GDA Step 4 TOs.

51 The major concern identified during GDA Step 4 relates to the closure of the CAE trail actions raised under **RO-UKEPR-62**. There have been a number of iterations (as a result of inadequate quality) of EDF and AREVA's submissions (i.e. in order address ND review comments). EDF and AREVA's planned final response with respect to an improved PCSR safety case CAE trail was submitted after the end of the GDA Step 4 assessment phase and was not assessed during Step 4.

52 During GDA Step 4, a part response to **RO-UKEPR-62 Action 1** was assessed. While the general approach outlined by EDF and AREVA was not unacceptable, the response substantially replicates the HSE SAP CAE trail (as provided in response to Action 2) without a clear identification of the source of the claims (e.g. arising from EDF and AREVA's own safety principles, criteria and standards) and the relevant location of the claims in the PCSR (see T13.TO1.01 in Annex 3).

53 EDF and AREVA were also requested to identify the evidence and related argument that demonstrates conformance to each of the HSE C&I SAPs (**RO-UKEPR-62 Action 2**). The review of EDF and AREVA's responses has determined that an acceptable methodology has been developed for demonstrating conformance to the HSE SAPs. However, there were still significant shortfalls in the presented argumentation and identification of evidence for many HSE SAPs, see below.

54 The TSC performed an initial review of the adequacy of the CAE trails for all 84 HSE C&I SAPs (see Table 5). This initial review considered the adequacy of coverage of the HSE SAP requirements, argumentation and appropriateness of the identified evidence. This initial review gave rise to 44 TSC TOs (see T13.TO1.02, and T13.TO2.01 to T13.TO2.43 in Annex 3). Following this initial review, it was determined that only 68 of these SAPs were within GDA C&I scope.

55 The TSC also undertook a detailed review of the evidence identified as demonstrating conformance to a subset of the HSE C&I SAPs (i.e. 26 of the 68 C&I SAPs declared to be within the scope of GDA by EDF and AREVA). As a result of this review, 92 TOs have been raised by the various TSC tasks that undertook the detailed evidence review (see table referenced by T13.TO1.03 in Annex 3). Many of these TOs relate to minor issues, such as the inclusion of already identified references in the CAE trails. However, there are also substantive matters which need to be addressed and these are identified in the Sections below. For example, EDF and AREVA needs to ensure that the sources of its key claims (e.g. as related to its own design requirements and safety criteria) are identified.

56 By the end of the GDA Step 4 assessment, the position on the adequacy of safety case argumentation and identification of evidence (e.g. improvement of the PCSR CAE trail) was not fully satisfactory. I raised a GDA Issue to cover the resolution of outstanding observations relating to **RO-UKEPR-62** actions.

*GDA Issue: **GI-UKEPR-CI-03**; Claims, Arguments, Evidence Trail - The quality of the assessed Claims, Arguments and Evidence (CAE trail) supporting documentation provided by EDF and AREVA requires revision and improvement (**RO-UKEPR-62**):-*

- ***GI-UKEPR-CI-03.A1**: The CAE trail documentation provided by EDF and AREVA requires revision and improvement. EDF and AREVA to revise and improve the CAE trail documentation. In particular to:*
    - *i) review the UK EPR™ PCSR C&I sections and ensure that a clear CAE trail is provided for all key claims;*
    - *ii) identify the evidence and related argument which demonstrates satisfaction of each of the C&I SAPs.*

For more detailed guidance on what is required to complete this work the following TOs provide comprehensive support information: T13.TO1.01, T13.TO1.02, T13.TO1.03 (including all TOs referenced in the TO Table) and T13.TO2.01 to T13.TO2.43 in Annex 3; T16.TO2.27 in Annex 6; T17.TO2.26 in Annex 7; and T18.TO2.08 in Annex 8.

57 As a result of the GDA Step 4 assessment of:

- EDF and AREVA's demonstration of conformance to the HSE SAPs;
- the safety case CAE trail as presented in the PCSR; and
- **RO-UKEPR-62** submissions,

it is concluded that, while an acceptable approach has been developed, there remain significant areas for improvement (related to GDA Issue Action **GI-UKEPR-CI-03.A1**).

4.1.2 Step 4 Findings

58 The GDA Issue identified in the section above is also recorded in Annex 2.

4.1.3 GDA Issue Close-out Assessment

59 Within this section I address the resolution of **GI-UKEPR-CI-03** on the PCSR and SAPS conformance CAE trails. This section also addresses **GI-UKEPR-CC-02** on review of the C&I sections of the consolidated final GDA submission and design changes.

4.1.3.1 PCSR and SAPS Conformance Claims, Argument, Evidence Trails - GI-UKEPR-CI-03

60 GDA Issue **GI-UKEPR-CI-03** requires EDF and AREVA to revise and improve the clarity of the CAE documentation for the UK EPR™ PCSR C&I sections' key claims and C&I SAPs conformance demonstration.

61 EDF and AREVA identified two documents in their Resolution Plan (Ref. 70) responding to the GDA Issue, these covered the:

- PCSR key claim CAE trail (Ref. 89); and
- SAPs conformance demonstration CAE trails (Ref. 91).

62 The submissions were reviewed; the former during the GDA Issue close-out phase and the latter during GDA Step 4 (see Section 4.1.1 above). During the GDA Issue close-

out phase a single TQ (i.e. TQ-EPR-1482, Ref. 86) was raised. As appropriate, the submitted documents were revised by EDF and AREVA to address the points in the TQ and identified in the GDA Issue. The scope of work undertaken by the TSC and the TOs arising from its work are contained in a TSC report (Ref. 76). Annex 13 provides a summary of the TSC's report including details of the TOs raised.

63 The PCSR CAE document (Ref. 89) presents the CAE trails in tabular form. The six high level claims (e.g. "The I&C conforms to standards appropriate to its category and class.") are broken down into 40 key claims (e.g. "All I&C systems important to safety are designed, manufactured and installed to standards appropriate to their class."). The 40 key claims are further divided into a total of 130 sub claims. For each of the 130 sub-claims there is a table that contains entries for the 'High level claim', 'Key claim', 'Sub-claim', 'Argument', 'Evidence' and 'Related claims'.

64 The PCSR CAE document (Ref. 89) fell short of my expectations (i.e. as defined in the SAPs and relevant guidance). The origin of the high level and key claims were not identified. The relationship of the high level claims, the key claims and sub-claims was unclear. The source of the sub-claims and their links to the PCSR were not well defined. The development of the arguments to link the claims and the evidence were incomplete (e.g. the 'Argument' was essentially a further claim).

65 I raised TQ-EPR-1482 (Ref. 86) to convey the review outcome to EDF and AREVA. EDF and AREVA's response included examples demonstrating how the matters identified in the TQ (see above) would be addressed in a revision of the PCSR CAE document (Ref. 89). EDF and AREVA also made numerous commitments in the TQ response to include evidence in the CAE trails from current GDA Issue resolution work and from future system development and commissioning work.

66 In addition to TQ-EPR-1482, I raised a meeting action (i.e. TATS GI 13-I&C-1, Ref. 170) that requested clarification of the source of the high level and key claims. EDF and AREVA's response (letter EPR01327N, Ref. 93) clarified the source as the PCSR and plant C&I requirements specification (Ref. 94). The plant C&I requirements are derived from the European Utility Requirements for LWRs (Ref. 95).

67 The revised PCSR key claim trail document (Ref. 90) provided a demonstration that the high level and key claims had been met, using the same tabular approach as in the previous revision (Ref. 89). Tables are presented for the 40 key claims and sub-claims are no longer used. My review revealed significant improvements had been made to the document. The table entry previously used for sub-claim now explicitly identified the sources of the key claims in the safety documents and included references to the plant C&I requirements document (Ref. 94) and PCSR (Ref. 62). The arguments presented provide a narrative link between the claims and evidence indicating how the evidence supports the claim. The table entry for evidence includes identification of the evidence to be generated during the Site Specific Phase (SSP). I identified areas where the clarity of the arguments could be improved and that a significant amount of the evidence is still to be included in the CAE trails (e.g. from the resolution of GDA Issues and future C&I system development).

68 EDF and AREVA's SAPs compliance CAE trails are also presented in tabular form. There is a table with entries for 'Claim', 'Argument' and 'Evidence' for each SAP and for each of the guidance paragraphs that accompanies the SAPs. I reviewed EDF and AREVA's revised compliance document (Ref. 92). I concentrated on a sample of those trails identified in GDA Step 4 as not having demonstrated an acceptable level of SAP conformance. I established that the shortfalls in the arguments and evidence, identified in the GDA Issue (Ref. 70) and associated TOs, had been addressed to produce an

adequate CAE trail. I also identified areas for improvement and completion. For example, some SAPs and related guidance paragraphs were not fully addressed, and in many cases the evidence to substantiate the claims and arguments is not currently available. In the latter case, the sources of evidence are identified (e.g. as that from GDA Issue resolution and from completion of the C&I systems' development lifecycles) and the evidence will become available during the SSP.

69 Following assessment of EDF and AREVA's submissions in response to GDA Issue **GI-UKEPR-CI-03** on the adequacy of the CAE trails, I am content that the information contained in the revised documents (Refs 90 and 92) together with the commitment to complete the CAE trails during the SSP is sufficient to close the GDA Issue. I have raised an Assessment Finding below to capture the matters arising from my assessment that need to be addressed in completing the CAE trails.

*GDA Assessment Finding: **AF-UKEPR-CI-034** – The Licensee shall:*

- *Revise the SAPS conformance CAE trails (Ref. 91) to ensure, as appropriate, the claims and argumentation for each SAP <u>and</u> its guidance paragraphs are fully addressed (see also **AF-UKEPR-010**, **AF-UKEPR-023** and **AF-UKEPR-028**) in the CAE trails.*
- *Include the additional claims, arguments and evidence generated during closure of the GDA Issues into the PCSR key claims (Ref. 89) and SAPS conformance CAE trails (Ref. 91).*
- *Reference the evidence generated during C&I systems' development, installation and commissioning in the PCSR key claims and SAPS conformance CAE trails.*

For further guidance on the completion of the CAE trails see Technical Observations GICI03.TO2.01 and GICI03.TO2.02, in Annex 13 for PCSR key claims, and GICI03.TO2.03, GICI03.TO2.*04 and* GICI03.TO2.*05 in Annex 13 and GICI06A9.TO2.17 in Annex 16 for SAP conformance.*

[Required Timescale: prior to power raise.]

4.1.3.2 Assessment of the Consolidated Final GDA Submission - GI-UKEPR-CC-02

70 GDA Issue **GI-UKEPR-CC-02** requires EDF and AREVA to deliver a final consolidated version of the PCSR as a key reference to the DAC to be issued at the end of GDA. GDA Issue **GI-UKEPR-CC-02** also required EDF and AREVA to provide an update of the Design Reference (Ref. 107) to include all design changes agreed for inclusion during GDA and to provide a design definition.

4.1.3.2.1 Final Consolidated PCSR

71 This section covers updates to the PCSR made to address resolution of the C&I GDA Issues and how Step 4 comments on the PCSR have been progressed. EDF and AREVA supplied a consolidated version of the PCSR at the end of Step 4 (Ref. 96). This was reviewed for factual accuracy and completeness and points for clarification were raised in letter EPR70323R (Ref. 97). The points raised on C&I matters included:

- elimination of inconsistencies in system and interface descriptions;
- clarification of CAE evidence trails;
- addition of references and referencing nomenclature; and

- scope omissions, principally associated with safety justifications.

The points identified were progressed under GDA Issue **GI-UKEPR-CC-02 Action 3** task 2 (Ref. 98). EDF and AREVA provided part responses to the points above in Refs 99, 100 and 101. I provided additional comments on the draft final PCSR sub-chapters in TQ-EPR-1631 (Ref. 86).

72 EDF and AREVA provided a final version of PCSR sub-chapters 7.1 to 7.7 (Refs 171 to 177) under cover of letters EPR01443N and EPR01452N (Refs 103 and 104). I have reviewed these sub-chapters against the points of clarification raised in letter EPR70323R (Ref. 97). I confirmed that EDF and AREVA had addressed the significant points raised (see the consolidated PCSR Step 4 review closure matrix, Ref. 105). For example, by extending the descriptions of the systems and safety arguments for diversity and standards compliance . Additional references and text addressing the close-out of the GDA Issues have also been included in the PCSR. I identified the need for (raised in PCSR review pro-forma entitled 'PCSR Chapter Review for CI Rev 2', Ref. 106) additional information in respect of capturing descriptions of existing justifications (i.e. for programmable complex electronic components, the UNICORN platform and NCSS) and elimination of inconsistencies (i.e. in the status of the PICS and the interfaces between the Class 1 PS and other systems) within the PCSR.

73 Following assessment of EDF and AREVA's submissions in response to GDA Issue **GI-UKEPR-CC-02** on provision of a final consolidated PCSR, I am content that the information provided is adequate and this element of the GDA Issue can be closed. I have raised an Assessment Finding below to capture the matters arising from the assessment that need to be addressed in development of the PCSR during the SSP.

*GDA Assessment Finding: **AF-UKEPR-CI-035** – The Licensee shall address the open points on the PCSR summarised below by updating the PCSR to:*

- *include the justification of the adequacy of programmable complex electronic components;*
- *include the UNICORN platform and NCSS justifications; and*
- *address the inconsistencies in the status of the PICS and the interfaces between the Class 1 PS and other systems.*

Further guidance on open points to be addressed in the development of the PCSR is provided in PCSR review pro-forma 'PCSR Chapter Review for CI Rev 2', *Ref. 106.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site]

4.1.3.2.2 Design Change Assessment

74 GDA Issue **GI-UKEPR-CC-02** requires EDF and AREVA to undertake the management and acceptance of changes to GDA submission documentation impacted by design changes agreed for inclusion in GDA. Change Management Forms (CMFs) are submitted by EDF and AREVA in order to obtain agreement that the changes can be included within GDA. The full list of CMFs covered by the C&I assessment that have been agreed for inclusion in GDA is presented in Annex 10. These CMFs address topics directly related to the close-out of C&I GDA Issues and cover, amongst others:

- Provision of Class 1 displays and controls (CMF 26 - introduction of Class 1 displays and controls in the MCR (SICS and Protection System Operating Terminal

(PSOT)) and the RSS (PSOT), and CMF 27 - upgrade of the SICS displays and controls to Class 1).

- Impact analysis of the change of SPPA-T2000 platform version from version S5 to S7 (CMF 29).
- Classification (CMF 40 - functional scope allocation of main reactor controls to Class 2 system (RCSL or SAS), CMF 60 - classification of maintenance and testing tools and CMF 61 - classification of the Rod Pilot to be Class 2).
- Safety justifications for CBSIS (CMF 62 - qualification of smart devices and CMF 63 - PE and ICBMs for software based C&I systems).
- Diversity justification (e.g. CMF 64 - sensors and sensor conditioning, CMF 65 - PAC modules and CMF 67 - addition of secondary side (VVP) pressure measurements to provide improved sensor diversity).
- PS reference configuration (CMF 15 - changes in the communication between the PS and other systems and CMF 66 - analysis of signals from the SAS / PAS to the PS, update to delete the signal for the periodic test of Emergency Feedwater Pump (EFWP)).
- Introduction of the NCSS (CMF 14 - introduction of the non-computerised C&I back up system, the NCSS and CMF 68 - additional functionality provided on the NCSS).
- C&I reference configuration, 2008 design freeze consistency review (CMF 81 presents five changes that provide enhancements to the C&I design such as provision of a separate Class 2 SAS network).

75 I have reviewed the C&I related CMFs submitted for inclusion in GDA and am content that a satisfactory position has been reached in relation to close-out of GDA. The majority of the C&I related CMFs address topics directly related to the close-out of C&I GDA Issues as discussed elsewhere in this report.

4.1.3.2.3 Design Definition

76 GDA Issue **GI-UKEPR-CC-02** required EDF and AREVA to provide a design definition. The text below addresses resolution of the C&I aspects of GDA Issue **GI-UKEPR-CC-02** on design definition.

77 EDF and AREVA stated that the UK reference design is defined principally by System Design Manuals (SDMs) together with specific design changes (Ref. 107). EDF and AREVA subsequently stated (Ref. 109) that UK specific C&I SDMs would not be available during GDA. Following discussion on the way forward, it was agreed (under action TATS GI 11-I&C-3, Ref. 110) that the design definition would be based on a demonstration that design documentation equivalent to a System Requirements Specification (SRS) (i.e. as defined in BS IEC 61513:2001 (Ref. 10) clause 6.1.1) was in place. To support this demonstration it was agreed that EDF and AREVA would provide:

- A matrix to show how each of the requirements in BS IEC 61513:2001 for a SRS is met for the SAS and PS.
- A description of the process that is followed for each of six systems (i.e. TXS platform based systems – PS, RCSL, SA I&C and PIPS; and SPPA-T2000 (version S7) platform based systems – SAS and PAS).

78 The submissions were reviewed and one TQ was raised on this topic. As appropriate, the submitted documents were revised by EDF and AREVA to address the points

identified in the TQ and GDA Issue. The scope of work undertaken by the TSC and the TOs arising from its work are contained in a TSC report (Ref. 111). Annex 18 provides a summary of the TSC's report including details of the TOs raised.

79 EDF and AREVA provided a mapping of the Flamanville 3 PS specification documents (Ref. 113) to the requirements of clause 6.1.1 of BS IEC 61513:2001 in letter EPR01238N (Ref. 112). My review of the mapping (Ref. 113) confirmed that a compliance argument and evidence are present for all parts of clause 6.1.1 bar one, on trip margins (6.1.1.1.1 a) 1)). EDF and AREVA stated that this information is currently unavailable and the values will be set on design finalisation.

80 The mapping is supported by a set of 51 references covering four categories, namely: 'Functional requirements', 'Interfaces', 'System specification and concepts', and 'Platform'. My review included an examination of a sample of the evidence contained in the referenced documents (i.e. in order to determine whether the evidence met the requirements of the BS IEC 61513:2001 clause 6.1.1 sub-clauses that it was claimed to address).

81 I reviewed documents 'EPR FA3 Functional Description of RRC-A C&I Functions - NEPR-F DC 52' (Ref. 114) and 'Reactor Trip Concept - NLE-F DC 124' (Ref. 115) identified in the 'Functional requirements' and 'Interfaces' categories respectively. I found that the evidence presented was comprehensive but not complete (e.g. parameter ranges, response times and accuracy were not defined for the Risk Reduction Category A (RCC-A) functions).

82 I requested (TQ-EPR-1624, Ref. 86) the provision of additional documents that provided evidence of the definition of 'Functional requirements'. EDF and AREVA provided a number of documents including a trip function specification (Ref. 117). I found the document to be adequate as a specification. In particular, it included the specification of the performance requirements (i.e. parameter ranges, response times and accuracy) identified as missing for the RCC-A functions above.

83 I also reviewed document 'Protection System detailed specification file - NLE-F DC 38' (Ref. 116), from the 'System specification and concepts' category (see above) as it is claimed extensively in the mapping. I established that it is in the form of a SRS, is comprehensive and responds to each of the sub-clauses it is claimed against. The document and sub-clause responses made extensive use of references, which while not reviewed in detail were confirmed as having appropriate content. Some omissions were identified (e.g. the definition of extreme environmental conditions) and these will need to be addressed (see below) in the production of a complete SRS.

84 I concluded, on the basis of my sample review, that the mapping (Ref. 113), system description document (Ref. 116) and supporting references in the main contain or reference the information that is required for a PS SRS.

85 EDF and AREVA stated in letter EPR01360N (Ref. 118) that the SRSs for other systems based on the TXS platform are created in the same way as that for the PS. The letter identified the RCSL, SA I&C, and PIPS specification documents (Refs 119, 120 and 121), these are the equivalent documents to the PS system description document (Ref. 116). My review of these documents identified that they contained similar information to, and the same types of referenced material as the PS system description (Ref. 116). A detailed review of the RCSL document (Ref. 119) established that, for the majority of BS IEC 61513:2001 clause 6.1.1 sub-clauses, appropriate information could be readily identified. I concluded that this is sufficient to demonstrate that an adequate design definition, equivalent to an SRS, is in place for the RCSL and hence also for the SA I&C and PIPS systems based on the TXS platform.

86 EDF and AREVA provided document 'Mapping the SAS documentation to the requirements of BS IEC 61513:2001 clause 6.1.1 - ECECC121435' (Ref. 122). The mapping was supported by 41 referenced documents in 4 categories: 'General', 'System Design Manuals (SDMs)', 'Standards', and 'Technical Specifications and Conditions for Standard I&C Systems' (CSCT). The majority of the documents fell into the last two categories of 'Standards' and CSCT.

87 My review of Ref. 122 confirmed that all sub-clauses of BS IEC 61513:2001 clause 6.1.1 are addressed. The discussion and evidence presented in the mapping identified equivalent EDF and AREVA requirements documents (i. e. specification of what is required) and some limited evidence of how the requirement had been met by the SAS. For example, for system classification, the identified evidence is the scheme used to classify systems (Ref. 123). Similarly, for accuracy and response time the identified evidence is a generic requirements document (Ref. 124). The mapping identifies that the functional requirements for the SAS are contained in the SDMs. A document defining the content of an SDM (Ref. 125) and a sample SDM were identified in the mapping.

88 My review of the SDMs' contents document (Ref. 125) found it consistent with that of a requirements specification document as defined in BS IEC 61513:2001. My review of a sample SDM, for the raw water circulation system (Ref. 126), found it to be incomplete. The omissions are due to the fact that at the time of the review the design had not been completed. Nevertheless, my review confirmed that it met the SDM requirements specification (Ref. 125) and also addressed the BS IEC 61513:2001 sub-clause requirements. I conclude that the mapping (Ref. 122) and supporting references identify information in alignment with the requirements of a SRS for the SAS.

89 EDF and AREVA provided a document (Ref. 127) that explained the approach to demonstrating the SAS design definition aligns with the SRS requirements, is equally applicable to the PAS. EDF and AREVA state that the set of documents supporting the PAS are generated by following the same engineering process as the SAS. The PAS functional and interface requirements are contained in the SDMs. EDF and AREVA state that there are circa 250 SDMs for the PAS. The PAS requirements are based on the equivalent 'Standards' and CSCT as the SAS but take into account the PAS's Class 3 classification.

90 I confirmed that the same engineering process is defined for the PAS and the scope of the requirements identified to be addressed in the PAS specification is the same as the SAS. I conclude that the approach set out by EDF and AREVA for the SAS is equally applicable to the PAS and that the information identified is in alignment with the requirements of a SRS for the PAS.

91 Following assessment of EDF and AREVA's submissions in response to GDA Issue **GI-UKEPR-CC-02** on the design definition of the C&I systems, I am content that the information provided is adequate and this element of the GDA Issue can be closed.

92 The TXS systems (i.e. PS, RCSL, SA I&C and PIPS) Quality Assurance (QA) plan (Ref. 128) requires compliance with BS IEC 61513:2001 and the production of a SRS (i.e. document D-01.4 'System Requirements Specification' referenced in Table 2 and Step S-01 etc. of the QA plan, Ref. 128). The PE arguments for both TXS based systems and SPPA-T2000 based systems (i.e. SAS, PAS, SAS Risk Reduction Category B (RRC-B) and PICs) (Refs. 85 and 88) also require compliance with BS IEC 61513:2001. The need for a demonstration of compliance with standards, including BS IEC 61513:2001, hence production of a SRS, was identified during GDA Step 4 and is addressed by **AF-UKEPR-CI-002**.

93 I identified a number of points that need to be addressed during the production of a comprehensive SRS including:

- Inclusion of missing content (e.g. on security plans and definition of interfaces).
- Inclusion of specification details (e.g. defining the margins between set-point limits and allowable values for the trip functions, and specification of extreme ranges of environmental conditions).
- Definition of the means of verifying the SRS to confirm all relevant functional definitions (e.g. as contained in SDMs) have been identified and that all the requirements are traceable.

94 I have added further guidance on these points (i.e. as provided by TSC observations GICC02.TO2.01 to 04 in Annex 18) to **AF-UKEPR-CI-002,** which seeks standards compliance demonstrations including for BS IEC 61513:2001 that requires production of an SRS for the C&I systems.

4.1.3.2.4 Consolidated Final GDA Submission Assessment Conclusion

95 I have reviewed the C&I sections of the final consolidated version of the PCSR, C&I related CMFs submitted for inclusion in GDA and C&I design definition submissions. I am content that a satisfactory position has been reached and that there are no C&I related matters that would prevent closure of GDA Issue **GI-UKEPR-CC-02**. I have raised Assessment Finding **AF-UKEPR-CI-052** below to capture the need for fully developed safety cases to be produced, which address the C&I CMFs submitted during GDA and the development of the safety cases outlined in the Basis of Safety Cases (BSCs) produced in response to the C&I GDA Issues (i. e. for the NCSS, PSOT and SPPA-T2000 version change).

*GDA Assessment Finding: **AF-UKEPR-CI-052** - The Licensee shall ensure that fully developed safety cases are produced that address:*

- *the C&I CMFs submitted during GDA; and*
- *development of the safety cases outlined in the Basis of Safety Cases (BSCs) produced in response to the C&I GDA Issues (i.e. for the NCSS, PSOT and SPPA-T2000 version change).*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

4.1.4 GDA Close-out findings

96 The Assessment Findings identified in the section above are also recorded in Annex 1.

4.2 C&I Systems' Classification and Standards

4.2.1 Step 4 Assessment

97 This section reports my assessment of the company level (i.e. non-project specific) standards and guidance for C&I SIS relevant to the UK EPR™. This assessment supports the assessment reported under Section 4.3 (covering the assessment of the C&I SIS platforms and pre-developed equipment proposed for the UK EPR™) and Section 4.4 (covering the assessment of the C&I systems, hosted on the equipment as covered by Section 4.3). There was no equivalent assessment of company level standards and guidance reported under GDA Step 3.

98 The C&I TSC's work provided support to my assessment. The description of the scope of work performed by the TSC and the TOs arising from the work are described in a TSC report (Ref. 29). Annex 4 provides a summary of the TSC's work (Ref. 29), which includes all of the TOs.

99 The assessment of the adequacy of EDF and AREVA's company level (i.e. generic rather than project specific) C&I SIS standards was performed in a progressive, logical and thorough manner and was effectively a four step process as shown below.

1) Determination of the relevant C&I SIS standards (i.e. those defining relevant good practice) considered applicable to EDF and AREVA's company level standards. This included consideration of relevant HSE SAPs.

2) Identification of the company Quality Management System (QMS).

3) Review of the relevant RP's company level standards and identification of differences between these standards and those documents defining relevant good practice.

4) Determination of the significance of observations arising from the review, and consideration of the GDA Issues or Assessment Findings that should be raised to address any concerns.

100 I consider relevant good practice for C&I SIS to be defined in a suite of international standards produced by the International Electro technical Commission (IEC) based in Geneva. Standards are developed by multi-disciplined committees and are subject to international review and voting prior to issue. Issued standards are regularly reviewed and revised, as necessary, to address improvements in technologies and techniques.

101 The British technical committee NCE/8 'Reactor Instrumentation' nominates UK technical experts to the IEC committees that develop and maintain the international C&I standards. The IEC standards relevant to this assessment are identified in 'BSi Technical Committee NCE/8 Nuclear Power Plants - I&C Systems, A Guide to Applicable IEC Standards, AFP – v7 – 2008_12_01' (Ref. 37). I also considered relevant HSE SAPs (e. g. EQU.1, ECS.1, ECS.2 and ECS. 3) under this aspect of my assessment.

102 The requirement for assignment of functions to categories and systems to class is set out in HSE SAPs ECS.1 and ECS.2. The relevant IEC C&I nuclear sector standard for categorisation of C&I functions is BS IEC 61226:2009 (Ref. 44). BS IEC 61226:2009 essentially uses deterministic criteria to place C&I functions into one of three safety Categories (i.e. A, B, or C) or identify them as non-safety / not categorised.

103 The IEC C&I nuclear sector SIS standards form a hierarchy with the top level standard BS IEC 61513 covering general requirements for SIS and overall C&I architectural requirements (Ref. 10). This standard is the nuclear sector equivalent of the generic IEC industry standard on functional safety of electrical / electronic / programmable electronic safety-related systems (see BS EN 61508 - Ref. 40), where safety-related covers all SIS.

104 Sitting below BS IEC 61513 in the hierarchy of IEC nuclear sector standards are standards addressing:

- software for CBSIS performing Category A functions (i.e. the highest safety significance), BS IEC 60880 (Ref. 17);
- software for CBSIS performing Category B and C functions, BS IEC 62138 (Ref. 36); and

- hardware design requirements for CBSIS Class 1 and 2 systems, BS IEC 60987 (Ref. 18).

EDF's QMS refers to a document produced by AFCEN (French Society for Design and Construction Rules for Nuclear Island Components) titled 'RCC-E Design and Construction Rules for Electrical components of nuclear islands' (Ref. 24). Each of the IEC standards previously mentioned in this paragraph is explicitly referenced by RCC-E, although not all relevant clauses are referenced (see T14.TO2.5 in Annex 4). Also, no guidance with respect to the use of Programmable Complex Electronic Components (PCECs) was found within RCC-E (see T14.TO1.02 in Annex 4).

105 In addition to the top-level IEC standards identified above, there are a range of supporting standards, covering topics such as equipment qualification, requirements in respect of common cause failure, segregation, and instrument and sensor specific standards (See Ref. 37).

106 Not all of the relevant requirements of the standards identified in Ref. 37 are explicitly referenced by RCC-E. However, EDF and AREVA have stated that, in addition to those standards' requirements referenced in RCC-E, other relevant standards' requirements will be referenced in project specific documents. Therefore, I have concluded that RCC-E provides necessary but not sufficient requirements and guidance for C&I SIS.

107 The use and application of relevant good practice, as defined by international standards, is an essential component of the required safety case for C&I SIS. The Licensee will need to ensure that the requirements of IEC standards not referenced by RCC-E, and as appropriate to the C&I SIS employed in the UK EPR™, are addressed in the C&I SIS lifecycle. The lifecycle covers design, procurement and implementation processes, etc.

108 In response to TQ-EPR-473 (see Ref. 7), EDF and AREVA have committed to specifying all relevant IEC standards (as identified in Ref. 37) by the use of project specific documents where necessary[2]. The following Assessment Finding is raised to cover this issue for all SIS.

*GDA Assessment Finding: **AF-UKEPR-CI-001** -The Licensee shall ensure that where RCC-E does not explicitly reference the requirements of relevant IEC SIS standards, or standard revisions (as appropriate to the C&I SIS employed in the UK EPR™) these requirements are adequately addressed in the C&I SIS lifecycle covering design, procurement and implementation processes, etc. For further guidance see T14.TO1.01, T14.TO1.03, T14.TO2.01, T14.TO2.02, T14.TO2.03, T14.TO2.04, T14.TO2.05 and T14.TO2.06 in Annex 4.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

Note: GDA Issue Action **GI-UKEPR-CI-06.A3** covers this issue for the PS.

109 EDF and AREVA are to provide detailed compliance matrices for a number of IEC standards (e.g. BS IEC 60880:2006 (Ref. 17)). However, these have not been provided within the time frame of this review (see T15.TO2.06 in Annex 5). I have raised the following finding to ensure production of a comprehensive demonstration of

[2] There is one exception, and that is for IEC 6150 4:2000 (Ref. 58), for which further justification is required, see **AF-UKEPR-CI-001,** T14.TO1.01 in Annex 4.

PS (TXS), and SAS / PAS (SPPA-T2000) compliance with the key international standards.

> *GDA Assessment Finding: **AF-UKEPR-CI-002** - The Licensee shall demonstrate the compliance of the PS and associated platform with BS IEC 61513:2001, BS IEC 60880:2006 and BS IEC 60987:2007, and SAS / PAS and associated platform with BS IEC 61513:2001, BS IEC 62138:2004 and BS IEC 60987:2007. This demonstration should address platform and system requirements separately. The demonstration shall include the supporting evidence generated as the designs are completed. For further guidance see T20.A1.5.2 in Annex 9; T15.TO2.05, T15.TO2.06, T15.TO2.08, T15.TO2.09, T15.TO2.10, T15.TO2.11, T15.TO1.39, T15.TO2.43 and T15.TO2.44 in Annex 5; T16.TO1.01, T16.TO2.11, T16.TO2.28, T16.TO2.29 and T16.TO2.31 in Annex 6; GICI06.A2.TO2.07, GICI06.A2.TO2.08, GICI06.A2.TO2.09, GICI06.A2.TO2.12, GICI06.A2.TO2.13, GICI06.A2.TO2.15 and GICI06.A2.TO2.16 in Annex 16, and GICC02.TO2.01 to 03 in Annex 18*.
>
> [Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

110 My GDA Step 4 assessment included a specific detailed review of a number of key Standards topics such as requirements management, independent verification and validation, and configuration management. With regard to configuration management, I found that while the standards' clauses required by RCC-E addressed configuration management at the level of individual C&I SIS, they did not address configuration management of the total C&I architecture. An overall Quality Plan (Ref. 63) was provided for assessment, and this set out the high level configuration management processes to be followed. However, the following finding is raised to ensure that configuration management arrangements are fully established for the UK EPR™ C&I architecture, including all SIS.

> *GDA Assessment Finding: **AF-UKEPR-CI-003** - The Licensee shall demonstrate that adequate company-level processes, or UK EPR™ project-level processes are established for configuration management of the set of all structures, systems and components that comprise the UK EPR™ C&I architecture including all SIS, which should be addressed within an overall Quality Assurance Plan or equivalent, as required by BS IEC 61513:2001 clause 5.4.1. For further guidance see T14.TO1.03 in Annex 4.*
>
> [Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

111 The application of relevant good practice to C&I SIS should be graded based upon the categorisation of safety functions as defined in BS IEC 61 226:2009 (Ref. 44) and the classification of systems which perform such functions, as defined in BS IEC 61513:2001 (Ref. 10). The document referenced by EDF's QMS, RCC-E (Ref. 24), defines three Categories (i.e. F1A, F1B, F2) and Non-Categorised (NC); and three Classes (i.e. E1A, E1B, E2) and NC. These are similar but not identical to the Categories defined by Ref. 13 and the Classes defined by Ref. 10.

112 The need to adequately address categorisation and classification for the C&I aspects of the UK EPR™ was raised in regulatory issue **RI-UKEPR-002** and was progressed under a "transverse / cross-cutting" RO (i.e. an issue covering more than one assessment discipline) on categorisation and classification, **RO-UKEPR-43** (see Ref. 20).

113 A number of detailed queries were raised under **RO-UKEPR-43** and submissions have been received from EDF and AREVA on this matter. The submissions included a commitment (see Ref. 42) to provide evidence to demonstrate that the classification of C&I systems is consistent with relevant good practice (e.g. to ensure that the class of the C&I systems such as the PAS and SAS align with expectations). A cross-cutting GDA Issue has been raised which contains a specific action addressing C&I categorisation and classification (i.e. cross-cutting GDA Issue Action CC-01.A6) and this is discussed further in Sections 2.3.4 and 4.5.

114 The C&I GDA Step 3 report raised two concerns (see Section 2.3.1), which have been considered further by the assessment work performed under GDA Step 4. One concern relates to the alignment of EDF and AREVA's safety categorisation and classification scheme to HSE SAPs and standards (see first bullet point below), and the other to clarification of the standards used by EDF and AREVA (see second bullet point). Both of these concerns have been addressed under GDA Step 4 as follows.

- EDF and AREVA have proposed four levels of categorisation for the UK EPR™ (F1A, F1B, F2 and NC) and four levels of classification (E1A, E1B, E2 and NC) and, although there are similarities, these levels do not fully align with HSE SAPs (Ref. 4) or BS IEC 61226 (Ref. 13). Cross-cutting GDA Issue Action CC-01.A6 has been raised on categorisation and classification (see above).
- EDF's QMS references RCC-E (Ref. 24) for requirements for SIS, and RCC-E references standards which are considered to constitute relevant good practice (e.g. BS IEC 60880:2006 (Ref. 17) and BS IEC 62138:2004 (Ref. 36)). The issue of the adequacy of EDF and AREVA's standard's coverage has already been considered in Section 4.2. EDF and AREVA have committed to provide a number of compliance matrices against relevant international standards, but these were not made available within the time frame of this review. I have raised GDA Issue Action **GI-UKEPR-CI-06.A3** to cover the general issue of the demonstration of the adequacy of CBSIS, and a specific Assessment Finding (see **AF-UKEPR-CI-002**) to cover the compliance of the PS and SAS / PAS with key standards.

115 EDF and AREVA undertook a review of standards applicable to the security of CBSIS and has proposed an acceptable way forward in relation to implementation of a security management system for CBSIS including selection of a security assessment methodology. The following Assessment Finding is raised to address the implementation of these proposals.

GDA Assessment Finding: ***AF-UKEPR-CI-004*** *- The Licensee shall:*

i) demonstrate that its CBSIS security management system aligns with appropriate standards such as ISO/IEC 27001 (Ref. 43); and

ii) implement a CBSIS security assessment methodology that uses the UK government standard methodology as its foundation.

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

116 As a result of my assessment I conclude the following.

- EDF and AREVA's company-level (i.e. non-project specific) standards and guidance provide necessary but not sufficient requirements for the UK EPR™ C&I SIS. The company level standards will require augmentation with project-specific standards and guidance. Note that the issue of the use of appropriate standards is discussed further under Sections 4.3 and 4.4, covering UK EPR™ platforms and systems.

- Although a way forward with respect to categorisation and classification of UK EPR™ C&I SIS and equipment has been proposed, which may address my concerns in this area, further assessment of the response to the associated GDA cross-cutting Issue is required.
- An acceptable way forward has been proposed in relation to the security of CBSIS.

4.2.2 GDA Step 4 Findings

117 The Assessment Findings recorded in the section above are listed in Annexes 1 and 2 respectively.

4.3 C&I SIS Platforms and Pre-Developed Equipment

4.3.1 GDA Step 4 Assessment

118 This section describes the outcome of the assessment of C&I SIS platforms and pre-developed SIS equipment for the UK EPR™ including the implementation of project specific standards and guidance. This assessment complements the assessment of the adequacy of company level standards and guidance reported in Section 4.2. The next section, Section 4.4, considers the implementation of standards and guidance relevant to C&I SIS (hosted on the platforms and equipment as covered by this section) of the UK EPR™. Progress with resolution of the relevant GDA Step 3 observations is also specifically identified and reported.

119 My assessment was supported by the work of the C&I TSC. The description of the scope of work performed by the TSC and the TOs arising from the work are described in a TSC report (Ref. 30). Annex 5 provides a summary of the TSC's report (Ref. 30) including details of the TOs raised.

120 The topic of the compliance and alignment of EDF and AREVA's categorisation and classification methodology with relevant good practice is discussed in Section 4.2. Assessment Finding **AF-UKEPR-CI-002** was raised in Section 4.2 requiring that a demonstration of compliance of the PS and SAS/PAS, and associated platforms with relevant standards be provided. This includes the provision of a number of compliance matrices against relevant international standards which are applicable to the platforms discussed in this section (e.g. see T15.TO2.05, T15.TO2.06 and T15.TO2.09 in Annex 5 which relate to the TXS platform).

121 A risk-based approach to assessment was followed, with the greatest assessment effort allocated to those platforms and pre-developed equipment performing the most important nuclear safety functions. All assessment was performed on a sample basis.

4.3.1.1 Assessment of the Teleperm XS Platform

122 The PS platform proposed for the UK EPR™ is Teleperm XS (TXS) produced by AREVA. Due to the many protection functions performed by the Class 1 PS and the high reliability claims made for this system, this platform was the main focus of the GDA Step 4 assessment.

123 TXS is AREVA NP's nuclear plant C&I safety system platform. This platform was developed specifically for use in the SS of nuclear power plant. Relevant nuclear

sector standards available at the time of the development of TXS were used to guide the development process (e.g. IEC 880:1986, see Ref. 17 for the current issue of this standard).

124 The scope of the platform includes the hardware components, software components and the software tools required for engineering, testing, commissioning, operation and maintenance. The qualification of the platform, including seismic qualification, was within the scope of my assessment.

125 The initial assessment of the adequacy of the TXS platform was based upon a review of documentation provided by EDF and AREVA. A number of TQs were raised as a result of this review and EDF and AREVA provided further documentation in response to those queries. In order to improve understanding between the designers and assessors, a series of technical meetings were held where issues such as the original process used to develop the platform, independent software verification, version control and the use of tools during development were reviewed. Some of these meetings were held at the London offices of AREVA where a network link to AREVA's offices in Germany was made available. This link facilitated the review of internal company documentation on-line. These facilities were also made available for the review of the PS (see Section 4.4).

126 One of the key requirements of Ref. 17 is that SSs exhibit deterministic characteristics, and under this assessment platform characteristics such as 'predictability of execution and communication' and 'memory management' were reviewed. From the samples assessed under this review, no platform characteristics were revealed which compromised this design principle. Deterministic operation is an important factor when considering the suitability of this platform for protection system use.

127 The extent and rigour of self checking for errors, and the safe handling of any errors detected by self checking, is also a key factor I considered for this platform. A number of aspects of the design of this system concerning self checking and error handling were assessed during the GDA Step 4 review. Although no system characteristics were revealed which compromised the ability of this platform to host Class 1 systems, a number of TOs have been raised in relation to demonstrating the adequacy of self checking and error handling (i.e. T15.TO2.33, T15.TO2.34 and T15.TO2.35 in Annex 5, and T17.TO2.05 in Annex 7).

> *GDA Assessment Finding: **AF-UKEPR-CI-005** - The Licensee shall produce a comprehensive demonstration of the adequacy of Teleperm XS self checking and error handling. For further guidance see T15.TO2.33, T15.TO2.34 and T15.TO2.35 in Annex 5; and T17.TO2.05 in Annex 7.*
>
> [Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

128 TXS is a distributed computing system which may be used in various configurations depending upon the requirements of a particular application. The TXS platform supports a four-train redundant configuration, and this is the configuration proposed for the UK EPR™. The ability to support this configuration is an important factor when considering the suitability of the TXS platform for protection system use.

129 Many protection system platforms available commercially today are based on non-nuclear equipment which has been qualified for nuclear sector use some time after the original development. From the results of my assessment I have determined this is not the case for TXS, as the nuclear sector standards available at the time of the original

development (some 20 years ago) were applied to guide the development process. The use of nuclear sector standards from the early stages of development is an important factor when considering the suitability of this platform for protection system use.

130 However, although EDF and AREVA have agreed to provide detailed compliance matrices for a number of IEC standards (e.g. BS IEC 60880:2006, (Ref. 17)) these have not been provided within the time frame of this review (see T15.TO2.06 in Annex 5). I have raised GDA Issue Action **GI-UKEPR-CI-06.A3** which requires that further evidence be provided covering software PE. An important component of the required evidence is further demonstration of compliance against relevant international standards. An Assessment Finding has been raised under Section 4.2 to cover the issue of compliance of the TXS platform against relevant standards (see **AF-UKEPR-CI-002**).

131 The information exchanged at technical meetings and responses to TQs have greatly advanced my understanding of the TXS platform. However, responses to a number of TQs, some of which have been outstanding for many months, have not been provided within the timescale of this review (unresolved matters are also covered by TSC TOs e.g.T15.TO2.01, T15.TO2.34, T15.TO2.35, and T15.TO2.36 in Annex 5). In particular, EDF and AREVA have not formally responded to observations arising from the TSC GDA Step 3 review (see TQ-EPR-571, Ref. 7). The TSC performed a review of these observations and identified those that were not addressed by the submissions provided during GDA Step 4, and this concern is addressed by Assessment Finding **AF-UKEPR-CI-009** (see below).

132 The initial overall C&I architecture proposed by EDF and AREVA placed reliability claims upon the Teleperm XS platform for the P S which were well beyond HSE SAP recommendations and international guidance (e.g. IAEA NS-G-1.1, Ref. 12), and this issue was raised under regulatory issue **RI-UKEPR-002**. In response to this issue the reliability claims were reduced to a level considered to be in alignment with standards for this type of platform. However, further justification is required in relation to substantiation of the reliability claims, and I have raised GDA Issue Action **GI-UKEPR-CI-06.A2** to address this issue (see Section 4.5).

133 An independent assessment organisation is used to support the TXS development lifecycle. However, the role of the independent assessment function does not fully align with the requirement of key nuclear sector safety standards (Refs 17 and 18) in that the independent team does not perform all assessment tasks independently, but rather reviews the scope and output of these tasks as performed by the development team.

*GDA Assessment Finding: **AF-UKEPR-CI-006** - The Licensee shall justify all variations from the requirements of BS IEC 60880 (Ref. 17) and BS IEC 60987 (Ref. 18) with respect to the role of the independent assessor within the Teleperm XS development lifecycle, and implement compensating measures where necessary. For further guidance see T15.TO2.22 in Annex 5.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

134 The original development of the TXS was initiated in the early 1990s, and the assessment performed sampled some of the records from that time period. A number of design documents were sampled and no inconsistencies were found. However, the

assessment did not identify a platform requirements specification (as required by BS IEC 61513:2001 (Ref. 10)).

GDA Assessment Finding: ***AF-UKEPR-CI-007*** *- The Licensee shall identify / produce documentation which clearly specifies the Teleperm XS platform requirements. For further guidance see T15.TO2.13 in Annex 5.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

135 My assessment reviewed samples of the platform development process. I was unable to clearly identify the process used to trace requirements through from high level to lower levels of the design, and then through to test specifications.

GDA Assessment Finding: ***AF-UKEPR-CI-008*** *- The Licensee shall produce documentation which clearly identifies the traceability of requirements from the high level Teleperm XS specifications to the lower level design documents, and through to the platform test documents. For further guidance see T15.TO2.12, T15.TO2.14, T15.TO2.15 and T15.TO2.16 in Annex 5.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

136 My assessment reviewed many aspects of the TXS lifecycle and identified areas where it is considered that further justification is required in order to produce a comprehensive demonstration of the fitness for purpose of the TXS platform (e.g. failure analysis, adequacy of qualification processes, verification and type test reports).

GDA Assessment Finding: ***AF-UKEPR-CI-009*** *- The Licensee shall produce a comprehensive demonstration of fitness for purpose for the Teleperm XS platform which addresses, amongst others:*

- *Mean Time Between Failure analysis;*
- *adequacy of hardware lifecycle data, independent verification;*
- *adequacy of type test reports;*
- *compliance with BS IEC 60780:1998 "qualification";*
- *adequacy of Qualified Target Life;*
- *justification of the application of AREVA's 'standard approach' to qualification;*
- *adequacy of the Teleperm XS qualification process with respect to Pre-Ageing;*
- *justification that worst case timing scenarios have been used when determining processor utilisation of the Teleperm XS platform software; and*
- *justification of the adequacy of the Teleperm XS platform fault/change management process.*

For further guidance see T15.TO2.01, T15.TO2.17, T15.TO2.23, T15.TO2.24, T15.TO2.25, T15.TO2.26, T15.TO2.27, T15.TO2.28, T15.TO2.29, T15.TO2.30, T15.TO2.31, T15.TO2.32, T15.TO2.36 and T15.TO2.37 in Annex 5.

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

137 Insufficient information has been made available within the timeframe of this review to facilitate an adequate depth of review of conformance to all relevant HSE SAPs. In particular, EDF and AREVA have not provided an up to date Failure Modes and Effects Analysis (FMEA) and hardware reliability justification.

GDA Assessment Finding: ***AF-UKEPR-CI-010*** *- For SAP EDR.3 the evidence referenced by EDF and AREVA for PS reliability and availability is to be superseded by Failure Mode Effects Analysis calculations which were scheduled to be provided in December 2010. The Licensee shall update the CAE trail for EDR.3 and EDR.1 as appropriate, and produce the cited FMEA evidence and required justification. For further guidance see T15.TO2.50, T15.TO2.54 and T15.TO2.62 in Annex 5.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

138 For HSE SAP EDR.3 the cited evidence for CCF analysis (see also T15.TO2.57 and T15.TO2.58 in Annex 5) is qualitative with no link provided to the quantitative reliability claims that are made for the TXS platform. Therefore, I have raised GDA Issue Action **GI-UKEPR-CI-06.A2** to address the generic issue of the justification of reliability claims for SIS.

139 I have also raised GDA Issue Action **GI-UKEPR-CI-03.A1** to cover the general issue of further evidence being required to support the HSE SAP CAE trail and demonstration of conformance.

140 I had planned to perform a sample based assessment of the selection and use of Programmable Complex Electronic Components (PCECs) performing safety functions (e.g. within the TXS platform), but insufficient information was provided to facilitate such an assessment. However, my assessment did determine that there are a number of devices containing PCECs (e.g. Application Specific Integrated Circuits (ASICs) and Complex Programmable Logic Devices (CPLDs)) within the TXS platform design. The following Assessment Finding is raised to cover this issue.

GDA Assessment Finding: ***AF-UKEPR-CI-011*** *- The Licensee shall produce a safety demonstration for the selection and use of Programmable Complex Electronic Components in the Teleperm XS platform, which form part of the Class 1 UK EPR™ Protection System, using appropriate standards and guidance. For further guidance see T14.TO1.02 in Annex 4; T15.TO1.2 and T15.TO1.3 in Annex 5; and T20.A1.5.5 in Annex 9.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

141 EDF and AREVA have proposed a programme of ICBMs in relation to the safety case for the TXS based PS software (see also T15.TO2.07, and T15.TO2.19 in Annex 5), but this programme has not yet been fully defined. I have raised GDA Issue Action **GI-UKEPR-CI-02.A1** to cover this issue. ND's expectations for ICBMs are outlined in a technical assessment guide (Ref. 9) and cover, for example, consideration of the application of statistical testing and static analysis of the final production software (this topic is discussed further in Section 4.5 below).

142 The United States Nuclear Regulatory Commission (US NRC) has completed a safety assessment of the TXS Platform (Ref. 38), and the assessment performed by the US NRC has been considered in my assessment (see T15.TO2.01 item 'b' in Annex 5 and Ref. 30 for further detail).

143 The UK EPR™ design includes a number of systems hosted on hardware platforms based on the TXS equipment family, but the highest probabilistic claims are placed on the Class 1 PS. My assessment has, therefore, focused on the use of TXS in a four-train configuration as proposed for the UK EPR™ PS.

144 EDF and AREVA have provided a sample of records to support claims made for this platform. Meetings were held in AREVA's London office where it was possible to:

- directly review company records relating to software requirements specification, development, testing and assessment as held on the AREVA corporate network, and
- follow documentation trails through the development and independent assessment processes.

Many of the documents reviewed at these meetings were in addition to those formally provided by EDF and AREVA to support the GDA assessment. However, there are gaps in the required evidence which I need to complete my assessment, and I have raised GDA Issues and Assessment Findings to address these gaps (as documented in this section).

145 As a result of my sample-based assessment of TXS platform I conclude that, providing the relevant GDA Issues and Assessment Findings are satisfactorily addressed, this platform is acceptable in relation to its proposed UK EPR™ role. Key factors guiding my judgement were:

- the deterministic behaviour of the platform;
- the reduced reliability claims now made for the PS, which is hosted on this platform;
- the option of four-train redundant configuration;
- the use of relevant nuclear sector standards to guide the development of the platform;
- the use of independent assessors during the development process; and
- the extent of self checking and error handling processes.

146 My conclusion with respect to the suitability of the TXS platform aligns with the Organisation for Economic Co-operation and Development (OECD) Multinational Design Evaluation Programme (MDEP) common position described in Section 4.7.

4.3.1.2 Assessment of the SPPA-T2000 Platform

147 The SPPA-T2000 platform is a distributed process control and plant monitoring platform which was developed for general commercial use. It is understood that this platform has been used on conventional power stations since 1993. This platform was developed to commercial standards rather than nuclear sector standards. This platform is being installed on variants of the EPR currently under construction in France and Finland. EDF and AREVA have proposed this platform for a number of UK EPR™ C&I systems (e.g. the PICS, SAS and PAS). The Class 2 SAS use of this platform is

the most safety significant application. Therefore, my assessment has been focused on the use of the platform in the SAS.

148 The SAS provides diverse functions (i.e. diverse to those provided by the PS) to support the provision of plant protection functions. Therefore, the SPPA-T2000 platform must be suitably qualified for use in a protection system support role. The SPPA-T2000 platform includes hardware and software components and the software tools required for engineering of the application functions, testing and commissioning, operation and maintenance. The environmental qualification of the SPPA-T2000 platform, as required for the SAS, was within the scope of assessment.

149 The platform provides the option of dual redundant processors and dual redundant input / output processors, where in the event of malfunction of an active processor, the system automatically switches to a redundant standby unit. Use of these options is proposed for the SAS and the PAS. The platform offers two communication bus options for communication between units in the same division. These options are the PAS Bus (as proposed for the UK EPR™ PAS), and the more secure SAS Bus, which consists physically of two independent busses (as proposed for the UK EPR™ SAS).

150 The assessment strategy took account of the lesser safety significance of this platform in the C&I architecture compared to TXS (i.e. it is used to host Class 2 and Class 3 systems, and the most demanding reliability claim made for a system hosted on this platform is $1x10^{-2}$ pfd).

151 The UK EPR™ safety case has a figure of $1x10^{-6}$ pfd for the total loss of C&I functions from the TXS and SPPA-T2000 platforms (Ref. 54). Considerable progress has been made in establishing the degree of diversity between these platforms. However, further detailed analysis and evidence is required in order to demonstrate diversity of the SPPA-T2000 platform from the TXS platform and I have raised GDA Issue Action **GI-UKEPR-CI-06.A1** to address this issue.

152 The scope of my assessment included hardware design, qualification and software design. I am broadly satisfied with the results of my assessment of the records provided by EDF and AREVA to support their claims. However, insufficient information was provided by EDF and AREVA in specific technical areas (e.g. hardware development lifecycle records, compliance with platform test records, pre-developed software assessment process and the extent of environmental qualification with respect to post accident conditions) to enable me to complete a review in sufficient depth. Note that compliance against key standards is covered by **AF-UKEPR-CI-002** raised in Section 4.2.

> *GDA Assessment Finding: **AF-UKEPR-CI-012** - The Licensee shall produce a comprehensive safety demonstration addressing the adequacy of the SPPA-T2000 platform for Class 2 use covering hardware design, qualification and software design processes. For further guidance see T15.TO2.39, T15.TO2.40, T15.TO2.41, T15.TO2.42 and T15.TO2.44 in Annex 5; T17.TO2.06 in Annex 7; and T20.A2.3.4 in Annex 9.*
>
> [Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

153 My assessment included a review of EDF and AREVA's CAE trail for a sample of applicable HSE SAPs (see Table 5). For HSE SAP ESS.15 the argument in the CAE trail provided by EDF and AREVA presents the principles for the security procedures that will be used to control access to the SPPA-T2000 Engineering System. However,

no argument is presented regarding measures to ensure that the Engineering System cannot cause unintended interference with the Class 2 SAS during plant operation.

> *GDA Assessment Finding: **AF-UKEPR-CI-013** - The Licensee shall produce adequate justification that the SPPA-T2000 Engineering System cannot cause unintended interference with the Class 2 SAS during plant operation. For further guidance see T15.TO2.61 in Annex 5.*
>
> [Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

154 I have raised GDA Issue Action **GI-UKEPR-CI-03.A1** in Section 4.1 to cover the general issue of further evidence being required to support HSE SAP conformance (for further guidance see T15.TO2.49, T15.TO2.51, T15.TO2.52, T15.TO2.53, T15.TO2.54, T15.TO2.55, T15.TO2.58, T15.TO2.59 and T15.TO2.62).

155 The SPPA-T2000 platform has been assessed, as this is the platform proposed in the current UK EPR™ design and this platform is being installed on EPR variants currently under construction in France and Finland. However, it is believed that elements of the SPPA-T2000 platform are obsolete and the following GDA Issue has been raised.

> *GDA Issue: **GI-UKEPR-CI-05** - Obsolescence of SPPA-T2000 platform - The EDF and AREVA C&I architecture includes systems based upon SPPA-T2000 (Siemens S5 based), but this platform is believed to be obsolete and will not be available for UK EPR™:*
>
> - ***GI-UKEPR-CI-05.A1**: The EDF and AREVA C&I architecture includes systems based upon the SPPA-T2000 (Siemens S5 based), but this platform is believed to be obsolete and will not be available for the UK EPR™. EDF and AREVA needs to define the platform that will be provided for the UK EPR™ and submit a Basis of Safety Case (BSC) that fully addresses the change from the SPPA-T2000 (Siemens S5 based) platform to the proposed system.*
>
> *For further guidance see **GI-UKEPR-CI-05.A1** in Annex 2, T15.TO1.45 in Annex 5 and T18.TO1.04 in Annex 8.*

156 A Basis of Safety Case in this context is expected, amongst others, to:

- define the safety principles and standards (i.e. company, national and international) that are to be adopted for the replacement systems (i.e. incorporating the replacement platform);
- justify how these safety principles and standards will be complied with at each step of the development and deployment of the replacement systems;
- justify how functional and performance requirements will be satisfied;
- demonstrate conformance with relevant HSE SAPs;
- provide a full analysis of the impact of the replacement platform on the overall C&I design; and
- provide precise details of the change and demonstrate that the systems (covering all new components, tools and methods etc.) are fit for purpose.

157 The TSC performed a review of selected HSE SAPs relevant to the SPPA-T2000 platform. This identified a particular concern in relation to software reuse. The

Licensee's adequacy of software reuse argument, as relevant to ESS.27 and ESR.5, should address all Class 2 components of the SPPA-T2000 that contain dedicated devices with embedded software, or if no su ch software exists, a positive statement saying so should be made. The Licensee is requested to update the CAE trail for HSE SAPs ESS.27 and ESR.5 to address this concern.

> *GDA Assessment Finding:* ***AF-UKEPR-CI-014*** *- The Licensee shall ensure that the software re-use argument presented addresses all Class 2 components of the SPPA-T2000 that contain dedicated devices with embedded software, or if no such software exists a positive statement saying so should be made. For further guidance see T15.TO2.60 in Annex 5.*
>
> [Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

158 The French regulator L'Autorité de Sûreté Nucléaire (ASN) has raised an issue concerning the adeq uacy of the quality system test records f or the original development of the SPPA-T2000 platform, and conf irmation is required t hat this issue does not compromise the claims made for the UK EPR™ design.

> *GDA Assessment Finding:* ***AF-UKEPR-CI-015*** *- The Licensee shall produce adequate justification that the issue raised by ASN concerning the adequacy of the quality system test records for the original development of the SPPA-T2000 platform does not compromise the claims made for this platform in the UK EPR™ design. For further guidance see T15.TO1.38 in Annex 5.*
>
> [Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

159 The generic issue of the need to a dequately consider issu es raised by other nati onal regulators assessing variants of the UK EPR™ is considered in the following Assessment Finding.

> *GDA Assessment Finding:* ***AF-UKEPR-CI-016*** *- The Licensee shall produce adequate justification that relevant issues raised by other national regulators concerning the adequacy of SIS have been adequately addressed where relevant to the UK EPR™ design and do not compromise the claims made for the UK EPR™ design.*
>
> [Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

160 From the sample based assessment of cla ims, arguments and e vidence I h ave concluded that, providing the rele vant GDA Issues and Assessment Findings a re satisfactorily addressed, this platform is acceptable for its proposed role. Key factors in reaching this conclusion are:

- the reduced reliability claims now made for this platform (following the changes resulting from **RI-UKEPR-002**);
- the addition of the NCSS to the C&I architecture; and
- the potential for dual redundant configurations of key platform components.

While broadly satisfied, the relevant GDA Issues and Assessment Findings need to be resolved.

4.3.1.3 Assessment of the NCSS Platform

161 In response to **RI-UKEPR-002** EDF and AREVA have committed to modify the C&I architecture and introduce the NCSS. This system provides diversity from the computer-based PS and SAS / PAS. It has not been possible to perform an assessment of the high level design of this system as insufficient information has been made available within the timeframe of this review. I have raised GDA Issue Action **GI-UKEPR-CI-01.A1** to address this issue in Section 4.5 (see also T15.TO1.46 in Annex 5).

162 The NCSS documentation provided by EDF and AREVA to date is consistent with a diverse platform (i.e. from TXS and SPPA-T2000) being selected for the NCSS, and I consider this to be a necessary characteristic of the system platform. Sections 4.5 and 4.6 contain further detail of the NCSS concerns that I raised under **RI-UKEPR-002** and a description of RP commitments made with respect to the NCSS.

4.3.1.4 Assessment of the SICS and Class 1 Display System Platform

163 I had planned to perform a sample based assessment of the Class 1 display system platform (this system is to be provided in response to concerns raised under **RI-UKEPR-002**). However, insufficient evidence has been made available within the timescale of this review and I have raised GDA Issue Action **GI-UKEPR-CI-06.A6** to cover this issue (see Section 4.5).

164 The SICS is based on conventional hardware and there is no 'platform' as such for this system. However, assessment of the SICS system is reported in Section 4.4.

4.3.1.5 Assessment of Pre-Developed Equipment

165 I had planned to perform an assessment of EDF and AREVA's arrangements covering the qualification and use of smart devices, and to perform a review of a sample of the evidence generated though the application of these arrangements. EDF and AREVA's arrangements for smart devices need to cover the processes for determining whether smart devices are used to perform nuclear safety functions, and the actual justification processes for smart devices at different safety classes. These processes have to ensure that adequate evidence is produced, which may then be made available for review. This topic has been discussed with EDF and AREVA, and a position paper provided. However, further definition of the methodology and examples of its implementation are required. A suitable submission on smart devices was not provided within the timescale of the GDA Step 4 review. I have raised the following GDA Issue to cover definition of the methodology and production of examples of the implementation of the methodology (for further guidance see also T15.TO1.48 in Annex 5), and the following Assessment Finding to address implementation of the methodology:

> *GDA Issue: **GI-UKEPR-CI-04** - Smart devices: EDF and AREVA have yet to define a methodology to be used to qualify smart devices for nuclear safety functions.*
>
> - ***GI-UKEPR-CI-04.A1**: EDF and AREVA to define the methodology to be used to qualify smart devices used in the implementation of nuclear safety functions and produce examples of the implementation of the methodology for two smart devices, one from Class 1 and one from Class 2.*

*GDA Assessment Finding: **AF-UKEPR-CI-017** - The Licensee shall implement the smart devices qualification methodology defined under GDA Issue **GI-UKEPR-CI-04** and ensure implementation evidence is available for review for all safety classes.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

166 The GDA scope excludes detailed design and manufacturing information for process sensors (see Section 2.3.5). However, under GDA Step 4 a review of key safety case documentation (e.g. specifications and system design manuals) for two in-core instrumentation systems was undertaken (see Annex 3). The evidence provided during GDA Step 4 did not allow the assessment against relevant IEC instrumentation standards to be completed. The Licensee will need to ensure there is an adequate safety case for such instrumentation (including demonstration of compliance to appropriate standards).

*GDA Assessment Finding: **AF-UKEPR-CI-018** - The Licensee shall ensure there is an adequate safety case for in-core instrumentation sensors and other sensors used in SIS. For further guidance see T13.TO2.44 in Annex 3.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

4.3.2 GDA Step 4 Findings

167 The Assessment Findings and GDA Issues recorded in the section above are listed in Annex 1 and 2 respectively.

4.3.3 GDA Close-out Assessment

168 This section addresses resolution of GDA Issue **GI-UKEPR-CI-05** on the change of the Siemens SPPA-T2000 platform from version S5 to S7 and GDA Issue **GI-UKEPR-CI-04** on development of a methodology for smart device qualification.

4.3.3.1 Siemens SPPA-T2000 Platform Version S5 Obsolescence - GI-UKEPR-CI-05

169 GDA Issue **GI-UKEPR-CI-05** relates to the change of the Siemens SPPA-T2000 platform from version S5 to S7 as a result of obsolescence of the version S5 equipment. GDA Issue **GI-UKEPR-CI-05** requires EDF and AREVA to submit a BSC that fully addresses the change.

170 EDF and AREVA submitted 14 documents (see Annex 10) in response to this GDA Issue covering:

- definition and impact assessment of the change;
- an outline of the BSC;
- the BSC; and
- supporting documents (nine) to the BSC.

171 EDF and AREVA's submissions under this GDA Issue included those documents identified in their Resolution Plan (Ref. 72) except for the justification of the diversity of the SPPA-T2000 and TXS platforms (Resolution Plan task 5). EDF AREVA addressed the diversity of the platforms under GDA Issue **GI-UKEPR-CI-06 Action 1**.

172 The submissions were reviewed and requests for clarification were raised by TQ (a single TQ form was raised on this topic). As appropriate, the submitted documents were revised by EDF and AREVA to address the points in TQ-EPR-1566 (Ref. 86). The description of the scope of work performed by the TSC and the TOs arising from the work are contained in a TSC report (Ref. 78). Annex 15 provides a summary of the TSCs' report including details of the TOs raised.

173 The CMF forms (Ref. 129 and 130) submitted by EDF and AREVA identified that the C&I systems impacted by the SPPA-T2000 platform version change are the SAS, PAS, SAS RRC-B, PICS and Plant Bus. The Terminal Bus and the operator stations are not impacted by the S5 to S7 version change.

174 EDF and AREVA described the scope and content of the BSC in letter EPR00852R (Ref. 131) and in a summary report (Ref. 132). I found the descriptions to be inconsistent and they did not align with my expectations. In particular, the scope of the BSC was for substantiation of the SPPA-T2000 platform and not of the change from the S5 to S7 versions. Further guidance on my expectations was provided in TQ-EPR-1566 (Ref. 86) that included an outline requirements definition and traceability matrix addressing the contents of a BSC.

175 Following provision of the further guidance, EDF and AREVA submitted a BSC document (Ref. 133) and completed requirements traceability matrix (Ref. 134). The BSC was reviewed against the six points outlining the expectations for the content of the BSC (e.g. definition of safety principles and standards, provision of precise details of the change and demonstration that the systems based on the SPPA-T2000 platform are fit for purpose etc.) identified in the statement of the GDA Issue (see Section 4.3.1.2 and Annex 2).

176 I found the BSC scope went beyond the substantiation of the SPPA-T2000 S5 to S7 platform version change. The BSC reported the changes made from the S5 to S7 version of the platform and identified the evidence against each of the six GDA Issue points discussed above. I confirmed that the BSC responded to each point in an acceptable way, for example, explaining at length how the change did not impact the functionality available from the platform. My review of the BSC included sampling of the supporting evidence. Areas for improvement of the BSC were identified, for example, in terms of its structure and the completeness of evidence. In particular, the demonstration of the fitness for purpose of systems based on the SPPA-T2000 S7 platform will need appropriate evidence to be identified as the systems are designed and implemented during the SSP.

177 I reviewed a sample of the BSC supporting documents provided by EDF and AREVA (submitted under cover of Ref. 135) to determine whether they support the claims made in the BSC. The outcome of my sampling of documentation on software development, hardware reliability and response time performance is described below.

178 EDF and AREVA's BSC claims that the software development processes are essentially unchanged and presents evidence, such as on regression testing, that the change from the S5 to S7 version is not detrimental to safety. EDF and AREVA also provided documents to support a claim that the processes comply with the BS EN 62138:2004 software standard for Class 2 and 3 systems (i.e. implementing Category B and C functions respectively). I confirmed the claims are appropriate given the current stage of systems' development. However, further evidence is required from the systems' development lifecycle phases as they are completed during the SSP.

179 EDF and AREVA provided documents on the hardware reliability and dependability studies for both the S5 and S7 versions of the platform. I confirmed the method used

was the same for both versions and that it complies with current practice for hardware reliability substantiation (i.e. as defined in current standards such as Refs 159 and 160). Sufficient evidence is available to give confidence the S7 platform version will meet the targets of 1x10^{-2} and 1x10^{-1} pfd / probability of dangerous failure per year (pdfy) for the Class 2 and 3 systems respectively. The reliability substantiation will need to be completed during the SSP as the systems' designs are completed.

180 The performance impact (i.e. in terms of response times) of the change from the S5 to S7 versions is described as acceptable by EDF and AREVA. This was reviewed as part of the resolution of GDA Issue **GI-UKEPR-CI-06 Action 8**, see Section 4.5.3.8.

181 Following assessment of EDF and AREVA's submissions in response to GDA Issue **GI-UKEPR-CI-05** on the change from SPPA-T 2000 platform version S5 to S7, I am content that the information contained in the BSC and supporting documents is adequate and the GDA Issue can be closed. I have raised an Assessment Finding below to capture the matters arising from the assessment that need to be addressed in completing the BSC (noting its extended scope in relation to the scope of the GDA Issue) and the safety case.

*GDA Assessment Finding: **AF-UKEPR-CI-036** – The Licensee shall develop the SPPA-T2000 platform BSC and complete the safety case to:*

- *Include a clear definition of the BSC scope and improvements to structure to clearly identify the impact of the S5 to S7 SPPA-T2000 platform version change.*
- *Revise the BSC / safety case claims and arguments to correctly and fully address each SAP and its guidance paragraphs (see also **AF-UKEPR-CI-010**, **AF-UKEPR-CI-023** and **AF-UKEPR-CI-028**).*
- *Include evidence generated during C&I system development, installation and commissioning including standards compliance, reliability and response time evidence to support the safety case claims and arguments (see also **AF-UKEPR-CI-002**, **AF-UKEPR-CI-020** and **AF-UKEPR-CI-029**).*

For further guidance on the completion of the BSC (including its extended scope and supporting documents) see Technical Observations GICI05.TO2.01 to GICI05.TO2.06 in Annex 15 and GICI06.A1.TO2.05 in Annex 16.

[Required Timescale: prior to power raise.]

4.3.3.2 Smart Device Qualification Methodology - GI-UKEPR-CI-04

182 This section addresses resolution of GDA Issue **GI-UKEPR-CI-04** on definition of the methodology to qualify smart devices used in the implementation of nuclear safety functions. GDA Issue **GI-UKEPR-CI-04** requires the definition of the qualification methodology and production of an example of its implementation for one Class 1 and one Class 2 smart device.

183 A smart device is a component utilising computer technology whose behaviour may be changed by use of field modifiable parameters. Where a smart device is used to perform functions important to safety, a design error, component failure, or incorrect parameter could prevent these functions being performed when required.

184 EDF and AREVA submitted 24 documents (see Annex 10) in response to this GDA Issue covering:

- lifecycle approach to the use of smart devices;
- evaluation of the suitability of the Emphasis tool to qualify smart devices;
- description of the approach to justify smart devices for nuclear safety applications;
- identification of scope, strategy and programme for the trial application of the smart device qualification methodology during GDA;
- qualification reports for a Class 2 smart device from the trial application, including Emphasis assessment report; and
- progress reports for the trial qualification of a Class 1 smart device.

185 The submissions were reviewed and requests for clarification were raised by TQ (11 TQ forms raised on this topic). As appropriate, the submitted documents were revised by EDF and AREVA to address the points in the TQs. The description of the scope of work performed by the TSC and the TOs arising from the work are contained in a TSC report (Ref. 77). Annex 14 provides a summary of the TSCs' report including details of the TOs raised.

186 Document Ref. 190 describes the graded process by which smart devices of different safety classes will be qualified and justified. International standards are used in the qualification process according to the highest category of safety function the smart device will perform, such as BS IEC 60880:2006 (Ref. 17) for Category A function software, BS EN 62138:2004 (Ref. 36) for Category B and C function software, and BS IEC 60987:2007 (Ref. 18) for Class 1 and 2 hardware. In the absence of a suitable nuclear sector standard for Class 3 hardware, the requirements of BS IEC 60987:2007 for Class 2 hardware will be applied.

187 EDF and AREVA have set the failure probability target for Class 1 smart devices at $1\text{x}10^{-3}$ to $1\text{x}10^{-4}$ pfd / pdfy, Class 2 at $1\text{x}10^{-2}$ pfd / pdfy and Class 3 at $1\text{x}10^{-1}$ pfd / pdfy (Ref. 190). A graded approach to the application of techniques and measures according to the failure probability target is described in document 'UK EPR Guideline for Application of Production Excellence and Independent Confidence Building' (Ref. 81). This graded approach meets my expectation for smart devices performing a nuclear safety function in a nuclear power plant.

188 EDF and AREVA evaluated the use of the Emphasis tool (Ref. 189) as a means of determining the strength of the PE leg of the safety argument for smart devices developed according to the requirements of non nuclear sector standards such as BS EN 61508:2002 (Ref. 40). EDF and AREVA concluded that the Emphasis tool is suitable for use in the qualification of smart devices. The Emphasis tool was used in the trial qualification of both Class 1 and Class 2 smart devices.

189 ICBMs are necessary for the qualification of smart devices (i.e. in addition to the identification of PE evidence). EDF and AREVA identified a range of ICBMs that would be effective, and specified a graded approach to the application of these according to the smart device safety class (Ref. 190).

190 EDF and AREVA identified that analysis of smart device software is important in developing confidence that reliability targets will be met. Therefore, access to source code for the qualification of Class 1 smart devices is always required. It is expected that source code will be accessible for Class 2 smart devices. If this is not possible, adequate justification as to why, and the application of other suitable ICBMs (Ref. 190) is required.

191 The trial qualification revealed omissions in the Class 2 Requirements Identification File (Ref. 192) relating to features of the smart device that had the potential to affect the operation of a safety function, and so TQ-EPR-1586 (Ref. 86) was raised. In response, EDF and AREVA improved the Requirements Identification File for the trial qualification of the selected device. It should be ensured that all smart device hardware and software features (e.g. clock synchronisation and removable data logging memory) that have the potential to adversely affect the operation of safety functions are identified and, as appropriate, included within the qualification. The smart device qualification should justify that these features either cannot interfere with the operation of the safety function(s) or that effective mitigating measures have been applied (see **AF-UKEPR-CI-051** below).

192 The Class 2 smart device Summary Qualification Report (Ref. 191) and supporting documents showed that the methodology was suitable for the qualification of Class 2 smart devices. The Class 2 smart device had previously been assessed using an earlier version of the Emphasis tool at the Safety Integrity Level 1 (SIL1) integrity level. EDF and AREVA audited the outcome of this earlier assessment, transferred the data to the current tool version, and updated and re-assessed it against SIL 2 requirements. EDF and AREVA concluded that the smart device is suitable for SIL 2 applications. However, some aspects of the qualification had not been completed (e.g. hardware assessment and statistical testing) and much of the evidence to back up the conclusions was not provided with the Emphasis assessment database (Ref. 193). These omissions would have to be remedied for full smart device qualification (see **AF-UKEPR-CI-051** below).

193 Early in the GDA closure phase EDF and AREVA identified that it would not be possible to complete a trial qualification of a Class 1 smart device in the time available, and instead proposed a Class 1 smart device qualification progress report to demonstrate the efficacy of the qualification processes.

194 The Class 1 smart device qualification progress report (Ref. 194) provided initial conclusions that confirmed the processes specified for a Class 1 device are adequate. Only samples of the software had been reviewed by the report delivery date and this limited the extent of the assessment carried out (i.e. limited evidence was available). However, progress has been sufficient to close the GDA Issue, with further work required during the SSP (see **AF-UKEPR-CI-051** below).

195 The Class 1 smart device 'Software Assessment Report' (Ref. 195) indicated that the parameterisation function was not part of the safety functionality (Question A7, Design Process), contrary to my belief that parameters have the potential to change the safety functionality of the device. I raised this question with EDF and AREVA (meeting action GI 14-I&C-4, Ref. 196). The response provided by letter EPR01396N (Ref. 197) indicated the smart device software that interfaces to infra-red link parameter input software obtained from a third party is designed to the same standard as the rest of the device software. Parameter changes are carried out over the infra-red link and initiated by a push button at the smart device. EDF and AREVA claimed that the third party parameterisation software cannot interfere with software performing safety functions. However, the response did not provide justification of this claim (i.e. that the smart device infra-red link Software Of Unknown Pedigree (SOUP) will not interfere with software performing safety functions or perform as required), and so further work is required during the SSP (see **AF-UKEPR-CI-051** below).

196 Following assessment of EDF and AREVA's submissions in response to GDA Issue **GI-UKEPR-CI-04** on definition of the methodology to qualify smart devices for nuclear

safety functions, I am content that the qualification methodology for smart devices at all safety classes has been adequately defined and that the GDA Issue can be closed. I have raised an Assessment Finding below to capture additional matters arising from the assessment that need to be addressed during the qualification of smart devices for the UK EPR™.

*GDA Assessment Finding: **AF-UKEPR-CI-051** - The Licensee shall:*

- *Complete the trial qualification of the Class 1 smart device, assess the effectiveness of the qualification, and update the smart device qualification documentation and processes where improvements are identified.*
- *Address the omissions in the Class 2 smart device trial qualification, assess the effectiveness of the qualification, and update the qualification documentation and processes where improvements are identified.*
- *Confirm that a change in the Emphasis version will not adversely affect the qualification of smart devices.*
- *Ensure that all smart device features (e.g. such as clock synchronisation and removable data logging memory), that have the potential to adversely affect the operation of safety functions are identified and, as appropriate, included within the qualification.*
- *Ensure that all smart devices are qualified in accordance with the updated procedures, see **AF-UKEPR-CI-017**.*
- *Where smart devices contain software that has been developed to a lower standard than that required by the classification of the device, a justification should be provided for the adequacy of this software (e.g. as Pre-Developed Software using appropriate standards and guidance), and that this software will not have an adverse affect on the safety functions (to include potential to corrupt program and data memory areas, and hardware settings).*

For further guidance on smart device qualification see Technical Observations GICI04.TO2.03 to GICI04.TO2.08 in Annex 14.

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

4.3.4 GDA Close-out Findings

197 The Assessment Findings identified in the section above are also recorded in Annex 1.

4.4 C&I Systems Important to Safety

4.4.1 GDA Step 4 Assessment

198 This section describes the outcome of the assessment of SIS, including conformance to the UK EPR™ project specific SIS standards and guidance. This assessment complements and builds upon the assessment reported in Sections 4.2 and 4.3. Progress with resolution of the relevant GDA Step 3 observations is specifically identified and reported.

199 The work of the C&I TSC supported my assessment. The description of the scope of work performed by the TSC, and the TOs arising from the work are described in the

relevant TSC report (Ref. 31). Annex 6 provides a summary of Ref. 31 including details of the TOs raised.

200 The topic of the compliance and alignment of EDF and AREVA's categorisation and classification methodology for SIS with relevant good practice is discussed in Section 4.2, and **AF-UKEPR-CI-002** was raised to address the provision of a number of compliance matrices against relevant international standards.

201 Three ND GDA Step 3 Assessment Report (Ref. 6) observations have been considered within the scope of this part of the GDA Step 4 assessment.

1) Further information was requested concerning the level of equipment redundancy within the SAS and PAS.

EDF and AREVA provided further information in response to GDA Step 4 TQs, and through responses to Level 3 meeting actions. The technical information provided included descriptions of the:

- operation of the fault tolerant Plant Bus network;
- design of the AP620 dual redundant automation processor (AP) units;
- segregation of SAS into four divisions;
- operation of a communications bus within divisions to communicate between devices of the same safety class;
- SAS inter-divisional communication;
- deterministic nature of the SAS Bus; and
- operation of the fault tolerant Terminal Bus.

The review of the further information on equipment redundancy within the SAS and PAS provided by EDF and AREVA has not revealed any aspects of the design that are considered unacceptable. I now consider this GDA Step 3 observation to be closed.

2) It was noted that the fail-safe principle as applied to C&I systems was not well covered in the PCSR.

During GDA Step 4, EDF and AREVA clarified that the fail-safe performance for C&I nuclear safety functions (including appropriate responses to C&I equipment failure and consideration of whether or not to actuate plant items given the resultant impact on plant safety) is determined in the detailed application design stage. This approach is considered acceptable. However, the following Assessment Finding has been raised to ensure that this issue is addressed by the Licensee.

> *GDA Assessment Finding:* ***AF-UKEPR-CI-019*** *- The Licensee shall ensure the fail-safe principle (including the application of the appropriate response to C&I equipment failures) is implemented in the design of UK EPR™ C&I nuclear safety functions. For further guidance see T16.TO2.18 in Annex 6.*
>
> [Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

3) Further clarification was required concerning how the independent confidence building and PE safety case legs for CBSIS were to be addressed.

This topic is still of concern, and is covered by GDA Issue Actions **GI-UKEPR-CI-02.A1** (see later in this section) and **GI-UKEPR-CI-06.A3** (see Section 4.5).

202 EDF and AREVA defined certain aspects of the C&I design as out of scope, see Section 2.3.6, including system installation and commissioning. RCC-E (Ref. 24) requires that SIS comply with a number of international C&I standards (e.g. BS IEC 61513:2001 (Ref. 10) and BS IEC 62138:2004 (Ref. 36)). These standards provide requirements covering installation and commissioning but it has not been possible to review evidence covering these later system lifecycle phases for the UK EPR™ C&I SIS (see also T16.TO2.28 and T16.TO2.30 in Annex 6).

GDA Assessment Finding: ***AF-UKEPR-CI-020*** *- The Licensee shall demonstrate that the UK EPR™ C&I SIS comply with relevant IEC standards in their installation, commissioning and operational lifecycle phases. For further guidance see T16.TO2.28 and T16.TO2.30 in Annex 6.*

[Required Timescale: - prior to power raise.]

203 A risk-based approach to assessment was followed, with the greatest assessment effort allocated to those systems performing the most important nuclear safety functions, in particular the Class 1 PS. All assessment was performed on a sample basis (e.g. by selection of key HSE SAPs and standards' clauses for detailed review).

4.4.1.1 Assessment of the Protection System

204 The Class 1 UK EPR™ PS is hosted on the TXS platform configured in a four-train redundant architecture. In this configuration two-out-of-four voting on selected outputs to plant is performed. The voting logic is reduced to two-out-of-three if one train is unavailable and one-out-of-two if two trains are unavailable. I consider this configuration to be consistent with relevant good practice for protection systems, and is consistent with the configuration used on the UK's only operational Pressurised Water Reactor (PWR) at Sizewell in Suffolk.

205 The production of project-specific application code and data for the TXS platform is supported by a suite of tools which were developed as part of the generic platform. These tools were within the scope of the assessment reported under Section 4.3.

206 The initial assessment of the adequacy of the PS was based upon a review of documentation provided by EDF and AREVA. In order to improve understanding between the designers and assessors, a series of technical meetings were held where aspects of the development were reviewed, such as:

- the allocation of functions to subsystems;
- the use of the platform tools to support the development of applications;
- the use of quality plans to control the applications' development process; and
- function block verification.

Some of these meetings were held at the London offices of AREVA where a network link to AREVA's offices in Germany was made available.

207 Relevant good practice for protection systems is documented in IEC standards, and I consider the most significant of these to be BS IEC 61513:2001 (Ref. 10), BS IEC 60880:2006 (Ref. 17) and BS IEC 60987:2007 (Ref. 18). During the GDA Step 4 assessment, samples of development records (many based on FA3 data) were selected and reviewed. No evidence was revealed within the scope of this section's assessment which directly contradicts EDF and AREVA's claim of compliance with these standards.

208 However, it was only possible to assess EDF and AREVA' s arrangements against a limited number of standards' clauses. EDF and AREVA gave a commitment to produce detailed standards' compliance matrices to improve the demonstration of standards' compliance, but these have not been provided within the time frame of this review. I have raised GDA Issue Action **GI-UKEPR-CI-06.A3** which requires EDF and AREVA to produce further evidence covering PE of the PS software. An important component of the required evidence is provision of the standards' compliance matrices, to further demonstrate compliance against relevant international standards (see also T16.TO1.1 in Annex 6 and Assessment Finding **AF-UKEPR-CI-002**).

209 Assessment of the application software development lifecycle revealed that, for some steps in the Verification and Validation process, the object code to be tested using the Simulation Based Validation Tool (SIVAT) tool will differ from the object code to be used on the target hardware. This is because a different compiler version will be used to generate object code for the target hardware and SIVAT. EDF and AREVA have not provided adequate justification for this aspect of the development lifecycle within the timeframe of this review.

GDA Assessment Finding: ***AF-UKEPR-CI-021*** *- The Licensee shall demonstrate that the use of a different complier with the SIVAT tool compared to that used to generate the object code which will run on the PS does not compromise the integrity of the PS application software development lifecycle. For further guidance see T16.TO2.19.b in Annex 6.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

210 Assessment of the application software development lifecycle identified a concern about the adequacy of the functional test coverage of the application code which will need to be addressed.

GDA Assessment Finding: ***AF-UKEPR-CI-022*** *- The Licensee shall demonstrate the adequacy of the Protection System application code testing process with respect to functional coverage. For further guidance see T16.TO2.19 item a in Annex 6.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

211 The assessment work reported under Section 4.1 covering Claims, Arguments and Evidence relevant to the HSE SAPs identified a number of SAPs relevant to the PS. It has not been possible to confirm full conformance to the following relevant sampled HSE SAPs within the timescale of this review:

- qualification records to address EQU.1 (qualification procedures), (see also T16.TO2.01 covering observations such as on the qualification of actuators and sensors);
- "design for reliability" requirements to address EDR.2 (redundancy, diversity and segregation), (see also T16.TO2.03 covering observations such as on cable separation);
- "design for reliability" requirements to address EDR.3 (common cause failure), (see also T16.TO2.04 covering this observation);
- maintenance, inspection and testing requirements to address EMT.7 (functional testing), (see also T16.TO2.05 covering observations such as on scope of testing performed);

- failure independence requirements to address ESS.18 (see also T16.TO2.06 covering observations such as on inter-module communications within the PS);
- error detection and management requirements to address ESS.21 (reliability), (see also T16.TO2.07 covering for example the handling of errors within function blocks);
- allowance for unavailability requirements to address ESS.23 (see also T16.TO2.08 in Annex 6 covering the unavailability of PS equipment); and
- scope of ICBMs to address ESS.27 (computer-based safety systems) requirements (see also T16.TO2.09 covering observations such as on the use of ICBMs), I have raised GDA Issue Action **GI-UKEPR-CI-06.A3** to cover this issue.

212 I have raised GDA Issue Action **GI-UKEPR-CI-03.A1** to cover the generic issue of the production of an adequate CAE evidence trail, and the following Assessment Finding is raised to ensure that PS conformance is demonstrated for the relevant HSE SAPs listed in the previous paragraph (the evidence trail to be addressed under GDA Issue Action **GI-UKEPR-CI-03.A1** should be updated accordingly):

*GDA Assessment Finding: **AF-UKEPR-CI-023** - The Licensee shall demonstrate the adequacy of conformance of the Protection System with EQU.1 (qualification procedures), EDR.2 (redundancy, diversity and segregation), EDR.3 (common cause failure), EMT.7 (functional testing), ESS.18 (failure independence), ESS.21 (reliability), and ESS.23 (allowance for unavailability). For further guidance see T15.TO2.52 in Annex 5; and T16.TO2.01, T16.TO2.03, T16.TO2.04, T16.TO2.05, T16.TO2.06, T16.TO2.07 and T16.TO2.08 in Annex 6.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

213 Assessment of EDF and AREVA's response to HSE SAP ESS.7 revealed that the approach to the determination of the number of parameters provided within the PS for the initiation of safety system action did not conform to the HSE SAP requirement. The expectation is that, for those postulated initiating events where a risk reduction of 1x10^{-4} pfd is required from the PS there should be diversity in detection of the fault sequence. EDF and AREVA's approach is to provide two parameters for frequent postulated initiating events. To determine whether this difference in approach would challenge the HSE SAP risk targets, EDF and AREVA undertook a sensitivity study that demonstrated that for situations where there is only one PS parameter, with a claim of 1 x10^{-3} pfd, the HSE SAP risk targets are met. See the GDA PSA Step 4 report (Ref. 41) for further details on the sensitivity study and ND's assessment thereof.

214 The PS is required to perform calculated trip functions (e.g. the departure from nucleate boiling ratio trip function), and I had intended to perform an assessment of these functions. However, insufficient information was provided by EDF and AREVA within the time scale of my assessment.

*GDA Assessment Finding: **AF-UKEPR-CI-024** - The Licensee shall produce evidence to demonstrate the adequacy of the design and implementation of the PS calculated trip functions. For further guidance see T16.TO2.33.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

215 A protection system with a full four-train redundant architecture performing a two-out-of-four voting arrangement (i.e. any two trains can initiate safety system action) should allow a train to be taken out of service. When a train is taken out of service, a two-out-

of-three vote should be taken on the remaining in-service trains. The PS has a four-train architecture, but the four trains are not functionally identical. When the functions across the trains are different then the impact of taking any one of these trains out of service for maintenance will depend upon the functionality performed by that particular train. I require further clarification with respect to the impact of failures within PS trains and with respect to taking trains of the PS out of service for maintenance.

> *GDA Assessment Finding: **AF-UKEPR-CI-025** - The Licensee shall demonstrate that the differences of functional coverage across the PS trains do not give rise to any safety concerns (such as an inability to meet the reliability requirements or the single failure functional criterion requirements) when failures occur within a train, or any train is taken out of service for maintenance. For further guidance see T17.TO2.09 in Annex 7, T18.TO2.01 in Annex 8 and T20.A1.4.3 in Annex 9.*
>
> [Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

216 Of particular importance to a system such as the PS (where high reliability claims are made and computer-based technology is used with considerable design complexity) is conformance with the recommendations of HSE SAP ESS.27. In addition to PE, this HSE SAP requires the application of ICBMs to the final production software to provide confidence in correct operation (e.g. by performing successful statistical testing). Further guidance on ICBMs is contained in T/AST/046 (Ref. 9).

217 EDF and AREVA were not initially familiar with the concept of ICBMs and, due to lack of progress addressing the requirements of ESS.27, the issue of an adequate ICBM programme (e.g. covering statistical testing and static analysis) was raised under **RI-UKEPR-002** and **RO-UKEPR-58**.

218 An important component of the ICBMs proposed for the PS is statistical testing. Given that the reliability claim for the PS is specified as a failure probability of $1x10^{-4}$ pfd, my expectation for Statistical Testing (ST) is that 50,000 tests will be performed on the PS. This figure is based on standard statistical theory and as such is the only way that probabilistic claims can be validated for complex systems. EDF and AREVA have committed to undertake a minimum of 5,000 tests and an analysis is to be undertaken to determine the reasonable practicability of increasing the number of tests within GDA. However, it is acknowledged that, due to the need to perform this task in the later phases of the project, assessment of the results of ST and of the detailed design of the test set-up cannot be performed within the timescale of this assessment, and the following Assessment Finding is raised.

> *GDA Assessment Finding: **AF-UKEPR-CI-026** - The Licensee shall implement a series of statistical-based tests (i.e. as justified in response to GDA Issue **GI-UKEPR-CI-02**, see below) as one component of the ICBMs for the UK EPR™ Protection System.*
>
> [Required Timescale: prior to power raise.]

219 However, a more definitive view on the number of tests that it is reasonably practicable to perform on representative hardware is required. Prior to the detailed implementation to be performed during the SSP, I expect EDF and AREVA to more fully define the ST approach in terms of the number of tests. A commitment to perform 5,000 of these tests on representative TXS hardware has already been made and the feasibility of increasing the number of tests performed on representative hardware needs to be investigated.

220 EDF and AREVA are to investigate the potential for performing 50,000 statistical tests on a simulator as a research activity. EDF and AREVA are required to submit its analysis of the number of tests that is considered reasonably practicable to undertake on representative hardware, having given full consideration to any time and programme constraints.

221 It remains my expectation that 50,000 tests will be performed on representative TXS hardware. I consider that the plant transients should be sufficiently defined to allow a reasonably accurate definition of the time to undertake the tests to be established. I believe that undertaking this analysis and developing a monitorable programme under the scope of GDA will give good guidance to the site specific programmes sufficiently early in the process to ensure that adequate time can be given to the ST process without causing delays to the plant going into operation.

222 Other elements of the ICBM safety case leg are static analysis (SA) and compiler validation (CV). EDF and AREVA's intentions for each of these important activities needs to be fully defined. The feasibility and full extent of the application of SA to the PS application code needs to be confirmed. To date, EDF and AREVA have reported that a feasibility study indicates that the technique is viable, but EDF and AREVA have stated that further work is required to ensure the technique is scaleable and applicable to the full scope of the PS application code.

223 With regard to CV, EDF and AREVA are considering a number of options, including either the use of a Source to Code Comparison (SCC) process (similar to that used to qualify the code of the Sizewell B Primary Protection System) or the use of a compiler validation test suite. My expectation is that SCC will be performed unless a convincing argument is presented that this approach is not reasonably practicable.

224 The ICBM approach (i. e. scope, depth and rigour) needs to be fully defined before I can come to a final conclusion on the adequacy of the safety case for the PS, and the following GDA Issue is raised.

> *GDA Issue:* ***GI-UKEPR-CI-02*** *- Protection System Independent Confidence Building Measures. The programme of Independent Confidence Building Measures (ICBMs) to support the safety case for the TXS Protection System to be fully defined and agreed.*
>
> - ***GI-UKEPR-CI-02.A1:*** *The programme of Independent Confidence Building Measures (ICBMs) to support the safety case for the TXS Protection System to be fully defined and agreed. The proposed elements that will constitute the ICBMs are ST, SA and CV. For further guidance see* ***GI-UKEPR-CI-02.A1*** *in Annex 2, T16.TO2.09 in Annex 6, and T15.TO2.07, T15.TO2.18 and T15.TO2.19 in Annex 5.*

225 In relation to the demonstration of the fitness for purpose of the PS, a number of requested documents were not made available within the timescale of this review. In addition, some versions of documentation provided did not align with the equipment and processes to be used for the UK EPR™ PS. The following GDA Assessment Finding has been raised requiring the Licensee to address the adequacy of these items.

> *GDA Assessment Finding:* ***AF-UKEPR-CI-027*** *- The Licensee shall produce a full set of UK EPR™ PS development records demonstrating compliance with the requirements of the development process (e.g. D-01.3: Master Test Plan, D-01.4: Protection System - System Requirements Specification) and method documents. Traceability of requirements and qualification of tools should also be addressed.*

For further guidance see T16.TO2.10, T16.TO2.12, T16.TO2.13, T16.TO2.14, T16.TO2.15, T16.TO2.16, T16.TO2.17 and T16.TO2.20 in Annex 6.

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

226 The findings arising from my assessment of the PS are documented in this section in GDA Issues and Assessment Findings, however, the report does not cover all the detailed assessment work performed where aspects of the PS were assessed and found to be satisfactory. A good example of such an aspect was that of inter-train PS communications. The PS design includes the use of communication links between the four redundant trains; such links have the potential to compromise the independence of trains and are a potential source of CCF across all four trains.

227 During my assessment, the justification for having such links (e.g. the four-train redundant architecture requires communications in order to perform two-out-of-four, two-out-of-three and one-out-of-two voting), and the design features which minimise the potential for such links to compromise the independence between trains and to introduce CCF were assessed. Design aspects assessed included communications protocols and arrangements for electrical segregation. The samples of data selected for assessment confirmed that the inter-train communications were constrained to the necessary exchange of information needed to perform voting of demands to initiate reactor trip or Engineered Safety Features Actuation System functions. Following my assessment, I was content that EDF and AREVA had provided adequate justification for the existence of the links and the sampled aspects of the links design that were assessed did not reveal any features that indicated the design was not adequate.

228 In conclusion, although the analysis of supporting evidence for the PS performed to date has not revealed any matters of concern which would preclude this system being used in its proposed role, there remains a significant programme of work to complete. In particular, it is essential that the current high-level proposals for ICBM activities are developed into a monitorable programme in order that I can gain sufficient confidence that adequate assessment will be performed before this system is placed in service. These concerns are reflected in the GDA Issues and Assessment Findings raised in this section of the report.

4.4.1.2 Assessment of SAS / PAS

229 The UK EPR™ Class 2 SAS and Class 3 PAS are to be hosted on the SPPA-T2000 platform. Although the SAS and PAS systems are hosted on the same hardware platform, the proposed configurations of these systems is different, with the design of the SAS reflecting the higher safety significance of the functions performed by this system (the SAS performs functions to back up the PS under certain fault conditions). Given the different safety significance of these systems, assessment resources have been focused on the SAS.

230 The main role of the SAS is to provide Category B and Category C safety functions. Part of the SAS is known as the Plant SAS and this part provides, amongst other functions, post-accident management automated and manual functions necessary to bring the plant to safe shutdown, functions related to support systems such as ventilation and functions preventing significant radioactivity release in the event of a severe accident occurring. There is also a part of the SAS known as the RRC-B (Risk Reduction Category – B) SAS, and this component is dedicated to severe accident RRC-B functions. The SAS is seismically qualified. In order to provide defence

against common cause failures, which can be potentially generated by internal and external hazards, the SAS contains four divisions which are physically and electrically independent.

231 The main role of the PAS is the monitoring and control of the plant in all normal operating conditions. In addition, the PAS performs some monitoring and control functions related to risk reduction. The functions implemented in the PAS are categorised as F2/NC (Category C / non-categorised) by EDF and AREVA.

232 The SAS and the PAS both perform:

- data processing, data acquisition and data conditioning;
- processing of application calculations: closed loop controls, generation of individual and grouped commands (simultaneous or sequential), controls prioritisation, generation of various information intended for other I&C units etc; and
- processing of monitoring signals and the generation of alarms.

233 An assessment of the compliance of the SAS / PAS against international standards, which constitute relevant good practice, was undertaken. The relevant standards are BS IEC 61513:2001 (Ref. 10) covering system-level requirements, BS IEC 62138:2004 (Ref. 36) covering software requirements and BS IEC 60987:2007 (Ref. 18) covering hardware requirements. Key supporting evidence was provided by EDF and AREVA in the form of Quality Plans, and assessment of EDF and AREVA records did not reveal any issues which indicated that the SAS / PAS systems were not appropriate for their proposed roles. Assessment against the hardware standard was limited due to insufficient records being made available by EDF and AREVA. Assessment Finding **AF-UKEPR-CI-002** was raised under Section 4.2 to ensure that adequate justification for these systems against relevant good practice is provided.

234 As a result of the changes implemented in response to **RI-UKEPR-002**, the safety case reliability claims for the SAS have been reduced to a probability of failure of 1x10^{-2} pfd. I consider that this claim is broadly compatible with my expectations for this type of system. However, although EDF and AREVA have provided a reliability justification based upon the hardware design of the platform / system, an equivalent justification for the software has not been provided, and I have raised GDA Issue Action **GI-UKEPR-CI-06.A3** to cover this issue.

235 The assessment work reported under Section 4.1 covering HSE SAPs identified a number of SAPs relevant to the SAS / PAS. It has not been possible to confirm conformance to all relevant sampled HSE SAPs within the timescale of this review, and I have raised GDA Issue Action **GI-UKEPR-CI-03.A1** to cover this issue. The TSC review has identified areas where further evidence is required in order to provide an adequate CAE trail, for example (see Annex 6):

- EDR.1 (failure to safety) - no FMEA for the SPPA-T2000 was provided (see T16.TO2.22 items a) and b));
- EDR.2 (redundancy, diversity and segregation, paragraph 170) - no consideration of systematic software failure was identified (see T16.TO2.23);
- EDR.3 (Common cause failure) - no consideration of CCF of PAS (SAS is considered) (see T16.TO2.24);
- EQU.1 (qualification procedures) - CAE trail for qualification not addressed for SPPA-T2000 (see T16.TO2.25);

- EMT.7 (functional testing) - justification of scope of periodic testing (see T16.TO2.26); and
- ESR.5 (standards for computer-based equipment) - relevant SAS information was provided but no PAS information was provided to justify standards compliance (see T16.TO2.27).

236 I have raised GDA Issue Action **GI-UKEPR-CI-03.A1** to cover the generic issue of provision of an adequate CAE evidence trail. The following Assessment Finding is raised to ensure that SAS / PAS conformance is achieved against the relevant HSE SAPs listed in the previous paragraph (the evidence trail to be addressed under GDA Issue Action **GI-UKEPR-CI-03.A1** should be updated accordingly):

> *GDA Assessment Finding: **AF-UKEPR-CI-028** - The Licensee shall demonstrate the adequacy of conformance of the SAS / PAS to EDR.1 (failure to safety), EDR.2 (redundancy, diversity and segregation), EDR.3 (Common cause failure), EQU.1 (qualification), EMT.7 (functional testing) and ESR.5 (standards for computer-based equipment). For further guidance see T16.TO2.22, T16.TO2.23, T16.TO2.24, T16.TO2.25, T16.TO2.26 and T16.TO2.27 in Annex 6.*
>
> [Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

237 In conclusion, my assessment has not revealed any issues which would preclude the use of the SAS and PAS systems in their proposed roles. While broadly satisfied, the relevant GDA Issues and Assessment Findings need to be resolved.

4.4.1.3 Assessment of the NCSS

238 In response to **RI-UKEPR-002** EDF and AREVA committed to modify the C&I architecture and introduce the Non-Computerised Safety System (NCSS). The NCSS will be implemented using diverse technology to that of the computer-based TXS and SPPA-T2000 platforms.

239 The NCSS 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. Allocation of functions to the NCSS should ensure that HSE SAP (Ref. 4) risk targets are met. The automatic functions will be implemented within the NCSS equipment in the four C&I divisions using a two-out-of-four 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 the time available under the relevant accident scenarios, as justified by human factor's analysis).

240 It has not been possible to complete the assessment of the system as insufficient information has been made available within the time frame of this review. I have raised GDA Issue Action **GI-UKEPR-CI-01.A1** (see Section 4.5) to cover this issue (see also T16.TO1.02 in Annex 6).

4.4.1.4 Assessment of Other SIS

241 The PICS is a Class 3 system that provides the main operator interface in the MCR, Technical Support Centre and the RSS. In the event of PICS failure, the SICS provides facilities to allow the operators to perform all necessary functions required with respect to maintaining plant safety. The PICS provides the display and data

logging facilities I would expect of a modern Data Processing System. The PICS has a considerable level of redundancy in that formats can be displayed at any of the multiple operator workstations and communications is by dual-redundant data highway (it is noted that the plant design does not require this system to meet the single failure criteria).

242 The role of the PICS, with respect to its communications interface with the PS, has changed in response to **RI-UKEPR-002** as in the original design PICS transmitted signals directly to the PS. In response to the RI, EDF and AREVA have proposed that a Class 1 Human Machine Interface (HMI) be provided, which may be used by operators to adjust and monitor PS parameters (e.g. permissives). The design of the Class 1 HMI has not been submitted within the timeframe of this assessment and I have raised GDA Issue Action **GI-UKEPR-CI-06.A6** to address this concern.

243 The Process Instrumentation Pre-Processing System (PIPS) provides signal processing (signal conditioning and / or signal multiplication) as required for the analogue and binary signals delivered by sensors and acquired by C&I systems based on the TXS platform. It also provides isolation between the sensors and downstream systems. The signals pre-processed by the PIPS are used by a number of systems, including the:

- Protection System (PS);
- Safety Automation System (SAS) for sensors shared with the PS; and
- Non-Computerised Safety System (NCSS) for the sensors shared with the PS.

244 The proposed UK EPR™ C&I architecture contains four sets of PIPS equipment, one located in each of the four plant divisions, with the RCC-E (Ref. 24) principles of electrical segregation to be applied between divisions.

245 TXS conditioning modules are used to implement the PIPS and these are generally designed using conventional electronics technology. However, there are some exceptions where computer-based technology is used (e.g. thermocouple signal processing modules). PIPS modules are classified depending upon their function (Class 1 to Class 3).

246 The PIPS has the potential to be the source of CCF of protection functions provided by a number of systems which are claimed to be diverse (e.g. PS, NCSS and SAS). The PIPS has a very high reliability claims and makes use of computer-based technology. Therefore, I have raised GDA Issue Action **GI-UKEPR-CI-06.A9** (see Section 4.5) to cover the production of further substantiation of the adequacy of the PIPS.

247 The Class 1 Priority and Actuation Control System (PACS) is described in the PCSR (Ref. 22) as being a system that controls and monitors each actuator under all plant operating conditions. The PACS prioritises actuation commands to the electrical switchgear powering an actuator received from the control systems (e.g. PAS) and protection systems (e.g. SAS and PS). The PACS proposed for the UK EPR™ will be implemented using conventional C&I technology (e.g. relays and contactors). No technical design details concerning the design proposed for the UK EPR™ PACS were available for assessment within the timescales of this review. I consider the correct operation of PACS to have very high nuclear safety significance.

> *GDA Assessment Finding: **AF-UKEPR-CI-029** - The Licensee shall demonstrate that adequate arrangements are in place to ensure that the UK EPR™ Class 1 PACS meets relevant design standards, adequate defences against CCF are*

provided and correct prioritisation is provided. For further guidance see T17.TO2.08, T17.TO2.19 and T17.TO2.27 in Annex 7.

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

248 EDF and AREVA have stated that the UK EPR™ SICS will be based on conventiona l C&I technology (e.g. pu sh buttons, light indicators, analogue displays and recorders). Such systems are generally amen able to a ri gorous safety demonstration due to t heir simplicity. However, insufficient information was provided to enable me to perform a n assessment of the UK EPR™ SICS within the timeframe of this revie w (e.g. the SICS quality plan was included within the sc ope of GDA by EDF and AREVA but was not provided).

GDA Assessment Finding: ***AF-UKEPR-CI-030*** *- The Licensee shall demonstrate that adequate arrangements are in place to ensure that the UK EPR™ Class 1 SICS meets relevant design standards. For further guidance see T16.TO2.32 in Annex 6.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

249 I had planned to perform a sample based assessment of EDF and AREVA's arrangements covering the development and qualification of the Class 1 display system, which was proposed in response to **RI-UKEPR-002**. However, insufficient evidence was made available within the timescale of this review and GDA Issue Action **GI-UKEPR-CI-06.A6** has been raised to cover this issue (for further guidance see T16.TO1.03 in Annex 6).

250 To summarise my conclusions.

- Assessment effort has been directed at the most safety significant systems, in particular the PS. The depth and breadth of the assessment of the PS achieved reflects the priority allocated to this system.
- Assessment of the PS has not revealed any issues which would preclude its use in the UK EPR™. However, there are GDA Issues and Assessment Findings that need to be resolved. Of particular importance is resolution of the scope and depth of the ICBMs.
- Assessment of the SAS / PAS was limited due to the lack of documentation provided within the timescale of the review. No issues have been revealed to date which would preclude their use in the UK EPR™. However, the proposed platform (SPPA-T2000 S5) may not be available for the UK EPR™ due to obsolescence.
- The assessment of the SICS, PIPS and PACS, was limited and GDA Issues and Assessment Findings have been raised to cover these systems.

4.4.2 GDA Step 4 Findings

251 The Assessment Findings and GDA Issues re corded in the section above are listed in Annex 1 and 2 respectively.

4.4.3 GDA Close-out Assessment

252 This section addresses resolution of GDA Issue **GI-UKEPR-CI-02** on d efinition of PS ICBMs. GDA Issue **GI-UKEPR-CI-02** requires the programme of ICBMs to support the

safety case for the TXS PS to be fully defined and agreed. A technical assessment guide (Ref. 9) addresses the expectations for ICBMs and covers, for example, consideration of the application of statistical testing and static analysis to the final production software. The main elements that comprise the PS ICBMs proposed by EDF and AREVA are statistical testing, static analysis and compiler validation.

253 EDF and AREVA submitted six documents (see Annex 10) in response to this GDA Issue covering:

- scope of the overall ICBMs;
- scope of compiler validation and static analysis;
- statistical testing of the PS and research proposals on use of platform simulation for statistical testing; and
- compiler validation and static analysis (using Malvern Program Analysis Suite (MALPAS)) feasibility studies.

254 The submissions were reviewed and requests for clarification were raised by TQ (13 TQ forms raised on this topic). As appropriate, the submitted documents were revised by EDF and AREVA to address the points in the TQs. The description of the scope of work performed by the TSC and the TOs arising from the work are contained in a TSC report (Ref. 75). Annex 12 provides a summary of the TSCs' report including details of the TOs raised.

255 In defining the PS ICBMs (Ref. 24 2), EDF and AREVA divided the PS into PS "c ore" and "interface" units. The PS interface units are not involved in the real time computation of reactor trip or Engineered Safety Features Actuation System (ESF AS) actuations but allow the operator to activate permissives and resets. Separate ICBM proposals were made for the PS core and interface units. EDF and AREVA use a reliability claim that is specified as a probability of failure of 1x10^{-4} pfd for the PS core units and 1x10^{-3} pfd / pdfy for the interface units. The use of a 1x10^{-3} pfd / pdfy figure for the PS interface units is justified by EDF and AREVA on the basis of probability of failure of operator actions (1x10^{-3} pdfy), non-interference arguments, the equipment is Class 1 (e.g. software to BS IEC 60880:2006) and the only difference in the ICB Ms is the absence of SCC.

256 EDF and AREVA provided an explanation of the potential impact of PS interface unit failures on the PS core (in response to TQ-EPR-1607, Ref. 86), which has shown that credible failures are limited to a small number that are the same as operator error for which further analysis will be undertaken during the SSP (see **AF-UKEPR-CI-033** below). The adequacy of the PS ICBMs for PS core and interface units is discussed below.

257 The statistical testing of the PS (Ref. 80) will involve 50,000 tests in total, including a run of 46,500 statistical tests on one division (i.e. using a test guardline configured to be representative of one of the PS divisions) with 500 statistical tests on each of the other divisions (i.e. using the test guardline configured to be representative of each of the other PS divisions). The balance of tests is made up of 500 tests on each division targeted at the functionality that is not implemented in all four divisions. The tests will challenge the functionality of the PS core units with the PS interface units being used to set up the correct conditions for the statistical tests. I am content with the proposal for statistical testing of the PS. However, statistical testing is an area of ongoing research and will need to be kept under review for developments that could enhance the efficacy of the statistical testing.

258 EDF and AREVA have reviewed the feasibility of undertaking SCC as a means of validation of the PS source code compilation tools (covering compiler, linker and loader). The PS makes use of a graphical language notation using pre-defined Function Blocks for the development of the application code. In addition, there are also pre-developed Function Block library code, and firmware within I/O and communication modules that have to be considered. Following completion of the feasibility studies EDF and AREVA confirmed that, for the PS core units, SCC will cover all of the application code, Function Block library code required by the application, TXS system software, and firmware embedded in the I/O and communications modules.

259 EDF and AREVA have provided a compilation tool chain justification for the PS interface units based on independent review of the compiler tool chain in accordance with BS IEC 60880:2006 and testing of the executable code (e.g. commissioning tests, independent review of the test programme and statistical testing). The measures are consistent with EDF and AREVA's ICBM recommendations (Ref. 81) for a reliability claim specified as a failure probability of $1x10^{-3}$ pfd / pdfy.

260 EDF and AREVA have stated that the reasonable practicability of applying the SCC to the PS interface modules is dependent upon the level of automation that can be achieved for the SCC process following development of the SCC tools. While the approach to PS interface units' ICBM is acceptable, I have raised an Assessment Finding to ensure that the licensee rigorously investigates the reasonable practicability of applying SCC to the PS interface units (see below).

261 EDF and AREVA have reviewed the feasibility of undertaking static analysis (using MALPAS) of the PS software. Following this review EDF and AREVA confirmed that static analysis using MALPAS (i.e. including compliance analysis) will cover the PS application code for the core and interface units, Function Block library code used by the PS, firmware within I/O and communication modules, and TXS system software (excluding the RTECONF module). The static analysis feasibility study (Ref. 82) concluded that MALPAS compliance analysis is not feasible on the RTECONF module, which is used to configure the TXS run time environment for the specific application. An alternative approach (Ref. 83) of integrity checking and functional analysis by back translation is proposed for the RTECONF module.

262 EDF and AREVA undertook a review of the Control and Instrumentation Nuclear Industry Forum (CINIF) research on approaches to assessing the adequacy of concurrent processes in real time multi-tasking systems (Ref. 84). Following this review, EDF and AREVA have proposed to undertake further work to determine the feasibility of applying concurrency analysis using SPIN / Promela. In particular, a Promela model of the code scheduler that runs on the TXS SVE2 processing module will be developed providing CINIF research confirms the feasibility of the approach. If not, other approaches such as manual review will need to be adopted in order for the ICBM proposals to satisfy the EDF and AREVA ICBM guidance contained in Ref. 81 (i.e. for concurrency analysis).

263 Following assessment of EDF and AREVA's submissions in response to GDA Issue **GI-UKEPR-CI-02** on definition of PS ICBMs, I am content that the programme of ICBMs to support the safety case for the TXS PS has been adequately defined and that the GDA Issue can be closed. I have raised an Assessment Finding below to capture those matters arising from the assessment that need to be addressed during the implementation of the ICBMs.

*GDA Assessment Finding: **AF-UKEPR-CI-033** - The Licensee shall implement a rigorous programme of PS ICBMs covering:*

- *Statistical and functional testing based on 50,000 tests of which 48,000 will be statistical (see also **AF-UKEPR-CI-026**), taking cognisance of any emerging research results.*
- *Static analysis (using MALPAS) and concurrency analysis (using SPIN / Promela if demonstrated to be feasible or other means such as manual review).*
- *Functional analysis (by reverse engineering) and integrity checking of the RTECONF module.*
- *Source to Code Comparison (including completion of an As Low As Reasonably Practicable (ALARP) demonstration if it is considered not reasonably practicable to apply the SCC technique to the PS interface units).*

Also, to ensure the justification of PS core units' non-interference by the interface units is completed (i.e. as committed to in the response to TQ-EPR-1607, Ref. 86).

For further guidance on development of a rigorous programme of PS ICBMs see Technical Observations GICI02.TO2.15 to GICI02.TO2.25 in Annex 12.

[Required Timescale: prior to power raise.]

4.4.4 GDA Close-out Findings

264 The Assessment Finding identified in the section above is also recorded in Annex 1.

4.5 C&I System Level Architecture

4.5.1 GDA Step 4 Assessment

265 At the start of GDA Step 3, an initial assessment of the UK EPR™ C&I architecture was undertaken. In addition to my initial UK EPR™ architecture review, the TSC undertook a detailed review of the UK EPR™ C&I architecture (Ref. 52). Further review of the C&I system level architecture has been undertaken during GDA Step 4, and EDF and AREVA's responses to GDA Step 3 observations and queries raised during GDA Step 4 have been considered. An important element of the GDA Step 4 work was a review of the evidence presented by EDF and AREVA that supports the architecture related claims and arguments presented in the PCSR and identified references. A summary of the outcome of the TSC's Step 4 review of C&I system level architecture and RP responses to **RI-UKEPR-002** including TOs can be found in Annexes 7 and 9 respectively.

266 The C&I system level architecture (see Ref. 22) is comprised of:

- systems implemented using the TXS platform;
    - i) Protection System,
    - ii) Reactor Control, Surveillance and Limitation System,
    - iii) Severe Accident I&C system;
- systems implemented using the SPPA-T2000 platform;
    - i) Safety Automation System,
    - ii) RRC-B Safety Automation System,
    - iii) Process Automation System,

iv) Process Information and Control System;

- Safety Information and Control System;
- Priority and Actuation Control System;
- Process Instrumentation Preprocessing System;
- sensors and actuators;
- networks (e.g. Class 2 network (SAS Bus) and Class 3 networks (Plant Bus and Terminal Bus));
- Non-Computerised Safety System (introduced in response to **RI-UKEPR-002**); and
- Class 1 displays and controls interfacing to the Protection System (introduced in response to **RI-UKEPR-002**).

267 The objective of the C&I system level architecture reviews was to consider the overall system architecture (C&I systems) looking at safety design features of the UK EPR™ submission, namely:

- defence-in-depth and failure mode management including CCF;
- independence and diversity;
- provision for automatic and manual safety actuation; and
- appropriateness of equipment type / class.

268 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. A key aspect of this is to establish that a failure in a lower safety class system does not frustrate the correct operation of systems of a higher safety class. Another important claim that should be justified is the robustness to failure of other systems involved in communication of important safety display information sent to the main control room. The rigorous 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. Further evidence should be made available to substantiate the adequacy of the UK EPR™ C&I architecture.

*GDA Assessment Finding: **AF-UKEPR-CI-031** - Definition and assignment of functions to C&I SIS - The Licensee shall ensure that for the UK EPR™ there is a rigorous definition of the overall system architecture, the assignment of functions to SIS, interfaces and independence requirements. For further guidance see T17.TO1.02, T17.TO1.25, T17.TO2.03, T17.TO2.10, T17.TO2.17, T17.TO2.26 and T17.TO2.27 in Annex 7; and T18.TO2.03 and T18.TO2.07 in Annex 8.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

269 The GDA Step 3 assessment revealed that the C&I architecture was overly complex with reliance on two computer-based systems (originally developed by the same company) and a high degree of connectivity between systems. My judgement was that the independence between the Class 1 PS and other SIS (Class 2 / 3) was significantly compromised.

270 A particular concern was that lower safety class systems were able to write (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 was not applied in the UK EPR™ design). Other significant concerns identified included:

- the absence of a safety Class 1 display system with no Class 1 manual controls or indications either in the Main Control Room or Remote Shutdown Station;
- alignment of the EPR function categories / equipment class assignments in accordance with UK expectations as defined in BS IEC 61226:2005 (Ref. 13); and
- substantiation of the reliability claims for the computer-based SIS that use the TXS and SPPA-T2000 platforms (e.g. PS, SAS and PAS).

271 I considered that the PCSR PSA reliability claims for C&I systems (i.e. specified as a probability of failure of 10^{-5} pfd for the common 'Processing (non-specific)' parts of the TXS PS and 10^{-4} pfd for the Siemens SPPA-T2000 platform) that provide reactor protection would prove very difficult if not impossible to substantiate. The original claim on the PS system was beyond the normal limit for reliability claims as stated in nuclear sector standards and guidance (i.e. specified as a probability of failure of 10^{-4} pfd), and the claim for the Siemens SPPA-T2000 platform was at the limit (for relevant guidance and standards see Refs 5, 9, 12, 13, 14 and 15, and also guidance of the French safety advisory group to ASN (Ref. 16)).

272 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 was unlikely to be any margin for reducing the claimed C&I system reliabilities to more credible values without significantly increasing the plant's risk estimates to levels which are close to or in excess of the HSE SAP Basic Safety Levels (i.e. Target 8 and Target 9, see Ref. 4).

273 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. 26). In response to **RI-UKEPR-002**, EDF and AREVA provided further substantiation of the UK EPR™ C&I design and provided a number of key commitments including to undertake a number of modifications to the UK EPR™ C&I architecture (Refs 50 and 54). The main commitments are summarised below:

- implementation of one way communication from the PS to the lower classified systems (exceptions to be justified on a case-by–case basis);
- classification of the SICS control and display system as Class 1, all signals transmitted between the SICS and the PS will use a Class 1 path;
- implementation of a Class 1 Qualified Display System (QDS) to provide PS commands that were previously initiated from the Class 3 PICS;
- reduction of reliability claims for the TXS (the specified failure probability limit is changed from 1 x 10^{-5} pfd to 1 x 10^{-4} pfd) and SPPA-T2000 (1 x 10^{-4} pfd to 1 x 10^{-2} pfd) platforms; and
- introduction of the NCSS (with a specified failure probability limit of 1 x 10^{-3} pfd) to provide protection and controls in case of total loss of C&I functions from the TXS and SPPA-T2000 platforms.

Note: Change modification forms (numbers 14, 15, 26 and 27) have been raised by EDF and AREVA to implement the associated design changes, see Ref. 66 for further details.

274 My assessment of EDF and AREVA's response to **RI-UKEPR-002** led me to conclude that, while there were outstanding actions to complete, the majority of the key actions associated with the RI had been addressed. As a result **RI-UKEPR-002** was closed in November 2010 and the remaining outstanding actions were transferred to a regulatory observation (i.e. **RO-UKEPR-82**). A number of **RO-UKEPR-82** actions remain open and a GDA Issue has been raised to cover the necessary actions. There are nine actions under this GDA Issue on C&I Architecture and related matters.

*GDA Issue: **GI-UKEPR-CI-06** - Issues Arising from **RI-UKEPR-002** – In response to our assessment, EDF and AREVA have agreed architecture changes, categorisation changes and have committed to develop a programme of Independent Confidence Building Measures to support the EPR C&I safety case. The nine actions under this GDA issue are concerned with C&I architecture and related matters.*

- ***GI-UKEPR-CI-06.A1**: EDF and AREVA to provide a comprehensive justification of diversity and independence between NCSS / PS, NCSS / SAS-PAS and PS / SAS-PAS commensurate with the level of design for a pre-construction safety report. For further guidance see **GI-UKEPR-CI-06.A1** in Annex 2; T16.TO2.21 in Annex 6; T18.TO1.03, T18.TO1.04 and T18.TO2.09 in Annex 8; and T20.A1.2.3 and T20.A1.3.4 in Annex 9.*

- ***GI-UKEPR-CI-06.A2:** EDF and AREVA to provide a justification of the reliability figures used for each of the protection systems when claimed independently and in combination. The response should include consideration of systematic and hardware failures, and compliance with appropriate guidance and standards. For further guidance see **GI-UKEPR-CI-06.A2** in Annex 2; T16.TO2.21 in Annex 6; and T20.A1.4.1 and T20.A1.4.2 in Annex 9.*

- ***GI-UKEPR-CI-06.A3:** EDF and AREVA to provide a justification of the approach to be used to demonstrate the adequacy of CBSIS including identification of production excellence and independent confidence building measures. For further guidance see **GI-UKEPR-CI-06.A3** in Annex 2 and T20.A1.4.1.a in Annex 9. Note that the Protection System's independent confidence building measures are addressed by **GI-UKEPR-CI-02** (see Section 4.1).*

- ***GI-UKEPR-CI-06.A4:** EDF and AREVA to revise the 'Protection System – System Description NLN-F DC 193' (Ref. 56) to reflect the revised design and to provide full justification for the design, including the justification of hardwired links to the PS. For further guidance see **GI-UKEPR-CI-06.A4** in Annex 2; T17.TO1.04 in Annex 7; and T20.A2.2.1 and T20.A2.2.3 in Annex 9.*

- ***GI-UKEPR-CI-06.A5:** EDF and AREVA to provide a detailed substantiation of independence between PICS Class 3 and SAS Class 2 systems. For further guidance see **GI-UKEPR-CI-06.A5** in Annex 2 and T20.A2.3.2 in Annex 9.*

- ***GI-UKEPR-CI-06.A6:** EDF and AREVA to provide detailed substantiation of the Class 1 control and display facilities to be provided in the MCR and RSS. A BSC for the Class 1 control and display system to be provided and also a justification in terms of the functional coverage of this system. For further guidance see **GI-***

UKEPR-CI-06.A6 in Annex 2; T16.TO1.03 in Annex 6; T17.TO1.14, T17.TO1.15 and T17.TO2.16 in Annex 7; and T20.A3.6 in Annex 9.

- ***GI-UKEPR-CI-06.A7:** EDF and AREVA to justify why it is not reasonably practicable for the SICS controls to be in a functional state during normal operation. For further guidance see **GI-UKEPR-CI-06.A7** in Annex 2.*
- ***GI-UKEPR-CI-06.A8:** EDF and AREVA to provide evidence, for those functions important to safety which use the Class 3 Terminal Bus and / or Plant Bus, that end-to-end response time requirements are achievable by design. For further guidance see **GI-UKEPR-CI-06.A8** in Annex 2; and T20.A5.4 and T20.A5.5 in Annex 9.*
- ***GI-UKEPR-CI-06.A9:** EDF and AREVA to provide detailed substantiation for the probabilistic claims for any C&I components used by more than one line of protection (e.g. sensors, smart devices, PIPS and PACS). The response to include consideration of the potential for common mode failure as a result of the use of these components. For further guidance see **GI-UKEPR-CI-06.A9** in Annex 2; T17.TO2.07, T17.TO2.08 and T17.TO2.28 in Annex 7; T18.TO1.02, T18.TO1.05 and T18.TO2.06 in Annex 8; and T20.A1.3.1 and T20.A1.3.5 in Annex 9.*

EDF and AREVA have provided submissions that might address some aspects of the above actions (e.g. **GI-UKEPR-CI-06.A4**, **GI-UKEPR-CI-06.A5** and **GI-UKEPR-CI-06.A7**) but they were provided too late for review within GDA Step 4.

275 Closure of the **RI-UKEPR-002** actions on categorisation and classification were progressed under a transverse issue **RO-UKEPR-43**. EDF and AREVA have provided a response that addresses the concerns raised in the RI and RO (Refs 42, 50 and 57). In particular, EDF and AREVA are to ensure the classification of C&I systems is consistent with current good practice as provided by BS IEC 61226:2009 (Ref. 44).

276 The changes already committed to (e.g. SICS will be classified as Class 1, NCSS and the RCSL will be classified as Class 2, and other plant controls will be reallocated to fully comply with BS IEC 61226:2009) have substantially addressed the concern on classification raised under **RI-UKEPR-002** (i.e. that a significant number of the systems were a Class lower than expectations). However, there are areas where the detailed allocation of functions to systems is not yet fully defined (e.g. implementation of diverse lines of protection in Class 2 systems as opposed to Class 3 and reallocation of plant controls). Therefore, further detail of delivery will be required before the issue can be considered closed. GDA Issue action CC-01.A6 has been raised under cross-cutting GDA Issue **GI-UKEPR-CC-01** on Categorisation and Classification (see Ref. 65) to address this concern (e.g. to ensure the class of the C&I systems such as the Class 3 PAS and Class 2 SAS align with ND expectations).

*GDA Issue: **GI-UKEPR-CC-01** - Categorisation and Classification:*[3]

- ***GI-UKEPR-CC-01.A6**: Classification of C&I Systems. - The completion of matters arising from **RI-UKEPR-002** and progressed under **RO-UKEPR-43 (Action 2)**. Classification of C&I systems to be consistent with current good practice as provided by BS IEC 61226:2009 (Ref. 44). For further guidance see*

[3] A summary of this cross-cutting issue action is provided for completeness only. Please refer to Ref. 65 for a full description.

also T17.TO1.01 in Annex 7, and T20.A1.3.1.b, T20.A1.4.1.c and T20.A4.6.2 in Annex 9.

277 EDF and AREVA have provided a commitment that the NCSS will be implemented in diverse technology to the computer-based protection systems. EDF and AREVA have defined the diversity criteria to be used in the selection of the NCSS platform (i.e. to ensure adequate diversity between the NCSS and computer-based protection systems). While EDF and AREVA have committed to provide the NCSS, the detail of the NCSS design was not made available within GDA Step 4. The GDA expectation is that adequate substantiation of the NCSS would be provided. Therefore, I have raised a GDA Issue to ensure adequate substantiation of the NCSS design.

*GDA Issue: **GI-UKEPR-CI-01** - Design Information for the Non-Computerised Safety System Required. Absence of adequate C&I architecture. The proposal to address the issues raised in **RI-UKEPR-002** includes provision of a hardware based backup system known as the NCSS. Detail of the NCSS design has not been made available within GDA. EDF and AREVA have provided a commitment that the NCSS will be implemented in diverse technology to the computer based protection systems. A Basis of Safety Case for the NCSS is required for GDA.*

- ***GI-UKEPR-CI-01.A1:** EDF and AREVA to provide a Basis of Safety Case that includes substantiation of the design of the Class 2 NCSS. An action plan for completion and supply of detailed evidence supporting the basis of safety case document should also be supplied. For further guidance see **GI-UKEPR-CI-01.A1** in Annex 2, and T15.TO1.46 in Annex 5, T16.TO1.02 in Annex 6, T17.TO1.24 in Annex 7 and T20.A1.2.4 in Annex 9.*

278 My assessment has determined that EDF and AREVA's defence-in-depth concept aligns with the five levels referred to in IAEA Safety Standard NS-R-1 (Ref. 27). EDF and AREVA have confirmed that the failure of a system implemented on one of the two main computer-based platforms (i.e. TXS and SPPA-T2000) is protected by functions implemented on the other platform. The introduction of the NCSS to provide protection against the total loss of the computer-based platforms has also significantly improved the C&I SIS defence-in-depth.

279 EDF and AREVA need to ensure that the PCSR is updated to take account of the changes made to address **RI-UKEPR-002** and **RO-UKEPR-43**.

*GDA Assessment Finding: **AF-UKEPR-CI-032** - PCSR Update - The Licensee shall update the PCSR and supporting documentation to take account of the changes made to address **RI-UKEPR-002** and **RO-UKEPR-43**. For further guidance see T17.TO1.11, T17.TO1.14 and T17.TO1.25 in Annex 7; and T18.TO1.01 in Annex 8.*

[Required Timescale: prior to fuel load.]

280 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, which addresses the key architecture related concerns raised in **RI-UKEPR-002**. In particular, the commitment to provide the NCSS, introduce one way network communication from the PS to lower classified systems, Class 1 displays and manual controls, and reduction of reliability claims for the computer-based systems have addressed my major concerns. I conclude that the revised overall C&I architecture is broadly in alignment with expectations for a modern nuclear reactor, but a number of aspects related to GDA Issues and Assessment Findings require resolution, as described in this section.

4.5.2 GDA Step 4 Findings

281 The Assessment Findings and GDA Issues recorded in the section above are listed in Annex 1 and 2 respectively.

4.5.3 GDA Close-out Assessment

282 This section addresses the close-out of GDA Issues arising from the closure of **RI-UKEPR-002** (see above) including outstanding **RO-UKEPR-82** actions (**GI-UKEPR-CI-06**), C&I systems' classification (**GI-UKEPR-CC-01.A6)** and provision of NCSS design information (**GI-UKEPR-CI-01)**. There are nine actions under GDA issue **GI-UKEPR-CI-06** covering C&I architecture and related matters such as demonstration of diversity between the protection systems, definition of CBSIS PE activities and ICBMs, and provision of Class 1 control and display facilities.

4.5.3.1 Diversity and Independence between NCSS / PS, NCSS / SAS-PAS, and PS / SAS-PAS – GDA Issue Action GI-UKEPR-CI-06.A1

283 This section addresses resolution of GDA Issue Action **GI-UKEPR-CI-06.A1** on provision of a comprehensive justification of diversity and independence between the NCSS and PS, NCSS and SAS-PAS, and PS and SAS-PAS commensurate with the level of design for a PCSR (see Ref. 102).

284 The Resolution Plan section addressing diversity (Ref. 73) stated that four documents would be provided as part of GDA Issues **GI-UKEPR-CI-01** and **GI-UKEPR-CI-05**, and that these documents were applicable to **GI-UKEPR-CI-06.A1**. Two of these documents addressed diversity between the two computer based platforms (i.e. TXS and SPPA-T2000) and systems (i.e. PS and SAS) implemented using these platforms (GDA Issue **GI-UKEPR-CI-05**). The other two documents addressed diversity between the non computer based NCSS and the computer based platforms and systems (GDA Issue **GI-UKEPR-CI-01**). Independence of the three systems is addressed under **GI-UKEPR-CI-06.A2** (see Section 4.5.3.2 below).

285 Following a change to the Resolution Plan (Ref. 136) and in response to TQs raised during my assessment, a total of eight documents were delivered for review as part of GDA Issue Action **GI-UKEPR-CI-06.A1** covering:

- overall approach, organisation and methodology for undertaking the diversity analysis;
- diversity criteria; and
- C&I systems' and computer based platforms' diversity analysis.

286 The submissions were reviewed and requests for clarification raised by TQ (three TQ forms were raised on this topic). As appropriate, the submitted documents were revised by EDF and AREVA to address the points in the TQs. The description of the scope of work performed by the TSC and the TOs arising from the work are contained in a TSC report (Ref. 79). Annex 16 provides a summary of the TSC's report including details of the TOs raised.

287 My review of the organisation and management of diversity document (Ref. 137) found it did not fully meet my expectations. For example, the overall approach to diversity management was not described, the criteria for assessing diversity were not identified, and there were a number of topics requiring clarification (e.g. use of complex AV42 modules for prioritising commands to actuators and connection of the service unit during operation). TQ-EPR-1604 (Ref. 86) was raised to convey the result of the

review to EDF AREVA and request responses to the identified concerns. Ref. 137 was updated (Ref. 138) and a supplementary process description was supplied (Ref. 139) to address the identified concerns. Additional documents were also provided to define the diversity criteria (Ref. 140) and the overall approach to diversity (Ref. 141).

288 My review of the updated organisation and management of diversity document (Ref. 138) and the supplement (Ref. 139) found EDF and AREVA had addressed the majority of the points raised in TQ-EPR-1604. This included making changes to the documents (e.g. to confirm the AV4 2 module is not used and the service unit is not connected in operation) or by the addition of references, including to the diversity criteria and overall approach documents (Refs 140 and 141). The residual points of clarification, for example, definition of terms (e.g. main component), were carried forward as part of TQ-EPR-1628 (Ref. 86). The response to TQ-EPR-1628 included a commitment to include the definition of 'main component' (i.e. 'the elements which allow the execution of the safety function') in a further update to Ref. 138.

289 EDF and AREVA have committed to make further improvements to Ref. 138 during the SSP (e.g. by sub-dividing the equipment making up the platform into its constituent parts and conducting a diversity analysis for each part). In addition, improved means for demonstrating and maintaining diversity are to be implemented during the SSP (e.g. introducing the requirement for a diversity review on selection of new equipment). These commitments are set out in a number of places including:

- 'key elements for diversity management methodology improvement - PTI 12.1072 ' (Ref. 143); and
- letter EPR01412N (Ref. 147).

I have captured these commitments in Assessment Finding **AF-UKEPR-CI-037**.

290 My review of the document describing the overall approach to diversity (Ref. 141) identified that it contained a description of the management arrangements for establishing and maintaining platform diversity and for undertaking a diversity analysis. I found the submission adequate, placing the diversity of the systems, sensors, conditioning modules, and actuators in context. I requested clarification of a significant omission in respect of definition of the through life management of diversity. EDF and AREVA's response, contained in letter EPR01412N (Ref. 147), provided a satisfactory description of how system diversity would be maintained through plant life.

291 My review of the diversity criteria for the PS and SAS (Ref. 140) found that EDF and AREVA have established a structured set of diversity criteria for the platforms and systems derived from established standards (e.g. Refs 11 and 169). The criteria covered five categories including design, human and software diversity, and set typically three or four diversity levels of increasing rigour for each category (e.g. human diversity 'Hd = 1' 'Different designers shall perform the design of the two systems' and 'Hd = 2' 'Different engineering management teams with no direct communication, within the same company or entity shall be in place for the design of the two systems').

292 I identified a number of points of inconsistency in the definition of the diversity requirements (e.g. related to the diversity level for 'Interfaces' and clarification of the requirements for software diversity). I asked EDF and AREVA to review these inconsistencies (raised in TQ-EPR-1628, Ref. 86). EDF and AREVA's response adequately addressed the points (e.g. by confirming that the Interface level for networks should be 'Dd = 3' thereby requiring different design methods and clarifying how software diversity requirements are addressed in the document).

293 The revised diversity criteria (Ref. 142) were also reviewed against those proposed for the NCSS, PACS, and the sensors and conditioning modules (Refs 144, 145 and 146). A number of inconsistencies in the definition of the criteria were identified, for example, the signal diversity levels 1 and 2 in one scheme are levels 2 and 3 in another. Resolution of these inconsistencies will need to be addressed during the SSP (see **AF-UKEPR-CI-037**).

294 EDF and AREVA provided a justification of the diversity of the C&I systems in Ref. 148 using the unrevised diversity criteria (Ref. 140). The justification did not meet my expectations. The shortfalls included a lack of clarity on the application of the criteria in different parts of the design and implementation life cycle, in the diversity argument for tools and methods, and in the definition of independence of the teams undertaking the design and implementation work. These concerns were raised with EDF and AREVA in TQ-EPR-1629 (Ref. 86).

295 The response to TQ-EPR-1629 provided by EDF and AREVA adequately addressed many of the points raised. EDF and AREVA also provided an update to the system diversity document (Ref. 149). I found the updated document had successfully addressed the majority of the points in agreement with the text of the TQ response (e.g. by linking the diversity life cycle phases to those of the BS IEC 61513:2001 standard). The points that were not addressed are on the justification of platform diversity (e.g. diversity of the design tools used for the development of the systems) and these will be resolved during the development work in the SSP (see **AF-UKEPR-CI-037** below). In addition, EDF and AREVA committed to undertake a diversity analysis using the improved diversity methodology and criteria (e.g. in the response to TQ-EPR-1629 (Ref. 86) and letter EPR01412N (Ref. 147)).

296 EDF and AREVA provided an analysis of the diversity of the TXS and SPPA-T2000 (version S7) platforms (Ref. 150) that had been undertaken prior to the development of the diversity method and criteria described above. The analysis was accompanied by a corrective action plan (Ref. 151). I confirmed that the key diversity issues, the use of common hardware and software components in the TXS and SPPA-T2000 (version S7) platforms, have been identified by the analysis. The corrective action plan proposes design changes to both platforms and the introduction of design restrictions to establish and maintain platform diversity. The changes are for the TXS platform to be modified to replace AMPRO firmware, and for the SPPA-T2000 platform to be modified to replace the ASPC2 ASIC for Profibus control and not use the Optical Link Module Application Specific integrated circuit (OLMAS).

297 I conclude that EDF and AREVA have submitted a methodology and set of diversity criteria that adequately meets the requirements of this part of the GDA Issue. EDF and AREVA have identified and committed to further work in the SSP to improve and complete the methodology and criteria. I have captured these commitments in Assessment Finding **AF-UKEPR-CI-037** (see below). I am also content that sufficient progress has been made with the platform and system diversity analyses submitted by EDF and AREVA. They have committed to completing the diversity analyses when the C&I design is finalised using the revised methodology and diversity criteria. EDF and AREVA have also committed to design changes to the TXS and SPPA-T2000 (version S7) platforms to improve diversity. These commitments are captured in Assessment Finding **AF-UKEPR-CI-037**.

298 Following assessment of EDF and AREVA's submissions in response to GDA Issue Action **GI-UKEPR-CI-06.A1**, I am content that sufficient progress has been made and that the GDA Issue Action can be closed. I have raised an Assessment Finding below

to capture the matters arising from the assessment that need to be addressed during the SSP.

GDA Assessment Finding: ***AF-UKEPR-CI-037*** *- The Licensee shall:*

- *Complete and update the diversity submission documents (i.e. Refs 138, 141 and 142) in line with the commitments made during the GDA closure phase (i.e. in Refs 141, 143, 147, and TQs TQ-EPR-1628 and TQ-EPR-1629 Ref. 86). For further guidance see Annex 16 Technical Observations GICI06.A1.TO2.06 and GICI06.A1.TO2.07.*
- *Remove inconsistencies in the definition of the diversity criteria for the PS / SAS (Ref. 140), NCSS (Ref. 144), PACS (Ref. 145), and the sensors and conditioning modules (146). For example, the signal diversity levels 1 and 2 in one scheme are levels 2 and 3 in another. For further guidance see Annex 16 Technical Observation GICI06.A1.TO2.08.*
- *Complete the diversity analysis, in line with the methodology and criteria, for the three major C&I platforms (i.e. Teleperm XS, SPPA-T2000 (version S7) and UNICORN), the three major C&I systems built on those platforms (i.e. PS, SAS and NCSS) and other C&I systems built on the platforms if diversity claims are made in the safety case. For further guidance see Annex 16 Technical Observations GICI06.A1.TO2.04, GICI06.A1.TO2.07 and GICI06.A1.TO2.09, and Annex 11 Technical Observation GICI01.TO2.31.*
- *Ensure the final systems using the Teleperm XS and SPPA-T2000 (version S7) platforms include the modifications proposed in Ref. 151. For the Teleperm XS platform replace the AMPRO firmware. For the SPPA-T2000 (version S7) replace the ASPC2 ASIC used for Profibus control. Also to implement the design constraint on SPPA-T2000 (version S7) to prevent the use of the AV42 module and the OLMAS ASIC. For further guidance see Annex 16 Technical Observation GICI06.A1.TO2.04.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site]

4.5.3.2 Justification of Protection Systems' Reliability Figures independently and in Combination - GI-UKEPR-CI-06.A2

299 This section addresses resolution of GDA Issue Action **GI-UKEPR-CI-06.A2** on the reliability and independence of the C&I systems. GDA Issue Action **GI-UKEPR-CI-06.A2** required EDF and AREVA to provide a justification of the reliability figures used for each of the protection systems (i.e. PS, SAS and NCSS) when claimed independently and in combination. The justification to include consideration of systematic and random hardware failures, and compliance with appropriate guidance and standards.

300 The Resolution Plan (Ref. 73) identified three tasks to be performed in order to demonstrate that the PS, SAS and NCSS C&I systems meet their reliability targets. The plan included a fourth task, the demonstration of the independence of the three systems.

301 The submissions were reviewed and requests for clarification were raised by TQ (six TQ forms raised on this topic). As appropriate, the submitted documents were revised by EDF and AREVA to provide the requested clarifications. The description of the scope of work performed by the TSC and the TOs arising from the work are contained

in a TSC report (Ref. 79). Annex 16 provides a summary of the TSCs' report including details of the TOs raised.

302 EDF and AREVA's Resolution Plan for the demonstration that the PS reliability target is met, addresses:

- compliance with standards BS IEC 60880:2006 and BS IEC 60987:2007 (Refs 17 and 18);
- hardware reliability demonstration; and
- definition of a programme of ICBMs.

The last item above was assessed as part of GDA Issues **GI-UKEPR-CI-02** (Section 4.4.3) and **GI-UKEPR-CI-06.A3** (Section 4.5.3.3).

303 EDF and AREVA provided three documents (Refs 152, 153 and 154) to address compliance with standards BS IEC 61513:2001, BS IEC 60880:2006 and BS IEC 60987:2007 (Refs 10, 17 and 18) for the PS. The scope set out in the Resolution Plan was extended to include the BS IEC 61513:2001 (Ref. 10) standard. My review identified that the standards compliance documents above (Refs 152, 153 and 154) did not include information for the TXS platform but referenced documents that contain the platform standards compliance demonstration. I requested submission of these referenced documents in TQ-EPR-1619 (Ref. 86).

304 I also found that entries in the document for compliance to key clauses for the system design and development lifecycle phases have still to be completed (e.g. by inclusion of process evidence). Clauses from the latter stages of the lifecycle, including maintenance and test, are also still to be addressed. Given the stage of the design, the demonstration of compliance for the PS system with the three standards was found to be adequate.

305 EDF and AREVA supplied the standards compliance documents for the TXS platform (Refs 155, 156 and 157) in response to TQ-EPR-1619 (Ref. 86). I found that these compliance documents do not always completely cover all parts of the standards' clauses, for example, the evidence documents required to underpin the claims of compliance including specifications and test results are not identified.

306 I have raised Assessment Finding **AF-UKEPR-CI-002** requiring a demonstration of standards compliance for both the PS system and TXS platform. This compliance demonstration will need to be completed during the SSP and address the points identified during the GDA Issue close-out phase. In particular, to include the evidence from platform and system development (e.g. process, verification and qualification evidence) and to complete the clauses on maintenance and modification (further guidance is provided by the TOs identified in **AF-UKEPR-CI-002**).

307 EDF and AREVA described their approach to determining the PS's hardware reliability in Ref. 158. I found the approach uses the methods set out in IEC 60812:2006 for Failure Modes and Effects Analysis (FMEAs) (Ref. 159) and IEC 61025:2006 Fault Tree Analysis (Ref. 160). The report contained a number of ambiguities, including the identification of the boards and their FMEAs, and lacked the results of the analysis. I raised TQ-EPR-1551 (Ref. 86) seeking clarification and supply of the Reliability, Availability and Maintainability Study (RAMS). EDF and AREVA provided the necessary clarification (e.g. by identifying which boards are used in the system and the identity of their FMEAs). These were also included in the revised report (Ref. 161) that was found to be satisfactory.

308 My review of the RAMS analysis (Ref. 162) identified that the target reliabilities were not met for a small number of functions (e.g. trip on low Departure from Nucleate Boiling Ratio (DNBR)). I sought clarification as to why these shortfalls were acceptable in TQ-EPR-1596 (Ref.86). EDF and AREVA's response confirmed that the PS design or the periodic test arrangements would be modified to ensure the targets are met. I have captured the need to track this commitment in Assessment Finding **AF-UKEPR-CI-038**.

309 EDF and AREVA's SAS reliability demonstration followed the same approach as that for the PS. EDF and AREVA's proposals for PE and ICBMs, which address software reliability demonstration, were assessed as part of GDA Issue **GI-UKEPR-CI-06.A3** and found to be satisfactory, subject to work in the SSP (see Section 4.5.3.3). Standards compliance (e.g. to BS EN 62138:2004) and hardware reliability were assessed as part of GDA Issue **GI-UKEPR-CI-05**, see Section 4.3.3.1. I conclude that EDF and AREVA have provided sufficient evidence, for the purpose of GDA Issue closure, in relation to:

- compliance with standard BS EN 62138:2004 (Ref. 36) for the software of Class 2 systems; and
- the reliability of the hardware (i.e. to give confidence that the S7 version of SPPA-T2000 (and SAS) will achieve the 1x10^{-2} pfd target).

310 The methodology for the reliability analysis of the NCSS, which is based on the UNICORN platform, was described in Refs. 185 and 186. Ref. 186 describes the methodology and identifies the analysis techniques (e.g. FMECA and FTA) used to estimate the reliability of each module. Ref. 185 describes the methodology for combining the module reliabilities to calculate the overall reliability of the NCSS for a function. However, no definitive NCSS reliability data for the actual modules to be used in the NCSS was available during GDA. The reliability data that was presented (Ref. 186) was for existing modules that will be further developed as part of the development of the UNICORN platform. I have raised an Assessment Finding requiring the NCSS reliability to be fully defined, justified and documented during the SSP, see Section 4.5.3.12.

311 My review of EDF and AREVA's submission on the demonstration of independence of the PS, SAS and NCSS (Ref. 163) found that it did not provide the requested demonstration. The document outlined what was needed to provide the demonstration and stated that it would be provided in future supporting deliverables. The document identifies specific areas requiring more work to complete the demonstration of independence including those to be undertaken as the design is completed. The specific areas identified include further work on the assessment of:

- system interconnections;
- dependencies on the Heating, Ventilation and Air Conditioning (HVAC) system and power supplies; and
- standards compliance (i.e. BS EN 62340:2007, Ref. 11 and BS EN 60709:2004, Ref. 164).

312 I raised TQ-EPR-1585 (Ref. 86) to convey the outcome of the review of Ref. 163 to EDF and AREVA. EDF and AREVA provided a comprehensive rewrite of the document (Ref. 165) that addressed the required demonstration of independence. The document also described the separation by division and the generic rules for electrical isolation (further detail on the generic rules for electrical isolation is contained in Ref.

166). Inter-connection of the systems was justified by reference to material arising from resolution of GDA Issue Actions **GI-UKEPR-CI-06.A4** and **GI-UKEPR-CI-06.A5** on non-interference of systems, see Sections 4.5.3.4 and 4.5.3.5. The adequacy of the independence of the redundancies of the HVAC and power supply systems was documented and improvements were also made to the standards compliance tables.

313 In conclusion my review of the revised document (Ref. 165) found it to be satisfactory for the purpose of GDA Issue closure noting that further work is required in the SSP (see **AF-UKEPR-CI-038** below). This includes further work on the demonstration of standards compliance (i.e. Refs 11 and 164) as the detailed design is completed. The adequacy of the failure independence of the HVAC and power supply systems was addressed under GDA Issues **GI-UKEPR-FS-05** and **GI-UKEPR-FS-02** (see fault studies assessment reports, Refs 215 and 87 respectively)**.** The fault studies assessment has led to significant changes to the HVAC and power supply systems , which in turn has necessitated the introduction of additional C&I systems. The new C&I systems designed to control the re-designed HVAC (two safety Class 1 systems) will be developed during the SSP (the Assessment Findings raised by the fault studies assessment of **GI-UKEPR-FS-05** capture the requirements for these new C&I systems, see Ref. 215).

314 My review of the generic rules for electrical isolation (Ref. 166) identified that clarification was required on the selection of isolation type and use of impedance isolation. These points were raised with EDF and AREVA in TQ-EPR-1508 (Ref. 86). EDF and AREVA confirmed that impedance isolation is to be used to protect against AC and DC power supply over voltage. It was clarified (Ref. 167) that impedance isolation may be used within a division and galvanic isolation is used between divisions. Further justification of the use of impedance isolation was sought by TQ-EPR-1558 (Ref. 86). I found EDF and AREVA's response, which included additional information on how the arrangements meet RCC-E (Ref. 24) requirements and an update to the generic rules for electrical isolation (Ref. 168) to include clarification of the approach to selection of impedance or optical electrical isolation, to be satisfactory.

315 EDF and AREVA provided reliability, independence and diversity (see Section 4.5.3.1,) submissions for the three protections systems (PS, SAS and NCSS). I conclude that the information provided by EDF and AREVA is sufficient to demonstrate that the approach to determining the reliability of the protection systems (i.e. PS, SAS and NCSS) is suitable at this stage of the systems' design and development. I also conclude that the submissions support the claim that the reliability of these systems can be claimed in combination. EDF and AREVA have committed to make equipment modifications and undertake further analyses (e.g. see Section 4.5.3.1) during the SSP (i.e. to complete the reliability, independence and diversity demonstration as the designs are completed).

316 Following assessment of EDF and AREVA's submissions in response to GDA Issue **GI-UKEPR-CI-06.A2** on the reliability and independence of the C&I SIS, I am content that the information provided is adequate and the GDA Issue Action can be closed. I have raised an Assessment Finding below to capture the matters that need to be addressed during completion of the detailed design of the PS, SAS and NCSS.

GDA Assessment Finding: ***AF-UKEPR-CI-038*** *– The Licensee shall complete the demonstrations of reliability and independence for inclusion in the safety case, in particular to:*

- *Undertake the modifications to the PS and / or its periodic test arrangements to allow the reliability targets (e.g. for trip on low DNBR by increasing the frequency of periodic tests) to be met.*
- *Complete the hardware reliability evaluations for the final designs of the SIS (i.e. the PS, SAS and NCSS).*
- *Complete the justification of inter divisional and inter system independence and isolation of the SIS.*

For further guidance see Annex 16 Technical Observations GICI06.A2.TO2.11, on the PS modifications and reliability, and GICI06.A2.TO2.06 and GICI06.A2.TO2.14 on independence and isolation.

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

*Note. The SAS and NCSS reliabilities are addressed as part of GDA Issues **GI-UKEPR-CI-05** and **GI-UKEPR-CI-01** respectively. Platform and system diversity is considered in GDA Issue **GI-UKEPR-CI-06.A1**. The adequacy of the independence of the HVAC and electrical supply systems is also considered in GDA Issues **GI-UKEPR-FS-05** (Ref. 215) and **GI-UKEPR-FS-02** (Ref. 87).*

4.5.3.3 Production Excellence and Independent Confidence Building Measures for Computer Based Systems Important to Safety (GI-UKEPR-CI-06.A3)

317 GDA Issue Action **GI-UKEPR-CI-06.A3** required EDF and AREVA to justify the approach to be used to demonstrate the adequacy of CBSIS including identification of PE and ICBMs. My expectations for PE and ICBMs are outlined under **GI-UKEPR-CI-06.A3** in Annex 2. The PS's ICBMs are addressed by **GI-UKEPR-CI-02** (see Section 4.4.3).

318 EDF and AREVA submitted three documents in response to this GDA Issue action, covering:

- generic guidelines for application of PE and ICBMs (Ref. 81); and
- justification of PE and ICBMs for Teleperm XS (Ref. 85) and SPPA T 2000 based systems (Ref. 88).

The two "justification" documents (Ref. 85 and 88) provide the realisation of the generic guidelines (Ref. 81) for each of the two platforms (i.e. Teleperm XS and SPPA-T2000).

319 The submissions were reviewed and requests for clarification were raised by TQ (five TQ forms raised on this topic). As appropriate, the submitted documents were revised by EDF and AREVA to address the points in the TQs. The description of the scope of work performed by the TSC and the TOs arising from the work are contained in a TSC report (Ref. 79). Annex 16 provides a summary of the TSCs' report including details of the TOs raised

320 My review of the generic guidelines for application of PE and ICBMs (Ref. 81) to CBSIS found that the document appeared to be based on the approach proposed by EDF and AREVA for smart devices. It did not fully meet my expectations, for example, in relation to standards compliance, source code analysis for Class 1 systems, statistical testing for Class 1 (1x10 $^{-3}$ pfd) systems and dynamic analysis. Two TQs (TQ-EPR-1504 and TQ-EPR-1550, Ref. 86) were raised to convey the results of my review to EDF and AREVA.

321 The guidelines (Ref. 81) were updated to address my concerns and include EDF and AREVA's proposals on dynamic analysis (i.e. following EDF and AREVA's review of a CINIF research report on analysis of real time multi-tasking software (Ref. 84)). The Licensee will need to ensure that the proposed dynamic analysis is fully comprehensive (e.g. addresses adequacy of tools such as the CodeSonar® tool potentially used for Class 1, 1x10 $^{-3}$ pfd systems and dynamic memory capacity) (see **AF-UKEPR-CI-039** below).

322 I reviewed EDF and AREVA's submission on 'Justification for PE and ICBMs for TXS based systems - ECECC111557' (Ref. 85) and provided comments to them in TQ-EPR-1530 (Ref. 86) and TQ-EPR-1577 (Ref. 86). Points raised with EDF and AREVA included clarification of the scope and rigour of the standards compliance exercises, and independence of staff undertaking ICBMs. Their responses adequately addressed the points, for example, clarifying the independence of EDF staff and the role of Nuclear New Build (NNB) Design Authority (i.e. NNB Design Authority has a separate reporting route to the NNB Hinkley Point C Project Director for reporting issues emerging from implementation of the ICBMs). The justification document (Ref. 85) has been revised to incorporate the responses to my comments (see also Section 4.5.3.2 and **AF-UKEPR-CI-002** on standards compliance).

323 The submission on justification of PE and ICBMs for SPPA-T2000 based systems (Ref. 88) was reviewed and comments raised with EDF and AREVA in TQ-EPR-1605 (Ref. 86). The main concern identified by my review was that EDF and AREVA needed to fully define the scope and depth of the software ICBM. Definition of the ICBM was a major challenge (e.g. as a result of the large amount of assembler code with documentation in German). Other concerns raised included clarification of the scope of the standards compliance exercises, QA process and comprehensiveness of the testing arrangements.

324 The response to TQ-EPR-1605 adequately addressed the points raised. For example, committing to undertake a manual review of key software elements and additional dynamic testing (i.e. 500 tests based on statistical testing principles). However, further detail of the proposed ICBM will need to be produced during the SSP and cover the identification and justification of the key elements to be analysed by the manual review, and the approach to integrity checking and dynamic testing.

325 Following assessment of EDF and AREVA's submissions in response to GDA Issue action **GI-UKEPR-CI-06 A3**, I am content that the GDA Issue action can be closed. I have raised an Assessment Finding below to capture those matters arising from the assessment that need to be addressed during the implementation of the UK EPR™ CBSIS.

GDA Assessment Finding: ***AF-UKEPR-CI-039*** *- The Licensee shall fully define the PE and ICBMs for CBSIS. In particular, to:*

- *Ensure that the generic guidance for CBSIS for concurrency analysis addresses adequacy of tools (e.g. such as the CodeSonar® tool used for Class 1, 1x10^{-3} pfd systems) and dynamic memory capacity.*
- *Complete the definition of the SPPA-T2000 ICBMs including identification and justification of the key elements to be analysed by the manual review, approach to software integrity checking and dynamic testing.*

For further guidance on the completion of the demonstration of the adequacy of the PE and ICBMs for CBSIS see Technical Observations GICI06.A3.TO2.07 and GICI06.A3.TO2.08 in Annex 16.

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

4.5.3.4 Justification of PS Hardwired Links - GI-UKEPR-CI-06.A4

326 This section addresses resolution of GDA Issue **GI-UKEPR-CI-06** on the provision of updated documentation to reflect the design of the PS, including a justification of the hardwired links to the PS. GDA Issue Action **GI-UKEPR-CI-06.A4** requires updated PS documentation and a justification that the hardwired links to the PS, including from systems of a lower safety class, cannot affect the operation of the PS.

327 EDF and AREVA submitted two key documents (see Annex 10) in response to this GDA Issue Action, namely:

- 'Protection System - System Description (Pilot Study) - NLN-F DC 193' (Ref. 56); and
- 'Analysis of the non disturbance of the Protection System by lower classified signals coming from systems in interface - PELL-F DC 252 rev. A' (Ref. 200).

328 The submissions were reviewed and requests for clarification raised by TQ (three TQ forms raised on this topic). As appropriate, the submitted documents were revised by EDF and AREVA to address the points in the TQs. The description of the scope of work performed by the TSC and the TOs arising from the work are contained in a TSC report (Ref. 79). Annex 16 provides a summary of the TSCs' report including details of the TOs raised.

329 The PS system description (Ref. 56) was identified in the Resolution Plan as addressing this GDA Issue Action. My review identified that the following changes had been made to the document.

- A commitment to reduce, as far as possible, the number of hardwired connections to the PS.
- Replacement of the bidirectional communication between PS and RCSL with a unidirectional link towards the RCSL.
- Removal of the bidirectional network link between the PS and the Class 3 C&I systems.
- Replacement of the Class 3 gateway GW1 and the Class 3 network connection to the Monitoring and Service Interface (MSI) with a dual redundant Class 1 Data Interface and Class 1 TXS Profibus network.

330 Whilst these changes reduce external influences on the PS, a full justification that hardwired links cannot affect the PS had not been provided. I also noted that a means to inhibit the signal to the Emergency Feedwater System (EFWS) under periodic test had not been provided. I raised TQ-EPR-1485 (Ref. 86) and TQ-EPR-1522 (Ref. 86) to bring these matters to the attention of EDF and AREVA.

331 The TQ responses indicated that a full justification would be provided in document 'Analysis of the non disturbance of the Protection System by lower classified signals coming from systems in interface - PELL-F DC 252 rev. A' (Ref. 200).

332 I reviewed Ref. 200 and Ref. 201, which is an update to Ref. 56 and found that a number of points were unclear. I sought clarification of the points in TQ-EPR-1611 (Ref. 86) as identified below.

- Clarification of the classification of the PS periodic tests, test scripts, test environment, and verification of test coverage and results.
- Why the signals relating to the Emergency Diesel Generator (EDG) "start up in test" and periodic test of the EFWS pump had not been included.
- Where a Category A function has two inputs that must always be in opposite states (i.e. one ON and the other OFF), if it is possible to detect a fault that causes the inputs to be both ON or OFF at the same time and thereby preventing the operation of the Category A function.

333 The TQ response provided the following clarifications.

- Class 2 test equipment will be used for the PS periodic tests where possible, and that compensating measures will be applied where this is not possible.
- A design change has resulted in the elimination of the EFWS pump periodic test signal and that this will be tracked by the change process (see CMF 66 above).
- There is only one case where a Category A function could be challenged by its two inputs being both ON or both OFF (the "Set AUTO / MANU LHx switchboard" commands), and if this condition occurs an alarm will be raised on the PICS.

334 The first bullet under TQ response above has been documented by the inclusion of a requirement in Chapter 7.2 of the PCSR (Ref. 172) for periodic test and maintenance functions to be categorised at one category below the function affected by the periodic test or maintenance. The PCSR states that any categorisation shortfall will be addressed by compensatory measures.

335 The TQ response also stated that the EDG "start up in test" signals are not included in the analysis provided in Ref. 200 because they are subject to a plant modification. I have not received a CMF for this modification during the GDA close-out phase. I have raised an Assessment Finding below to record this (see **AF-UKEPR-CI-040** below).

336 I have assessed EDF and AREVA's submissions in response to GDA Issue Action **GI-UKEPR-CI-06.A4** on the definition of the PS design and a justification that the hardwired links to the PS from systems of a lower safety class cannot adversely affect the operation of the PS. I am content that the design has been adequately defined and that a justification has been provided that lower class systems cannot adversely affect the operation of the PS. Therefore, the GDA Issue Action can be closed. I have raised an Assessment Finding below to capture matters arising from the assessment that need to be addressed during the UK EPR™ detail design.

*GDA Assessment Finding: **AF-UKEPR-CI-040** - The Licensee shall:*

- *Ensure the analysis of the non disturbance of the PS by signals coming from lower classified systems is updated to reflect any future design changes and the final PS design.*
- *Confirm whether there is an EDG "start up in test" signal into the PS, and if so update the relevant non disturbance justification or produce a CMF for the change.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

4.5.3.5 Independence of Class 2 SAS from the Class 3 PICS - GI-UKEPR-CI-06.A5

337 This section addresses resolution of GDA Issue Action **GI-UKEPR-CI-06.A5** on the independence of the Class 3 PICS and Class 2 SAS. GDA Issue Action **GI-UKEPR-CI-06.A5** requires EDF and AREVA to demonstrate that the Class 3 PICS cannot adversely affect the Class 2 SAS.

338 EDF and AREVA's Resolution Plan identified letter EPR00823R entitled 'RO-UKEPR-082 - Full response to Action A6' (Ref. 202) as the response to this GDA Issue Action. EDF and AREVA also submitted document 'Independence of the PICS and the SAS - ECECC121458' (Ref. 203) in response to this GDA Issue Action (see below).

339 During my assessment requests for clarification were raised by TQ (two TQ forms raised on this topic). The description of the scope of work performed by the TSC and the TOs arising from the work are contained in a TSC report (Ref. 79). Annex 16 provides a summary of the TSCs' report including details of the TOs raised.

340 My review of letter EPR00823R (Ref. 202) identified that EDF and AREVA believed that electrical isolation, independence of power supply, physical separation, and independence of the different communication networks (i. e. the PAS Island, SAS, Plant and Terminal Buses) would be sufficient to prevent the Class 3 PICS from affecting the Class 2 SAS. The response confirmed that the Plant Bus connects the SAS to the PICS. The response did not address my concern that erroneous communications received by the SAS from the lower class systems could adversely affect the SAS. I raised TQ-EPR-1483 (Ref. 86) requesting a response to this specific concern.

341 The response to TQ-EPR-1483 provided more information on the measures in place within the communication system to identify and correct communication errors and failures of network components. However, this did not address the potential for spurious but valid commands or data received by the SAS to propagate to field devices or within the SAS. I raised TQ-EPR-1532 (Ref. 86) asking EDF and AREVA to describe the functional challenges (using BS EN 61784: 2010 (Ref. 228) as a guide to typical challenges) that the SAS could be exposed to via the communication system, and the measures employed by the SAS to protect against each functional challenge.

342 EDF and AREVA provided a response to TQ- EPR-1532 describing seven categories of functional challenge considered for analysis, namely:

- "command sent at the wrong time";
- "repeated command";
- "out of sequence command";
- "command not valid for system state";
- "command erroneously sent to the incorrect actuator";
- "operator command (single or grouped) not transmitted to SAS"; and
- "spurious but valid command sent to the SAS from the PICS".

343 The analysis presented by EDF and AREVA addressed the functional challenges as outlined below.

- A "command sent at the wrong time" is equivalent to either the "command not valid for system state" or "spurious but valid command sent to the SAS from the PICS" (see later in this list).
- The "repeated command" will have no effect because the command will already have been requested legitimately or will fail as a result of functional or safety interlocks.

- An "out of sequence command" cannot occur because command sequences are generated within SAS (not sent by PICS) and if a manual command is sent to the SAS out of sequence the operation will be prevented by the functional and safety interlocks.
- A "command not valid for system state" would typically either reinforce existing commands or be inhibited (e.g. if the plant is in the SICS operation mode the PICS command is inhibited).
- The "command erroneously sent to the incorrect actuator" will be identified by the operator and the impact is considered further under "spurious but valid command sent to the SAS from the PICS" (see below).
- The "operator command (single or grouped) not transmitted to SAS" will be noted by the operator as a failure of the system to respond to commands.
- The "spurious but valid command sent to the SAS from the PICS" will affect at the very worst only one division and the consequences can be managed.

344 EDF and AREVA included the TQ-EPR-1532 response, discussed in the paragraph above, in document 'Independence of PICS and SAS – Addressing Issues Raised by ONR during GDA' (Ref. 203). I reviewed this document and concluded that the response to TQ-EPR-1532 has been accurately recorded, and that this satisfies the requirements of the Issue Action. However, I identified that, following the change to the SPPA-T2000 platform version S7 technology, there will be a need to review the justification of independence of PICS, SAS, and other C&I systems based on SPPA-T2000 platform version S7 technology (i.e. where communication between systems of different safety class occurs). My major concern in relation to a Class 3 system frustrating the correct operation of the SAS, which is used to implement protection functions, has been adequately addressed for the purpose of GDA Issue closure. However, there is also a need to justify that other Class 2 systems (such as the RCSL that performs control and limitation functions) cannot be adversely affected by lower class systems. I have, therefore, raised an Assessment Finding to address these matters (see **AF-UKEPR-CI-041** below).

345 EDF and AREVA's analysis (Ref. 203) identified an exception to the claim (TQ-EPR-1532) that the "spurious but valid command sent to the SAS from the PICS" will in the worst case affect only one division. The exception to this claim is that there is the potential for a multi-division grouped command (i.e. single command that can affect all divisions simultaneously) to be erroneously sent by the PICS, and that this could cause a safety effect on all divisions. EDF and AREVA indicated that this will be analysed further during the SSP, and I have raised an Assessment Finding to record this (see **AF-UKEPR-CI-041** below).

346 I am satisfied that the analysis included in the response to TQ-EPR-1532 and Ref. 203 has shown that the SAS will not be adversely affected by most functional challenges. I identified that functional and safety interlocks were relied on to reject certain functional challenges. However, the detail of these interlocks was not available during the GDA close-out phase. I have, therefore, raised an Assessment Finding requiring confirmation that the SAS functional and safety interlocks inhibit spurious commands from the PICS (see **AF-UKEPR-CI-041** below).

347 Following assessment of EDF and AREVA's submission in response to GDA Issue Action **GI-UKEPR-CI-06.A5** on the independence of the Class 2 SAS from the Class 3 PICS, I am content the substantiation provided is sufficient to close the GDA Issue Action. I have

raised an Assessment Finding below to capture additional matters arising from the assessment that need to be addressed during the SSP.

GDA Assessment Finding: ***AF-UKEPR-CI-041*** *- The Licensee shall:*

- *Confirm that the SAS functional and safety interlocks referred to in TQ-EPR-1532 response inhibit spurious commands from the PICS, and produce a justification of the adequacy of the interlocks.*
- *Produce a comprehensive justification that Class 2 systems cannot be adversely affected by lower class systems. This justification to include the RCSL and systems based on SPPA-T2000 platform version S7 technology.*
- *Produce an analysis for the final UK EPR™ SAS design that demonstrates that a "spurious but valid command sent to the SAS from the PICS" will affect at the very worst only one division and the consequences can be managed (e.g. by an update of Ref. 203). The analysis to include justification that the consequences of a spurious multi-division grouped command being received and enacted by the SAS are acceptable, for all such commands (as committed to in Ref. 203).*

For further guidance on independence of SAS from PICS see Technical Observations GICI06.A5.TO2.03 to GICI06.A5.TO2.06 in Annex 16.

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

4.5.3.6 Class 1 Control and Display Facilities in MCR and RSS - GI-UKEPR-CI-06.A6

348 This section addresses resolution of GDA Issue Action **GI-UKEPR-CI-06.A6** on the provision of a detailed substantiation of the Class 1 control and display facilities in the MCR and RSS. GDA Issue Action **GI-UKEPR-CI-06.A6** requires a BSC for the Class 1 control and display system to be provided including justification of the functional coverage of the system.

349 There are four Computerised Operator Workstations (COWs) providing control and display facilities in the MCR. Each COW comprises a Class 3 computerised PICS workstation and a Class 1 computerised PSOT. The PICS workstation provides control and display facilities during normal plant operations. The PSOT, which is connected to the PS, provides Class 1 facilities for decision support information and manual actions such as PS reset and permissive control. The Class 1 non-computerised SICS panel provides the means of reaching the safe shutdown state upon failure of the COW. The SICS displays are always active and the controls are manually enabled following a failure of the COW. A non computerised panel, the Pupitre Inter Poste Opérateur (PIPO) or Inter-workstation console, provides hardwired reactor trip controls. The RSS provides an additional control location in the event of the MCR becoming uninhabitable, and contains two COWs which are manually enabled.

350 EDF and AREVA submitted 15 documents (see Annex 10) in response to this GDA Issue Action covering:

- description of Class 1 control and display facilities in the MCR and RSS (Ref. 205);
- PSOT BSC and supporting documents; and
- PSOT and SICS functional scope.

351 The submissions were reviewed and requests for clarification were raised by TQ (six TQ forms raised on this topic). As appropriate, the submitted documents were revised by EDF and AREVA to address the points in the TQs. The description of the scope of work performed by the TSC and the TOs arising from the work are contained in a TSC report (Ref. 79). Annex 16 provides a summary of the TSCs' report including details of the TOs raised.

352 EDF and AREVA submitted document 'Class 1 Control and Display Facilities in the Main Control Room and the Remote Shutdown Station' (Ref. 204), which describes the general organisation of the MCR and RSS, the functional scope of the Class 1 information and controls, and a description of the proposed Class 1 information and controls provided by each Class 1 system. I found that many design details were not included in the submission, so I asked for clarification of a number of points in TQ-EPR-1538, TQ-EPR-1563 and TQ-EPR-1599 (Ref. 86), including:

- whether SICS controls would be active if control from PICS is selected;
- how the PSOT controls in the MCR are inhibited when the RSS switch has been selected; and
- whether the reset and permissive functions are Category A.

353 The response to the TQs met my expectations. For example, EDF and AREVA confirmed that when control from PICS is active the SICS controls will be disabled by hardwired means, and also identified an acceptable method for deactivating the MCR PSOT controls when the RSS has been selected (i.e. the PS is engineered so that it will not respond to MCR PSOT commands when the RSS has been selected). The response to TQ-EPR-1599 stated that the reset and permissive functions will be the same category as the protective functions on which they operate (e.g. permissive and reset functions associated with Category A functions will be Category A). The information provided in the TQ responses has been included in Ref. 205.

354 In GDA Step 4, a response to TQ-EPR-1130 (Ref. 206) provided by EDF and AREVA had noted that some information displayed on the Class 1 SICS did not come from Class 1 sources. I raised TQ-EPR-1517 (Ref. 86), asking EDF and AREVA to consider the reasonable practicability of obtaining this information from Class 1 sources. The response noted that the Reactor Coolant System (RCS) Hot and Cold leg temperatures could be sourced from the Class 1 PS, and this was documented in Ref. 205. A description of the Class 1 SICS displays was also included in this document. These are in line with my expectations (e.g. general alignment with US NRC Regulatory Guide 1.97, Revision 3 (Ref. 210)), but EDF and AREVA noted that these will be updated during the SSP. I have therefore raised an Assessment Finding (see **AF-UKEPR-CI-042** below) for the Class 1 displays and controls to be justified when the design has been completed.

355 My review of the document 'Outline of content of the Basis of Safety Case for the Protection System Operator Terminal' (Ref. 207) identified a number of general (regarding the content of the BSC) and specific points that needed clarification. I requested clarification of these points in TQ-EPR-1507 (Ref. 86) and also provided a guidance document on the expected content of a BSC to EDF and AREVA. My questions included;

- whether the PSOT can send commands to the PS regardless of the state of the PICS / SICS switch;
- whether the PSOT remains active in the RSS in the event of a failure of the PICS; and
- the qualification status of the tools used to generate the Class 1 PSOT software.

356 The response to TQ-EPR-1507 and Ref. 205 adequately addressed my concerns. For example, the PSOT controls will not be active when the PICS / SICS switch is set to SICS mode, the failure of PICS will not affect the PSOT in the MCR or RSS, and the qualification processes for the software development tools will be defined in the PSOT BSC.

357 EDF and AREVA submitted the PSOT BSC (Ref. 208) together with supporting documents, and my review confirmed the guidance provided to EDF and AREVA on the content of a BSC had been followed. The BSC describes how the PSOT is based on the QDS platform (part of the Teleperm XS family of equipment), and notes that the QDS is currently qualified to Class 2 standards. The BSC acknowledges that the UK EPR™ PSOT will need to be qualified to Class 1 standards.

358 I am satisfied the QDS system software, developed according to the requirements of IEC 60880, has the potential to be qualified (with further ICBM work in accordance with Ref. 81) to Class 1 standards in order to perform Category A functions. The approach to the qualification of tools and Commercial Off the Shelf (COTS) components appears feasible. I have raised an Assessment Finding (see **AF-UKEPR-CI-042** below) addressing the need for the development of the PSOT, including the QDS system (hardware and software), to be carried out according to appropriate international standards including BS IEC 61513:2001, BS IEC 60880:2006, and BS IEC 60987:2007, and tools and COTS to be suitably qualified.

359 I reviewed the submitted document 'PSOT Functional Scope' (Ref. 209) and determined that it met my expectations (e.g. the functional coverage aligns with the displays recommended in the US NRC Regulatory Guide 1.97, Revision 3, Ref. 210). Ref. 209 also provides outline details of resets, permissives, and manual controls, but confirmation is required that indication is provided to operators of the status of these. This is raised as an Assessment Finding (see **AF-UKEPR-CI-042** below).

360 Following assessment of EDF and AREVA's submissions in response to GDA Issue **GI-UKEPR-CI-06.A6** on the provision of a detailed substantiation of the Class 1 control and display facilities in the MCR and RSS, I am content that the provisions including functional coverage have been adequately defined such that the Class 1 control and display facilities meet my expectations, and that the GDA Issue can be closed. I have raised an Assessment Finding below to capture matters arising from the assessment that need to be addressed during detailed design of the Class 1 controls and displays for the UK EPR™.

*GDA Assessment Finding: **AF-UKEPR-CI-042** - The Licensee shall:*

- *Ensure that the development of the PSOT, including the QDS system (hardware and software), is carried out according to appropriate international standards, including BS IEC 61513, BS IEC 60880, and BS IEC 60987, that tools and COTS components are suitably qualified, that justification is produced, and documentation updated.*
- *Ensure that indication is provided to operators of the status of all resets, permissives, and manual controls, or where this is not to be done, produce a justification as to why this is acceptable and is not reasonably practicable.*
- *Once the design has been completed, fully document the Class 1 displays and controls to be provided for the UK EPR™, and produce full justification of adequacy, to include the functional coverage of controls and displays in the MCR and RSS for all operational states.*

For further guidance on Class 1 controls and displays see Technical Observations GICI06.A6.TO2.08 to GICI06.A6.TO2.16 and GICI06.A6.TO2.18 in Annex 16.

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

4.5.3.7 Status of SICS Controls During Normal Operation - GI-UKEPR-CI-06.A7

361 GDA Issue Action **GI-UKEPR-CI-06.A7** requested EDF and AREVA to justify why it is not reasonably practicable for the SICS controls to be in a functional state during normal operation (for further background to the issue see **GI-UKEPR-CI-06.A7** in Annex 2). It was noted that the OL3 / US EPRs are designed to operate with these controls enabled. This matter was discussed at a technical meeting and raised with EDF and AREVA in TQ-EPR-1486 (Ref. 86). The work performed by the TSC is recorded in Ref. 79 (see Annex 16 for a summary of the TSCs' report).

362 EDF and AREVA's TQ response confirmed that there is no particular design impediment to leaving the controls active and that the design was based on the preferred operating mode. EDF and AREVA stated that the preferred operating mode was to have either the PICS or SICs controls active but not both at the same time (i.e. since plant operation is via either the SICS or PICS workstations but not both). Discussion with ONR human factors assessors has confirmed that the current approach of leaving SICS controls disabled until the PICS / SICS changeover switch is manually actuated is acceptable since it helps to enforce the preferred operating mode. I conclude that the current engineering design is acceptable since it is in accordance with the preferred operating mode and the action is, therefore, closed.

4.5.3.8 Class 3 Terminal Bus and Plant Bus Response Times - GI-UKEPR-CI-06.A8

363 GDA Issue Action **GI-UKEPR-CI-06.A8** required EDF and AREVA to provide a fully comprehensive demonstration that end-to-end response time requirements are achievable by design for functions important to safety that use the Class 3 Terminal Bus and / or Plant Bus. In response to this action EDF and AREVA provided one document entitled 'UK EPR: Justification of time response end to end on Terminal Bus Plant Bus - ECECC111368 revision A' (Ref. 225).

364 The submission was reviewed and requests for clarification were raised by TQ (four TQ forms raised on this topic). The submitted document was revised by EDF and AREVA to address the points in the TQs. The description of the work performed by the TSC and the TOs arising from the work are contained in a TSC report (Ref. 79). Annex 16 provides a summary of the TSCs' report including details of the TOs raised.

365 The document (Ref. 225) did not provide a fully comprehensive demonstration that the response time requirements were achievable by design. The analysis only addressed simple events and did not appear to be fully representative of real plant events and excursions. The concerns were raised with EDF and AREVA in four TQs (TQ-EPR-1513, TQ-EPR-1568, TQ-EPR-1601 and TQ-EPR-1626, Ref. 86).

366 The topic was discussed at a technical meeting where EDF and AREVA provided a presentation (Ref. 226) on the approach to the determination of response times. EDF and AREVA explained the difficulty of completing a more detailed design analysis given the complexity of the SPPA-T2000 subsystems (e.g. such as the OM690 operator interface system and AS620 Automation System). EDF and AREVA's preference is to

confirm the response times by test on representative equipment using appropriate test challenges.

367 EDF and AREVA explained that the values obtained by the design analysis presented in Ref. 225 are typically maximum worst case theoretical values and that the test values provide mean and worst case measured values. Initial test results as presented in Ref. 225 had demonstrated that one of EDF and AREVA's performance requirements had not been met (i.e. response time of 1.7 seconds compared to the requirement of 1.5 seconds) and further actions are planned to address this issue (e.g. additional tests using representative application software under avalanche conditions in order to fully characterise the response times). It was also noted that further analyses and test would be required to address the change from the SPPA-T2000 platform S5 to S7 version (Ref. 227). These activities would be undertaken during the SSP when the necessary SPPA-T2000 platform S7 version information is available.

368 EDF and AREVA stated that the performance requirements are operational targets and not safety requirements (response to TQ-EPR-1568, Ref. 86). The response times need to be considered in the light of overall operator response times. However, the concern remains that extended response times could lead to operators losing confidence in the PICS. EDF and AREVA need to ensure that an accurate predictability model for SPPA-T2000 response times is developed to inform the design decisions for the UK EPR™, in particular, in relation to the allocation of functions to processor modules and the need for point-to-point communications (see **AF-UKEPR-CI-043**).

369 I conclude that EDF and AREVA have submitted a design analysis of the Class 3 Terminal Bus and / or Plant Bus end-to-end response times. In addition, the need to fully characterise the response times has been recognised, testing of Flamanville 3 equipment has been undertaken and further representative tests are planned. In relation to the UK EPR™, further work is dependent upon the provision of SPPA-T2000 platform S7 version information that will become available during the SSP (Ref. 227). Following assessment of EDF and AREVA's submissions in response to GDA Issue Action **GI-UKEPR-CI-06.A8**, I am content that sufficient progress has been made and that the GDA Issue Action can be closed. I have raised an Assessment Finding below to capture those matters arising from the assessment that need to be addressed during the implementation of the UK EPR™ CBSIS.

*GDA Assessment Finding: **AF-UKEPR-CI-043** - The Licensee shall complete the demonstration of the adequacy of the UK EPR™ end-to-end response times for those functions important to safety which use the Class 3 Terminal Bus and / or Plant Bus using SPPA-T2000 platform version S7 information. The Licensee to:*

- *Perform a design analysis of the end-to-end response times using SPPA-T2000 platform S7 version information (i.e. updating the SPPA-T2000 platform S5 version analyses provided during GDA).*
- *Undertake a programme of performance / response time tests on fully representative UK EPR™ equipment (including SPPA-T2000 platform version S7 components) that include consideration of avalanche conditions both generated by the plant and internal to the SPPA-T2000 platform S7 version equipment).*
- *Ensure an accurate predictability model for the SPPA-T2000 platform S7 version level 1 (AS620B and SAS network) response times is developed (drawing on the results of the design analyses and performance / response*

time tests) to inform the design decisions for the UK EPR™, in particular, in relation to the allocation of functions to processor modules and the need for point-to-point communications.

For further guidance on the completion of the demonstration of the adequacy of the end-to-end response times see Technical Observations GICI06.A8.TO2.04 and GICI06.A8.TO2.06 in *Annex 16.*

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

4.5.3.9 Common Cause Failure and Reliability Assessment of Diverse Systems - GI-UKEPR-CI-06.A9

370 GDA Issue Action **GI-UKEPR-CI-06.A9** required EDF and AREVA to provide detailed substantiation for the probabilistic claims for any C&I components used by more than one line of protection (e.g. sensors, smart devices, PIPS and PACS). The response to include consideration of the potential for common cause failure as a result of the use of these components.

371 EDF and AREVA submitted 23 documents in response to this GDA Issue Action, covering:

- sensors and signal conditioning equipment / PIPS;
- PACS; and
- design principles and guidance influencing the provision of diversity and defence-in-depth, and allocation of functions to diverse systems.

It should be noted that the substantiation of a single smart device such as a smart sensor is addressed by GDA Issue **GI-UKEPR-CI-04**. Since the procurement of sensors for the UK EPR™ has not yet taken place, the need to provide a diversity justification for two smart devices has not been identified but is addressed by the approach to sensor diversity described below.

372 The submissions were reviewed and requests for clarification raised by TQ (10 TQ forms raised on this topic). As appropriate, the submitted documents were revised by EDF and AREVA to address the points in the TQs. The TSC's work and the TOs arising are described in Ref. 79. Annex 16 provides a summary of Ref . 79 including details of the TOs raised.

373 EDF and AREVA's approach for addressing the GDA Issue for sensors, signal conditioning equipment and PACS actuated equipment included the provision of diversity criteria and outline plans for implementing the required diversity, and defining the basis for substantiating the reliability of the components.

4.5.3.9.1 Sensors and Signal Conditioning Equipment / PIPS

374 I reviewed document 'Diversity Criteria for Sensors and Conditioning - PELL-F DC 82 revision A' (Ref. 146) and provided comments to EDF and AREVA in TQ-EPR-1484 (Ref. 86). The document defines the diversity criteria that will be applied to sensors and conditioning modules to ensure the design supports the reliability targets for independent functions. The selection of the criteria was informed by standards BS IEC 61513:2001 (Ref. 10), BS IEC 62340:2007 (Ref. 11) and NUREG 6303 (Ref. 216) with the following categories of criteria being used for sensors and conditioning; Equipment diversity (Ed), Human diversity (Hd), Signal diversity (Sgd) [applicable for sensors only], Software diversity (Swd) and Separation criteria (Spc)

375 Following my review, I raised TQ-EPR-1486 (Ref. 86) requesting a number of clarifications. For example, I asked EDF and AREVA to define the reliability limit used when two diversified groups of sensors and conditioning modules are claimed, and provide a justification for the reliability claim specified as a failure probability of 1x10^{-6} pfd for simple equipment. The response to TQ-EPR-1484 and the document update incorporating the responses to the TQ was found to be acceptable (e. g. claim limit of 1x10^{-8} pfd is used for two diversified groups and 1x10^{-6} pfd is only claimed when simple passive devices are used).

376 My review of the ‘UK EPR: Diversity Implementation Plan For Sensors & Conditioning - PELA-F DC 3’ (Ref. 230) and the supporting document ‘Functional Analysis for Sensors‘ Common Cause Failure - PEPR-F DC 83’ (Ref. 231) found that there were significant shortfalls in the diversity provisions. In particular, only one plant parameter was used for the initiation of many protective actions undertaken by all of the C&I safety systems. My comments were provided to EDF and AREVA in TQ-EPR-1555 (Ref. 86). Comments were also provided to EDF and AREVA by the fault studies team in TQ-EPR-1578.

377 EDF and AREVA’s response (e.g. to TQ-EPR-1578) to the concerns included an analysis of the cases for which diverse parameters were not claimed and in the main stated there were no suitable diverse parameters. EDF and AREVA provided clarification that its application of the sensor diversity criteria for those cases requiring parameter diversity (criteria ‘Sgd = 3’) would firstly consider whether a diverse parameter was available and if not devices using diverse measuring principles (e.g. pressure measurement using strain gauges and linear variable differential transformer devices as used on Sizewell B) would be adopted (i.e. where reasonably practicable). EDF and AREVA updated PELL-F DC 82 (Ref. 232) to clarify the application of the criteria outlined above.

378 To improve the resilience of the sensor signal conditioning modules to common cause failure, EDF and AREVA introduced diverse conditioning modules. My review of the response to TQ-EPR-1555 identified a small number of cases where there was one type of conditioning module in two trains and the diverse module in the other two trains. With this arrangement common cause failure on two trains using the same module coupled with maintenance on a third train would have disabled the protective function (a consequence of the 2 out of 4 (2oo4) voting logic).

379 I queried why the diversity was not implemented on a functional basis (i.e. given the functional diversity present in the safety systems) and it was identified that the conditioning modules could be arranged to remove the concern on operability with common cause failure during maintenance for the current design. EDF and AREVA updated PELA-F DC 3 (Ref. 233) to reflect the revised arrangement. However, the fault studies assessment team has identified that the work on excessive increase in steam flow, performed in response to GDA Issue **GI-UKEPR-FS-02**, may mean that the selected solution (i.e. in-core and ex-core neutron detectors using the same type of conditioning modules) is not adequately diverse. See the fault studies assessment report (Ref. 87) for discussion of the fault studies assessment and related Assessment Findings.

380 My review identified that the analyses contained in the submissions on sensor and conditioning module diversity were not fully comprehensive and that some tasks remained to be completed during the SSP. The functional analysis of sensor and conditioning modules needs to be completed to address, for example:

- Diversity cases associated with conditioning modules involved in the mitigation of faults in support functions and the spent fuel pool, as stated in Section 4.2.3 of Ref. 233.
- Determination of the diversity requirements to be applied to the conditioning modules associated with specific sensor pairs, as marked by "XC" in Table 6 of Ref. 233.

381 I reviewed EDF and AREVA's submission on 'UK EPR GDA - Basis of Substantiation of C&I Components - PELA-F DC 7' (Ref. 234) and sought a worked example of the process (TQ-EPR-1602, Ref. 86), which was not fully explained in the submission. EDF and AREVA clarified that the process to be adopted is different to that used for the reference plant FA3 and data for new modules was not available at this time. The document was updated (Ref. 235) to further clarify the intended methodology, which includes justification of one sensing channel (up to 1×10^{-4} pfd) coupled with a justification for diversified channels (up to 1×10^{-8} pfd).

382 While I am content that an acceptable outline of the approach to the demonstration of the adequacy of sensors and signal conditioning equipment / PIPS has been provided the approach needs to be fully developed and implemented during the SSP.

*GDA Assessment Finding: **AF-UKEPR-CI-044** - The Licensee shall:*

- *Produce a comprehensive sensor and conditioning diversity implementation plan that identifies the main activities to be carried out during the SSP, including completion of the functional analysis of sensor and conditioning modules CCF (e.g. see PELA-F DC 3 (Ref. 233), diversity cases associated with conditioning modules involved in the mitigation of faults in support functions and the spent fuel pool).*
- *Where signal diversity criteria Sgd=3 is identified and no diverse parameter is available, employ devices that use diverse measuring principles.*
- *Produce a comprehensive substantiation of the reliability claims for sensors and conditioning modules using the methodology defined in PELA-F DC 7 (Ref. 235).*

For further guidance on what is needed to address this Assessment Finding see Technical Observations GICI06.A9.TO2.19 and GICI06.A9.TO2.25 in Annex 16.

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

4.5.3.9.2 Adequacy of Sensor Allocation to the PS, SAS and NCSS

383 Following the introduction of the NCSS into the UK EPR™ C&I architecture the question arose as to how to allocate sensors to the safety systems (i.e. the NCSS, PS and SAS). EDF and AREVA provided a document 'UK GDA - Allocation of sensors and conditioning when 3 lines of defence are involved - PEPS-F DC 148 rev A' (Ref. 236) to address this topic. The document considered three possible solutions, namely:

- three independent and diversified lines of protection;
- PS and NCSS share the same sensors and conditioning modules; and
- SAS and NCSS share the same sensors and conditioning modules.

384 On the basis of a preliminary estimation, EDF and AREVA concluded that in terms of plant risk the configuration with the NCSS and SAS sharing the same conditioning modules and sensors was acceptable. However, EDF and AREVA noted that if the detailed calculations show that UK probabilistic requirements are not met then the solution with three independent and diversified lines of defence will be considered. Since this could have an impact on plant layout and design this matter will need to be resolved early in the SSP.

*GDA Assessment Finding: **AF-UKEPR-CI-045** - The Licensee shall confirm the adequacy of the allocation of conditioning modules and sensors (i.e. one group to the PS and other to the SAS / NCSS) by completing sufficient detailed calculations (e.g. as referred to in PEPS-F DC 148, Ref. 236).*

For further guidance on what is needed to address this Assessment finding see Technical Observation GICI06.A9.TO2.24 in Annex 16.

[Required Timescale: prior to nuclear island safety related concrete.]

4.5.3.9.3 PACS Modules

385 EDF and AREVA have introduced two types of PACS modules to provide additional defence against common cause failure of one PACS module type. EDF and AREVA reviewed the means of introducing the PACS modules; either on a functional basis or by having different PACs modules in different divisions (i.e. type A in two divisions and type B in the other two divisions). EDF and AREVA determined that sufficient defence against common cause failure could be provided by placing different types of PACS modules in different divisions (i.e. divisions 1 and 2 using type A and the other two divisions using type B, referred to as PACS A and PACS B below).

386 I reviewed document 'Diversity criteria definition for Priority Actuation Control (PAC) module - ECECC1204 43' (Ref. 145). The document defines the requirements to ensure adequate diversity between the two types of PACS modules such that the reliability claims for functions depending on these modules can be justified. The criteria will be used to inform the processes of selection and / or development of diverse PACS modules and associated components during the detailed engineering phase of the UK EPR™. The approach to the development of the criteria is similar to that for sensors and conditioning modules (see above). For example, the criteria are based on the same reference guidance (e.g. NUREG 6303). For the PACS modules criteria are set for design, equipment and human diversity, and separation. Software diversity is not considered as it is required that the PACS modules are based on simple components with no software.

387 My review of document 'UKEPR Basis of Substantiation for the Reliability Claims for the PACS Modules - ECECC121662' (Ref. 237) found that a full reliability analysis will be carried out during the SSP. While the basis for the substantiation is not unacceptable the full demonstration of PACS adequacy will need to fully substantiate the reliability claims for the actual PACS modules used in the UK EPR™ implementation and amongst others, address compliance with standards, hardware qualification, assessment of common cause failure, diversity justification and substantiation of PACS reliability (i.e. singly and in combination).

388 I reviewed EDF and AREVA's submission entitled 'UK EPR Diversity implementation plan for PAC Modules - ECESN120 472' (Ref. 238). The document defines a generic design solution for allocation of different types of PAC modules, namely; PAC A in divisions 1 and 2 and PAC B in divisions 3 and 4. The document then analyses the

acceptability of this general allocation and notes that there were five functions where further analysis was required. These further analyses either resulted in a change to the generic allocation of PACS modules (i.e. steam line isolation) or outlined why the situation was considered to be acceptable (e.g. isolation of Main Coolant Pump (MCP) seal injection where a diversified function is provided that does not rely on PACs modules).

389 My review identified some shortfalls (see below) in the comprehensiveness of the analysis presented in Ref. 238 that will need to be addressed during the SSP. As a result a comprehensive PAC module diversity implementation plan should be produced that identifies the main activities to be carried out and includes the items below.

- Completion of the PAC module diversity analysis (e.g. diversity cases associated with support functions as stated at the end of Section 7.3).
- Demonstration of meeting the equipment diversity requirements for the selected modules.

390 Following my review of the PACS submissions I asked for further justification of the adequacy of the diverse group of PACS A and PACS B modules including the impact of power supply maintenance. In particular, to specifically address the situation where, for example, one train using a PACS A module is in maintenance and the PACS B modules are subject to common cause failure.

391 EDF and AREVA's response was contained in letter EPR01413N 'Response to C&I Meeting Actions GI 15-I&C-2 and GI 16-I&C-4' (Ref. 239). EDF and AREVA explained that no routine preventive maintenance is to be performed on the PACS modules. Periodic testing will be performed from the C&I systems through to the PACS modules. If the PS safety function logic determines a need for ESFAS actuation during the periodic test, the PS automatically stops the test and initiates the ESFAS actuation. EDF and AREVA also explained that routine maintenance on electrical switchboards can be scheduled to take place only at appropriate times during plant outages so resulting unavailability of plant at power or in other states where its availability is required is not expected. However, the response did not fully address the consequence of the C& I SIS driving the PACS modules being in maintenance. The fault studies assessment team has reviewed the allocation of PACS modules and considers that there may be scope for allocating the modules on a functional basis (i.e. diverse safety functions use diverse PACS modules) (see Ref. 87).

*GDA Assessment Finding: **AF-UKEPR-CI-046** - The Licensee shall produce a comprehensive PACS module diversity implementation plan that identifies the main activities to be carried out during the SSP, including: completion of the PACS module diversity analysis (e.g. diversity cases associated with support functions (see Ref. 238), impact of SIS maintenance and potential for allocation on a functional basis).*

For further guidance on what is needed to address this Assessment Finding see Technical Observations GICI06.A9.TO2.16, GICI06.A9.TO2.20 and GICI06.A9.TO2.21 in Annex 16 and Fault Studies Assessment Report (Ref. 87).

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

Note the Fault Studies Assessment Report (Ref. 87) includes Assessment Findings related to the need to review the PACS module allocation.

4.5.3.9.4 Other Actuation Equipment.

392 The PACS modules are the only actuation elements covered in the scope of GDA Issue **GI-UKEPR-CI-06 Action 9**. However, it is recognised that there will be some actuators that are not driven by PACS modules and / or switchgear, for example modulating control valves driven by analogue signals. The diversity head document (Ref. 141) states that "For those actuators that are not driven via electrical switchgear an assessment will be performed to identify any embedded or associated C&I components such as positioners, variable speed drives, feedback devices etc. and in a similar way as for the PACS modules, diversity criteria, implementation plans and substantiations will be developed. This assessment will be performed during the NSL phase when detailed designs are available and equipment has been selected. If any of the C&I equipment associated with actuators is SMART the appropriate assessment and qualification processes will be followed". While this is acceptable at this stage, given progress with selection of such equipment to date, justifications for any such equipment will need to be developed early in the SSP and before the equipment is delivered to site.

> *GDA Assessment Finding:* ***AF-UKEPR-CI-047*** *- The Licensee shall, for those actuators that are not driven by PACS modules and / or switchgear, perform an assessment to identify any embedded or associated C&I components such as positioners, variable speed drives, feedback devices etc. and provide a justification of their adequacy (e.g. in a similar way as for the PACS modules, by developing and implementing diversity criteria, implementation plans and component reliability substantiations).*
>
> [Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

393 I have assessed EDF and AREVA's submissions in response to GDA Issue Action **GI-UKEPR-CI-06.A9** on provision of substantiation for the probabilistic claims for any C&I components used by more than one line of protection (e. g. sensors, smart devices, PIPS and PACS). I am content that an adequate process for the detailed substantiation of the C&I components used by more than one line of protection has been presented and that the GDA Issue Action can be closed. I note that further work will be needed during the SSP as the detailed design of the UK EPR™ is progressed. I have raised Assessment Findings above to capture those matters arising from the assessment that need to be addressed during the SSP.

4.5.3.9.5 Design Principles and Guidance Influencing Diversity and Defence-in-Depth Provisions

394 EDF and AREVA submitted four documents outlining the design principles and guidance influencing the provision of diversity and defence- in-depth, and allocation of functions to diverse systems, in response to this GDA Issue Action, namely:

- 'Safety Principles applied to the UK EPR I &C Architecture in terms of the Requirements for Diversity and Independence - PEPS-F DC 90', Ref. 211;
- 'UK EPR GDA - Classification of I&C safety features - ECEF091489', Ref. 214;
- 'Definition of I&C architecture design requirements in the UK context - ECECC120414', Ref. 217; and

- 'Architecture of instrumentation and control system UK EPR. Design: principles and defence-in-depth - ECECC100831', Ref. 218.

395 My review of the safety principles document (Ref. 211) and a later revision B of this document (Ref. 212) found that the requirements did not align with the guidance in BS IEC 61226:2009 (Ref. 44), with some requirements and terminology being ambiguous. I therefore raised a number of general and specific questions in TQ-EPR-1495, TQ-EPR-1541 and TQ-EPR-1613 (Ref. 86), such as requesting clarification of the following points.

- The terminology used in Ref. 211, including 'safety limits', 'best estimates', 'line of protection', 'line of defence', 'frequent' and 'conservative'.
- Whether, "does not have to inhibit the severe accident line from performing its intended functions", should be interpreted as "shall not inhibit the severe accident line from performing its intended functions".
- Why RS10010-FS in Section 4.5 requiring fail-safe states only applies to Class 1 systems and components, and does not cover all systems and components important to safety (e.g. those at Class 2), as in requirement R16 in Section 3.6.1.

396 Following technical meetings, a technical workshop, and submission of TQ responses, revision C of the document was submitted (Ref. 213) and was found to meet my expectations. For example, by conforming to the standard BS IEC 61226:2009 (Ref. 44) and principally through improvements in the definition of the requirements. I noted that Ref. 213 did not clearly define the requirements for design in respect of common cause failure during maintenance. I have captured the need to address this point under Assessment Finding **AF-UKEPR-CI-048** (see below).

397 Document 'UK EPR GDA - Classification of I&C safety features - ECEF091489' (Ref. 214) was not in the Resolution Plan, but was submitted to complement Ref. 212, and describes the defence-in-depth concept as consisting of the following lines of defence:

- preventive line of defence;
- main line of defence, first line of protection;
- main line of defence, diverse line of protection;
- risk reduction line of defence, back-up line; and
- risk reduction line of defence, severe accident line.

398 I reviewed this document and found that the allocation of functions to C&I systems is based on the safety requirements of the functions and 'safety features' (group of components working together to achieve a single action) to be implemented by each line of defence (e.g. first line of protection). The resulting system allocations are contrary to that described in the response to TQ-EPR-1541, so I raised TQ-EPR-1623 (Ref. 86), requesting:

a) justification for the use of a Class 2 automation system (e.g. SAS or RCSL) to carry out a Category A function in the first line of protection;

b) justification for the use of a Class 3 automation system in the diverse line of protection that has a minimum safety class of Class 2;

c) justification for the use of a Class 3 automation system in the severe accident line of protection that has a minimum safety class of Class 2; and

d) clarification that the Rod Pilot will be Class 2.

399 The TQ response addressed these points by stating that a re-allocation of systems to functions will be performed during the SSP (points a) and b)), clarifying that a Class 3 system is only allocated to a severe accident line function with a minimum safety class 2 where an additional Class 2 system is already in place to implement the function (point c), and confirming the Rod Pilot will be Class 2 (point d).

400 The subsequent document update (Ref. 123) incorporated the TQ-EPR-1623 response. A note has been added to Ref. 123 to identify each shortfall in system allocation, describing how this will be corrected in the SSP (e.g. the chilled water production allocation has been identified as requiring re-assessment with a note (c) that new Class 1 safety features will be defined in the SSP). I have recorded this in Assessment Finding **AF-UKEPR-CI-048** (see below).

401 Document 'Definition of I&C architecture design requirements in the UK context' (Ref. 217) was not in the Resolution Plan but was supplied in support of Ref. 211. I reviewed this document and found it to be satisfactory. However, I noted that the C&I requirements in the document did not identify how all the C&I SAPs and their related guidance paragraphs have been addressed. I have recorded this in an Assessment Finding (**AF-UKEPR-CI-048** see below).

402 An update of document 'Architecture of instrumentation and control system UK EPR. Design: principles and defence-in-depth' (Ref. 218) was delivered under cover of letter EPR01375N (Ref. 219) in response to a meeting request (i.e. action TATS GI 4-I&C-7) for it to include a table summarising lines of defence and protection, and associated C&I systems. My review found that the requested information had been included as Tables 1 and 2, and this met my expectations, although my review did raise a number of points. For example, Figure 2 shows outputs from the PS and NCSS passing through an SPPA-T2000 PACS interface, contrary to my expectation. Also, F1B functions are still referenced despite the document claiming to use the categorisation and classification scheme described in Ref. 224. These discrepancies have the potential to cause confusion and should be corrected (see Assessment Finding **AF-UKEPR-CI-048** below).

403 EDF and AREVA indicated that the design is not complete and re-allocation of functions is likely to occur during the UK EPR™ C&I detailed design process. Whilst the final allocation of functions to systems has not been completed within GDA, I conclude that the allocation requirements have been adequately defined (e.g. within Ref. 213) to complete this element of the GDA Issue Action. I have recorded the need for the final design to meet the requirements on diversity and defence-in-depth, and allocation of functions to diverse systems in Assessment Finding **AF-UKEPR-CI-048**.

*GDA Assessment Finding: **AF-UKEPR-CI-048** - The Licensee shall:*

- *Update document PEPS-F DC 90 so that it clearly defines the requirements for design in respect of common cause failure during maintenance.*
- *When C&I categorisation and classification is complete, update the documentation (e.g. ECEF091489) to record the final categorisations of functions and classifications of systems, identifying any categorisation shortfalls and providing full justification, as necessary.*
- *Ensure that the requirements (e.g. PEPS-F DC 90 rev. C) in respect of diversity and defence-in-depth are followed during the detailed design of the UK EPR™, and where the requirements are not met, produce a justification.*

- *Review the C&I design requirements documents (e.g.* ECECC120414) *to identify whether all relevant ONR C&I SAPs and their related guidance paragraphs are considered, updating these where relevant SAPs are not found, or not comprehensively met (i.e. including the related guidance paragraphs).*
- *Review the document 'UK EPR I&C Architecture' ECECC100831 Rev B to identify discrepancies with other UK EPR™ documentation, and resolve these (e.g. Figure 2, shows outputs from the PS and NCSS passing through an SPPA T2000 PACS interface and FA3 references should be replaced by UK specific ones).*

For further guidance on ensuring the adequacy of the design principles and guidance influencing the provision of diversity and defence-in-depth, and allocation of functions to diverse systems see Technical Observations GICI06.A9.TO2.14, GICI06.A9.TO2.17, GICI06.A9.TO2.18, GICI06.A9.TO2.22 and GICI06.A9.TO2.23 in Annex 16.

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

4.5.3.10 Overall Conclusion on GDA Issues Arising from the Closure of RI-UKEPR-002 - GI-UKEPR-CI-06 Actions A1 to A9 (see above))

404 I have assessed EDF and AREVA's submissions in response to GDA Issue **GI-UKEPR-CI-06** on resolution of mat ters identified during the closure of regulatory issue **RI-UKEPR-002**. The GDA Issue has nine actions (see a bove) covering provision of adequate reliability, diversity and defence-in-depth (Actions A1, A2 , A3 and A9), independence of SIS (Actions A4 and A5), Cl ass 1 controls (Actions A6 and A7) and network response times (Action A8). I am cont ent that an adequate position has been reached for all of the nine actions and that the GDA Issue can be closed. I have raised Assessment Findings above to capture those matters arising from the assessment that need to be addressed during the SSP.

4.5.3.11 Classification of C&I systems - GI-UKEPR-CC-01.A6

405 This section addresses resolution of GDA I ssue Action **GI-UKEPR-CC-01.A6** on categorisation and classification. GDA Issue Action **GI-UKEPR-CC-01.A6** requires the production of evidence to demonstrate that the categorisation of C&I systems is consistent with current good practice as provided by BS IEC 61226:2009 (Ref. 44), and with the probabilistic claims given in guidance document TAG 46 (Ref. 9).

406 EDF and AREVA submitted five documents (see Annex 10) that related to this GDA Issue covering:

- safety principles and design rules for the UK EPR™ C&I Architecture;
- design processes for categorisation of functions; and
- classification of C&I systems.

407 The submissions were reviewed and requests f or clarification were raised by TQ (five TQ forms related to this topic, in cluding one raised in the f ault studies technical area). As appropriate, the submitted documents were revised by EDF and AREVA to address the points in the TQs. The descript ion of the scope of work performed by the TSC a nd

the TOs arising from the work are contained in a TSC report (Ref. 229). Annex 17 provides a summary of the TSCs' report including details of the TOs raised.

408 I reviewed the categorisation and classification requirements contained within the safety principles document (Ref. 211). I found that the probabilistic claim limits met my expectations (Ref. 9) for computer based systems performing a nuclear safety function in a nuclear power plant (i.e. Class 1 at $1x10^{-3}$ to $1x10^{-4}$ pfd / pdfy, Class 2 at $1x10^{-2}$ pfd / pdfy and Class 3 at $1x10^{-1}$ pfd / pdfy). However, some requirements did not conform to Ref. 44 (e.g. the requirement R25 provided safety function categorisation definitions of F1A, F1B and F2 that did not agree with those of Categories A, B and C in Ref. 44). I raised this in TQ-EPR-1495 (Ref. 86), and also raised TQ-EPR-1515 (Ref. 86) to request a response to GDA Step 4 observations related to this GDA Issue (e.g. T17.TO1.01, which noted that the categorisation and classification scheme in 'Methodology for Classification of Structures, Systems, Safety Features and Components - NEPS-F DC 557' (Ref. 224) does not conform to Ref. 44 and UK expectations).

409 The TQ responses stated that the safety principles document Ref. 211 and classification methodology document Ref. 224 would be updated to align with Ref. 44. However, I noted that the response to TQ-EPR-1515 (Ref. 86) did not align with Ref. 44 (i.e. my expectation is that Category A functions will be used to achieve and maintain the non-hazardous stable state, and that functions will be assigned to Category B where these functions meet the Category B criteria and are not otherwise allocated to Category A). I raised this in TQ-EPR-1569 (Ref. 86).

410 The response to TQ-EPR-1569 confirmed that the categorisation process follows Ref. 44 and is top down (i.e. Category A functions are assigned first if they meet the criteria in Ref. 44, with Category C functions being those that are not otherwise assigned to Categories A or B). My review of revision B of the safety principles document (i.e. Ref. 212) found that requirement R25 (see paragraph 408) is replaced by a new requirement R9 whose categorisation definitions conform to Ref. 44 (i.e. the Categories A, B and C of Ref. 44), and so this document meets my expectations in respect of categorisation and classification.

411 It was not clear to me how EDF and AREVA perform the functional categorisation process, and so I requested information on this by placing a meeting action (TATS GI 4-I&C-1). A response to this was received in letter EPR01030N (Ref. 223) and the document 'Engineering and Projects Organisation EPR overall I&C design process' (Ref. 220) was submitted to outline the UK EPR™ C&I design process including functional categorisation. My review found that the C&I design process was claimed to be consistent with BS IEC 61513:2001 (Ref.10), but Ref. 220 did not reference all appropriate clauses of the standard. I raised this concern and requested a number of clarifications in TQ-EPR-1589 (Ref. 86) including requesting that EDF and AREVA address the points below.

- EDF and AREVA to provide a demonstration of how the major sub-clauses of BS IEC 61513:2011 (Ref. 240) Sections 5.2, 5.4, 6.1 and 6.2 are complied with by the overall C&I design and development process.
- EDF and AREVA to clarify why no output document(s) are shown on the flowchart for the multiple activities labelled "*System Life-Cycle of I&C systems*".

412 The response to the TQ and update of this document (Ref. 241) answered my questions. For example, the TQ response explained the correspondence between the two versions of BS IEC 61513 (i.e. Refs 10 and 240), and compliance with Ref. 10 is now addressed in Table 1 of the document. In addition, it was clarified that the output

documents for the 'system life-cycle of I&C systems' activities are not addressed in the document but covered by dedicated processes for each C&I system.

413 Following the submission of an advanced draft of the classification methodology document (Ref. 221), I raised a concern at a technical meeting that the C&I classification did not appear to meet the requirements of Ref. 44 (e.g. C&I components and systems embedded in electrical components appeared to be excluded from the classification process). EDF and AREVA decided that the main focus of the document would be on classification of non C&I systems, and that C&I classification would be addressed in detail in an update of the submission 'UK EPR GDA - Classification of I&C system features - ECEF0914 89' (Ref. 214) (submitted under GDA Issue **GI-UKEPR-CI-06 Action 9**, see above).

414 My review of the update of the classification methodology document (Ref. 222) identified that it states that C&I components are assigned a safety class at the system level, based on the highest safety class of the safety features / safety feature groups they are supporting. EDF and AREVA define (Ref. 222) the following terms that are relevant to the understanding of the categorisation and classification process (starting at the highest level of abstraction).

- Main Safety Function – "One of the three high level safety functions – Control of fuel reactivity, Fuel heat removal, Confinement (also known as Fundamental safety function)".
- Plant Level Safety Function – "Safety Functions derived from the Main Safety Functions, on the highest level.…" (e.g. H3 - remove heat from the react or coolant to the ultimate heat sink).
- Lower Level Safety Function - "Safety Functions decomposed from a Plant Level Safety Function with a level of defence in depth" (e.g. Heat removal by steam generators – emergency shutdown mode to reach the non hazardous stable state).
- Safety Feature Group (SFG) - "All the components that must work together to perform a Lower Level Safety Function" (e.g. ASG-SFG-01 Emergency Feed Water System automatic actuation on Steam Generator level (Wide Range) is less than MIN2P).
- Safety feature - "Group of components generally belonging to a single system and working together to achieve a single action which is part of an SFG. They are in essence mechanical features, I&C instrumentation features, I&C automation features and electrical features" (e.g. ASF-FS-01 Start-up of an Emergency Feed Water System train).

415 Section 7.4.6 of Ref. 222 states that C&I requirements defined in the RCC-E code (Ref. 24) and relevant IEC standards will be applied to C&I components embedded in electrical components. However, the document notes that a limited number of safety classified components will not be designed to RCC-E or IEC standards, but "similar appropriate high standards will be adopted and will be justified by an ALARP analysis". It is my expectation that, where C&I components have not been designed to appropriate IEC standards, a justification will be provided that the components have a suitable qualification according to the classification required. I also note that the failure probability limits for Class 2 and 3 computer based C&I systems in Section 9 do not agree with Ref. 81 Section 4, being one decade too low (e.g. the Class 2 pfd limit is $1x10^{-3}$ when it should be $1x10^{-2}$). I have raised an Assessment Finding to record these points (**AF-UKEPR-CI-049** *see* below).

416 Document 'UK EPR Generic Design Assessment – Classification of I&C safety features - ECEF091489 Rev D' (Ref. 214) was submitted to complement PELL-F DC 90 Rev. B (Ref. 212). I reviewed the document under GDA Issue Action **GI-UKEPR-CI-06.A9** (see Section 4.5.3.9.5) and after provision of an update of the document (Ref. 123) concluded that it provides sufficient evidence that the categorisation and classification conforms to Ref. 44. However there are some categorisation and classification assignments (see Section 4.5.3.9.5) that need to be reviewed during the SSP (see Assessment Finding **AF-UKEPR-CI-048** above).

417 EDF and AREVA note in Section 2.1 of Ref. 123 that the electrical and C&I design of the UK EPR™ has not been completed, and therefore the system classifications are not finalised. However the information provided to support the GDA Issue is adequate to demonstrate that the approach to categorisation and classification aligns with BS IEC 61226:2009 (Ref. 44), and the probabilistic claim limits meet my expectations. This is sufficient to close the GDA Issue. I have raised an Assessment Finding below to capture additional matters arising from the assessment that need to be addressed during the SSP.

*GDA Assessment Finding: **AF-UKEPR-CI-049** - The Licensee shall update NEPS-F 557 to align this with the probabilistic claim limits for Class 2 and 3 computer based systems given within other safety documentation such as PEPS-F DC 90 and ECECC111134 (e.g. the Class 2 pfd claim limit should be 1x10^{-2}).*

For further guidance see Technical Observation GICC01.A6.TO2.01 in Annex 17

[Required Timescale: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

4.5.3.12 Non-Computerised Safety System (NCSS) Design Information - GI-UKEPR-CI-01

418 This section addresses resolution of GDA Issue **GI-UKEPR-CI-01** on production of a BSC for the NCSS. GDA Issue **GI-UKEPR-CI-01** includes the identification of the technology to be used for the NCSS. The NCSS is to be implemented using the UNICORN platform.

419 The NCSS is a non-computerised system consisting of four trains of equipment, one per plant division. The automatic functions are arranged in a 2oo4 voting configuration. Each NCSS train is built from a number of different UNICORN platform modules that are selected and configured to achieve the required safety actions.

420 EDF and AREVA submitted 24 documents (see Annex 10) in response to this GDA Issue covering:

- justification note for NCSS platform selection;
- NCSS BSC and schedule of supporting documentation;
- NCSS system specification, functional requirements and diversity criteria;
- UNICORN platform quality plans, module specifications and qualification programme; and
- justification of typical response times and reliability allocation.

421 The submissions were reviewed and requests for clarification were raised by TQ (13 TQ forms raised on this topic). As appropriate, the submitted documents were revised by EDF and AREVA to address the points in the TQs. The description of the scope of work performed by the TSC and the TOs arising from the work are contained in a TSC report

(Ref. 74). Annex 11 provides a summary of the TSCs' report including details of the TOs raised.

422 The document submission 'Justification note for NCSS platform selection' (Ref. 178) described the process used by EDF and AREVA to select the supplier for the NCSS platform, covering design criteria, technology options and organisational capability. AREVA TA was selected as the supplier of the NCSS platform. The chosen platform, known as UNICORN, requires development of existing modules. The UNICORN platform will use dynamic logic implemented by digital and analogue components for safety function realisation, and computerised components for annunciation and data logging.

423 My review of the outline of the NCSS BSC (Ref. 179) resulted in the identification of a number of general concerns regarding the content of the BSC, which I raised in TQ-EPR-1533 (Ref. 86). I also raised detailed technical questions, including on the classification of test equipment, justification of the final voting logic module (known as AVACT), display of NCSS status on the computerised PICS, and the omission of the standards BS IEC 62340:2007 (Ref. 11) on requirements for coping with CCF and BS IEC 61226:2009 (Ref. 44) on categorisation and classification. Following the response to this TQ, it was agreed that the outline of the NCSS BSC document (Ref. 179) would not be updated, but a NCSS BSC contents list (Ref. 180) would be delivered prior to submission of the completed NCSS BSC.

424 The response to TQ-EPR-1533 resolved my concern that the computerised PICS needs to be operable for the NCSS status to be displayed. The concern was resolved by EDF and AREVA confirming the NCSS status will also be displayed on the non-computerised SICS. EDF and AREVA also indicated that use of the standards BS IEC 62340:2007 and BS IEC 61226:2009 would be included in the BSC. However, the TQ response did not fully address the other technical issues (e.g. the periodic test and maintenance modules are listed as non-classified, and the effect of maintenance on one AVACT channel was not described). Subsequently, the concern on classification of test equipment was resolved by the response to TQ-EPR-1570 (Ref. 86) (i.e. test equipment to meet Class 3 standards), the justification of the AVACT module was progressed as a meeting action (TATS GI 10-I&C-6) (see section on reliability below), and the requirement to use standards BS IEC 62340:2007 and BS IEC 61226:2009 was included in the NCSS BSC (Ref. 181).

425 EDF and AREVA's NCSS BSC (Ref. 181) generally met my expectations. The BSC describes the NCSS and UNICORN platform, outlines the functional and performance requirements, lists the standards to which the NCSS is to be designed, and describes how quality is managed. It also provides design substantiation including an arguments and evidence based safety demonstration. However, design and development of the NCSS platform modules is currently incomplete. The detailed information and justifications will be produced during the SSP (e.g. the justification of the approach to testing, fail safe capability and selection of single or dual chain architecture for manual functions) and will need to be incorporated into the NCSS safety case (see **AF-UKEPR-CI-050** below).

426 EDF and AREVA presented the NCSS functional requirements in Ref. 187, which is supported by the NCSS functional justification document (Ref. 188). The former document describes, for each automatic and manual NCSS function, the functional task, fault sequences covered by the function, initiating parameters for automatic functions, setpoints for action initiation, and the action carried out. The NCSS functional coverage was assessed by the fault studies and PSA teams and found to generally meet expectations (see Refs 198 and 199 respectively). However, the adequacy of the final

NCSS design, in relation to reduction of plant risk, will need to be confirmed by inclusion of NCSS design details into the PSA (see **AF-UKEPR-CI-050** see below).

427 Although the NCSS functions have been described (Ref. 187), the means by which functions are reset following actuation have not been defined in detail within GDA. It is my expectation that, in accordance with SAP ESS.14, once a NCSS function has been triggered, this will continue to take action regardless of the state of the initiating parameter(s) until the operator performs a reset. This concern is raised within Assessment Finding **AF-UKEPR-CI-050**.

428 The NCSS function response times and reliability requirements are described in Ref. 185 with further detail provided in a supporting document (Ref. 186). The documents provide a preliminary justification of adequacy for a single representative function based on data from existing modules. My review of Ref. 185 identified that the Licensee will need to assess the effect of power loss within the NCSS system on plant safety (e.g. power loss leading to failure to actuate when required or send alarms to operators). I have captured the need to address this concern in Assessment Finding **AF-UKEPR-CI-050**. I found that Ref. 181 provided some detail on the voting logic (including the AVACT module), but it is not fully defined (e.g. a reliability substantiation that includes consideration of the impact of equipment maintenance needs to be completed). The information provided was preliminary but is sufficient to demonstrate that the approach to determining reliability and response times is suitable, and therefore to close the GDA Issue. However, function response times and reliabilities will have to be fully defined and justified within the SSP (see **AF-UKEPR-CI-050** below).

429 The quality management arrangements for the NCSS system and UNICORN platform were described by EDF and AREVA in the 'NCSS quality plan' (Ref. 183) and the 'Unicorn Project - Platform Quality Plan' (Ref. 182). The verification and validation arrangements were outlined in the 'NCSS System Verification and Validation Plan' (Ref. 184). Whilst these generally met my expectations, a number of matters remain to be resolved, including demonstration of conformance to the requirements of standards BS IEC 61513:2001 (Ref. 10) and BS IEC 60987:2007 (Ref. 18), regression testing of engineering and test tools following a version change, and independence of qualification teams. These matters have been captured in Assessment Finding **AF-UKEPR-CI-050** (see below).

430 Detailed NCSS design information was not available during the GDA closure phase and so a detailed justification of diversity between the NCSS and other systems has been deferred until the SSP when the detailed design information becomes available. An Assessment Finding to capture the need to perform a detailed diversity justification during the SSP has therefore been raised (see **AF-UKEPR-CI-037** in Section 4.5.3.1 on diversity justification and independence of the C&I systems important to safety).

431 Following assessment of EDF and AREVA's submissions in response to GDA Issue **GI-UKEPR-CI-01** on provision of a BSC for the NCSS, I am content that the BSC is acceptable and the GDA Issue can be closed. I have raised an Assessment Finding below to capture those matters arising from the assessment that need to be addressed during the implementation of the NCSS.

*GDA Assessment Finding: **AF-UKEPR-CI-050** - The Licensee shall:*

- *Document and justify the adequacy of the final NCSS design in the safety case (e.g. the approach to testing, fail safe capability and selection of single or dual chain architecture for manual functions, etc.).*

- *Confirm the adequacy of the final NCSS design, in relation to reduction of plant risk, by including NCSS design details into the PSA.*
- *Define how, once triggered, the action of an NCSS automatic function will be reset and confirm this meets the requirements of SAP ESS.14.*
- *Assess the effect of power loss within the NCSS system on plant safety (e.g. power loss leading to a failure to actuate when required or send alarms to operators).*
- *Define and justify the response times and reliabilities for all NCSS functions (including the energise to actuate AVACT module and consideration of the impact of maintenance on system reliability).*
- *Review the quality control procedures and update these to ensure adequate coverage of standards and activities (e.g. including demonstration of conformance to the requirements of standards BS IEC 61513 and BS IEC 60987, regression testing of engineering and test tools following a version change, and independence of qualification teams).*

For further guidance on the completion of the NCSS safety case see Technical Observations GICI01.TO2.18 to GICI01.TO2.21 and GICI01.TO2.23 to GICI01.TO2.34 in Annex 11.

[Required Timescale: prior to mechanical, electrical and C&I safet y systems, structures and components delivery to site.]

4.5.4 GDA Close-out findings

432 The Assessment Findings identified in the section above are also recorded in Annex 1.

4.6 Diversity of Systems Implementing Reactor Protection Functionality

4.6.1 GDA Step 4 Assessment

433 I have completed a review of the diversity of those systems implementing reactor protection functionality. The C&I systems included in the diversity review were the PS (TXS) and SAS / PAS (Siemens SPPA-T2000). These systems were selected because they perform the UK EPR™ protection functions.

434 The approach included consideration of various forms of diversity, including:

- equipment diversity (including diversity of platform);
- diversity of verification and validation;
- diversity of physical location (segregation);
- software diversity;
- functional / data / signal diversity;
- diversity of design / development; and
- diversity of specification.

435 The work required the definition of a list of reactor-independent diversity characteristics derived from relevant standards and guidance. I used the HSE SAPs, TAGs, nuclear sector C&I standards (i.e. Refs 10 and 11), regulatory guidance (Ref. 5) and relevant research (Ref. 61) as a basis for determining the diversity characteristics.

436 The main finding of the preliminary review undertaken during GDA Step 3 (e.g. Ref. 53) on the diversity of systems implementing reactor protection functionality was that the submission made by EDF and AREVA for adequacy of the diversity between the primary (PS) and secondary (SAS / PAS) protection systems did not demonstrate accordance with many of the relevant principles, standards criteria and guidance clauses used in the review. The main concerns arising from the review were:

- excessive reliability claims for the diverse protection systems;
- lack of evidence of platform diversity;
- lack of evidence of diversity within system s such as the P S when high reliability is needed; and
- absence of key information in the PCSR.

437 A major observation identified during GDA Step 3 was that the protection functions were provided by two computer-based platforms (i.e. TX S and SPPA-T2000). The introduction of the NCSS in response to **RI-UKEPR-002** has addressed this concern. The adequacy of protection provided for the postulated initiating events (PIEs) by the functions implemented in the SSs has been considered in the ND fault studies assessment (Ref. 51). The fault studies assessment concluded that adequate functional diversity had not been demonstrated (e.g. across the PS and an adequately diverse protection system) and a GDA Issue (**GI-UKEPR-FS2**) has been raised to cover this topic.

438 In responding to **RI-UKEPR-002**, EDF and AREVA have provided further substantiation of the diversity between the TX S and SPPA-T2000 platforms, and reduced the reliability claims for these platforms. The changes proposed to the UK EPR™ architecture and reliability claims have been considered during the TSC's GDA Step 4 diversity review (Ref. 33). I conclude that an acceptable way forward on the major diversity concerns has been achieved. This conclusion is subject to satisfactory resolution of GDA Issue Action **GI-UKEPR-CI-06.A1** and related TOs which address, amongst other observations:

- diversity of verification and validation (covering methods, tools and programming environment, see T20.A1.3.4 in Annex 9);
- software (development tools, met hods and programming environment, see T20.A1.3.4 in Annex 9); and
- communication networks such as the TX S Profibus and SPPA-T2000 'Profibus DP' (i.e. if it is used as a result of modifications to addr ess the S PPA-T2000 obsolescence issue - see T13.TO1.04 in Annex 3).

439 The main finding to arise from the GDA Step 4 diversity assessment is that a comprehensive justification of diversity and independence between the NCSS / PS, NCSS / SAS-PAS and PS / SAS-PAS needs to be provided (see GDA Issue Action **GI-UKEPR-CI-06.A1** in Section 4.5.1). While the diversity analysis provided for the PS / SAS-PAS has indicated that they are in principle diverse, more detailed information is required before this concern can be closed. For example, a demonstration of the diversity of the TX S and SPPA-T2000 methodology for requirements specification is required (see T18.TO2.09 in Annex 8).

440 EDF and AREVA have committed to implementing the NCSS in diverse technology to that of the computer-based systems and has provided a set of diversity criteria to be used in the selection of the NCSS platform. These criteria have been reviewed and

observations on areas for improvement provided to EDF and AREVA by TQ. EDF and AREVA's revision of the NCSS diversity criteria to address the areas for improvement (see T20.A1.2.3 in Annex 9) will require assessment during the GDA closure phase. This concern is covered by GDA Issue Action **GI-UKEPR-CI-06.A1** (see Section 4.5.1).

441 Substantiation of the probabilistic claims for any C&I components used by more than one SIS, and potentially by more than one line of protection (e.g. PIPS and PACS) is required. The response on this topic needs to include consideration of the potential for common cause failure as a result of the use of these shared components. This concern is covered by GDA Issue Action **GI-UKEPR-CI-06.A9** (see Section 4.5.1). This issue relates to the use of any common components (e.g. sensors or actuators) used across more than one SIS (e.g. the same sensor type used across the PS, SAS and NCSS or PAS and PS) where a common cause failure of the components could prevent the SIS from delivering the required safety function(s) (see T18.TO1.01, T18.TO1.02 and T18.TO1.TO5 in Annex 8).

442 The GDA Step 4 assessment is based on the SPPA-T2000 S5 platform but it is believed that elements of this platform are obsolete and a new platform will be required. Therefore, the detailed diversity analysis required under GDA Issue Action **GI-UKEPR-CI-06.A1** (see Section 4.5.1) will need to take account of any changes necessary to address the SPPA-T 2000 S5 obsolescence issue (see GDA Issue **GI-UKEPR-CI-05**).

443 The diversity related changes will need to be incorporated into the PCSR and supporting documentation (see Assessment Finding in 4.4.1 and TO.18.TO1.01 in Annex 8).

444 The response of EDF and AREVA to the concerns raised in **RI-UKEPR-002** on the UK EPR™ C&I architecture have addressed my significant diversity concerns. In particular, the reduction of the reliability claims on the computer-based systems and introduction of the NCSS have addressed my major diversity concerns. I conclude that, in broad terms, the diversity of those systems implementing reactor protection functionality is acceptable but a number of aspects related to GDA Issues and Assessment Findings require resolution. For example, detailed analysis of NCSS / Teleperm TXS / SPPA-T2000 diversity and the potential for common mode failure of components used across multiple SIS / lines of protection.

4.6.2 GDA Step 4 Findings

445 No Assessment Findings or GDA Issues have been raised in this section but relevant issues and findings are raised in the previous Sections (e.g. see Section 4.5.1).

4.7 Overseas Regulatory Interface

446 ND's GDA strategy for working with overseas regulators is set out in 'Strategy for working with overseas regulators. Version 1. HSE' (Ref. 59). In accordance with this strategy, ND collaborates with overseas regulators, both bilaterally and multinationally.

4.7.1 Bilateral Collaboration

447 ND has formal information exchange arrangements to facilitate greater international co-operation with the nuclear safety regulators in a number of key countries with civil nuclear power programmes. These include:

- US NRC;
- ASN; and
- the Finnish nuclear safety regulator (STUK).

448 During my assessment a significant concern was identified in relation to the C&I architecture (raised with EDF and AREVA under **RI-UKEPR-002**). The issue was primarily around ensuring the adequacy of the SS (those used to maintain control of the plant if it goes outside normal conditions), and their independence from the control systems (those used to operate the plant under normal conditions). Bilateral discussions were held with both ASN and STUK in relation to the C&I architecture concerns. The culmination of this collaboration was the publication of a joint regulatory position statement outlining the common view of the three regulators (Ref. 60). All parties recognised the importance of resolving the concern and undertook to progress the matter to conclusion, taking into account licensees' requirements and national regulatory requirements or practices. The way in which this issue has been resolved in the UK is discussed in Section 4.5.

4.7.2 Multilateral Collaboration

449 ND collaborates through the work of the IAEA and the OECD Nuclear Energy Agency (NEA). ND also represents the UK in MDEP - a multinational initiative taken by national safety authorities to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities tasked with the review of new reactor power plant designs. The aim of this programme is to promote consistent nuclear safety assessment standards among different countries.

450 To support the GDA C&I assessment, process insights from other regulators have been gained through participation in MDEP. ND has also shared assessment views and findings with our MDEP partners assessing EPR variants (USA, France, Finland and China) and has contributed to joint working. Some countries have more advanced plans for construction of the EPR design than the UK and it has been particularly beneficial to have had access to the experience of regulators from those countries.

451 One of the major achievements of the MDEP EPR Working Group was the development of common positions covering important C&I topics such as design complexity and independence within the C&I architecture.

452 MDEP is expected to continue beyond GDA and ND will continue to take an active role.

5 CONCLUSIONS

453 This report presents the findings of the C&I Step 4 and GDA Issue close-out assessment of the EDF and AREVA UK EPR™ reactor.

454 To conclude, I am broadly satisfied with the claims, arguments and evidence laid down within the PCSR and supporting documentation for the C&I which is included in the Submission Master List (Ref. 66). I consider that, from a C&I view point, the EDF and AREVA UK EPR™ design is suitable for construction in the UK. However, this conclusion is subject to satisfactory assessment of additional information that becomes available as the GDA Design Reference is supplemented with additional details on a site-by-site basis.

5.1 Key Findings from the GDA Step 4 and Close-out Assessment

455 The major conclusions of my GDA Step 4 assessment are that:

- the PCSR and supporting documentation cover the main C&I SIS expected in a modern nuclear reactor;
- the principal design and implementation standards used by EDF and AREVA for all C&I SIS are broadly in accordance with those expected in the nuclear sector;
- EDF and AREVA's safety case for the sampled key C&I SIS and platforms used to implement the SIS is broadly in line with expectations (noting that further implementation detail needs to be added to the safety cases following design completion); and
- significant C&I architecture concerns raised in **RI-UKEPR-002** have been addressed by the introduction of a safety Class 2 NCSS, one way network communication from the PS to lower classified systems, Class 1 displays and manual controls, and reduction of reliability claims for the computer-based SIS.

456 However, some of the observations identified during Step 4 were of particular significance and required resolution before ONR would agree to the commencement of nuclear safety related construction of a UK EPR™ reactor in the UK. These are identified in this report as GDA Issues and the C&I GDA Issues are listed in Annex 2. In summary these relate to:

- revision of the safety case to address the introduction of the NCSS including the demonstration of its diversity from the computer-based safety systems;
- revision of the safety case to address PS changes to ensure there are only outward network communications to other systems from the PS and justification of the small number of hardwired links to the PS;
- justification of the revised reliability figures used for the protection systems (PS, SAS / PAS and NCSS) when claimed independently and in combination;
- provision of detailed substantiation of the Class 1 control and display facilities including justification of functional coverage;
- revision of the safety case to classify the C&I systems (e.g. PAS and SAS) in accordance with international standards and commitments provided by EDF and AREVA;

- finalisation of the PS ICBM activities' scope (covering statistical testing, static analysis and compiler validation), and definition of PE and ICBMs for other SIS;
- enhancements to the safety case, in particular, to the presentation of the claims-arguments-evidence trail (i.e. covering key safety case claims and HSE SAP conformance);
- fully defining the approach to the justification of smart devices (based on computer technology) used in SIS including provision of a programme showing when implementation evidence will be available; and
- revision of the SAS / PAS safety case to address obsolescence of the SPPA-T2000 (Siemens S5 based) platform.

457 In response to the GDA Issues, EDF and AREVA published Resolution Plans for each GDA Issue. My GDA Issue close-out assessment focussed on the submissions identified within the Resolution Plans. The submissions have included provision of additional safety case information (e.g. BSC documents for the NCSS, SPPA-T2000 platform version change and PSOT Class 1 display system), methodologies to be implemented during the SSP (e.g. approach to smart device qualification and diversity assessment methodology) and proposals for plant modifications (e.g. provision of diverse sensor conditioning and PACS actuator modules). I conclude that the submissions are satisfactory and sufficient for closing out the C&I GDA Issues.

5.1.1 Assessment Findings

458 In some areas there has been a lack of detailed information, which has limited the extent of my assessment. As a result, I will need additional information to underpin my conclusion and these are identified as Assessment Findings to be carried forward as normal regulatory business, such as standards compliance demonstration for SIS and sensors, and implementation of process improvements (e.g. relating to PS requirements traceability and production of method statements). I conclude that the Assessment Findings listed in Annex 1 should be addressed during the forward programme of this reactor as part of normal regulatory business.

5.1.2 GDA Issues

459 I conclude that the GDA Issues listed in Annex 2, GDA Issue Action **GI-UKEPR-CC-01.A6** and C&I aspects of GDA Issue Action **GI-UKEPR-CC-02.A1** have been satisfactorily addressed.

6 REFERENCES

1 *GDA Step 4 Control and Instrumentation Assessment Plan for the EDF and AREVA UK EPR.* HSE-ND Assessment Plan AR 09/056. February 2010. TRIM Ref. 2009/464081.

2 ND BMS. *Assessment Process*. AST/001 Issue 4. April 2010. www.hse.gov.uk/foi/internalops/nsd/assessment/ast001.htm.

3 Not used.

4 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition Revision 1. HSE. January 2008. www.hse.gov.uk/nuclear/saps/saps2006.pdf.

5 *Licensing of Safety Critical Software for Nuclear Reactors. Common position of seven European nuclear regulators and authorised technical support organisations*. Revision 2010. www.hse.gov.uk/nuclear/software.pdf.

6 *Step 3 Control and Instrumentation Assessment of the EDF and AREVA UK EPR*. HSE-ND. AR 09/038. November 2009. TRIM Ref. 2009/339202.

7 *EDF and AREVA UK EPR - Schedule of Technical Queries Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600726.

8 *ND BMS. Safety Systems*. T/AST/003, Issue 5. September 2009. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast003.htm.

9 *ND BMS. Technical Assessment Guide - Computer Based Safety Systems*. T/AST/046 Issue 2. June 2008. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast046.htm.

10 *BS IEC 61513:2001 Nuclear power plants - Instrumentation and control for systems important to safety – general requirements for systems. International Electrotechnical Commission*. British Standard Institution (BSI) (IEC). 2001.

11 *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.

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

13 *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.

14 *The Tolerability of Risk from Nuclear Power Stations*. HSE. 1992. ISBN 0-11-886368-1. www.hse.gov.uk/nuclear/tolerability.pdf.

15 Not used.

16 *Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Pressurized Water Plant Units* - adopted during plenary meetings of the 'Groupe Permanent Chargé des Réacteurs' and German experts on the 19 and 26 October 2000.

17 *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. ISBN 978 0 580 63962 3.

18 *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. ISBN 978 0 580 63961 6.

19 Not used.

20 *EDF and AREVA UK EPR - Schedule of Regulatory Observations Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600727.

21 *EDF and AREVA UK EPR - Schedule of Regulatory Issues Raised during Step 4*. HSE-ND. TRIM Ref. 2010/600728.

22 *UK EPR Pre-Construction Safety Report – November 2009 Submission*. Submitted under cover of letter UN REG EPR00226N, 30 November 2009. TRIM Ref. 2009/481363 and as detailed in UK EPR Master Submission List. November 2009. TRIM Ref. 2011/46364.

23 *UK EPR Master Submission List*. November 2009. TRIM Ref. 2011/46364.

24 *Design and Construction Rules for Electrical Components of Nuclear Islands. RCC-E. December 2005*. ©AFCEN French Association for design, construction and in-service inspection rules for nuclear island components. ©AFCEN 105-2005.

25 *Control and Instrumentation - Scope GDA*. Letter from UK EPR Project Front Office to ND. Unique Number EPR00686N. 22 December 2010. TRIM Ref. 2010/640659.

26 *Control and Instrumentation - Architecture Regulatory Issue RI-UKEPR-002*. Letter from ND to UK EPR Project Front Office. Unique Number EPR70085R. 16 April 2009. TRIM Ref. 2009/152909.

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

28 Frazer Nash/Altran Report - NII GDA Technical Review – C&I SAP Conformance and Adequacy of Safety Case Review for UKEPR Step 4 Tasks 11-13 Report. 37194/36614R. TRIM Ref. 2011/297600.

29 Frazer Nash/Altran Report - Generic Design Assessment Technical Review - C&I Step 4 Report for Task 14 - Review of EDF/Areva QMS processes against Principal Design and Implementation Standards –UK EPR. S.P1440.74.30. TRIM Ref. 2011/297636.

30 Frazer Nash/Altran Report - Generic Design Assessment Technical Review - C&I Task 15 Class 1 & 2 System Platforms and Pre-Developed Complex Components Review for UK EPR Reactor. S.P1440.74.25. TRIM Ref. 2011/297657.

31 Frazer Nash/Altran Report - Generic Design Assessment Technical Review - C&I Step 4 Report for Task 16 – Review of Systems. S.P1440.74.26. TRIM Ref. 2011/297676.

32 Frazer Nash/Altran Report - Generic Design Assessment Technical Review - C&I Step 4 Report for Task 17: Review of C&I Architecture - UK EPR. S.P1440.77.14. TRIM Ref. 2011/297709.

33 Frazer Nash/Altran Report - Generic Design Assessment Technical Review - C&I Report for Task 18: Review of Diversity of Systems contributing to Category A functions - UK EPR. S.P1440.77.15. TRIM Ref. 2011/297738.

34 Frazer Nash/Altran Report - NII GDA Technical Review - C&I - Step 4 Review of Responses to Regulatory Issue RI-UKEPR-002 - Task 20. S.P1440.80.01. TRIM Ref. 2011/297752.

35 Not used.

36 *BS EN 62138:2004. Nuclear power plants. Instrumentation and control important for safety. Software aspects for computer-based systems performing category B or C Functions.* British Standards Institution (BSI). 2004. ISBN 978 0 580 63963 0.

37 *BSI Technical Committee NCE/8 Nuclear Power Plants - I&C Systems. A Guide to Applicable IEC Standards*. AFP – v7 – 2008_12_01. TRIM ref. 2011/386499

38 *United States Nuclear Regulatory Commission Safety Evaluation Report for Siemens Power Corporation*. EMF-2110 (NP). Office of Nuclear Reactor Regulation. May 2000.

39 Not used.

40 BS EN 61508:2002*. Functional Safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission (IEC). 2004.

41 *Step 4 Probabilistic Safety Analysis Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-019 Revision 0. TRIM Ref. 2010/581512.

42 *Control and Instrumentation – RO-UKEPR-43 – Safety Function Categorisation and SSC Classification for the UK EPR – Actions 1 and 2*. Letter from UK EPR Project Front Office to ND. Unique Number EPR00723N. 22 December 2010. TRIM Ref. 2010/640645.

43 *ISO IEC 27001:2005. Information technology - Security techniques - Information security management systems - Requirements*. International Organisation for Standardization (IOS). 2005.

44 *BS IEC 61226:2009. Nuclear power plants. Instrumentation and control important to safety. Classification of instrumentation and control functions.* British Standards Institution (BSI). 2009. ISBN 978 0 580 70133 7.

45 Not used.

46 *UK EPR Pre-construction Safety Report*. UK EPR-0002-011 Issue 00. EDF and AREVA. April 2008. Submitted under cover of EDF and AREVA Letters EPR00039R and EPR0044R (CD003, CD004, CD005 and CD006). 30 April 2008. TRIM Refs 2008/173181 and 2008/255670.

47 *UK EPR Pre-Construction Safety Report*. UK EPR-0002-132 Issue 02. EDF and AREVA. June 2009. TRIM Ref. 2011/24373.

48 NII GDA Technical Review - C&I UK EPR - PCSR Impact Assessment – 36331/3593R, Issue 1.0. June 2009. TRIM Ref. 2011/424563.

49 *New nuclear power stations. Generic Design Assessment. Guidance on the Management of GDA Outcomes*. HSE. Version 1. 23 June 2010. www.hse.gov.uk/newreactors/reports/management-gda-outcomes.pdf

50 *Control and Instrumentation – UK EPR (C&I) – Conclusions of Level 3 & 2 Meetings on 4th and 7th October 2010*. Letter from UK EPR Project Office to ND. Unique Number EPR00607N. 15 October 2010. TRIM Ref. 2010/522508.

51 *Step 4 Fault Studies – Design Basis Faults Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-020a Revision 0. TRIM Ref. 2010/581404.

52 NII GDA Technical Review – C&I System Architecture safety Review for UK EPR – S.P1440.57.11, Issue 2.2. TRIM Ref. 2011/221355.

53 NII GDA Technical Review – C&I Diversity Aspects of C&I Category A Functional systems Design Review for UK EPR – S.P1440.57.12, Issue 2.2. TRIM Ref. 2011/221404.

54 *Control and Instrumentation – RI-UKEPR-002 – C&I Architecture Issues*. Letter from UK EPR Project Office to ND. EPR00180R. 30 September 2009. TRIM Ref. 2009/386051.

55 *New Nuclear Power Stations. Generic Design Assessment. Guidance to HSE and Environment Agency Inspectors on the Content of: GDA Issues, Assessment Findings, resolution plans and GDA Issue Metrics.* HSE-ND. 3 June 2011. TRIM Ref. 2011/302633.

56 *Protection System - System Description (Pilot Study).* NLN-F DC 193 Revision B. EDF and Areva. February 2011. TRIM Ref. 2011/128840.

57 *Control and Instrumentation – RO-UKEPR-43 – Safety Function Categorisation and SSC Classification for the UK EPR – Actions 1 and 2*. Letter from UK EPR Project Front Office to ND. Unique Number EPR00738N. 4 January 2011. TRIM Ref. 2011/1730.

58 *IEC 61504:2000. Nuclear power plants. Instrumentation and control systems important to safety. Plant-wide radiation monitoring.* November 2000. ISBN 0 580 36630 8.

59 *UK Generic Design Assessment: Strategy for working with overseas regulators*. HSE. March 2009. www.hse.gov.uk/newreactors/ngn04.pdf.

60 *Joint Regulatory Position Statement on the EPR Pressurised Water Reactor* (see HSE website www.hse.gov.uk/newreactors/pressurised-water-reactor.htm).

61 *Guidance on means to achieve system diversity: DIPO 6 view.* Littlewood B, Popov P, Strigini L, Version V1.0 PP_DISPO6_01, 27th October 2008.

62 *UK EPR Consolidated Pre-construction Safety Report – March 2011 Submission.* Detailed in EDF and AREVA letter UN REG EPR00997N. November 2011. TRIM Ref. 2011/552663.

63 *UK EPR - Overall I&C System Quality Plan.* NLN-F DC 132 TRIM Ref. 2011/92852.

64 *BS IEC 60780:1998. Nuclear power plants — Electrical equipment of the safety system—Qualification.* British Standards Institution (BSI). 1998. ISBN 0 580 32301 3.

65 *Step 4 Cross-cutting Topics Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-032 Revision 0. TRIM Ref. 2010/581499.

66 *UK EPR Master Submission List.* UKEPR-0018-001, Issue 01, EDF and AREVA. November 2011. TRIM Ref. 2011/552512.

67 Control and Instrumentation Assessment Plan - EPR GDA Closure. TRIM Ref. 2011/482607.

68 *Resolution Plan for GDA Issue GI-UKEPR-CI-01 Revision 0.* EDF and AREVA. 2011. TRIM Ref. 2011/352069.

69 *Resolution Plan for GDA Issue GI-UKEPR-CI-02 Revision 0.* EDF and AREVA. 2011. TRIM Ref. 2011/352071.

70 *Resolution Plan for GDA Issue GI-UKEPR-CI-03 Revision 0.* EDF and AREVA. 2011. TRIM Ref. 2011/352072.

71 *Resolution Plan for GDA Issue GI-UKEPR-CI-04 Revision 0.* EDF and AREVA. 2011. TRIM Ref. 2011/352073.

72 *Resolution Plan for GDA Issue GI-UKEPR-CI-05 Revision 0.* EDF and AREVA. 2011. TRIM Ref. 2011/352077.

73 *Resolution Plan for GDA Issue GI-UKEPR-CI-06 Revision 0.* EDF and AREVA. 2011. TRIM Ref. 2011/352079.

74 Frazer Nash/Altran Report - GDA Issues Resolution - C&I Review for EDF/Areva UK EPR Design - Review of Responses to GI-UKEPR-CI-01 - S.P1440.101.011 Issue 1.3 (Definitive). TRIM Ref. 2013/14637.

75 Frazer Nash/Altran Report - GDA Issues Resolution - C&I Review for EDF/Areva UK EPR Design - Review of Responses to GI-UKEPR-CI-02 - S.P1440.101.012 Issue 1.5 (Definitive). TRIM Ref. 2013/2671.

76 Frazer Nash/Altran Report - GDA Issues Resolution - C&I Review for EDF/Areva UK EPR Design - Review of Responses to GI-UKEPR-CI-03 - 39075/37981R Issue 1.6 (Definitive). TRIM Ref. 2013/2728.

77 Frazer Nash/Altran Report - GDA Issues Resolution - C&I Review for EDF/Areva UK EPR Design - Review of Responses to GI-UKEPR-CI-04 - 39075-38029R Issue 1.3 (Definitive). TRIM Ref. 2013/2763.

78 Frazer Nash/Altran Report - GDA Issues Resolution - C&I Review for EDF/Areva UK EPR Design - Review of Responses to GI-UKEPR-CI-05 - 39075-38099R Issue 1.4 (Definitive). TRIM Ref. 2013/14774.

79 Frazer Nash/Altran Report - GDA Issues Resolution - C&I Review for EDF/Areva UK EPR Design - Review of Responses to GI-UKEPR-CI-06 - S.P1440.101.016 Issue 1.3 (Definitive). TRIM Ref. 2013/23169.

80 *UK EPR - Programme of Statistical Testing Activities.* ECECC111521 Revision B. EDF. June 2012. TRIM Ref. 2012/241333.

81 *UK EPR Guideline for Application of Production Excellence and Independent Confidence Building*. ECECC111134 Revision C. EDF. July 2012. TRIM Ref. 2012/298715.

82 *Feasibility Study into the use of MALPAS for UK EPR.* 5094205-rep-01 version V3.0 June 2012 - Atkins. EDF and AREVA. June 2012. TRIM Ref. 2012/241187.

83 *UK EPR Protection System - scope and programme of work to address functional static analysis and compiler validation*. ENSECC110123 Revision B. EDF. June 2012. TRIM Ref. 2012/241312.

84 *Analysis of Real-time, Multitasking Software (ARMS)*. 5100191-rep-02 version 2.0 February 2012 – Atkins. CINIF. February 2012. TRIM Ref. 2012/335265.

85 *Justification for PE and ICBMs used for TELEPERM XS based systems*. ECECC111557 Revision B. EDF CNEN. July 2012. TRIM Ref. 2012/290717.

86 *EDF and AREVA UK EPR™ - Schedule of Technical Queries Raised during GDA Close-out.* Office for Nuclear Regulation. October 2012. TRIM Ref. 2011/389411.

87 GDA Close-out for the EDF and AREVA UK EPR™ Reactor – GDA Issue GI-UKEPR-FS-02 Revision 0 – Diversity for Frequent Faults. Office for Nuclear Regulation. March 2013. TRIM Ref. 2012/11.

88 *Justification for PE and ICBMs used SPPA-T2000 based systems.* ECECC120398 Revision B. EDF CNEN. August 2012. TRIM Ref. 2012/336458.

89 *PCSR I&C Claims, Arguments and Evidence (CAE) Final*. 16626-709-000-RPT-0003 Issue 1. EDF and AREVA. April 2011. TRIM Ref. 2011/209970.

90 *UKEPR GDA I&C System CAE Document*. 216626-709-000-RPT-0028 Issue 03. EDF and AREVA. June 2012. TRIM Ref. 2012/263127.

91 *Claims-Argument-Evidences trail for satisfaction of SAPs relevant to I&C*. PELL-F DC 9 Revision C. EDF and AREVA. September 2010. TRIM Ref. 2011/93023.

92 *Update of Claims-Argument-Evidences trail for satisfaction of SAPs relevant to I&C*. 16626-709-000-RPT-0031 Issue 2. EDF and AREVA. June 2012. TRIM Ref. 2012/262241.

93 *Response to C&I Meeting Action GI 13-I&C-1*. Letter EPR01327N. 20 August 2012. TRIM Ref. 2012/330683.

94 *Plant I&C requirement specification*. ECECC100744 Revision A. EDF and AREVA. June 2010. TRIM Ref. 2011/85888.

95 European Utility Requirements for LWRs. http://www.europeanutilityrequirements.org/eur.htm

96 *ENCLOSURE OF GDA SUBMISSION #21: CONSOLIDATED STEP 4 SSER*. Letter EPR00844N. EDF and AREVA. 31 March 2011. TRIM Ref. 2011/200260.

97 *Consolidated PCSR Chapter Review actions under GI-UKEPR-CC-02 plus Annex 1*. Letter EPR70323R. Office for Nuclear Regulation. 22 June 2011. TRIM Refs 2011/334790 & 334794.

98 *Resolution Plan for GI-UKEPR-CC02*. Revision 1. EDF and AREVA. July 2011. TRIM Ref. 2011/349105.

99 *Part response to GI-UKEPR-CC02 Action 3 Task 2 – Provision of Responses to ONR/EA comments on March 2011 SSER*. Letter EPR00964N. 20 September 2011. TRIM Ref. 2011/506745.

100 *Part response to GI-UKEPR-CC02 Action 3 Task 2 – Provision of Updated Responses to ONR C&I Related Comments on UK EPR GDA Consolidated Step 4 PCSR*. Letter EPR01059N. 18 January 2012. TRIM Ref. 2012/30799.

101 *GDA Issues GI-UKEPR-CI-01 to CI-06 – Advance Version of PCSR Chapter 7*. Letter EPR01264N. EDF and AREVA. 20 July 2012. TRIM Ref. 2012/290763.

102 T/AST/051 Guidance on the Purpose, Scope and Content of Nuclear Safety Cases.

103 *Final Versions of PCSR Sub-chapters 7.1, 7.4, 7.5 and 7.6*. Letter EPR01443N. EDF and AREVA. 31 October 2012. TRIM Ref. 2012/425045.

104 *Final Versions of PCSR Sub-chapters 7.2, 7.3 and 7.7*. Letter EPR01452N. EDF and AREVA. 6 November 2012. TRIM Ref. 2012/433046.

105 *Consolidated PCSR Step 4 review closure matrix*. Office for Nuclear Regulation. November 2012. TRIM Ref. 2012/467674.

106 *PCSR Chapter 7 Review for CI Rev 2*. Office for Nuclear Regulation. November 2012. TRIM Ref. 2012/467903.

107 *UKEPR-I-002 Rev 14. UK EPR design reference*. EDF and AREVA. October 2012. TRIM Ref. 2012/425015.

108 *UK EPR Control and Instrumentation (C&I) – Scope of GDA.* Letter EPR00686N. EDF and AREVA. 22 December 2010. TRIM Ref. 2010/643430. (Resubmission of Ref. 25 to correct anomalies in table headings)

109 GI-UKEPR-CC02 – *SDMs Update – C&I Systems Design Reference January 2012*. Letter. EDF and AREVA. January 2012. TRIM Ref. 2012/50766.

110 *C&I UK EPR Level 3 Meeting – Minutes of Meeting 19/4/2012*. EDF and AREVA. April 2012. TRIM Ref. 2012/483712.

111 Frazer Nash/Altran Report - GDA Issues Resolution - C&I Review for EDF/Areva UK EPR Design - Review of response to GI-UKEPR-CC-02 Action A.1 Task 5 - 39075-38876R Issue 1.1 (Definitive). TRIM Ref. 2013/2777.

112 *System Requirements Specification Mapping of FA3 PS to the clauses of IEC61513:2001 section 6.1.1*. Letter EPR01238N. EDF and AREVA. 29 June 2012. TRIM Ref. 2012/261849.

113 *System Requirements Specification Mapping of FA3 PS to the clauses of IEC61513:2001 section 6.1.1. AREVA. June 2012.* TRIM Ref. 2012/262140.

114 *EPR FA3 Functional Description of RRC-A C&I Functions*. NEPR-F DC 52 Revision B. AREVA. December 2007. TRIM Ref. 2011/94212.

115 *Reactor Trip Concept*. NLE-F DC 124 Revision B. AREVA. June 2008. TRIM Ref. 2011/91662.

116 *Protection System detailed specification file*. NLE-F DC 38 Revision F. AREVA. August 2008. TRIM Ref. 2011/85721.

117 *UK GDA – Response to TQ-EPR-1624: (NEPR-F DC 114 Revision G Reactor trip on low PZR pressure)*. PEPRF.12.1121. AREVA. August 2012. TRIM Ref. 2012/317566.

118 *Response to TATS Action GI 11-I&C-3 I&C System Design Definition*. Letter EPR01360N. EDF and AREVA. 10 September 2012. TRIM Ref. 2012/353601.

119 *RCSL Detailed Specification*. NLP-G/2006/en/1007 Revision G. AREVA. July 2008. TRIM Ref. 2012/216680.

120 *Severe Accident I&C Detailed Specification File*. NLE-F DC 106 Revision C. AREVA. August 2009. TRIM Ref. 2011/92832.

121 *Process Instrumentation Pre-processing System Detailed Specification*. NLE-F DC 173 Revision C. AREVA. February 2010. TRIM Ref. 2011/92833.

122 *Mapping the SAS documentation to the requirements of IEC61513 clause 6.1.1*. ECECC121435 Revision A. EDF. August 2012. TRIM Ref. 2012/320333.

123 *UK EPR Generic Design Assessment – Classification of I&C Safety Features*. ECEF091489 Revision E. EDF. October 2012. TRIM Ref. 2012/417591.

124 *CCF 05b Overall Sizing and Performance*. ECECC100565.

125 *ENG 3-03 EPR plant system specification – content and update*. ECEF050611 Revision A1. EDF. December 2005. TRIM Ref. 2011/155716.

126 *CRF Raw water circulation system Part 5 Instrumentation and Control*. ETDOFC/080077 Revision C1. EDF. September 2009. TRIM Ref. 2011/155993.

127 *SRS Equivalence Justification Note for PAS and PACS*. ECECC121609 Revision A. EDF. August 2012. TRIM Ref. 2012/320334.

128 *PS (incl. RPI sw) / RCSL / SA I&C / PIPS Teleperm XS I&C system engineering quality plan*. PEL-F DC 7 Revision A. AREVA. June 2012. TRIM Ref. 2012/263128.

129 *Change SPPA-T2000 platform version from S5 to S7 (S5 obsolescence)*. UKEPR-CMF-029 Stage 1. EDF and AREVA. May 2011. TRIM Ref. 2011/306576.

130 *Impact study of the change from SPPA T2000 S5 to S7 – CMF Stage 2*. PEL-F/11-0245. EDF and AREVA. September 2011. TRIM Ref. 2011/479490.

131 *I&C – Structure of a Basis of Safety Case*. Letter EPR00852R. EDF and ARREVA. 15 April 2011. TRIM Ref. 2011/225129.

132 *Outline of Basis of Safety Case for the SPPA-T2000 based I&C systems (SAS, PAS, SAS RRC-B, PICS and Plant Bus) and SPPA-T2000 platform*. PEL-F/11.0353. AREVA. December 2011. TRIM Ref. 2011/648745.

133 *Basis of Safety Case of SPPA-T2000*. PEL-F DC 13 Revision A. AREVA. June 2012. TRIM Ref. 2012/263148.

134 *SPPA-T2000 - BSC Requirements Traceability Matrix V1*. Letter EPR01242N. EDF and AREVA. 2 July 2012. TRIM Ref. 2012/263145.

135 *Response to GI-UKEPR-CI05 – Action 1 – Supporting documentation for Basis of Safety Case for the Change from SPPA T2000 S5 to S7*. Letter EPR01261N. EDF and AREVA. 13 July 2012. TRIM Ref. 2012/280555.

136 *Resolution Plan for GDA Issue GI-UKEPR-CI06* Revision 1. EDF and AREVA. June 2012. TRIM Ref. 2012/262766.

137 *Methodology and organisation for diversity management between I&C platforms and I&C systems*. PTL-F DM 1 Revision A. AREVA. April 2012. TRIM Ref. 2012/148880.

138 *Methodology and organisation for diversity management between I&C platforms and I&C systems*. PTL-F DM 1 Revision B. AREVA. June 2012. TRIM Ref. 2012/243631.

139 *RS/PTL Organisational note for I&C platforms diversity management*. PTL-F DC 4 Revision A. AREVA. June 2012. TRIM Ref. 2012/244350.

140 *Diversity criteria between the protection system and safety automation system*. PTL-F DC 3 Revision A. AREVA. July 2012. TRIM Ref. 2012/282221.

141 *Overall Approach to Diversity of UK EPR I&C Systems*. ECECC121713 Revision A. EDF. August 2012. TRIM Ref. 2012/337777.

142 *Diversity criteria between protection system and safety automation system*. PTL-F DC 3 Revision B. AREVA. August 2012. TRIM Ref. 2012/343777.

143 *Key elements for diversity management methodology improvement*. PTI12.1072 Revision A. AREVA. September 2012. TRIM Ref. 2012/381536.

144 *Non Computerised Safety System – Diversity Criteria*. PELL-F DC 11 Revision C. AREVA. August 2012. TRIM Ref. 2012/343776.

145 *Diversity criteria definition for Priority Actuation Control (PAC) module*. ECECC120443 Revision B. EDF. July 2012. TRIM Ref. 2012/315332.

146 *Diversity Criteria for sensors and conditioning*. PELL-F DC 82 B Revision A. AREVA. December 2011. TRIM Ref. 2011/651597.

147 *Response to C&I meeting Actions GI 15-I&C-1 and GI 16-I&C-3*. Letter EPR01412N. EDF and AREVA. 22 October 2012. TRIM Ref. 2012/411788.

148 *Justification of diversity between I&C systems implemented in I&C platforms*. PELZ-F DC 2 Revision A. AREVA. July 2012. TRIM Ref. 2012/284472.

149 *Justification of diversity between I&C systems implemented in I&C platforms*. PELZ-F DC 2 Revision B. AREVA. October 2012. TRIM Ref. 2012/410350.

150 *Exclusion of CCF between SPPA T2000 (S7) and TELEPERM XS by using diversity*. NLTC-G/2009/en/0018 Revision B. AREVA. February 2011. TRIM Ref. 2012/325926.

151 *Current Diversity Analysis between SPPA-T2000 (S7) and TELEPERM XS – Corrective action plan*. PTI.12.1071 Revision A. AREVA. September 2012. TRIM Ref. 2012/381535.

152 *TELEPERM XS I&C System Compliance Analysis with IEC 61513*. PEL-F DC 8 Revision A. AREVA. June 2012. TRIM Ref. 2012/251140.

153 *TELEPERM XS I&C Systems Compliance Analysis with IEC 60880*. PEL-F DC 9 Revision A. AREVA. June 2012. TRIM Ref. 2012/251141.

154 *TELEPERM XS I&C Systems Compliance Analysis IEC 60987*. PEL-F DC 10 Revision A. AREVA. June 2012. TRIM Ref. 2012/251142.

155 *Compliance of the TXS Hardware design and Engineering process with IEC60987 Ed.2*. NLTC-G 2008 en 0053 Revision A. AREVA. July 2008. TRIM Ref. 2012/290975.

156 *Compliance of the TXS system platform and development processes with IEC 61513*. PTLC-G 2010 en 0047 Revision B. AREVA. June 2012. TRIM Ref. 2012/290976.

157 *TXS Platform: Compliance Analysis IEC 60880 Ed. 2.0. PTLD-G 2010 en 0383 Rev A*. AREVA. December 2011. TRIM Ref. 2012/290977.

158 *Justification of PS reliability*. PELL-F DC 233 Revision A. AREVA. December 2011. TRIM Ref. 2011/621858.

159 IEC 60812 *Analysis techniques for system reliability – Procedure for failure modes and effects analysis (FMEA)*. Ed. 2 2006.

160 IEC 61025 *Fault tree analysis (FTA)*. Ed. 2 2006.

161 *Justification of PS reliability*. PELL-F DC 233 Revision B. AREVA. June 2012. TRIM Ref. 2012/237452.

162 *Protection System – Reliability and Availability Study*. NEPS-F DC 29 Revision G. AREVA. December 2011. TRIM Ref. 2012/124449.

163 *Independence of the Class 1 Protection System (PS), the Safety Automation System (SAS) and the Non-Computerised Safety System (NCSS)*. ECECC111963 Revision B. EDF. February 2012. TRIM Ref. 2012/63019.

164 BS IEC 60709 *Nuclear Power Plants – Instrumentation and control systems important to safety – Separation*. Ed. 2 2004.

165 *Independence of the Class 1 Protection System (PS), the Safety Automation System (SAS) and the Non-Computerised Safety System (NCSS)*. ECECC111963 Revision C. EDF. August 2012. TRIM Ref. 2012/307164.

166 *Generic rules for the electrical isolation of EPR UK Instrumentation and Control systems (internal connections and interfaces)*. ECECC111058 Revision A. EDF. July 2011. TRIM Ref. 2011/402683.

167 *TELEPERM XS based systems – Concept for Electrical Separation*. NLE-F DC 249 Revision E. AREVA. January 2011. TRIM Ref. 2012/3466.

168 *Generic rules for the electrical isolation of EPR UK Instrumentation and Control systems (internal connections and interfaces)*. ECECC111058 Revision B. EDF. June 2012. TRIM Ref. 2012/231930.

169 *Method for performing diversity and defence in depth analyses of reactor protection systems*. NUREG 6301 Dec 1994.

170 *C&I UK EPR Level 3 Meeting – Minutes of Meeting. EDF and AREVA. 5 July 2012*. TRIM Ref. 2012/483169.

171 *UK EPR PCSR Sub-chapter 7.1 - Design principles of the Instrumentation and Control systems*. UKEPR0002-071- Issue 04. EDF and AREVA. October 2012. TRIM Ref. 2012/425069.

172 *UK EPR PCSR Sub-chapter 7.2 - General architecture of the Instrumentation and Control systems*. UKEPR0002-072- Issue 04. EDF and AREVA. November 2012. TRIM Ref. 2012/433581.

173 *UK EPR PCSR Sub-chapter 7.3 - Class 1 Instrumentation and Control systems.* UKEPR0002-073 - Issue 04. EDF and AREVA. November 2012. TRIM Ref. 2012/433586.

174 *UK EPR PCSR Sub-chapter 7.4 - Class 2 instrumentation and control systems.* UKEPR0002-074- Issue 04. EDF and AREVA. October 2012. TRIM Ref. 2012/425072.

175 *UK EPR PCSR Sub-chapter 7.5 - Class 3 Instrumentation and Control Systems.* UKEPR0002-711- Issue 01. EDF and AREVA. October 2012. TRIM Ref. 2012/425076.

176 *UK EPR PCSR Sub-chapter 7.6 – Instrumentation.* UKEPR0002-075 – Issue 04. EDF and AREVA. October 2012. TRIM Ref. 2012/425078.

177 *UK EPR PCSR Sub-chapter 7.7 - I&C tools, development process and substantiation*. UKEPR0002-076 – Issue 04. EDF and AREVA. November 2012. TRIM Ref. 2012/433590.

178 *Justification note for NCSS platform selection*. PTI DC 5 Revision A. AREVA. June 2011. TRIM Ref. 2011/348047.

179 *Outline of Basis of Safety Case of Non-Computerized Safety System*. PEL-F/11.0309. AREVA. October 2011. TRIM Ref. 2011/559493.

180 *List of contents of NCSS Basis of Safety Case*. PTLI 12.1060 Revision A. AREVA. June 2012. TRIM Ref. 2012/262204.

181 *Non-Computerised Safety System - Basis of Safety Case*. PTL-F DC 5 Revision A. A REVA. August 2012. TRIM Ref. 2012/309805.

182 *Unicorn Project - Platform Quality Plan*. TA-2057230 Revision D. AREVA. June 2012. TRIM Ref. 2012/264201.

183 *NCSS Quality Plan*. TA-2061589 Revision C. AREVA. July 2012. TRIM Ref. 2012/271260.

184 *NCSS System Verification and Validation Plan*. TA-2065953 Ind. C. AREVA. July 2012. TRIM Ref. 2012/304887.

185 *UNICORN Project Justification of Platform reliability & Response Time on a typical automatic function*. TA-2082935 Ind. B. AREVA. July 2012. TRIM Ref. 2012/300352.

186 *UNICORN Project Justification of Reliability Allocation*. TA-2096900 Ind. A. AREVA. June 2012. TRIM Ref. 2012/300353.

187 *EPR UK Functional Requirements on Non-Computerised Safety I&C Functions*. NEPR-F DC 551 Revision C. AREVA. July 2012. TRIM Ref. 2012/284449.

188 *EPR UK – Functional Justification of the Non-Computerised Safety System Design*. PEPR-F DC 105 Revision A. AREVA. July 2012. TRIM Ref. 2012/284451.

189 *EMPHASIS Tool Evaluation*. ENSECC11 0110 Revision B. EDF. March 2012. TRIM Ref. 2012/114491.

190 *Justification of smart devices for nuclear safety applications*. ENSECC110102 Revision B. EDF. May 2012. TRIM Ref. 2012/216195.

191 *Summary Qualification Report for …* [Digital chart recorder]. ECECC1 21091 Revision A. EDF. June 2012. TRIM Ref. 2012/261696.

192 *SICS chart recorder - Requirements Identification File*. ECECC120 095 Revision A. EDF. February 2012. TRIM Ref. 2012/77841.

193 *Emphasis assessment database* [Digital chart recorder]. ECECC121338 Revision A. EDF. July 2012. TRIM Ref. 2012/294001.

194 *Progress Report on Class 1 Smart Device Trial Assessment*. ECECC121403 Revision A. EDF. July 2012. TRIM Ref. 2012/309902.

195 *Software Assessment Report for STT1 Temperature Transmitter*. ECECC121336 Revision A. EDF. July 2012. TRIM Ref. 2012/309897.

196 *C&I UK EPR Level 3 Meeting – Minutes of Meeting.* EDF and AREVA. August 2012. TRIM Ref. 2012/0491927.

197 *Response to C&I Meeting Actions GI 14-I&C-4*. Letter EPR01396N. EDF and AREVA. 5 October 2012. TRIM Ref. 2012/390926.

198 *Fault Studies Assessment Report: Assessment of the Non-Computer Based Safety System (NCSS) functional requirements 12th November 2012*. Office for Nuclear Regulation. November 2012. TRIM Ref. 2012/441927.

199 *Probabilistic Safety Assessment Report: Review of the adequacy from the PSA point of view of the NCSS "Safety Frame" 24th October 2012*. Office for Nuclear Regulation. October 2012. TRIM Ref. 2012/339247.

200 *Analysis of the non disturbance of the Protection System by lower classified signals coming from systems in interface.* PELL-F DC 252 Rev. A. AREVA. April 2012. TRIM Ref. 2012/186996.

201 *Protection System- System Description (Pilot Study)*. NLN-F DC 193 Revision C. AREVA. April 2012. TRIM Ref. 2012/186993.

202 *RO-UKEPR-082 – Full response to Action A6*. Letter EPR00823R. EDF and AREVA. 11 March 2011. TRIM Ref. 2011/145670.

203 *Appendix A Independence of the PICS and the SAS*. ECECC121458 Revision A. EDF. July 2012. TRIM Ref. 2012/304938.

204 *Class 1 Control and Display Facilities in the Main Control Room and the Remote Shutdown Station*. ECECC111829 Revision A. EDF. December 2011. TRIM Ref. 2012/1349.

205 *Class 1 Control and Display Facilities in the Main Control Room and the Remote Shutdown Station*. ECECC111829 Revision B. EDF. July 2012. TRIM Ref. 2012/308513.

206 TQ-EPR-1130 *SICS Class 1 Displays and Controls 20/01/2011*. EDF. January 2011. TRIM Ref. 2011/45594.

207 *Outline of content of the Basis of Safety Case for the Protection System Operator Terminal*. ECECC111181 Revision A. EDF. August 2011. TRIM Ref. 2011/436271.

208 *Protection System Operator Terminal Basis of Safety Case*. ECECC120489 Revision A. EDF. May 2012. TRIM Ref. 2012/215687.

209 *PSOT Functional Scope*. ECECC120711 Revision A. EDF. July 2012. TRIM Ref. 2012/271172.

210 *US Nuclear Regulatory Commission Regulatory Guide 1.97 "Instrumentation for Light-Water-Cooled Nuclear Power Plants to assess plant and environs conditions during and following an accident"*, Revision 3. May 1983.

211 *Safety Principles Applied to the UK EPR I&C Architecture in terms of the Requirements for Diversity and Independence*. PEPS-F DC 90 Revision A. AREVA. August 2011. TRIM Ref. 2011/436456.

212 *Safety Principles Applied to the UK EPR I&C Architecture in terms of the Requirements for Diversity and Independence*. PEPS-F DC 90 Revision B. AREVA. April 2012. TRIM Ref. 2012/180325.

213 *Safety Principles Applied to the UK EPR I&C Architecture in terms of the Requirements for Diversity and Independence*. PEPS-F DC 90 Revision C. AREVA. August 2012. TRIM Ref. 2012/342262.

214 *UK EPR GDA - Classification of I&C system features*. E CEF091489 Revision D. E DF. June 2012. TRIM Ref. 2012/259023.

215 *GDA Close-out for the EDF and AREVA UK EPR™ Reactor – GDA Issue GI-UKEPR-FS-05 Revision 0 – DBA of Essential Support Systems*. Office for Nu clear Regulation. March 2013 . TRIM Ref. 2012/13.

216 NUREG / CR-6 303 *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*. 1994.

217 *Definition of I&C architecture design requirements in the UK context*. ECECC120414 Revision A. EDF. July 2012. TRIM Ref. 2012/314765.

218 *Architecture of instrumentation and control system UK EPR. Design: principles and defence-in-depth*. ECECC100831 Revision B. EDF. October 2012. TRIM Ref. 2012/396558.

219 *Response to GI-UKEPR-CC01- Action 6 Categorisation and Classification*. Letter EPR0 1375N. EDF and AREVA. 10 October 2012. TRIM Ref. 2012/396551.

220 *Engineering and Projects Organisation EPR overall I&C design process*. PELA-F 12. 1004. AREVA. February 2012. TRIM Ref. 2012/82826.

221 *Methodology for Classification of Structures, Systems, Safety Features and Components*. NEPS-F DC 557 Revisi on D Advance. E DF and AREVA. October 2012. TRIM Ref. 2012/397307.

222 *Methodology for Classification of Structures, Systems, Safety Features and Components*. NEPS-F DC 557 Revision D Final. EDF and AREVA. October 2012. TRIM Ref. 2012/424300.

223 *GI-UKEPR-CI06 and GI-UKEPR-CC01: Response to C&I Meeting Actions GI 4-I&C-1 to GI 4-I&C-7*. Letter EPR01030N. EDF and AREVA. 9 January 2012. TRIM Ref. 2012/13578.

224 *Methodology for Classification of Structures, Systems, Safety Features and Components.* NEPS-F DC 557 Revision C. EDF and AREVA. January 2011. TRIM Ref. 2011/85983.

225 *UK EPR: Justification of time response end to end on Terminal Bus Plant Bus.* ECECC111368 Revision A. EDF. September 2011. TRIM Ref. 2011/505960.

226 *SPPA T2000 Response time – AREVA presentation on 19 April 2012*. TRIM Ref. 2012/224120.

227 *UK EPR: Justification of time response end to end on Terminal Bus Plant Bus*. ECECC1 11368 Revision B. EDF. August 2012. TRIM Ref. 2012/322568.

228 BS EN 6178 4 part 3 *Industrial communication networks. Profiles. Functional safety fieldbuses. General rules and profile definitions* 2010. ISBN 978 0 580 61647 1

229 Frazer Nash/Altran Report - GDA Issues Resolution - C&I Review for EDF/Areva UK EPR Design - Review of Responses to GI-UKEPR-CC-01 - 39075-38102R Issue 1.2 (Definitive). TRIM Ref. 2013/23237.

230 *UK EPR: Diversity Implementation Plan For Sensors & Conditioning*. PELA-F DC 3 Revis ion A. AREVA. December 2011. TRIM Ref. 2011/651597.

231 *UK EPR: Functional Analysis for Sensors‘ Common Cause Failure*. PEPR-F DC 83 Revision A. AREVA. November 2011. TRIM Ref. 2011/651612.

232 *Diversity Criteria for sensors and conditioning*. PELL-F DC 82 Revision C. AREVA. October 2012. TRIM Ref. 2012/424866.

233 *UK EPR: Diversity Implementation Plan For Sensors & Conditioning*. PELA-F DC 3 Revision C. AREVA. October 2012. TRIM Ref. 2012/425767.

234 *UK EPR GDA - Basis of Substantiation of C&I Components.* PELA-F DC 7 Revision A. AREVA. March 2012. TRIM Ref. 2012/138773.

235 *UK EPR GDA - Basis of Substantiation for the Reliability Claims for Sensors and Conditioning Modules*. PELA-F DC 7 Revision B. AREVA. October 2012. TRIM Ref. 2012/391227.

236 *UK GDA – Allocation of sensors and conditioning when 3 lines of defence are involved*. PEPS-F DC 148 Revision A. AREVA. October 2012. TRIM Ref. 2012/411783.

237 *UKEPR Basis of Substantiation for the Reliability Claims for the PACS Modules*. ECECC121662 Revision A. EDF. August 2012. TRIM Ref. 2012/336366.

238 *EPR UK Diversity implementation plan for PAC Modules*. ECESN120472 Revision A. EDF. July 2012. TRIM Ref. 2012/319795.

239 *Response to C&I Meeting Actions GI 15-I&C-2 and GI 16-I&C-4*. Letter EPR01413N. 24 October 2012. EDF and AREVA. October 2012. TRIM Ref. 2012/414441.

240 *BS IEC 61513:2011 Nuclear power plants - Instrumentation and control important to safety – general requirement for systems. International Electrotechnical Commission*. British Standard Institution (BSI) (IEC). 2011.

241 *Engineering and Projects Organisation EPR overall I&C design process*. PELA-F 12.1004 Revision B. AREVA. August 2012. TRIM Ref. 2012/310148.

242 *UK EPR Protection System - Overall Scope of Independent Confidence Building Measures*: ENSECC110173 Revision B. EDF. June 2012. TRIM Ref. 2012/261811.

Table 5

Relevant Safety Assessment Principles for Control & Instrumentation Considered During GDA Step 4[4]

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 and standards
ECS.2	Safety classification of structures, systems and components
ECS.3	Standards
ECS.4	Codes and standards
ECS.5	Use of experience, tests or analysis
EQU - Equipment qualification	
EQU.1	Qualification procedures
EDR - Design for reliability	
EDR.1	Failure to safety
EDR.2	Redundancy, diversity and segregation
EDR.3	Common cause failure
EDR.4	Single failure criterion
ERL - Reliability claims	
ERL.1	Form of claims
ERL.2	Measures to achieve reliability
ERL.3	Engineered safety features
ERL.4	Margins of conservatism
ECM – Commissioning	
ECM.1	Commissioning testing
EMT - Maintenance Inspection and Testing	
EMT.1	Identification of requirements
EMT.2	Frequency

[4] The assessment of the design agai nst the SAPs was completed in Step 4 (see paragraph 22). However , those SAPs relevant to closing out GDA Issues were considered during the GDA close-out phase.

Table 5

Relevant Safety Assessment Principles for Control & Instrumentation Considered During GDA Step 4[4]

SAP No.	Assessment Topic / SAP Title
EMT.3	Type-testing
EMT.4	Validity of equipment qualification
EMT.5	Procedures
EMT.6	Reliability claims
EMT.7	Functional testing
EAD - Aging and degradation	
EAD.1	Safe working life
EAD.2	Lifetime margins
EAD.3	Periodic measurement of material properties
EAD.5	Obsolescence
ELO – Layout	
ELO.1	Access
ELO.2	Unauthorised access
EHA - External and internal hazards	
EHA.10	Electromagnetic interference
ESS - Safety systems	
ESS.1	Requirement for safety systems
ESS.2	Determination of safety system requirements
ESS.3	Monitoring of plant safety
ESS.4	Adequacy of initiating variables
ESS.5	Plant interfaces
ESS.6	Adequacy of variables
ESS.7	Diversity in the detection of fault sequences
ESS.8	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.13	Confirmation of operating personnel
ESS.14	Prohibition of self-resetting of actions and alarms

Table 5

Relevant Safety Assessment Principles for Control & Instrumentation Considered During GDA Step 4[4]

SAP No.	Assessment Topic / SAP Title
ESS.15	Alteration of configuration, operational logic or associated data
ESS.16	No dependency on external sources of energy
ESS.17	Failure identification
ESS.18	Failure independence
ESS.19	Dedication to a single task
ESS.20	Avoidance of connections to other systems
ESS.21	Reliability
ESS.22	Avoidance of spurious operation
ESS.23	Allowance for unavailability of equipment
ESS.24	Minimum operational equipment requirements
ESS.26	Maintenance and testing
ESS.27	Computer based safety systems
ESR - Control and instrumentation of safety related systems	
ESR.1	Provision in control rooms and other locations
ESR.2	Performance requirements
ESR.3	Provision of controls
ESR.4	Minimum operational equipment
ESR.5	Standards for computer based equipment
ESR.6	Power supplies
ESR.7	Communications systems
ESR.8	Monitoring of radioactive substances
ESR.9	Response of control systems to normal plant disturbances
ESR.10	Demands on safety systems in the event of control system faults
EES - Essential services	
EES.1	Provision
EES.2	Sources external to the site
EES.3	Capacity, duration, availability and reliability
EES.4	Sharing with other plants
EES.5	Cross-connections to other services
EES.6	Alternative sources
EES.7	Protection devices

Table 5

Relevant Safety Assessment Principles for Control & Instrumentation Considered During GDA Step 4[4]

SAP No.	Assessment Topic / SAP Title
EES.8	Sources external to the site
EES.9	Loss of service
EHF - Human factors	
EHF.7	User interfaces
EHF.8	Personnel competence
ECV - Containment and ventilation	
ECV.6	Monitoring devices
ECV.7	Leakage monitoring
ERC - Reactor core	
ERC.2	Shutdown systems
DC – Decommissioning	
DC.1	Design and operation
DC.2	Decommissioning strategies

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-001	The Licensee shall ensure that where RCC-E does not explicitly reference the requirements of relevant IEC SIS standards, or standard revisions (as appropriate to the C&I SIS employed in the UK EPR™) these requirements are adequately addressed in the C&I SIS lifecycle covering design, procurement and implementation processes, etc. For further guidance see T14.TO1.01, T14.TO1.03, T14.TO2.01, T14.TO2.02, T14.TO2.03, T14.TO2.04, T14.TO2.05 and T14.TO2.06 in Annex 4.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-002	The Licensee shall demonstrate the compliance of the PS and associated platform with BS IEC 61513:2001, BS IEC 60880:2006 and BS IEC 60987:2007, and SAS / PAS and associated platform with BS IEC 61513:2001, BS IEC 62138:2004 and BS IEC 60987:2007. This demonstration should address platform and system requirements separately. The demonstration shall include the supporting evidence generated as the designs are completed. For further guidance see T20.A1.5.2 in Annex 9; T15.TO2.05, T15.TO2.06, T15.TO2.08, T15.TO2.09, T15.TO2.10, T15.TO2.11, T15.TO1.39, T15.TO2.43 and T15.TO2.44 in Annex 5; T16.TO1.01, T16.TO2.11, T16.TO2.28, T16.TO2.29 and T16.TO2.31 in Annex 6; GICI06.A2.TO2.07, GICI06.A2.TO2.08, GICI06.A2.TO2.09, GICI06.A2.TO2.12, GICI06.A2.TO2.13, GICI06.A2.TO2.15 and GICI06.A2.TO2.16 in Annex 16, and GICC02.TO2.01 to 03 in Annex 18.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-003	The Licensee shall demonstrate that adequate company-level processes, or UK EPR™ project-level processes are established for configuration management of the set of all structures, systems and components that comprise the UK EPR™ C&I architecture including all SIS, which should be addressed within an overall Quality Assurance Plan or equivalent, as required by BS IEC 61513:2001 clause 5.4.1. For further guidance see T14.TO1.03 in Annex 4.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-004	The Licensee shall: i) demonstrate that its CBSIS security management system aligns with appropriate standards such as ISO/IEC 27001 (Ref. 43); and ii) implement a CBSIS security assessment methodology that uses the UK government standard methodology as its foundation.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-005	The Licensee shall produce a comprehensive demonstration of the adequacy of Teleperm XS self checking and error handling. For further guidance see T15.TO2.33, T15.TO2.34 and T15.TO2.35 in Annex 5; and T17.TO2.05 in Annex 7.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-006	The Licensee shall justify all variations from the requirements of BS IEC 60880 (Ref.17) and BS IEC 60987 (Ref.18) with respect to the role of the independent assessor within the Teleperm XS development lifecycle, and implement compensating measures where necessary. For further guidance see T15.TO2.22 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-007	The Licensee shall identify / produce documentation which clearly specifies the Teleperm XS platform requirements. For further guidance see T15.TO2.13 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-008	The Licensee shall produce documentation which clearly identifies the traceability of requirements from the high level Teleperm XS specifications to the lower level design documents, and through to the platform test documents. For further guidance see T15.TO2.12, T15.TO2.14 and T15.TO2.15 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-009	The Licensee shall produce a comprehensive demonstration of fitness for purpose for the Teleperm XS platform which addresses, amongst others: • Mean Time Between Failure analysis; • adequacy of hardware lifecycle data, independent verification; • adequacy of type test reports; • compliance with BS IEC 60780:1998 "qualification"; • adequacy of Qualified Target Life; • justification of the application of AREVA's 'standard approach' to qualification; • adequacy of the TXS qualification process with respect to Pre-Ageing ; • justification that worst case timing scenarios have been used when determining processor utilisation of the TELEPERM XS platform software; and • justification of the adequacy of the TXS platform fault/change management process. For further guidance see T15.TO2.01, T15.TO2.17, T15.TO2.23, T15.TO2.24, T15.TO2.25, T15.TO2.26, T15.TO2.27, T15.TO2.28, T15.TO2.29, T15.TO2.30, T15.TO2.31, T15.TO2.32, T15.TO2.36 and T15.TO2.37 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-010	For SAP EDR.3 the evidence referenced by EDF and AREVA for PS reliability and availability is to be superseded by Failure Mode Effects Analysis calculations which were scheduled to be provided in December 2010. The Licensee shall update the CAE trail for EDR.3 and EDR.1 as appropriate, and produce the cited FMEA evidence and required justification. For further guidance see T15.TO2.50, T15.TO2.54 and T15.TO2.62 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-011	The Licensee shall produce a safety demonstration for the selection and use of Programmable Complex Electronic Components in the Teleperm XS platform, which form part of the Class 1 UK EPR™ Protection System, using appropriate standards and guidance. For further guidance see T14.TO1.02 in Annex 4; T15.TO1.2 and T15.TO1.3 in Annex 5; and T20.A1.5.5 in Annex 9.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-012	The Licensee shall produce a comprehensive safety demonstration addressing the adequacy of the SPPA-T2000 platform for Class 2 use covering hardware design, qualification and software design processes. For further guidance see T15.TO2.39, T15.TO2.40, T15.TO2.41, T15.TO2.42 and T15.TO2.44 in Annex 5; T17.TO2.06 in Annex 7; and T20.A2.3.4 in Annex 9.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-013	The Licensee shall produce adequate justification that the SPPA-T2000 Engineering System cannot cause unintended interference with the Class 2 SAS during plant operation. For further guidance see T15.TO2.61 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-014	The Licensee shall ensure that the software re-use argument presented addresses all Class 2 components of the SPPA-T2000 that contain dedicated devices with embedded software, or if no such software exists a positive statement saying so should be made. For further guidance see T15.TO2.60 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-015	The Licensee shall produce adequate justification that the issue raised by ASN concerning the adequacy of the quality system test records for the original development of the SPPA-T2000 platform does not compromise the claims made for this platform in the UK EPR™ design. For further guidance see T15.TO1.38 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-016	The Licensee shall produce adequate justification that relevant issues raised by other national regulators concerning the adequacy of SIS have been adequately addressed where relevant to the UK EPR™ design and do not compromise the claims made for the UK EPR™ design.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-017	The Licensee shall implement the smart devices qualification methodology defined under GDA Issue GI-UKEPR-CI-04 and ensure implementation evidence is available for review for all safety classes.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-018	The Licensee shall ensure there is an adequate safety case for in-core instrumentation sensors and other sensors used in SIS. For further guidance see T13.TO2.44 in Annex 3.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-019	The Licensee shall ensure the fail-safe principle (including the application of the appropriate response to C&I equipment failures) is implemented in the design of UK EPR™ C&I nuclear safety functions. For further guidance see T16.TO2.18 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-020	The Licensee shall demonstrate that the UK EPR™ C&I SIS comply with relevant IEC standards in their installation, commissioning and operational lifecycle phases. For further guidance see T16.TO2.28 and T16.TO2.30 in Annex 6.	Prior to power raise.
AF-UKEPR-CI-021	The Licensee shall demonstrate that the use of a different complier with the SIVAT tool compared to that used to generate the object code which will run on the PS does not compromise the integrity of the PS application software development lifecycle. For further guidance see T16.TO2.19.b in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-022	The Licensee shall demonstrate the adequacy of the Protection System application code testing process with respect to functional coverage. For further guidance see T16.TO2.19 item a) in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-023	The Licensee shall demonstrate the adequacy of conformance of the Protection System with EQU.1 (qualification procedures), EDR.2 (redundancy, diversity and segregation), EDR.3 (common cause failure), EMT.7 (functional testing), ESS.18 (failure independence), ESS.21 (reliability), and ESS.23 (allowance for unavailability). For further guidance see T15.TO2.52 in Annex 5; T16.TO2.01, T16.TO2.03, T16.TO2.04, T16.TO2.05, T16.TO2.06, T16.TO2.07 and T16.TO2.08 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-024	The Licensee shall produce evidence to demonstrate the adequacy of the design and implementation of the PS calculated trip functions. For further guidance see T16.TO2.33.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-025	The Licensee shall demonstrate that the differences of functional coverage across the PS trains do not give rise to any safety concerns (such as an inability to meet the reliability requirements or the single failure functional criterion requirements) when failures occur within a train, or any train is taken out of service for maintenance. For further guidance see T17.TO2.09 in Annex 7, T18.TO2.01 in Annex 8 and T20.A1.4.3 in Annex 9.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-026	The Licensee shall implement a series of statistical-based tests (i.e. as justified in response to GDA Issue GI-UKEPR-CI-02, see below) as one component of the ICBMs for the UK EPR™ Protection System.	Prior to power raise.
AF-UKEPR-CI-027	The Licensee shall produce a full set of UK EPR™ PS development records demonstrating compliance with the requirements of the development process (e.g. D-01.3: Master Test Plan, D-01.4: Protection System - System Requirements Specification) and method documents. Traceability of requirements and qualification of tools should also be addressed. For further guidance see T16.TO2.10, T16.TO2.12, T16.TO2.13, T16.TO2.14, T16.TO2.15, T16.TO2.16, T16.TO2.17 and T16.TO2.20 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-028	The Licensee shall demonstrate the adequacy of conformance of the SAS / PAS to EDR.1 (failure to safety), EDR.2 (redundancy, diversity and segregation), EDR.3 (Common cause failure), EQU.1 (qualification), EMT.7 (functional testing) and ESR.5 (standards for computer-based equipment). For further guidance see T16.TO2.22, T16.TO2.23, T16.TO2.24, T16.TO2.25, T16.TO2.26 and T16.TO2.27 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-029	The Licensee shall demonstrate that adequate arrangements are in place to ensure that the UK EPR™ Class 1 PACS meets relevant design standards, adequate defences against CCF are provided and correct prioritisation is provided. For further guidance see T17.TO2.08, T17.TO2.19 and T17.TO2.27 in Annex 7.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-030	The Licensee shall demonstrate that adequate arrangements are in place to ensure that the UK EPR™ Class 1 SICS meets relevant design standards. For further guidance see T16.TO2.32 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-031	Definition and assignment of functions to C&I SIS - The Licensee shall ensure that for the UK EPR™ there is a rigorous definition of the overall system architecture, the assignment of functions to SIS, interfaces and independence requirements. For further guidance see T17.TO1.02, T17.TO1.25, T17.TO2.03, T17.TO2.10, T17.TO2.17, T17.TO2.26 and T17.TO2.27 in Annex 7; and T18.TO2.03 and T18.TO2.07 in Annex 8.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-032	PCSR Update - The Licensee shall update the PCSR and supporting documentation to take account of the changes made to address **RI-UKEPR-002** and **RO-UKEPR-43**. For further guidance see T17.TO1.11, T17.TO1.14 and T17.TO1.25 in Annex 7; and T18.TO1.01 in Annex 8.	Prior to fuel load.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-033	The Licensee shall implement a rigorous programme of PS ICBMs covering: • Statistical and functional testing based on 50,000 tests of which 48,000 will be statistical (see also **AF-UKEPR-CI-026**), taking cognisance of any emerging research results. • Static analysis (using MALPAS) and concurrency analysis (using SPIN/Promela if demonstrated to be feasible or other means such as manual review). • Functional analysis (by reverse engineering) and integrity checking of the RTECONF module. • Source to Code Comparison (including completion of an As Low As Reasonably Practicable (ALARP) demonstration if it is considered not reasonably practicable to apply the SCC technique to the PS interface units). Also, to ensure the justification of PS core units' non-interference by the interface units is completed (i.e. as committed to in the response to TQ-EPR-1607, Ref. 86). For further guidance on development of a rigorous programme of PS ICBMs see Technical Observations GICI02.TO2.15 to GICI02.TO2.25 in Annex 12.	Prior to power raise.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-034	The Licensee shall: • Revise the SAPS conformance CAE trails (Ref. 91) to ensure, as appropriate, the claims and argumentation for each SAP and its guidance paragraphs are fully addressed (see also **AF-UKEPR-010**, **AF-UKEPR-023** and **AF-UKEPR-028**) in the CAE trails. • Include the additional claims, arguments and evidence generated during closure of the GDA Issues into the PCSR key claims (Ref. 89) and SAPS conformance CAE trails (Ref. 91). • Reference the evidence generated during C&I systems' development, installation and commissioning in the PCSR key claims and SAPS conformance CAE trails. For further guidance on the completion of the CAE trails see Technical Observations GICI03.TO2.01 and GICI03.TO2.02, in Annex 13 for PCSR key claims, and GICI03.TO2.03, GICI03.TO2.04 and GICI03.TO2.05 in Annex 13 and GICI06A9.TO2.17 in Annex 16 for SAP conformance.	Prior to power raise.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-035	The Licensee shall address the open points on the PCSR summarised below by updating the PCSR to: • include the justification of the adequacy of programmable complex electronic components; • include the UNICORN platform and NCSS justifications; and • address the inconsistencies in the status of the PICS and the interfaces between the Class 1 PS and other systems. Further guidance on open points to be addressed in the development of the PCSR is provided in PCSR review pro-forma 'PCSR Chapter Review for CI Rev 2', Ref. 106.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-036	The Licensee shall develop the SPPA-T2000 platform BSC and complete the safety case to: • Include a clear definition of the BSC scope and improvements to structure to clearly identify the impact of the S5 to S7 SPPA-T2000 platform version change. • Revise the BSC / safety case claims and arguments to correctly and fully address each SAP and its guidance paragraphs (see also **AF-UKEPR-CI-010**, **AF-UKEPR-CI-023** and **AF-UKEPR-CI-028**). • Include evidence generated during C&I system development, installation and commissioning including standards compliance, reliability and response time evidence to support the safety case claims and arguments (see also **AF-UKEPR-CI-002**, **AF-UKEPR-CI-020** and **AF-UKEPR-CI-029**). For further guidance on the completion of the BSC (including its extended scope and supporting documents) see Technical Observations GICI05.TO2.01 to GICI05.TO2.06 in Annex 15 and GICI06.A1.TO2.05 in Annex 16.	Prior to power raise.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-037	The Licensee shall: • Complete and update the diversity submission documents (i.e. Refs 138, 141 and 142) in line with the commitments made during the GDA closure phase (i.e. in Refs 141, 143, 147, and TQs TQ-EPR-1628 and TQ-EPR-1629 Ref. 86). For further guidance see Annex 16 Technical Observations GICI06.A1.TO2.06 and GICI06.A1.TO2.07. • Remove inconsistencies in the definition of the diversity criteria for the PS / SAS (Ref. 140), NCSS (Ref. 144), PACS (Ref. 145), and the sensors and conditioning modules (146). For example, the signal diversity levels 1 and 2 in one scheme are levels 2 and 3 in another. For further guidance see Annex 16 Technical Observation GICI06.A1.TO2.08. • Complete diversity analysis, in line with the methodology and criteria, for the three major C&I platforms (i.e. Teleperm XS, SPPA-T2000 (version S7) and UNICORN), the three major C&I systems built on those platforms (i.e. PS, SAS and NCSS) and other C&I systems built on the platforms if diversity claims are made in the safety case. For further guidance see Annex 16 Technical Observations GICI06.A1.TO2.04, GICI06.A1.TO2.07 and GICI06.A1.TO2.09, and Annex 11 Technical Observation GICI01.TO2.31. • Ensure the final systems using the Teleperm XS and SPPA-T2000 (version S7) platforms include the modifications proposed in Ref. 151. For the Teleperm XS platform replace the AMPRO firmware. For the SPPA-T2000 (version S7) replace the ASPC2 ASIC used for Profibus control. Also to implement the design constraint on SPPA-T2000 (version S7) to prevent the use of the AV42 module and the OLMAS ASIC. For further guidance see Annex 16 Technical Observation GICI06.A1.TO2.04.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-038	The Licensee shall complete the demonstrations of reliability and independence for inclusion in the safety case, in particular to: • Undertake the modifications to the PS and / or its periodic test arrangements to allow the reliability targets (e.g. for trip on low DNBR by increasing the frequency of periodic tests) to be met. • Complete the hardware reliability evaluations for the final designs of the SIS (i.e. the PS, SAS and NCSS). • Complete the justification of inter divisional and inter system independence and isolation of the SIS. For further guidance see in Annex 16 Technical Observations GICI06.A2.TO2.11, on the PS modifications and reliability, and GICI06.A2.TO2.06 and GICI06.A2.TO2.14 on independence and isolation.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-039	The Licensee shall fully define the PE and ICBMs for CBSIS. In particular, to: • Ensure that the generic guidance for CBSIS for concurrency analysis addresses adequacy of tools (e.g. such as the CodeSonar® tool used for Class 1, 1x10^{-3} pfd systems) and dynamic memory capacity. • Complete the definition of the SPPA-T2000 ICBMs including identification and justification of the key elements to be analysed by the manual review, approach to software integrity checking and dynamic testing. For further guidance on the completion of the demonstration of the adequacy of the PE and ICBMs for CBSIS see Technical Observations GICI06.A3.TO2.07 and GICI06.A3.TO2.08 in Annex 16.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-040	The Licensee shall: • Ensure the analysis of the non disturbance of the PS by signals coming from lower classified systems is updated to reflect any future design changes and the final PS design. • Confirm whether there is an EDG “start up in test” signal into the PS, and if so update the relevant non disturbance justification or produce a CMF for the change.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-041	The Licensee shall: • Confirm that the SAS functional and safety interlocks referred to in TQ-EPR-1532 response inhibit spurious commands from the PICS, and produce a justification of the adequacy of the interlocks. • Produce a comprehensive justification that Class 2 systems cannot be adversely affected by lower class systems. This justification to include the RCSL and systems based on SPPA-T2000 platform version S7 technology. • Produce an analysis for the final UK EPR™ SAS design that demonstrates that a "spurious but valid command sent to the SAS from the PICS" will affect at the very worst only one division and the consequences can be managed (e.g. by an update of Ref. 203). The analysis to include justification that the consequences of a spurious multi-division grouped command being received and enacted by the SAS are acceptable, for all such commands (as committed to in Ref. 203). For further guidance on independence of SAS from PICS see Technical Observations GICI06.A5.TO2.03 to GICI06.A5.TO2.06 in Annex 16.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-042	The Licensee shall: • Ensure that the development of the PSOT, including the QDS system (hardware and software), is carried out according to appropriate international standards, including BS IEC 61513, BS IEC 60880, and BS IEC 60987, that tools and COTS components are suitably qualified, that justification is produced, and documentation updated. • Ensure that indication is provided to operators of the status of all resets, permissives, and manual controls, or where this is not to be done, produce a justification as to why this is acceptable and is not reasonably practicable. • Once the design has been completed, fully document the Class 1 displays and controls to be provided for the UK EPR™, and produce full justification of adequacy, to include the functional coverage of controls and displays in the MCR and RSS for all operational states. For further guidance on Class 1 controls and displays see Technical Observations GICI06.A6.TO2.08 to GICI06.A6.TO2.018 in Annex 16.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-043	The Licensee shall complete the demonstration of the adequacy of the UK EPR™ end-to-end response times for those functions important to safety which use the Class 3 Terminal Bus and / or Plant Bus using SPPA-T2000 platform version S7 information. The Licensee to: • Perform a design analysis of the end-to-end response times using SPPA-T2000 platform S7 version information (i.e. updating the SPPA-T2000 platform S5 version analyses provided during GDA). • Undertake a programme of performance / response time tests on fully representative UK EPR™ equipment (including SPPA-T2000 platform version S7 components) that include consideration of avalanche conditions both generated by the plant and internal to the SPPA-T2000 platform S7 version equipment). • Ensure an accurate predictability model for SPPA-T2000 platform S7 version level 1 (AS620B and SAS network) response times is developed (drawing on the results of the design analyses and performance / response time tests) to inform the design decisions for the UK EPR™, in particular, in relation to the allocation of functions to processor modules and the need for point-to-point communications. For further guidance on the completion of the demonstration of the adequacy of the end-to-end response times see Technical Observations GICI06.A8.TO2.04 and GICI06.A8.TO2.06 in Annex 16.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-044	The Licensee shall: • Produce a comprehensive sensor and conditioning diversity implementation plan that identifies the main activities to be carried out during the SSP, including completion of the functional analysis of sensor and conditioning modules CCF (e.g. see PELA-F DC 3 (Ref. 233), diversity cases associated with conditioning modules involved in the mitigation of faults in support functions and the spent fuel pool). • Where signal diversity criteria Sgd=3 is identified and no diverse parameter is available, employ devices that use diverse measuring principles. • Produce a comprehensive substantiation of the reliability claims for sensors and conditioning modules using the methodology defined in PELA-F DC 7 (Ref. 235). For further guidance on what is needed to address this Assessment finding see Technical Observations GICI06.A9.TO2.19 and GICI06.A9.TO2.25 in Annex 16.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-045	The Licensee shall confirm the adequacy of the allocation of conditioning modules and sensors (i.e. one group to the PS and other to the SAS / NCSS) by completing sufficient detailed calculations (e.g. as referred to in PEPS-F DC 148, Ref. 236). For further guidance on what is needed to address this Assessment finding see Technical Observation GICI06.A9.TO2.24 in Annex 16.	Prior to nuclear island safety related concrete.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-046	The Licensee shall produce a comprehensive PACS module diversity implementation plan that identifies the main activities to be carried out during the SSP, including: completion of the PACS module diversity analysis (e.g. diversity cases associated with support functions (see Ref. 238), impact of SIS maintenance and potential for allocation on a functional basis). For further guidance on what is needed to address this Assessment Finding see Technical Observations GICI06.A9.TO2.16, GICI06.A9.TO2.20 and GICI06.A9.TO2.21 in Annex 16 and Fault Studies Assessment Report (Ref. 87).	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-047	The Licensee shall, for those actuators that are not driven by PACS modules and / or switchgear, perform an assessment to identify any embedded or associated C&I components such as positioners, variable speed drives, feedback devices etc. and provide a justification of their adequacy (e.g. in a similar way as for the PACS modules, by developing and implementing diversity criteria, implementation plans and component reliability substantiations).	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-048	The Licensee shall: - Update document PEPS-F DC 90 so that it clearly defines the requirements for design in respect of common cause failure during maintenance. - When C&I categorisation and classification is complete, update the documentation (e.g. ECEF091489) to record the final categorisations of functions and classifications of systems, identifying any categorisation shortfalls and providing full justification, as necessary. - Ensure that the requirements (e.g. PEPS-F DC 90 rev. C) in respect of diversity and defence-in-depth are followed during the detailed design of the UK EPR™, and where the requirements are not met, produce a justification. - Review the C&I design requirements documents (e.g. ECECC120414) to identify whether all relevant ONR C&I SAPs and their related guidance paragraphs are considered, updating these where relevant SAPs are not found, or not comprehensively met (i.e. including the related guidance paragraphs). - Review the document 'UK EPR I&C Architecture' ECECC100831 Rev B to identify discrepancies with other UK EPR™ documentation, and resolve these (e.g. Figure 2, shows outputs from the PS and NCSS passing through an SPPA T2000 PACS interface and FA3 references should be replaced by UK specific ones). For further guidance on ensuring the adequacy of the design principles and guidance influencing the provision of diversity and defence-in-depth, and allocation of functions to diverse systems see Technical Observations GICI06.A9.TO2.14, GICI06.A9.TO2.17, GICI06.A9.TO2.18, GICI06.A9.TO2.22 and GICI06.A9.TO2.23 in Annex 16.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-049	The Licensee shall update NEPS-F 557 to align this with the probabilistic claim limits for Class 2 and 3 computer based systems given within other safety documentation such as PEPS-F DC 90 and ECECC111134 (e.g. the Class 2 pfd claim limit should be $1x10^{-2}$). For further guidance see Technical Observation GICC01.A6.TO2.01 in Annex 17.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-050	The Licensee shall: • Document and justify the adequacy of the final NCSS design in the safety case (e.g. the approach to testing, fail safe capability and selection of single or dual chain architecture for manual functions, etc.). • Confirm the adequacy of the final NCSS design, in relation to reduction of plant risk, by including NCSS design details into the PSA. • Define how, once triggered, the action of an NCSS automatic function will be reset and confirm this meets the requirements of SAP ESS.14. • Assess the effect of power loss within the NCSS system on plant safety (e.g. power loss leading to a failure to actuate when required or send alarms to operators). • Define and justify the response times and reliabilities for all NCSS functions (including the energise to actuate AVACT module and consideration of the impact of maintenance on system reliability). • Review the quality control procedures and update these to ensure adequate coverage of standards and activities (e.g. including demonstration of conformance to the requirements of standards BS IEC 61513 and BS IEC 60987, regression testing of engineering and test tools following a version change, and independence of qualification teams). For further guidance on the completion of the NCSS safety case see Technical Observations GICI01.TO2.18 to GICI01.TO2.21 and GICI01.TO2.23 to GICI01.TO2.34 in Annex 11.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-051	The Licensee shall: • Complete the trial qualification of the Class 1 smart device, assess the effectiveness of the qualification, and update the smart device qualification documentation and processes where improvements are identified. • Address the omissions in the Class 2 smart device trial qualification, assess the effectiveness of the qualification, and update the qualification documentation and processes where improvements are identified. • Confirm that a change in the Emphasis version will not adversely affect the qualification of smart devices. • Ensure that all smart device features (e.g. such as clock synchronisation and removable data logging memory), that have the potential to adversely affect the operation of safety functions are identified and, as appropriate, included within the qualification. • Ensure that all smart devices are qualified in accordance with the updated procedures, see **AF-UKEPR-CI-017**. • Where smart devices contain software that has been developed to a lower standard than that required by the classification of the device, a justification should be provided for the adequacy of this software (e.g. as Pre-Developed Software using appropriate standards and guidance), and that this software will not have an adverse affect on the safety functions (to include potential to corrupt program and data memory areas, and hardware settings). For further guidance on smart device qualification see Technical Observations GICI04.TO2.03 to GICI04.TO2.08 in Annex 14.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business – Control and Instrumentation – UK EPR™

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-052	The Licensee shall ensure that fully developed safety cases are produced that address: • the C&I CMFs submitted during GDA; and • development of the safety cases outlined in the Basis of Safety Cases (BSCs) produced in response to the C&I GDA Issues (i.e. for the NCSS, PSOT and SPPA-T2000 version change).	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site

Note: It is the responsibility of the Licensees / Operators to have adequate arrangements to address the Assessment Findings. Future Licensees / Operators can adopt alternative means to those indicated in the findings which give an equivalent level of safety.

For Assessment Findings relevant to the operational phase of the reactor, the Licensees / Operators must adequately address the findings during the operational phase. For other Assessment Findings, it is the regulators' expectation that the findings are adequately addressed no later than the milestones indicated above.

Annex 2

GDA Issues – Control & Instrumentation – UK EPR™

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

DESIGN INFORMATION FOR NON-COMPUTERISED SAFETY SYSTEM REQUIRED

GI-UKEPR-CI-01 REVISION 2

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-01**	**GDA Issue Action Reference**	**GI-UKEPR-CI-01.A1**
GDA Issue	Absence of adequate C&I architecture. The proposal to address the issues raised in RI 02 includes provision of a hardware based backup system known as the NCSS. Detail of the NCSS design has not been made available within GDA. EDF and AREVA have provided a commitment that the NCSS will be implemented in diverse technology to the computer based protection systems. A Basis of Safety Case for the NCSS is required for GDA.		
GDA Issue Action	EDF and AREVA to provide a Basis of Safety Case (BSC) that includes substantiation of the design of the Class 2 Non-Computerised Safety System. An action plan for completion and supply of detailed evidence supporting the basis of safety case document should also be supplied. The BSC should consider: • The safety principles and standards (i.e. company, national and international) that EDF and AREVA has adopted for the NCSS. • The identification of arguments for assigning safety functions and performance requirements to the NCSS in compliance with these principles and standards. • The basis of the safety case should demonstrate how the safety principles and standards adopted have or will be complied with at each step of the development and deployment of the NCSS. • It should outline why the NCSS is considered to be fit for purpose and demonstrate how all of the safety principle, standards, functional and performance requirements will be satisfied. • It is expected that these demonstrations and examinations would identify the detailed evidence supporting the claims and arguments. • The BSC is also expected to identify any supporting analysis such as hazards analysis, FMEAs, reliability analysis, environmental qualification and link them to claims made and the demonstration of fitness for purpose of the systems. • It is expected that in undertaking this exercise compliance with ONR's SAPS would also be demonstrated with deviations justified. • The BSC should describe the system, breaking it down such that the major elements can be identified (such as input/output and logic cards). The BSC should include the demonstration of adequacy for each of these elements (including identification of revisions) as well as the NCSS as a whole. • The BSC should set down the production excellence arguments and identify the independent confidence building measures. • The BSC should describe the project QA arrangements, e.g. ISO 9001, this		

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

DESIGN INFORMATION FOR NON-COMPUTERISED SAFETY SYSTEM REQUIRED

GI-UKEPR-CI-01 REVISION 2

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		None	
GDA Issue Reference	**GI-UKEPR-CI-01**	**GDA Issue Action Reference**	**GI-UKEPR-CI-01.A1**
	should include a clear description of the interface to the NCSS supplier (and any other suppliers). The BSC would also be expected to outline the NCSS supplier QA arrangements. • The BSC should identify the pedigree of any COTS, pre-developed components as this might influence how they are justified for use. • The BSC should demonstrate that the management arrangements for COTS/pre-developed components has been and remains adequate. This demonstration should cover, amongst others, configuration management, collection of Operating Experience and any changes along with their cause and how the change was implemented (capturing the evolution of the QA regime and processes by which this has been done). • The BSC should address the process by which the individual components will be brought together and integrated as a system. It is anticipated this would be detailed in the BSC (or other documents referenced from the BSC) covering factory and commissioning testing as well as environmental qualification work that might be called upon to support system justification. For completeness, it should also address through life operating and maintenance, for example identifying the scope and frequency of any proof testing that is required. • Should elements of the implementation of the NCSS system make use of complex electronic devices e.g. FPGAs (but not microprocessors) then the basis of the safety case would be expected to demonstrate how the design and implementation of the NCSS complies with relevant EDF/Areva safety principles and standards. The basis of safety case should also identify how ND guidance, for example, that contained in ESS.21 which requires the safety demonstration to include measures such as independent third party assessment (para. 355) will be addressed. Given the programmable nature of such complex devices, the justification should draw on elements of ESS.27 and the special case procedure with an argument of excellence in production and independent confidence building in respect of the systems fitness for purpose. It is expected, as above, that the demonstration would identify the detailed evidence supporting the claims and arguments made. For further guidance see also T15.TO1.46 in Annex 5, T16.TO1.02 in Annex 6, T17.TO1.24 in Annex 7 and T20.A1.2.4 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

PROTECTION SYSTEM INDEPENDENT CONFIDENCE BUILDING MEASURES

GI-UKEPR-CI-02 REVISION 2

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-02**	**GDA Issue Action Reference**	**GI-UKEPR-CI-02.A1**
GDA Issue	The programme of Independent Confidence Building Measures (ICBMs) to support the safety case for the TXS Protection System to be fully defined and agreed.		
GDA Issue Action	The programme of Independent Confidence Building Measures to support the safety case for the TXS Protection System to be fully defined and agreed. The proposed elements that will constitute the ICBMs are: • Statistical testing (ST) EDF and AREVA have proposed 5000 tests on the TXS equipment with the potential for 50000 on a simulator to be investigated as a research activity. ONR expects the RP to more fully define the ST approach in terms of number of tests. The RP is required to submit its analysis of the number of tests that it considers is reasonably practicable to undertake having given full consideration to any time and programme constraints. It remains ONR's expectation that 50,000 tests will be performed. ONR considers that the plant transients are sufficiently defined to allow a reasonably accurate definition of the time to undertake the tests to be established. Undertaking this analysis will give good guidance to the site specific programmes sufficiently early in the process to ensure that adequate time can be given to the statistical testing process without causing delays to the plant going into operation. In addition the RP needs to demonstrate, by the provision of a monitorable programme, that all of the activities required to implement ST have been defined and can be delivered to a timescale which allows ST to commence following completion of Factory Acceptance Testing of the PS (i.e. the final validation activity before the equipment is shipped to site). It should be noted the ICBM activities should be undertaken on the final version of the software (i.e. following the end of the software production process – see ONR TAG 46). The activities required to undertake ST are defined in a report produced by CINIF (Ref. Further development of Dynamic Testing 2 – Phase 2 (NewDDT2-3 PP/40115457/MB – Guidelines on Statistical Testing for logic or Software Elements used in Nuclear Safety Related Systems.) • Static analysis The feasibility and full extent of the application of MALPAS analysis to the Protection System application code needs to be confirmed. To date the RP has reported that it has undertaken a feasibility study which indicates that the technique is viable but the RP has stated that further work is required to ensure the technique is scaleable and applicable to the full scope of the PS application code. • Compiler validation. With regard to compiler validation, ONR is aware that the RP is considering a number of options from a Sizewell B type Source to Code Comparison to running a compiler		

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

PROTECTION SYSTEM INDEPENDENT CONFIDENCE BUILDING MEASURES

GI-UKEPR-CI-02 REVISION 2

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		None	
GDA Issue Reference	**GI-UKEPR-CI-02**	**GDA Issue Action Reference**	**GI-UKEPR-CI-02.A1**
	validation test suite (along the lines of an approach developed by NPL). The ICBM approach (Scope, depth and rigour) for each of the above needs to be fully defined before ONR can come to a conclusion on the adequacy of the safety case for the Protection System. Currently there are too many elements that have not been fully defined and as a result further work will be required to confirm the adequacy of the proposed ICBMs, or alternative means agreed by the Regulator. For further guidance see also T16.TO2.09 in Annex 6 and T15.TO2.07, T15.TO2.18 and T15.TO2.19 in Annex 5.		

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

CLAIMS, ARGUMENTS, EVIDENCE TRAIL

GI-UKEPR-CI-03 REVISION 2

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		None	
GDA Issue Reference	**GI-UKEPR-CI-03**	**GDA Issue Action Reference**	**GI-UKEPR-CI-03.A1**
GDA Issue	The quality of the assessed Claims, Arguments and Evidence supporting documentation provided by EDF and AREVA requires revision and improvement.		
GDA Issue Action	The CAE trail documentation provided by EDF and AREVA requires revision and improvement. EDF and AREVA to revise and improve the CAE trail documentation. In particular to: • review the UK EPR™ PCSR C&I sections and ensure that a clear CAE trail is provided for all key claims; • identify the evidence and related argument which demonstrates satisfaction of each of the ONR C&I SAPs. For more guidance see: T13.TO1.01, T13.TO1.02, T13.TO1.03 (including all TOs referenced in the TO Table) and T13.TO2.01 to T13.TO2.43 in Annex 3; T16.TO2.27 in Annex 6; T17.TO2.26 in Annex 7; and T18.TO2.08 in Annex 8. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

SMART DEVICES

GI-UKEPR-CI-04 REVISION 1

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		Electrical Engineering	
GDA Issue Reference	**GI-UKEPR-CI-04**	**GDA Issue Action Reference**	**GI-UKEPR-CI-04.A1**
GDA Issue	EDF and AREVA have yet to define a methodology to be used to qualify Smart Devices for Nuclear Safety functions.		
GDA Issue Action	EDF and AREVA to define the methodology to be used to qualify smart devices used in the implementation of nuclear safety functions and produce examples of the implementation of the methodology for two smart devices, one from Class 1 and one from Class 2. EDF and AREVA have yet to define a methodology to be used to qualify smart devices for use in Nuclear Safety functions. A significant programme of work may be required to justify equipment that incorporates smart devices. This topic has been discussed with EDF and AREVA, and a position paper provided. However, further definition of the methodology and examples of its implementation are required. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT
GDA ISSUE
OBSOLESCENCE OF SPPA T2000 PLATFORM
GI-UKEPR-CI-05 REVISION 2

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-05**	**GDA Issue Action Reference**	**GI-UKEPR-CI-05.A1**
GDA Issue	The EDF and AREVA C&I architecture includes systems based upon SPPA T2000 (Siemens S5 based), but this platform is believed to be obsolete and will not be available for UK EPR.		
GDA Issue Action	The EDF and AREVA C&I architecture includes systems based upon SPPA T2000 (Siemens S5 based), but this platform is believed to be obsolete and will not be available for UK EPR™. The RP needs to define the platform that will be provided for the UK EPR™ and submit a Basis of Safety Case that fully addresses the change from the SPPA T2000 (Siemens S5 based) to the proposed system. A Basis of Safety Case in this context is expected, amongst others, to: • define the safety principles and standards (i.e. company, national and international) that are to be adopted for the replacement systems (i.e. incorporating the replacement platform); • justify how these safety principles and standards will be complied with at each step of the development and deployment of the replacement systems; • justify how functional and performance requirements will be satisfied; • demonstrate conformance with relevant ONR SAPs; • provide a full analysis of the impact of the replacement platform on the overall C&I design; and • provide precise details of the change and demonstrate that the systems (covering all new components, tools and methods, etc.) are fit for purpose. It is understood that the proposed system is likely to be based on the Siemens S7 product and that the main impact of the change is the use of a different processor board. This will have an impact on the current SPPA T2000 (Siemens S5 based) based safety demonstration which may affect, amongst others, ability to reuse application code already developed , tool qualification, test records and proven in use arguments etc. At first sight this may appear to be a site licensing issue but our reason for including it as a GDA Issue is because of the profound importance that the platform selection of the SAS and PAS has on the safety of the EPR. In particular the diversity of these systems with the TXS is fundamental and therefore our view that the selection criteria for a replacement platform technology should be reviewed as a part of the GDA process. For further guidance see also T15.TO1.45 in Annex 5 and T18.TO1.04 in Annex 8. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A1**
GDA Issue	In response to our assessment, EDF and AREVA have agreed architecture changes, categorisation changes and have committed to develop a programme of Independent Confidence Building Measures to support the EPR C&I safety case. The nine actions under this GDA issue are concerned with C&I architecture and related matters.		
GDA Issue Action	EDF and AREVA to provide a comprehensive justification of diversity and independence between NCSS/PS, NCSS/SAS-PAS and PS/SAS-PAS commensurate with the level of design for a pre-construction safety report. One of the C&I architectural changes introduced in response to RI02 was the addition of a Non-Computerised Safety System as a backup to the computer- based Safety Automation System/Process Automation System and the Protection System. The EDF and AREVA safety case claims diversity and independence between each of these systems, however, this claim has not been fully substantiated. The regulator expects that this detailed diversity analysis will draw on appropriate standards and guidance. It is also expected that this analysis will be rigorous and ensure all common components are identified together with argumentation as to why any such components identified do not have the potential to induce Common Cause Failure of the identified systems. Where final detailed design information is not available, but which is identified as having a potential impact on the diversity analysis, this should be noted and ONR will use the vehicle of an assessment finding to track the gathering of this evidence from a future licensee. For further guidance see also T16.TO2.21 in Annex 6, T18.TO1.03, T18.TO1.04 and T18.TO2.09 in Annex 8 and T20.A1.2.3 and T20.A1.3.4 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		**PSA**	
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A2**
GDA Issue Action	EDF and AREVA to provide a justification of the reliability figures used for each of the protection systems when claimed independently and in combination. The response should include consideration of systematic and hardware failures, and compliance with appropriate guidance and standards. The EDF and AREVA safety case makes a claim of 1x10 $^{-4}$ probability of failure on demand (pfd) for the Class 1 Protection System (PS), 1x10^{-2} pfd for the Safety Automation System (SAS) and 1x10 $^{-3}$ pfd for the Non-Computerised Safety System (NCSS). However, a justification for each of these figures needs to be provided, for example, drawing on appropriate international standards (covering random and systematic failures). In addition, for the claims to be used in a way which allows their multiplication, additional argumentation will be required (e.g. claims of independence and diversity which will need to be substantiated) – see GI-UKEPR-CI-06.A1. For further guidance see also T16.TO2.21 in Annex 6, and T20.A1.4.1 and T20.A1.4.2 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

<table>
<tr><td colspan="2"><b>Technical Area</b></td><td colspan="2"><b>CONTROL AND INSTRUMENTATION</b></td></tr>
<tr><td colspan="2"><b>Related Technical Areas</b></td><td colspan="2">None</td></tr>
<tr><td><b>GDA Issue Reference</b></td><td><b>GI-UKEPR-CI-06</b></td><td><b>GDA Issue Action Reference</b></td><td><b>GI-UKEPR-CI-06.A3</b></td></tr>
<tr><td><b>GDA Issue Action</b></td><td colspan="3">EDF and AREVA to provide a justification of the approach to be used to demonstrate the adequacy of computer based systems important to safety including identification of production excellence and independent confidence building activities.
SAP ESS.27 requires that where a safety system's reliability is significantly dependent upon the performance of computer software, the establishment of and compliance with appropriate standards and practices throughout the software development life-cycle should be made, commensurate with the level of reliability required, by a demonstration of 'production excellence' and 'confidence-building' measures.
Note that the Protection System's independent confidence building measures are to be addressed under GI-UKEPR-CI-02.
For further guidance see also T20.A1.4.1.a in Annex 9.
With agreement from the Regulator this action may be completed by alternative means.</td></tr>
</table>

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		None	
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A4**
GDA Issue Action	EDF and AREVA to provide a revised document NLN-F DC 193 'Protection System – System Description' to reflect the current design and to provide full justification for the design, including the justification of hardwired links to the PS. The assessed revision of NLN-F DC 193 does not reflect agreed architectural changes and does not provide justification for all the hardwired links from lower class systems to the Class 1 Protection System (noting that there may be detailed implementation issues which cannot be fully addressed under GDA). For further guidance see also T17.TO1.04 in Annex 7, T20.A2.2.1 and T20.A2.2.3 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		None	
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A5**
GDA Issue Action	EDF and AREVA to provide detailed substantiation of independence between Process Instrumentation and Control System (PICS) Class 3 system and the Safety Actuation System (SAS) Class 2 system. There are data highway based communications from the Class 3 to the Class 2 system and EDF and AREVA are required to provide detailed substantiation that failure of the lower class system cannot compromise operation of the higher class system. For further guidance see also T20.A2.3.2 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		None	
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A6**
GDA Issue Action	EDF and AREVA to provide detailed substantiation of the Class 1 control and display facilities to be provided in the MCR and RSS. A Basis of Safety Case for the Class 1 control and display system to be provided and also a justification in terms of the functional coverage of this system. In response to our assessment a number of C&I architectural changes were introduced to eliminate network communications from lower class systems to the Class 1 protection system, and one such change was the introduction of Class 1 control and display panels in the Main Control Room and the Remote Shutdown Station. EDF and AREVA has indicated that the arrangements will be enhanced by provision of a Qualified Display System (QDS). However, the proposed technical solution, and the scope of the displays/controls needs to be confirmed. For further guidance see also: T16.TO1.03 in Annex 6; T17.TO1.14, T17.TO1.15 and T17.TO2.16 in Annex 7; and T20.A3.6 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		None	
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A7**
GDA Issue Action	EDF and AREVA to justify why it is not reasonably practicable for the SICS controls to be in a functional state during normal operation. Normal control is through use of the PICS controls with a switch mechanism used to activate the SICS controls on detection of PICS failure. EDF and AREVA is to describe the arrangements used for this changeover including detection of PICS failure. The SICS displays remain active but the audible alarms are muted. The description to be provided by EDF and AREVA will include an argument as to why leaving the SICS controls inactive until needed following PICS failure is preferable to having them active. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		None	
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A8**
GDA Issue Action	EDF and AREVA to provide evidence, for those functions important to safety which use the Class 3 Terminal bus and/or Plant bus, that end-to-end response time requirements are achievable by design. EDF and AREVA have yet to provide adequate substantiation to confirm that performance is guaranteed by design for those functions which use the Class 3 Terminal bus and/or Plant bus with respect to the end-to-end response time. For further guidance see also T20.A5.4 and T20.A5.5 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	**PSA**		
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A9**
GDA Issue Action	EDF and AREVA to provide detailed substantiation for the probabilistic claims for any C&I components used by more than one line of protection e.g. sensors, smart devices, PIPS, PACS (response to include consideration of the potential for common mode failure as a result of the use of these components). A comprehensive analysis should be provided by EDF and AREVA to address the potential for Common Cause Failure due to the use of common components in different nominally diverse systems. Also to address the use of items used to provide inputs to more than one line of protection, such as PIPS, and items which combine outputs from nominally diverse/independent systems such as the PACS. For further guidance see also: T17.TO2.07, T17.TO2.08 and T17.TO2.28 in Annex 7; T18.TO1.02, T18.TO1.05 and T18.TO2.06 in Annex 8; T20.A1.3.1 and T20. A1.3.5 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 3

TSC Summary – C&I SAP Conformance and Adequacy of PCSR Review for UK EPR™[5]

Note this information has been imported from a TSC report (Ref. 28) and the formatting of the TSC report has been retained.

[5] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 3

Annex: TSC Task Summary – C&I SAP Conformance and Adequacy of PCSR Review for UK EPR

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of C&I SAP conformance and adequacy of PCSR for the UK EPR reactor design (TSC Task 11-13).

The Requesting Party (RP) for the UK EPR reactor design is EDF and AREVA.

The aim of the Task 13 review has been to gain confidence that EDF and AREVA have adequate evidence to demonstrate that the claims and arguments presented in the PCSR are adequately substantiated, and that the design of the C&I for the UK EPR can be shown to be in conformance with the HSE/ND C&I SAPs or that adequate justifications have been provided for any non-conformances.

The main areas of activity covered in the Task 13 review were:

- the EDF and AREVA demonstration of Conformance with the HSE/ND C&I Safety Assessment Principles (SAP), including the EDF and AREVA response to RO-UKEPR-62 Action A2;
- the adequacy of the Pre-Construction Safety Report (PCSR) with respect to a clear Claims/Arguments/Evidence (CAE) trail, including EDF and AREVA's response to RO-UKEPR-62 Action A1;
- the safety case for selected sample Sensors;
- PCSR updates received during the period of the Step 3 (TSC Tasks 1 to 3), and
- Technical Observations raised by Step 3 Task 1 to 3 and Step 4 Task 11 and 12 Technical Queries in relation to Claims and Arguments for conformance with HSE/ND C&I SAPs.

This Task 13 review follows on from the review of Claims and Argumentation in support of conformance with HSE/ND C&I SAPs carried out in preliminary Step 3 activities (TSC Tasks 1 to 3). In the absence of a clearly documented demonstration of SAP conformance during Step 3, the TSC reviewed the June 2008 version of the UK EPR PCSR in an attempt to identify Claims and Arguments relating to a demonstration of conformance with the HSE/ND C&I SAPs and to identify links to supporting evidence for review during Step 4. During Steps 3 Task 1 to 3 the Claims/Argumentation and identification of supporting evidence review was concluded for 63 First and Second Tier SAPs (identified by HSE/ND for Step 3 review) of the 84 HSE/ND C&I SAPs

The Task 11 and 12 review activity has covered the Claims and Arguments for the remaining 21 Third Tier SAPs not previously addressed in Step 3 and the Task 13 activity covered the sampled review of evidence identified by EDF and AREVA that supports the Claims and Arguments in relation to conformance with all 84 HSE/ND C&I SAPs. EDF and AREVA presented CAE documentation to support a demonstration of conformance to HSE/ND C&I SAPs during Step 4.

The scope of the evidence that is specific to UK EPR is defined by EDF and AREVA in *"UK EPR CONTROL AND INSTRUMENTATION (C&I) – SCOPE OF GDA"* (letter ND(NII)EPR00686N). The review of the evidence in support of the RP's Claims-Argument-Evidence information (CAE Trail) and the review of Sensors are consistent with this scoping letter.

Annex 3

A total of 47 technical observations resulting from the review have been raised. These technical observations (TO) have been designated TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher – 3 of these have been designated TO1 and 44 have been designated TO2.

SAP Conformance and Adequacy of PCSR

During GDA Step 2, HSE/ND raised a number of Observations against the EDF and AREVA 'Claims' made in document *'UKEPR-0005-001 Issue 00 'COMPARISON OF EPR DESIGN WITH HSE/NII* SAPs'. The adequacy of the Claims-Argument-Evidence to support the EDF and AREVA demonstration of conformance with HSE/ND C&I SAPs is addressed by Step 3 Tasks 1-3 and Step 4 Tasks 11-13. The technical aspects of the Observations raised by HSE/ND during Step 2 are being addressed by the appropriate TSC Step 4 Tasks and the status of these Observations is reported in the respective TSC Step 4 Task reports.

The reviews of Claims, Arguments and identification of Evidence carried out during TSC Step 3 Tasks 1 - 3 and Step 4 Task 11 and 12 revealed areas for improvement (AFI) in the demonstration of SAP conformance presented by EDF and AREVA. During the conduct of the Step 3 Tasks 1-3 reviews the AFI were raised as technical queries (TQ) and were included as 'SAP Assessment' related Step 3 observations in the HSE/ND GDA Step 3 report. During the conduct of the Step 4 Task 11 and 12 reviews the AFI were raised as a single technical query (TQ). These have either been cleared (i.e. transferred to other tasks) or resolved (no further action required).

The lack of a clear CAE Trail within the PCSR to demonstrate conformance to HSE/ND C&I SAPs resulted in a Regulatory Observation (RO-UKEPR-62) being raised with EDF and AREVA. RO-UKEPR-62 has two actions:

RO-UKEPR-62 A.1 - *The Requesting Party is required to review and revise the UK EPR PCSR C&I sections so that a clear claims-argument evidence trail exists within the document for all claims.*

The initial EDF and AREVA response to this action, '*RO-UK EPR -62 – ACTION A1 PCSR I&C Claims, Arguments and Evidence (CAE) Report on the CAE Approach,'* was received under letter ND(NII)EPR618N dated 27 October 2010. Review comments on this CAE Approach were provided via a technical query issued by the HSE/ND (TQ-EPR-1364). Although the general structure of the approach was generally acceptable, the main conclusions were that it effectively replicated the SAP based CAE Trail in the EDF and AREVA document PELL-F DC 9 (see RO-UKEPR-62 action A2 below) and neither the derivation of High Level Claims and Key Claims nor their location within the PCSR was clearly identified. It was not clear how this initial part response to RO-UKEPR-62 A.1 demonstrated that '*a clear claims argument evidence trail exists within the document (PCSR)*' as required by RO-UKEPR-62 A1.

The second EDF and AREVA response '*RO-UK EPR -62 – ACTION A1 PCSR I&C Claims, Arguments and Evidence (CAE) Interim Report*' received under cover of letter EPR00707N dated 17 December 2010 took cognisance of TQ-EPR-1364. However, there remain a number of similarities to the PELL-F DC 9 CAE Trail and there is no clearly defined link to the UK EPR C&I Requirements Specification, or other applicable source, for the derivation of Claims made against the C&I design. Also, the wording of many of the Sub-Claims appears to be taken directly from the HSE/ND SAPs whereas these Claims (High Level, Key and Sub Claims) should be generated by the RP independent of the SAPs. A Step 4 technical observation (TO) (T13.TO1.01) has been raised to address these AFI.

Annex 3

RO-UKEPR-62 A.2 - *The Requesting Party is required to identify the evidence and related argument which demonstrates satisfaction of each of the HSE C&I SAPs.*

Following review of the initial EDF and AREVA response to RO-UKEPR-62 A.2 received under cover of letter ND(NII)00360R dated 15 April 2010, EDF and AREVA provided a more detailed and focused SAP conformance document (PELL-F DC 9) that was used as the CAE Trail against which the sampled review of evidence was undertaken. A key aim of this review has been to gain confidence that an adequate level of conformance against the HSE/ND C&I SAPs is demonstrated through the EDF and AREVA CAE Trail.

The 84 SAPs intended to be reviewed by Task 13 were divided into 4 Phases to prioritise the review process. Specific SAPs were apportioned to a number of other TSC Step 4 Tasks for detailed sampled evidence review in the context of these Tasks. The CAE Trail documents were delivered by EDF and AREVA in three stages to address Phase1, Phase 2, and then Phases 3 & 4 SAPs.

An initial review has been undertaken of the CAE Trails for all 84 Phase 1, 2, 3 and 4 C&I SAPs to determine the level of adequacy based on the coverage of SAP requirements, adequacy of argument, relation to any areas for improvement identified in earlier reviews, and appropriateness of the evidence identified by EDF and AREVA.

From this initial review of these 84 SAPs, 16 have been declared Out of Scope of GDA or not relevant to C&I by EDF and AREVA. For the remaining 68 in scope SAPs, this initial high level review of the CAE Trails indicates that 38 of the CAE Trails have significant areas for improvement. However, most CAE Trails have a number of areas for improvement and a Step 4 technical observation (T13.TO1.02) has been raised by TSC Task 13 to address these. T13.TO1.02 is supported by 43 further Step 4 Task 13 technical observations (T13.TO2.01 to T13.TO2.43).

Due to the timing of issue of the CAE Trail documents by EDF and AREVA, it was only possible to complete a sampled evidence review of the twenty four Phase 1 and two Phase 2 SAPs within the timeframe of the GDA Step 4 review. The sampled review of evidence against the CAE Trails for these SAPs concluded that EDF and AREVA has demonstrated a ‘broadly acceptable’ level of SAP conformance for 6 SAPs; these included 4 Phase 1 and the 2 Phase 2 SAPs. However, there remain some areas for improvement associated with these 6 SAPs that need to be addressed. It was also concluded that EDF and AREVA did not demonstrate an ‘acceptable’ level of SAP conformance for 19 SAPs. One SAP (ESR.7 – Communications Systems) was declared Out of Scope of GDA by EDF and AREVA. The SAPs sampled evidence reviews have identified areas for improvement and a technical observation (TO) (T13.TO1.03) has been raised by TSC Task 13 to address these. T13.TO1.03 is supported by 92 technical observations raised by TSC Step 4 Tasks 14-18 during the sample review of evidence against the CAE Trails. The specific context of the supporting TOs is presented in a matrix *‘NII GDA Technical Review – C&I - Step 4 Tasks UKEPR CAE Trail & Evidence Review Matrix, 37194/64262V Issue 1.0’*.

Sampled supporting evidence against the CAE Trails was reviewed for the following SAPs:

Phase 1: ECS.1, ECS.2, ECS.3, EQU.1, EDR.1, EDR.2, EDR.3, EDR.4, ERL.3, EMT.7, ESS.1, ESS.2, ESS.3, ESS.7, ESS.8, ESS.18, ESS.21, ESS.23, ESS.27, ESR.1, ESR.3, ESR.5, ESR.7, ERC.2.

Phase 2: EKP.3 and ESS.15.

Annex 3

Sensor Review

A review of Sensors (excluding Smart sensors that use microprocessors) used within the UK EPR C&I design was undertaken. This covered In-core, Ex-core and Process Instrumentation sensors/detectors. Detailed design or manufacturing of process sensors is out of scope for GDA. The GDA Scope for Process Sensors is set out in letters ND(NII)EPR00376N and ND(NII)EPR00686N and is limited to examples of instrumentation requirement specifications for the UKEPR and examples of qualification reports or qualification programmes related to the Flamanville 3 (FA3) project, to be provided by EDF and AREVA. These 'examples' were further requested by Technical Query (TQ) TQ-EPR-1283 but were not received in the timescale of the review.

The review concentrated (as agreed with HSE/ND) on two In-Core Instrumentation systems; the Self Powered Neutron Detectors (SPND) and the Core Outlet Thermocouple (COT) system. This decision was driven by the availability of specification information and importance of these two systems to reactor protection. A review of the SPND System Specification and the In-core Reactor Instrumentation System (RIS) System Design Manual (SDM) was conducted against third tier standard IEC 61468:2000 '*Nuclear Power Plants – In-core instrumentation – Characteristics and test methods of self-powered neutron detectors (SPND)*'. This review has shown that some design requirements specified in IEC 61468:2000 have been addressed in the System Specification documents and RIS SDM. The latter documents have been reviewed but no clear supporting evidence was identified within them to demonstrate conformance with many areas of IEC 61468:2000. A TO (T13.TO2.44) has been raised to address these areas for improvement.

A similar review of the COT System Specification and the RIS SDM was conducted against third tier standard IEC 60737:2010 '*Nuclear Power Plants - Instrumentation Important to Safety - Temperature Sensors (in-core and primary coolant) - Characteristics and test methods*'. Again, this review has shown that some design requirements specified in IEC 60737:2010 have been addressed in the System Specification documents and RIS SDM reviewed but no clear supporting evidence was identified within these documents to demonstrate conformance with many areas of IEC 60737:2010. In both cases, further detailed evidence is needed as the specific design and procurement progresses. A TO (T13.TO2.44) has been raised to address these areas for improvement.

A technical query (TQ) (TQ-EPR-1283) was raised by HSE/ND requesting information on IEC standards used or required to be used in relation to sensors (In-core, Ex-core and Process) and demonstration of compliance with them; no response was provided within the timescale for this review. Additionally, evidence of Sensor Qualification for normal and emergency operating conditions was requested but was not provided within the timescale of the review. A TO (T13.TO2.44) has been raised to address these areas for improvement.

PCSR Update Impact Review

The April 2008 issue 1 of the UK EPR PCSR, which was used during Step 3 task 1-3 activity, was updated on two occasions; June 2009 and November 2009. After each update a review was conducted of the C&I sections to determine the impact of the update on the outcome of preliminary activities. The conclusions of these reviews are presented below:

Annex 3

The review of the June 2009 Issue 2 of the PCSR concluded that it has not introduced significant changes to the C&I architecture, nor significant improvements to the safety argumentation presented in the PCSR, compared to the April 2008 Issue 1. In particular, major observations remained over:

- the reliability claims for the Teleperm XS and SPPA-T2000 platforms,
- the platform diversity claims and reliance on two computer based platforms only;
- inputs into the Class 1 system from non-Class 1 sources,
- absence of common cause failure analysis,
- absence of architectural requirements,
- absence of safety group definitions, and
- absence of application of single failure criterion to safety group members.

The Issue 2 June 2009 PCSR had no discernable impact on the preliminary activities conducted under GDA Step 3 TSC Tasks 1 to 3, Task 7 and Task 8.

The review of the November 2009 Issue 3 of the PCSR concluded that the C&I sub-chapters and Appendices were sufficiently similar to those in the June 2009 issue to be considered to be identical. As such, the November 2009 issue had no impact on any GDA Step 3 review work by the TSC Tasks previously undertaken.

Technical Observations

During the conduct of the Step 3 Tasks 1-3 reviews of the Claims and Arguments and identification of evidence the AFI were raised as technical queries (TQ) and were included as 'SAP Assessment' related Step 3 observations in the HSE/ND GDA Step 3 report. During the conduct of the Step 4 Task 11 and 12 reviews the AFI were raised as a single technical query (TQ). These have either been cleared (i.e. transferred to other tasks) or resolved (no further action required). There are no outstanding Step 3 Task 1-3 or Step 4 Tasks 11 and 12 TQs or TOs.

A review of RO-UKEPR-62 A.1 and A.2 responses and In-Core Instrumentation sensors has been performed by Task 13. A total of 47 technical observations resulting from this review have been raised by Task 13; 3 of these observations have been designated as TO1 (T13.TO1.01 to T13.TO1.03). However, 43 of these technical observations, designate TO2 (T13.TO2.01 to T13.TO2.43), have been raised by Task 13 that support the TO raised by Task 13 (T13.TO1.02) against the CAE Trail presented as the basis of the EDF and AREVA demonstration of conformance with the HSE/ND C&I SAPs (i.e. response to RO-UKEPR-62 A.2). Additionally, 92 technical observations have been raised by other TSC Step 4 Tasks 14 to 18 that support the TO raised by Task 13 (T13.TO1.03) against the sampled review of evidence from the CAE Trails that the RP claims support SAP conformance. These other Step 4 TSC Task observations are reported in the applicable Step 4 TSC Task reports. One observation has been designated as TO2 (T13.TO2.44) against Sensors (In-Core, Ex-Core and Process).

Technical Observations designated TO1:

The three TO1 technical observations relating to RO-UKEPR-62 are as follows:

Annex 3

T13.TO1.01 – Although the initial part responses to RO-UKEPR-62 A.1; *'RO-UK EPR -62 – ACTION A1 PCSR I&C Claims, Arguments and Evidence (CAE) Report on the CAE Approach,'* received under letter ND(NII)EPR618N dated 27 October 2010 and '*RO-UK EPR -62 – ACTION A1 PCSR I&C Claims, Arguments and Evidence (CAE) Interim Report*' received under cover of letter EPR00707N dated 17 December 2010, demonstrate a sound approach methodology, the designer or future operator/licensee is requested to address the following in further developing this methodology and its output to ensure that a clear claims-argument evidence trail exists within the document for all claims:

a. provide a clear explanation or demonstration of how High Level and Key Claims are derived from appropriate sources, such as C&I Design Requirements Specification, Criteria or Principles, or other appropriate sources.

b. clearly identify the location of the Claims and Arguments within the PCSR, and identification of appropriate supporting Evidence.

c. The wording of the Claims, particularly the Sub-Claims should be derived independently from the SAPs and relate to the designer or future operator/licensee's key claims such as satisfaction of safety principles/criteria.

T13.TO1.02 – Although the C&I SAP CAE Trail in document PELL-F DC 9 has developed as an acceptable methodology for the demonstration of conformance to the HSE/ND C&I SAPs, there are still significant areas for improvement (AFI) in the presented Argument and identified Evidence for a large number of SAPs. The AFI relating to the CAE Trails for HSE/ND C&I SAPs are addressed in 43 Technical Observations (TO) (T13.TO2.01 to T13.TO2.43). The designer or future operator/licensee is requested to take all AFI in the 43 supporting TOs into account in further development of a robust demonstration of conformance with HSE/ND C&I SAPs.

T13.TO1.03 – Following sampled evidence review against the CAE Trails, TSC Step 4 Tasks 14 to 18 identified areas for improvement (AFI) and raised 89 TOs, as listed in the Table below that are reported in detail in the respective TSC Task reports. The designer or future operator/licensee is requested to take all AFI in these TOs raised by TSC Tasks 14 to 18 into account in further development of a robust demonstration of conformance with HSE/ND C&I SAPs.

SAP	Title	Task 14	Task 15	Task 16	Task 17	Task 18	Task 20
ECS.1	Safety categorisation and standards.				T17.TO1.01.a T17.TO1.01.b		
ECS.2	Safety classification of structures, systems and components.				T17.TO1.01a T17.TO1.01.b T17.TO1.02a T17.TO1.02.b T17.TO1.02.c T17.TO1.04 T17.TO2.03		T20.A2.3.2
ECS.3	Standards.	T14.TO1.01					

Annex 3

SAP	Title	Task 14	Task 15	Task 16	Task 17	Task 18	Task 20
		T14.T01.02 T14.T02.01					
EQU.1	Qualification procedures.	T14.T02.05	T15.T02.28 T15.T02.29 T15.T02.30 T15.T02.31 T15.T02.32 T15.T02.41	T16.T02.01 T16.T02.25			
EDR.1	Failure to safety.		T15.T02.49 T15.T02.50 T15.T02.62	T16.T02.22	T17.T01.04 T17.T02.05 T17.T02.06		T20.A2.2.1
EDR.2	Redundancy, diversity and segregation.		T15.T01.55	T16.T02.03 T16.T02.23	T17.T02.08	T18.T02.01 T18.T02.03 T18.T02.07	T20.A1.2.4 T20.A1.3.1 T20.A1.3.2 T20.A1.3.3 T20.A1.3.4 T20.A1.4.1 T20.A2.3.4
EDR.3	Common cause failure.		T15.T02.51 T15.T02.54 T15.T02.57 T15.T02.58	T16.T02.04 T16.T02.24	T17.T01.01.b	T18.T01.02	
EDR.4	Single failure criterion.				T17.T02.08 T17.T02.09a T17.T02.09b		T20.A1.3.1
ERL.3	Engineered safety features.				T17.T02.10		
EMT.7	Functional testing.			T16.T02.05 T16.T02.26			
ESS.1	Requirement for safety systems.				T17.01.02a		
ESS.2	Determination of safety system requirements.						
ESS.3	Monitoring of plant safety.				T17.T01.01a T17.T01.02a T17.T01.14 T17.T01.15		

Annex 3

SAP	Title	Task 14	Task 15	Task 16	Task 17	Task 18	Task 20
					T17.T02.16		
ESS.7	Diversity in the detection of fault sequences.				T17.T01.02a T17.T02.17		
ESS.8	Automatic initiation.						
ESS.18	Failure independence.			T16.T02.06	T17.T01.04	T18.T02.01 T18.T02.07	T20.A1.3.1 T20.A2.3.2
ESS.21	Reliability.	T14.T01.02		T16.T02.18 T16.T02.07	T17.T01.04 T17.T02.05 T17.T02.06 T17.T02.19		
ESS.23	Allowance for unavailability of equipment.		T15.T02.52	T16.T02.08	T17.T02.20		
ESS.27	Computer based safety systems.	T14.T02.06	T15.T01.18 T15.T01.38 T15.T02.05 T15.T02.53 T15.T02.59 T15.T02.60	T16.T01.01 T16.T02.09			
ESR.1	Provision in control rooms and other locations.				T17.T01.11 T17.T01.14 T17.T01.15		
ESR.3	Provision of controls.		T15.T02.62		T17.T01.01a T17.T01.14 T17.T02.21		T20.A4.6.2
ESR.5	Standards for computer based equipment.	T14.T01.02 T14.T02.02 T14.T02.03 T14.T02.04	T15.T01.46 T15.T02.60	T16.T02.27 T16.T02.28 T16.T02.29 T16.T02.30 T16.T02.31			
ESR.7	Communications systems.				T17.T02.22		
ERC.2	Shutdown systems.					T18.T02.03 T18.T02.06	

Annex 3

SAP	Title	Task 14	Task 15	Task 16	Task 17	Task 18	Task 20
EKP.3	Defence in depth.				T17.TO1.01.a		
ESS.15	Alteration of configuration, operational logic or associated data.		T15.TO2.61				

Technical Observation designated TO2:

T13.TO2.01 - From the review of the CAE Trail for ECS.3 the following area for improvement is raised:

- There is reference to System Description reports but no indication of specific document identification. Also, the third point against guidance paragraph 159 states that *'Evidence will be provided that standards.....'* with no indication as to what form that evidence will take. The designer or future operator/licensee is requested to ensure that appropriate specific document references are included in the CAE Trails.

T13.TO2.02 - From the review of the CAE Trail for EDR.2 the following areas for improvement are raised:

- An argument is put forward for Redundancy in the PICS with no supporting evidence. The designer or future operator/licensee is requested to ensure that appropriate specific document references to support the argument for redundancy in the PICS are included in the CAE Trails.

- There is reference to Reliability Analyses for the SAS & PAS, but not for the F1A PS. The designer or future operator/licensee is requested to ensure that reliability analyses are identified for the PS and included in the CAE Trail.

T13.TO2.03 - From the review of the CAE Trail for EDR.4 the following area for improvement is raised:

- The response to TQ-EPR-315 quotes the PSA as modelling assumed single failures, yet the PSA (NEPS-F DC 355 Rev B) is not cited as evidence to this SAP. The designer or future operator/licensee is requested to ensure that the appropriateness of NEPS-F DC 355 to support this SAP is reassessed and included in the CAE Trail if relevant.

T13.TO2.04 - From the review of the CAE Trail for ERL.3 the following areas for improvement are raised:

- The evidence pointed to is all PCSR Sub-chapters, predominantly Sub-chapters 18.1 and 14.7; the latter being the Fault Schedule. A new Fault Schedule (PEPR-F DC 4 B) has been provided and commented on by HSE/ND but is not included here. The designer or future operator/licensee is requested to ensure that the correct reference to the UKEPR Fault Schedule is used in PELL-F DC 9.

- A reference to PCSR Chapter 18.1 Section 3.1.3.1 is *ECEF021855 Revision B1 - ENG 2.21 Procedure: Degree of automation for plant systems*, but this is not listed as evidence. The

Annex 3

designer or future operator/licensee is requested to ensure that where Sections of the PCSR Sub-chapters are quoted in the CAE Trail and they have specific references linked to them, these references are included in the CAE Trail.

- The evidence to support guidance paragraph 180 is 'to be provided', but it has not been stated what is to be provided. The designer or future operator/licensee is requested to ensure that appropriate specific document references are included in the CAE Trails.

T13.TO2.05 - From the review of the CAE Trail for EMT.7 the following areas for improvement are raised:

- The argument against paragraph 192 states '*More specific evidence for each F1 system: (PS, PACS, SICS and SAS) is presented* below'. However, no specific evidence is identified to support guidance paragraph 192 requirements except for the Protection System. The designer or future operator/licensee is requested to ensure that appropriate specific evidence is identified and included in the CAE Trail.

- The argument against guidance paragraph 193 states that two examples are provided yet there appears to be only one. The designer or future operator/licensee is requested to ensure that the argument against paragraph 193 is revised to include the correct number of examples.

T13.TO2.06 - From the review of the CAE Trail for ESS.1 the following areas for improvement are raised:

- The evidence to demonstrate that safety systems are provided to achieve the requirements of the SAP is the Fault Schedule provided in PCSR Chapter 14.7 introduced in the Nov 09 issue 3 of the PCSR. This has since been superseded with the issue of a new Fault Schedule (PEPR-F DC 4 B) that has not been referenced here. The designer or future operator/licensee is requested to ensure that the correct reference to the UKEPR Fault Schedule is used in PELL-F DC 9.

- The argument and evidence to support the first half of guidance paragraph 336 is quoted as 'to be provided' with no indication of what. The designer or future operator/licensee is requested to ensure that appropriate specific evidence is identified and included in the CAE Trail.

T13.TO2.07 - From the review of the CAE Trail for ESS.2 the following area for improvement is raised:

- Section 2.4 of ECECC080669 B is cited as evidence for Defence in Depth Assumptions and Requirements for I&C, but this is a FA3 document. This document does not address the changes to the C&I architecture for UK EPR. A more appropriate (or additional) evidence document for the UK EPR is ECECC100832 A Section 2.1.2 that contains the same Defence-in-Depth information. The designer or future operator/licensee is requested to ensure that appropriate specific UKEPR relevant evidence is identified and included in the CAE Trail.

T13.TO2.08 - From the review of the CAE Trail for ESS.3 the following area for improvement is raised:

Annex 3

- PCSR Sub-chapters 7.2 (Section 1.3.3), 7.3 (Section 3) and 18.1 (Section 5.1) are cited as evidence. However, applicable evidence documents that are references from the identified PCSR chapters include:

  - ECECC060019 Revision A. EDF. December 2006. [Main Control Room (KSC [MCR]) System Specification].

  - ECECC070760 B. EDF. December 2008. [System Design Description Main Control Room (KSC [MCR]), Part 5: Control and Instrumentation System (KSC [MCR]) EPR FA3 (Stage 2)].

  - ECECC040729 Revision A. EDF. September 2004 [Process Information and Control System (KIC [PICS]) System Specification.]

  - ECECC080097 Revision B. EDF. December 2008. Process Information and Control System (KIC [PICS]) Part 5: Control and Instrumentation System EPR FA3 (Stage 2).

  The designer or future operator/licensee is requested to ensure that where Sections of the PCSR Sub-chapters are quoted in the CAE Trail and they have specific references linked to them, these references are included in the CAE Trail.

T13.T02.09 - From the review of the CAE Trail for ESS.7 the following areas for improvement are raised:

- The argument states that diversity in detection of fault sequences is covered in PCSR Chapter 7.3; however, the evidence quoted is the Fault Schedule in Chapter 14.7 that has now been replaced with PEPR-F DC 4 B. The designer or future operator/licensee is requested to ensure that the correct reference to the UKEPR Fault Schedule is used in PELL-F DC 9.

- There is no technical evidence presented to support the PCSR on how diversity in detection of fault sequences is implemented. The designer or future operator/licensee is requested to ensure that appropriate specific evidence that demonstrates the implementation of diversity in detection of fault sequences is identified and included in the CAE Trail.

- On diversity in safety system action initiation, the argument and evidence appear to concentrate on Reactor Trip only. The designer or future operator/licensee is requested to ensure that the CAE Trail is reviewed and revised to include diversity in the initiation of all safety system actions.

- The argument quotes PCSR Sub-chapter 7.3. Evidence documents that are references from PCSR Chapter 7.3 but not included in the CAE Trail are:

  - NLE-F DC 38 Rev F - Protection System detailed specification file

  - NLN-F DC 89 A - Protection System - Functional Diagrams.

  - NLE-F DC 59 Revision C. - System Design Manual - Reactor Protection System (RPR), Part 2 – System operation.

Annex 3

The designer or future operator/licensee is requested to ensure that where Sections of the PCSR Sub-chapters are quoted in the CAE Trail and they have specific references linked to them, these references are included in the CAE Trail.

T13.TO2.10 - From the review of the CAE Trail for ESS.8 the following areas for improvement are raised:

- The evidence for automatic initiation by the safety systems is given as the Fault Schedule (in the form of PCSR Ch 14.7 rather than PEPR-F DC 4 B). No technical description of the PS that addresses automatic initiation of safety systems has been identified. The designer or future operator/licensee is requested to identify appropriate technical evidence that demonstrated that safety systems are automatically initiated and included this in the CAE Trail.

- The prevention of negating PS action by the PACS electrical switchgear and other functionality of the PACS has not been addressed, neither has evidence been identified to support the first part of guidance paragraph 343 requirements, not even PCSR chapter reference. The response to TQ-EPR-276 provides some information. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to demonstrate the role of the PACS to prevent facility personnel negating safety system action.

- The second part of guidance paragraph 343 mentions permissives and resets and points to PCSR Ch 14 Section 7.3.5 for supporting evidence. There are 7 Sub-chapters and 2 Appendices to Ch 14; it is not clear in which of these Sections 7.3.5 is to be found. Further supporting evidence beyond the PCSR would be expected. The designer or future operator/licensee is requested to ensure that appropriate specific evidence is identified and included in the CAE Trail.

T13.TO2.11 - From the review of the CAE Trail for ESS.18 the following areas for improvement are raised:

- The SAP is about faults and hazards (both internal and external). However, there is no reference to the Fault Schedule, FMEA or any Hazard Analysis to demonstrate the architecture design satisfies the SAP requirements. PCSR Chapters 13.1 and 13.2 discuss External and Internal Hazards respectively but they, or any of their supporting references, are not mentioned here. The designer or future operator/licensee is requested to review and revise the argument and evidence to demonstrate that a safety system is not disabled by an internal or external hazard and that appropriate specific evidence is identified and included in the CAE Trail.

- Much of the evidence is Sub-chapters and Appendices of the PCSR and in some cases, such as Appendix 7D in support of the guidance paragraph 352, the wording of the 'argument' comes directly from the 'evidence'. More detailed supporting evidence should be identified that supports the arguments presented in the PCSR, such as NLE-F DC 33 C - Concept for I&C Failure Handling. The designer or future operator/licensee is requested to review and revise the evidence so that appropriate specific evidence is identified and included in the CAE Trail.

T13.TO2.12 - From the review of the CAE Trail for ESS.21 the following areas for improvement are raised:

Annex 3

- The first part of this SAP is about avoiding complexity in the design of the safety systems. There is no claim (or argument) that complexity is avoided during the system design process or no demonstration via specific evidence that complexity has been avoided. The argument for the UKEPR implies complexity in the design of safety systems has not been avoided and instead it is intended to justify the complexity of the systems via PE&ICB for software, and a safety demonstration for hardware; hence the link direct to guidance paragraph 355 that only applies when this SAP cannot be achieved. There is no justification presented for why use of complex safety systems is acceptable. Having been directed to guidance paragraph 355, it is stated that the safety demonstration for the complex hardware is yet to be developed, with no indication of timescales. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to include a justification for why use of complex safety systems is acceptable and that appropriate specific evidence is identified and included in the CAE Trail.

- For the SPPA-T2000 it is left to a Self-test coverage analysis (SIE QU633) to demonstrate fail-safe with a module FMEA and a system level reliability study (unreferenced). Individual module FMEAs and the Reliability Analysis for SPPA-T2000 [QU627] are not mentioned in the evidence column. The designer or future operator/licensee is requested to ensure that appropriate specific evidence is identified and included in the CAE Trail.

- There is no argument or evidence to support revealing internal faults for SPPA-T2000. The designer or future operator/licensee is requested to ensure that appropriate specific evidence is identified and included in the CAE Trail.

- For guidance paragraph 356, the use of periodic tests is claimed where faults cannot be revealed until this time. The evidence column states: 'the principles of the periodic tests that will be implemented for the different I&C systems are given in the following evidence'. However, it goes on to say that this will all be addressed during Site Licensing. It is unclear why such evidence as NLE-F DC 34 Rev D - Protection System - Concept for Periodic Tests is not cited here. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to ensure accurate statements and appropriate specific evidence is included in the CAE Trail.

T13.TO2.13 - From the review of the CAE Trail for ESS.23 the following areas for improvement are raised:

- The argument mentions, as a general point, that the four-fold redundancy of the design mitigates against unavailability in any one division and more specifically, in determining the safety system provisions for the I&C system, that allowance has been made for the unavailability of equipment due to causes including; testing and maintenance, non-repairable equipment failures and unrevealed failures. However, the evidence cited to support this argument is either Operating Technical Specifications that are out of scope for GDA or evidence to be adapted from that for EMT.6. The designer or future operator/licensee is requested to ensure that appropriate specific evidence is identified that demonstrates that unavailability of equipment has been addressed in determining Safety System provision and that it is included in the CAE Trail.

Annex 3

- Unavailability due to testing and maintenance is quoted in the evidence column as addressed by application of SFC[6]. This is effectively repeating the argument. There should be specific evidence referenced that explains how the removal of equipment for test or maintenance has been taken into account. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised and appropriate specific evidence is included in the CAE Trail.

- Non-repairable failures and unrevealed failures (guidance paragraph 357 refers) were the subject of TQ-EPR-375 the response to which quoted PCSR Chapter 7 Appendix A Section 3.1.7 as discussing this point. However, this is not provided as part of the argument. The response to TQ-EPR-375 also quoted an FMEA assessment activity as part of a Quantitative assessment process and listed module FMEA that are not referenced. References quoted in the response to TQ-EPR-375 as supporting demonstration that I&C design has been assessed for unavailability in support of this SAP include:

  - NLE-F DC 33 C - Concept for I&C Failure Handling.
  - NLE-F DC 34 Rev D - Protection System - Concept for Periodic Tests.
  - NLTC-G/2008/en/0079 Rev B - TXS Self-monitoring and fail-safe behaviour.

  These are not included in the CAE Trail. The designer or future operator/licensee is requested to ensure that appropriate specific evidence is included in the CAE Trail.

T13.T02.14 - From the review of the CAE Trail for ESS.27 the following areas for improvement are raised:

- For 'Production Excellence' the evidence identified is relevant but there are some evidence documents cited (e.g. NLF-F DC 14 Hardware Qualification) that are hardware based where this is a software based SAP. Also, the argument mentions a System QA Plan as well as a System Quality Plan; there is no System QA Plan listed in the evidence column. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to ensure accurate statements and appropriate specific evidence is included in the CAE Trail.

- For the 'Independent Confidence Building' leg the argument cites much independent checking and surveillance work by parties other than AREVA. However, apart from one CEIDRE inspection report (with no specific document reference) there is no other actual evidence of the independent checks/surveillance carried out. Other evidence is documents that would be checked by ICB or explanation of the ICB process. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to ensure accurate statements and appropriate specific evidence is included in the CAE Trail.

T13.T02.15 - From the review of the CAE Trail for ESR.1 the following areas for improvement are raised:

- Supporting evidence is quoted as PCSR chapters (Sub-chapters 7.2 and 18.1) that effectively provide an argument. More detailed evidence on the MCR, RSS or the PICS/SICS would be expected. References from Sub-chapters 7.2, 7.3 and 7.4 of the PCSR that have not been cited include:

[6] ONR note: SFC is an abbreviation of Single Failure Criterion.

Annex 3

- ECECC060019 Revision A - Main Control Room (KSC [MCR]) System Specification.
- ECECC070760 B - System Design Description Main Control Room (KSC [MCR]), Part 5: Control and Instrumentation System (KSC [MCR]) EPR FA3 (Stage 2).
- ECECC040729 Revision A - Process Information and Control System (KIC [PICS]) System Specification.
- ECECC080097 Revision B - Process Information and Control System (KIC [PICS]) Part 5: Control and Instrumentation System EPR FA3 (Stage 2).

The designer or future operator/licensee is requested to ensure that appropriate specific evidence is included in the CAE Trail.

- ECEF021069 Revision C1 - Sizing of SICS was mentioned in response to TQ-EPR-364 in relation to ESR.1, but has only been cited as evidence to support guidance paragraph 366. The response to TQ-EPR-364 also quoted *'Design documents to provide evidence that the MCR and RSS I&C will provide the described tasks and functions will be available during step 4 when they have been completed'*. Also, in relation to guidance paragraph 366, the PICS is quoted in the argument yet it is only ECEF 021069 'Sizing of SICS' that is cited as evidence. It would be expected that more specific information on the PICS, as well as the SICS, would be identified (see list above). The designer or future operator/licensee is requested to ensure that the CAE Trail is revised and appropriate specific evidence is included in the CAE Trail.

T13.TO2.16 - From the review of the CAE Trail for ESR.3 the following areas for improvement are raised:

- No specific evidence has been identified against any argument. More detailed system requirements specifications etc. that set out what controls are provided to 'maintain variables within specified ranges' and why they are considered to be adequate would be expected. The arguments refer to PCSR Sub-chapter 7.4. There are many references listed in the PCSR for Chapter 7.4 Sections 1, 2 and 3 that are not listed here. There is no identified evidence to demonstrate that controls that maintain variables within specified ranges are 'Adequate and Reliable'. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised and appropriate specific evidence is included in the CAE Trail.

- The FMEA referred to in support of demonstration that the controls are reliable is just a 'Methodology' for an FMEA for the TXS based PS. The PS is not relevant to this SAP. The only one of the three systems addressed by the argument (PAS, RCSL and PICS) based on TXS is the RCSL. The PAS and PICS are both based on SPPA-T2000. The SPPA-T2000 reliability analysis (QU627) and module dependability analysis is not cited. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised and appropriate specific evidence is included in the CAE Trail.

T13.TO2.17 - From the review of the CAE Trail for ESR.5 the following area for improvement is raised:

- The note in the 'Claim' makes reference to both hardware and software in relation to ESS.27 whereas ESS.27 is only software related. Additionally, the applicable safety related systems are quoted as; PAS, RCSL, SA I&C and PICS. Then only SAS and RCSL are addressed. The SAS seems to have been introduced from nowhere and the PICS, PAS and SA I&C have disappeared. The evidence then cited is for either the SPPA-T2000 or TXS. The designer or

Annex 3

future operator/licensee is requested to ensure that the CAE Trail is revised to ensure accurate statements and appropriate specific evidence is included in the CAE Trail.

T13.TO2.18 - From the review of the CAE Trail for ERC.2 the following areas for improvement are raised:

- No evidence has been identified to support the argument that the EBS/SIS systems can be actuated to perform extra boration when required, by diverse functions within PS and SAS/PAS. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised and appropriate specific evidence is included in the CAE Trail.

- EDF and AREVA claim that guidance paragraph 445 is not applicable to I&C, However, this relates to, for example, situations where the control rods fail to insert on a RT signal from the PS. In this situation an ATWS signal is initiated by the C&I to actuate the EBS and SIS to inject borated water. Some argument and supporting evidence on this should be provided. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised and appropriate specific evidence is included in the CAE Trail.

T13.TO2.19 - From the review of the CAE Trail for EKP.3 the following area for improvement is raised:

- The PCSR Chapters 3.1 and 14.7 are cited as providing a discussion on the application of defence in depth with the latter providing the Fault Schedule analysis that provides identification of the functions of the C&I systems to address fault scenarios. It is noted that the Fault Schedule in Chapter 14.7 has now been replaced with PEPR-F DC 4 B. However, this Fault Schedule does not identify the actual C&I systems used to manage a fault condition; it just provides a 'Main Line' function and a 'Diverse Line' function and the Class of system required. The designer or future operator/licensee is requested to ensure that the UKEPR Fault Schedule (PEPR-F DC 4 B) is updated to reflect these comments and to ensure that the statement in the CAE Trail of what the document presents as evidence is correct.

T13.TO2.20 – From the review of the CAE Trail for EKP.5 the following areas for improvement are raised:

- The Fault Schedule in Chapter 14.7 of the Nov 2009 PCSR is quoted but it is understood that this has now been replaced with PEPR-F DC 4 B. This also applies to ESS.9. The designer or future operator/licensee is requested to ensure that the correct reference to the UKEPR Fault Schedule is used in PELL-F DC 9.

- Reviewing PEPR-F DC 4 it is noted that the 'Preventative Line' is not identified; it is only the 'Main Line' and 'Diverse Line' identified. Although the Safety Measure (e.g. Reactor Trip) required to deliver a safety function (e.g. Shutdown and remain sub-critical) is identified in the Fault Schedule, there is no mention of the associated C&I System that delivers that safety function. The designer or future operator/licensee is requested to ensure that the UKEPR Fault Schedule is updated to reflect these comments and to ensure that the statement in the CAE Trail of what the document presents as evidence is correct.

- Document ECECC 070637B that list the manual controls and provides the substantiation for their selection, referenced from TQ-EPR-323, has not been listed in the CAE Trail. The designer or future operator/licensee is requested to consider the appropriateness of this

Annex 3

document to support conformance with EKP.5 guidance paragraph 146 c) and ensure its inclusion in the CAE Trail if applicable.

- In most cases the evidence cited is sub-chapter and section of the PCSR that might not be most appropriate. Taking 3 examples:

  Chapter 7.3 Section 1 is cited but this has numerous References listed in the PCSR that are not mentioned here as supporting evidence; e.g. NLE-F DC 124 Concept for Reactor Trip.

  Chapter 7.4 Section 1.0.1 is cited against guidance paragraph 146c), but the wording of the 'Argument' is taken directly from this PCSR Section cited as 'Evidence'.

  Chapter 7.3 Section 5.0.1 is cited against guidance paragraphs 146e) and 147 in relation to Severe Accident I&C.

  - Ch 7.3 (F1 Systems) does not have a Section 5.
  - Ch 7.4 (F2 & NC Systems) does have a Section 5 related to SA I&C.
  - Ch 7.4 Section 5.0.1 simply states that the SA I&C 'Limits the radioactive release at the site boundary to an acceptable level and maintains the integrity of the primary and secondary systems'. This is effectively the same as the first line of the 'Argument' in both cases.

  The designer or future operator/licensee is requested to review all cited evidence and ensure that the references to supporting evidence are appropriate and correct.

T13.TO2.21 - From the review of the CAE Trail for ERL.1 the following areas for improvement are raised:

- Much of the 'Argument' appears to discuss qualification requirements rather than how derivation of reliability claims take account of the various aspects required. Hence Qualification Reports (cited as evidence) would demonstrate that qualification had been carried out, but it is not clear if they provide derivation of reliability claims. The designer or future operator/licensee is requested to ensure clearly referenced evidence is cited in the CAE Trail that provides a derivation of reliability claims.

- 'Reliability Analyses' are cited as evidence for most aspects of the SAP. However, for the final point on 'uncertainties in physical data and design' and against guidance paragraph 176, specific reliability analysis documents are listed for both systems and platforms. It is not clear why specific references have been quoted in these cases but not others. The designer or future operator/licensee is requested to ensure that where specific references are available they are correctly cited against all applicable aspects of the CAE Trail.

T13.TO2.22 - From the review of the CAE Trail for ERL.2, EMT.1 and EMT.3 the following area for improvement is raised:

Annex 3

- There needs to be more focused referencing to specific areas within the referenced evidence documents. The designer or future operator/licensee is requested to ensure that references to evidence cited within the CAE Trail are to a specific and appropriate Section rather than a general document reference.

T13.TO2.23 - From the review of the CAE Trail for ELO.2 the following area for improvement is raised:

- The evidence description in the CAE Trail calls both NLF-F DC 98 and SY719 4.0 the 'Information Security Plan'. The designer or future operator/licensee is requested to provide clarification as to whether both NLF-F DC 98 and SY719 4.0 are entitled 'Information Security Plan' and ensure correct and accurate referencing of evidence in the CAE Trail.

T13.TO2.24 - From the review of the CAE Trail for EHA.10 the following area for improvement is raised:

- The quoting of EMC IEC Standards, 61000-6-2 & 61000-6-4, and other standards/requirements as evidence is inappropriate as the standards provide the requirement, not evidence that the requirement has been met. The designer or future operator/licensee is requested to ensure that where a claim and argument in a CAE Trail cites compliance with an International Standard, the evidence to demonstrate compliance with the standard is cited.

T13.TO2.25 - From the review of the CAE Trail for ESS.10 the following areas for improvement are raised:

- More focused/specific document references would be expected. The designer or future operator/licensee is requested to ensure that references to evidence cited within the CAE Trail are to a specific and appropriate Section rather than a general document reference.

- The list of evidence documents includes 'Qualification Documents'. However, the documents referenced in TQ-EPR-359, NLZ-F DC 3 'I&C TXS cabinets qualification program' and NLF-F DC 14 'System qualification program', have not been listed against this SAP. The designer or future operator/licensee is requested to ensure that appropriate specific document references are included in the CAE Trail instead of a generic list of document types.

- The argument against capability exceeding service requirement by a clear margin (para 345) does not appear to address this well. The same generic document list is provided as evidence where specific evidence showing the margin between maximum service requirement and system capability would be expected. The designer or future operator/licensee is requested to ensure that appropriate evidence is identified and included in the CAE Trail that demonstrates that the margin between maximum service requirement and system capability is acceptable.

T13.TO2.26 - From the review of the CAE Trail for ESS.11 the following areas for improvement are raised:

- Under 'achieving the specified function' - The PAS is missing from the SPPA-T2000 based systems; it is assumed this would be covered under the QP for SPPA-T2000 cited. There is no evidence identified for the SICS and PACS. Also, under the 'For SICS' the PACS is mentioned instead. The designer or future operator/licensee is requested to ensure that ensure that the

Annex 3

CAE Trail is correct and accurately covers the appropriate systems and that appropriate evidence is included for all systems addressed by this SAP.

- Under 'achieving the specified reliability' - Against 'For SICS' it states 'see RAMS for SPPA or TXS'. It has been mentioned in the CAE Trail that the RAMS for PS (NLE-F DM 10032) will not be available until end 2010, but RAMS for TXS or SPPA are not specifically referenced. The designer or future operator/licensee is requested to ensure that specific references to RAMS for TXS and SPPA are included in the CAE Trail.

- The Fault Schedule is cited as PCSR Chapter 14.7 which has been replaced by PEPR-F DC 4 B. It is stated against guidance paragraph 346 that the new fault schedule is currently being produced, whereas it has been issued, and that it allocates safety functions to C&I systems. PEPR-F DC 4 does identify safety functions but it does not identify the specific C&I systems that carry out those function, as required by SAP guidance paragraph 346. The designer or future operator/licensee is requested to ensure that the UKEPR Fault Schedule is updated to identify the specific C&I systems that carry out the safety functions.

T13.TO2.27 - From the review of the CAE Trail for ESS.13 the following areas for improvement are raised:

- In relation to b) in the 'Clam', it was identified during the Step 3 review that Sub-chapter 18.1 Section 3.2.2.2 states *'The Process Displays .... provide information on the ....status of actuators*'. However, the evidence column relates to Emergency Operating Procedures (EOPs) being provided at Site Licensing. There is no information or supporting evidence regarding Process Displays and Status of Actuators in the CAE Trail. The designer or future operator/licensee is requested to ensure that appropriate evidence is identified and included in the CAE Trail that demonstrates the confirmation to operating personnel of the status of actuators.

- The SAP paragraph in the second row of the table should be preceded with the paragraph number 349. The designer or future operator/licensee is requested to ensure that the CAE Trail is updated accordingly.

T13.TO2.28 - From the review of the CAE Trail for ESS.16 the following area for improvement is raised:

- This SAP is addressed by discussion of continued power supply to the C&I systems and self contained battery back-up supplies within the systems, whereas the SAP relates to maintaining a safe state after a safety system action has put the plant in that safe state. This could be seen, for instance, as no external power required to hold the control rods in the core following initiation of RT by the PS. The designer or future operator/licensee is requested to ensure that the CAE Trail addresses non-dependence on external power supply to maintain a safe state after safety system action.

T13.TO2.29 - From the review of the CAE Trail for ESS.20 the following areas for improvement are raised:

- Reference is made to 'Security Plans' with no specific information or delivery dates, but SAP ELO.2 has identified:
  - NLN-F DC 3, Teleperm XS based I&C systems IT Security Plan

Annex 3

- NLF-F DC 98, Information Security Plan
- SY719 4.0, Information Security Plan

It is not clear why these are not referenced here. The designer or future operator/licensee is requested to ensure that specific documents are cited as evidence if available and appropriate.

- There is no document identification or delivery date for the 'Detailed Requirement Specification for Interfaces'. The designer or future operator/licensee is requested to ensure that specific references to evidence documents are included in the CAE Trail.

T13.TO2.30 - From the review of the CAE Trail for EMT.5 the following areas for improvement are raised:

- The designer or future operator/licensee is requested to ensure that the evidence cited addresses the requirement to maintain quality and reliability.

- For guidance paragraph 189, the evidence is a RAMS Methodology which is unlikely to demonstrate that in-service testing (Periodic Testing) will detect degradation before loss of Safety Function. The designer or future operator/licensee is requested to ensure evidence is identified and cited in the CAE Trail that demonstrates that in-service testing (Periodic Testing) will detect degradation before loss of Safety Function.

T13.TO2.31 - From the review of the CAE Trail for ESS.4 the following areas for improvement are raised:

- It is not clear where the demonstration is that the initiating variables are 'shown to be sufficient for the purpose of protecting the facility'. Additionally, it appears that the evidence is only related to the Protection System, rather than including other Safety Systems such as SAS. The designer or future operator/licensee is requested to ensure that evidence is identified and included in the CAE Trail that demonstrates that the initiating variables are sufficient for protecting the facility for all Safety Systems.

- In relation to guidance paragraph 339, the interpretations in the argument both appear to miss the point. The 'Limiting Conditions on the Variables' is the limit beyond which an initiating parameter should no go; i.e. if Reactor Trip were to be initiated on high Primary Coolant pressure, then the 'limiting condition' for Primary Coolant pressure (max PC pressure allowed) should not be reached following initiation of Reactor Trip. Hence there should be a suitable margin between initiating value and maximum value to allow for all expected transients. It is not clear that this has been adequately addressed. The designer or future operator/licensee is requested to ensure that the CAE Trail in relation to ESS.4 paragraph 339 is readdressed to demonstrate that Safety Systems respond so that limiting conditions are not transgressed.

T13.TO2.32 - From the review of the CAE Trail for ESS.5 the following area for improvement is raised:

- Mention is made of 'Sensor qualification documentation' for provision of response time requirement, but specific reference of these documents is not included in the CAE Trail. The designer or future operator/licensee is requested to ensure that specific reference to supporting evidence documents is included in the CAE Trail.

Annex 3

T13.TO2.33 - From the review of the CAE Trail for ESS.6 the following area for improvement is raised:

- It is noted that Primary Coolant Flow is indirectly derived from Main Coolant Pump speed. As this is used in a significant computed variable used for Reactor Trip, there needs to be sufficient justification of the relationship between MCP speed and coolant flow. The designer or future operator/licensee is requested to ensure that a justification of the relationship between MCP speed and coolant flow is produced and referenced in the CAE Trail.

T13.TO2.34 - From the review of the CAE Trail for ESS.17 the following area for improvement is raised:

- The argument does not address whether potential faults (that should be detected by measures to detect failures within safety systems) have been identified that could cause an unsafe change in plant variables (e.g. coolant temperature or pressure rise) if avoidance measures are not initiated. The designer or future operator/licensee is requested to ensure that evidence is identified and cited in the CAE Trail that such faults have been identified.

T13.TO2.35 - From the review of the CAE Trail for ESS.25 the following area for improvement is raised:

- The argument for the use of Permissives, Resets and Vetoes is provided against guidance paragraph 358 and applicable evidence documents have been referenced. It would be advantageous if the Argument sections pointed to where this is addressed within the PCSR. The designer or future operator/licensee is requested to ensure that the argument is revised to include reference to appropriate Sections in the PCSR.

T13.TO2.36 - From the review of the CAE Trail for ESR.2 the following area for improvement is raised:

- The designer or future operator/licensee is requested to ensure that more specific reference to System Design Manuals (SDMs) and Contract documents is included in the CAE Trail.

T13.TO2.37 - From the review of the CAE Trail for ESR.10 the following area for improvement is raised:

- The argument and evidence appear more focused on the control of plant parameters by LCO and Limitation Functions as is discussed more under ESS.9. Whereas this SAP is about failure of control systems, e.g. RCSL, not causing excess demand on safety systems. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to provide sufficient argument and evidence to demonstrate control system failures will not cause excessive demands and evidence of analysis that identifies foreseeable control system faults.

T13.TO2.38 - From the review of the CAE Trail for EHF.7 the following area for improvement is raised:

- From a C&I point of view there is no actual argument or evidence relating to the provision of controls, indications, recording equipment and alarms, as required by this SAP. The designer or future operator/licensee is requested to ensure that more specific evidence is identified and cited in the CAE Trail relating to the MCR, RSS, PICS and SICS detailing provisions to meet the requirements of this SAP, not just Human Factors studies related information.

T13.TO2.39 - From the review of the CAE Trail for ECS.5 the following area for improvement is raised:

- ECS.5 requires that *'In the absence of applicable or relevant codes and standards, the results of experience, tests, analysis, or a combination thereof, should be applied to demonstrate that*

Annex 3

the item will perform its safety function(s) to a level commensurate with its classification'. The only evidence cited is RCC-E that includes the requirements for previous experience, practice, the use of experience feedback for existing components and the use of pre-existing components where standards are not used, but there is no evidence to demonstrate that these requirements have been applied. The designer or future operator/licensee is requested to ensure that specific evidence of having to adopt results of experience, tests and analysis in the absence of applicable codes and standards is identified and cited in the CAE Trail.

T13.TO2.40 - From the review of the CAE Trail for EMT.4 the following areas for improvement are raised:

- The argument put forward for 'no unacceptable degradation of qualification due to maintenance, inspection and testing' all seems to relate to the requirement for EMIT[7] activity with no mention of the requirement to maintain qualification during such activity. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to demonstrate that qualification (e.g. the activities do not stress the system beyond the qualification limits) is maintained during EMIT activities.

- The evidence cited is the 'Requirements for maintenance and test activity'; it is not clear if this stipulates the requirement to maintain qualification or carry out repeat qualification testing following such activity. The designer or future operator/licensee is requested to ensure that the appropriateness of cited evidence is reviewed and specific evidence relating to maintenance of qualification during maintenance activity is included.

T13.TO2.41 - From the review of the CAE Trail for EAD.1 the following area for improvement is raised:

- The SAP requires safe working life (SWL) to be defined at the design stage and the 'Claim' states this to be the case. However, the 'argument' discusses the use of maintenance and inspection to detect failures before loss of safety function with no mention of evaluation of SWL (e.g. capacitors, battery backed functions etc.) to define the timescales for EMIT or the replacement date regardless of condition found at EMIT. Guidance paragraphs 194 and 195 are similarly poorly addressed. Additionally, paragraph 195 requires that the SWL exceeds the intended operational life (i.e. time of replacement regardless of condition) by an adequate margin. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to address the evaluation of Safe Working Life at the design stage.

T13.TO2.42 - From the review of the CAE Trail for EAD.2 the following area for improvement is raised:

- Guidance paragraph 196 to this SAP is about understanding the effects of material ageing and degradation in the design and making due allowance for it and the rate at which it occurs. The 'arguments' seem to be all about Qualification and EMIT to detect any ageing or degradation. Additionally, the evidence cited is predominantly Site specific processes for EMIT and management of ageing and degradation, whereas evidence that such mechanisms had been taken into account during the design process should be included. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to address the consideration of material ageing and degradation at the design stage (e.g. insulation materials and tin whiskers etc.).

[7] ONR note: EMIT is an abbreviation of Examination, Maintenance, Inspection, and Test.

Annex 3

T13.TO2.43 - From the review of the CAE Trail for EES.9 the following area for improvement is raised:

- This SAP is related to the simultaneous loss of both normal and back-up essential services. The RP has stated that, for C&I, essential services are electrical supplies and ventilation. The argument only mentions double power supply without discussion of the simultaneous loss of both. Additionally, there is no reference in the argument or cited evidence to ventilation systems. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to address the simultaneous loss of both normal and back-up services, including ventilation systems important to C&I systems and equipment.

T13.TO2.44 – Due to unavailability of information from EDF and AREVA, the review of Sensors (In-Core, Ex-Core and Process) was limited to 2 In-Core systems (Self Powered Neutron Detectors (SPND) and Core Outlet Thermocouples (COTs)) against third tier IEC standards using the System Specifications and the RIS System Design Manual. The designer or future operator/licensee is requested to ensure appropriate standards (such as those listed in the BSI NCE 8 list) and processes used in the design, manufacture, procurement, qualification and testing of Sensors are identified and ensure evidence of implementation and compliance to these standards and procedures is produced; this should include evidence of Sensor Qualification for normal and emergency operating conditions.

<u>Conclusions of Task Reviews</u>

With regards to the Adequacy of the PCSR, it is concluded that the general structure of the CAE Approach in response to RO-UKEPR-62 Action A1 demonstrates a sound approach methodology. However, the following need to be addressed in further developing this methodology and its output:

- There needs to be a clear explanation or demonstration of how High Level and Key Claims are derived from appropriate sources, such as C&I Design Requirements Specification, Criteria or Principles, or other appropriate sources.

- There needs to be a clear identification of the location of the Claims and Arguments within the PCSR, and identification of appropriate supporting Evidence.

- The wording of the Claims, particularly the Sub-Claims, appears to be taken directly from the NII SAPs whereas all Claims should be derived independently from the SAPs and relate to the designer's of future operator/licensee's own key claims such as satisfaction of safety principles/criteria. Note: Conformance to HSE C&I SAPs is addressed by RO-UKEPR-62 A.2.

With regards to SAP conformance demonstration, it is concluded that the C&I SAP CAE Trail in document PELL-F DC 9 has developed as an acceptable methodology for the demonstration of conformance to the HSE/ND C&I SAPs. However, there are still significant areas for improvement in the presented Argument and identified Evidence for a large number of SAPs, and most conformance demonstrations for the C&I SAPs have areas for improvement.

With regards to the Sensor review, a sample review of the SPND and COTs System Specifications and the RIS SDM against IEC 61468:2000 and IEC 60737:2010 has shown that some design requirements specified in these IEC standards have been addressed in the System Specification documents and RIS SDM but no clear supporting evidence was identified within them to demonstrate conformance with many areas of the standards. Further detailed evidence is needed as the specific design and procurement progresses.

Annex 3

With regards to the PCSR Updates, it is concluded that:

- The June 2009 Issue 2 of the PCSR did not introduced significant changes to the C&I architecture, nor significant improvements to the safety argumentation presented in the PCSR, compared to the April 2008 Issue 1. The June 2009 Issue 2 of the PCSR had no discernable impact on the preliminary activities conducted under GDA Step 3 Tasks 1 to 3, Task 7 and Task 8.

- The November 2009 Issue 3 of the PCSR C&I sub-chapters and Appendices were sufficiently similar to those in the June 2009 issue to be considered to be identical. As such, the November 2009 Issue 3 of the PCSR had no impact on any GDA Step 3 review work by the TCS Tasks previously undertaken.

In the opinion of the TSC subject to sufficient and adequate responses being made to the TOs/Potential GDA Issues it is anticipated that an adequate position could be confirmed for:

Demonstration of conformance with HSE/ND C&I SAPS.

Demonstration of derivation and identification of a clear CAE Trail for all claims within the UKEPR PCSR.

Confirmation of design, manufacture, test and qualification of Sensors to international standards.

Annex 4

TSC Summary – Review of EDF and AREVA QMS Processes Against Principal Design and Implementation Standards[8]

Note this information has been imported from a TSC report (Ref. 29) and the formatting of the TSC report has been retained.

[8] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 4

A Annex: TSC Task Summary - Review of EDF and AREVA QMS processes against Principal Design and Implementation Standards

This annex summarises the outcome of the Technical Support Contractor's (TSC) review of EDF and AREVA Quality Management System (QMS) processes against principal design and implementation standards and selected Safety Assessment Principles (SAPs) that relate to processes. This review follows on from the review of company-level process-related claims and argumentation carried out in a preliminary activity (Task 4). The aim of the review has been to gain confidence that the Requesting Party (Electricité de France SA and Areva NP SAS, hereafter referred to as EDF and AREVA) have adequate and sufficient evidence to support these process-related claims and arguments. This has included a review of samples of the evidence to support further claims and argumentation presented by EDF and AREVA relating to the conformance of specific C&I systems to selected Safety Assessment Principles (SAPs) that relate to company-level processes.

The task has reviewed C&I company level process-related evidence presented by EDF and AREVA via:

- the claims-argument-evidence table that provides the RP's basis of the demonstration of SAP conformance;
- responses to Technical Queries;
- responses to actions from meetings involving EDF and AREVA, HSE/NII and the TSC;
- and responses to technical observations raised by Task 4, including relevant observations in the HSE/NII Step 2 and 3 reports.

The scope of the task includes company level processes which are applicable to the development of UK EPR Safety and Safety Related C&I equipment. The scope of the evidence that is specific to UK EPR is defined by EDF and AREVA in *"UK EPR CONTROL AND INSTRUMENTATION (C&I) – SCOPE OF GDA"* (letter ND (NII) EPR00686N).

The Pre Construction Safety Report (PCSR) indicates that RCC-E (Design and Construction Rules for Electrical Components of Nuclear Islands, December 2005) defines the process related requirements which are applicable to C&I equipment. This review has therefore sought to confirm that:

- RCC-E addresses the process related requirements of relevant international standards specified by 'BSi Technical Committee NCE/8 Nuclear Power Plants - I&C Systems, A Guide to Applicable IEC standards' (from here on referred to as the 'BSi NCE/8 List');
- RCC-E is encapsulated within the EDF and Areva Quality Management Systems (QMS) and
- RCC-E and the QMS collectively define adequate and sufficient measures for production excellence and independent confidence building.

Regarding standards conformance:

1 Of the IEC standards defined by the BSi NCE/8 List there are 35 standards which are not addressed by RCC-E. However, the standards to be applied on UK EPR will be specified by

Annex 4

reference to RCC-E, plus specific standards identified in technical specifications. With the exception of IEC 61504:2000, EDF and AREVA have committed in response to TQ-EPR-473 to specifying all standards in the BSi NCE/8 List.

2 Based on the sampled evidence, no areas for improvement have been identified with the project-independent processes used by EDF and Areva for the design and implementation of Class 1, 2 and 3 C&I equipment with respect to the requirements of IEC 60880:2006 and IEC 62138:2004.

3 Based on the samples considered in the review, there is adequate and sufficient evidence to demonstrate that project-independent processes used by EDF and Areva for Class 1, 2 and 3 C&I systems satisfy most of the applicable design and implementation, and verification and validation requirements of IEC 61513:2001, IEC 60987:2007 and IEC 61508-2:2000 (where IEC 61508-2:2000 has been the basis of the review for Class 3 hardware.) However there are a number of clauses within the standards for which insufficient evidence has been provided during the period of this review to demonstrate that they are satisfied by project-independent processes.

4 Insufficient evidence has been provided during the period of this review to demonstrate that RCC-E is sufficiently prescriptive in the requirements for the design and implementation of Programmable Complex Electronic Components.

5 Insufficient evidence has been provided during the period of this review to demonstrate that there are adequate company-level processes for the configuration management of the set of all structures, systems and components that comprise the C&I architecture.

6 Based on the sampled evidence, there is adequate and sufficient evidence to demonstrate that RCC-E includes adequate requirements for Independent Verification and Validation and Requirements Management, as required by appropriate IEC standards.

7 Regarding the EDF and Areva Quality Management Systems, based on the sampled evidence there is adequate and sufficient evidence to demonstrate that these systems encapsulate the requirements of RCC-E, and no areas for improvement with the quality assurance arrangements have been identified.

Regarding Independent Confidence Building Measures, the EDF Quality Management System includes processes for quality assessments of system documents, audits and supervision of software development. However, potential GDA Issue pGI-UKEPR-C&I-03.01[9] has been raised for the designer or future operator/licensee to justify the adequacy of independent confidence building activities.

Regarding the demonstration by EDF and AREVA of conformance to SAPs that relate to company-level processes via their claims-argument-evidence submission, no major areas for improvement have been identified. However a number of detailed technical observations (TO) have been raised.

The observations in the HSE/NII report for GDA Steps 2 and 3 have been apportioned to tasks 14 through 18.

The observations in the HSE/NII report for GDA Step 2 which are relevant to this task have been reviewed. Of the 5 that are relevant, 2 are considered by the TSC to be resolved. Some progress has

[9] ND note: GI-UKEPR-CI-02 is the issued version of the provisional GDA Issue (pGI).

Annex 4

been made on the other 3 observations. Outstanding points are covered by the following Technical Observations (TOs) which have been raised in relation to them: T14.TO1.01, T14.TO1.02, T14.TO2.01, T14.TO2.02, T14.TO2.03, T14.TO2.04 and T14.TO2.06. The original Step 2 observations are adequately addressed by these TOs and pGI-UKEPR-C&I-03.01.

None of the observations in the HSE/NII report for GDA Step 3 are relevant to Task 14.

A total of nine technical observations have been raised from this review. These technical observations have been designated TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher. Three of these have been designated TO1, and the other six have been designated TO2.

The TO1 technical observations are:

1 **T14.TO1.01** - The designer or future operator/licensee is requested to ensure that the commitment to apply the standards identified in 'BSi Technical Committee NCE/8 Nuclear Power Plants - I&C Systems, A Guide to Applicable IEC standards' on UK EPR has been fulfilled. EDF and AREVA have stated that this evidence will be in the form of Technical Specifications which will identify standards which complement those identified in RCC-E. The designer or future operator/licensee is also requested to justify why IEC 61504:2000 will not be applied on UK EPR.

2 **T14.TO1.02** - The designer or future operator/licensee is requested to justify the use of programmable complex electronic components (PCECs) in Class 1, 2 and 3 C&I systems. The justification should:

- demonstrate how the requirements of SAPs ECS.3 and ESS.21 paragraph 355 are satisfied and

- identify the standards, guidance and criteria that are used to demonstrate that the components are fit for purpose. In particular the justification should demonstrate that the relevant requirements of IEC 61513:2001 and IEC 60987:2007 have been addressed. (It should be noted that consideration of specific examples of PCECs is addressed as part of Task 15, see S.P1440.74.25 "*Task 15 Class 1&2 System Platforms and Pre-Developed Components Review for UK EPR Reactor*").

3 **T14.TO1.03** - The designer or future operator/licensee is requested to demonstrate that adequate company-level processes, or UK-EPR project-level processes are established for configuration management of the set of all structures, systems and components that comprise the C&I architecture, which should be addressed within an Overall Quality Assurance Plan, or equivalent, as required by IEC 61513:2001 clause 5.4.1.

The TO2 technical observations are:

1 **T14.TO2.01** - The standards identified below are referenced from RCC-E but at an earlier version than that specified by 'BSi Technical Committee NCE/8 Nuclear Power Plants - I&C Systems, A Guide to Applicable IEC standards'.

The designer or future operator/licensee is requested to confirm that the appropriate version of the following standards are specified for UK EPR, or justify the use of earlier versions.

- IEC 60671: 2007

Annex 4

- IEC 60709: 2004
- IEC 61227:2007

2 **T14.TO2.02** - There are some clauses within IEC 61513:2001 for which insufficient specific references to sections within RCC-E have been provided to confirm that the requirements of the clause are satisfied.

The designer or future operator/licensee is requested to demonstrate how the following IEC 61513:2001 clauses are addressed within RCC-E or the quality management systems that apply to C&I Safety and Safety Related equipment:

a. Clause 5.1 (Deriving the I&C Requirements from the Plant Safety Design Base)

Insufficient evidence has been found in RCC-E to confirm that the requirements related to the defence in depth concept are satisfied. EDF and AREVA have referred to chapter C6000 of RCC-E, and although it does address issues such as redundancy, independence and reliability, it does not address the principles described in the standard (e.g. prevention from and detection of deviation from normal operation, control of consequences).

b. Clauses 5.2 and 5.5 (Output Documentation):

Chapter C1200 of RCC-E describes at a high level the type of documents to be produced. However, there is insufficient detail to confirm that the requirements of clauses 5.2 and 5.5 are satisfied.

It is also noted that chapter C5231 defines some documentation requirements. However, these only apply to Class 1 and 2 systems, not Class 3.

c. Clauses 5.4.3 and 7 (Overall Integration and Commissioning)

No requirements have been found within RCC-E for an Overall Integration and Commissioning Plan.

d. Clause 5.4.4 and 8 (Operation Plan)

No requirements have been found in RCC-E for an Overall Operation Plan.

3 **T14.TO2.03** - There are some clauses within IEC 60987:2007 for which insufficient specific references to sections within RCC-E have been provided to confirm that the requirements of the clause are satisfied.

The designer or future operator/licensee is requested to demonstrate that the following IEC 60987:2007 clauses are addressed within RCC-E or the quality management systems that apply to C&I Safety and Safety Related equipment:

a. Clause 5.2 (Functional and Performance Requirements)

Chapter C5200 of RCC-E identifies the need for a Hardware Specification, however it states that this is outside the scope of this chapter, and does not indicate where it is addressed.

Annex 4

b. Clause 5.5 (Documentation Requirements)

Chapter C1200 of RCC-E describes at a high level the type of documents to be produced. However, there is insufficient detail to confirm that the requirements of clause 5.5 are satisfied.

c. Clauses 6.1, 6.2 (Design Activities)

Chapter C5000 of RCC-E "*Development of Programmable Systems*" provides requirements for the design and production of programmable systems (e.g. definition of requirements, production of architectural documents). However, it does not describe the development lifecycle for hardware components.

d. Clause 6.7 (Power Failure)

No evidence has been found in RCC-E to demonstrate that clause 6.7 is satisfied.

e. Clause 9 (Manufacture)

Chapters A3300 and B1000 of RCC-E provide some information on the procurement for components. However, there is no indication that they are assessed against the requirements of IEC 60987.

f. Clause 11 (Maintenance)

Chapter C3400 of RCC-E provides some information on Maintenance. However, no requirements have been found in RCC-E for the recording of failure data, or maintenance records.

4 **T14.TO2.04** - There are some clauses within IEC 61508-2:2000, which apply to Electrical/Electronic/Programmable Electronic Systems (E/E/PS), for which insufficient specific references to sections within RCC-E have been provided to confirm that the requirements of the clause are satisfied (where IEC 61508-2:2000 has been the basis of the review of the processes for Class 3 hardware.)

The designer or future operator/licensee is requested to demonstrate that the following IEC 61508-2:2000 clauses are addressed within RCC-E or the quality management systems that apply to C&I Safety and Safety Related equipment:

a. Clause 7.4 (design and development)

Chapter C5000 provides information on the development of programmable systems (e.g. definition of requirements, production of architectural documents).

However, it does not describe a development lifecycle for hardware components.

b. Clause 7.4 (E/E/PES design and development)

Annex 4

Chapter C5200 identifies the need for a Hardware Specification, and Architecture Definition. However it states that these are outside the scope of this chapter, and does not indicate where they are addressed.

c. Clause 7.4 (E/E/PES design and development)

There is insufficient evidence to confirm that RCC-E satisfies the detailed hardware related requirements of clauses 7.4.3, 7.4.7 and 7.4.8.

d. Clause 7.6 (E/E/PS/Operation and Maintenance Procedures)

Chapter C3400 provides some information on Maintenance. However, no requirements have been found in RCC-E for the recording of failure data, or maintenance records.

e. Annexes A, B, C

Insufficient evidence has been found in RCC-E to confirm that RCC-E satisfies the detailed hardware related requirements of Annexes A, B and C.

5 **T14.TO2.05** - The designer or future operator/licensee is requested to address the following observation which has arisen from the review of the Claims-Argument-Evidence (CAE) for Safety Assessment Principle (SAP) EQU.1 (Equipment Qualification).

Chapter B3500 of RCC-E states that qualification shall be in accordance with IEC 60780:1998 clause 5.3. However, it does not indicate which chapters within RCC-E address other clauses in IEC 60780:1998.

The designer or future operator/licensee is requested to update the CAE to demonstrate that the requirements of IEC 60780:1998 are satisfied within RCC-E or the quality management systems that apply to C&I,

6 **T14.TO2.06** - The designer or future operator/licensee is requested to address the following observations which have arisen from the review of the CAE for SAP ESS.27 (Safety Systems - Computer-based safety systems).

a. The CAE refers to NLF-F DC 369, “Qualification of SPPA T2000 Systems”. The purpose of the document in the context of the argument is not explained.

The designer or future operator/licensee is requested to update the CAE to explain the purpose of NLF-F DC 369 in the context of the argument.

b. There is no evidence referenced from the claim and argument for processes for independent assessment of the test programme, covering the full scope of test activities.

The designer or future operator/licensee is requested to update the CAE to demonstrate that the requirements for independent assessment of the test programme are satisfied.

<u>Conclusion of Task Review</u>

Annex 4

In the opinion of the TSC, based on the sampled evidence, and subject to satisfactory resolution of the technical observations, no evidence was found to indicate that the claims and argument made for the inclusion of requirements for standards conformance within company-level processes are not supported. There is insufficient evidence to demonstrate that company-level processes define an adequate set of independent confidence building measures such as independent testing and software static analysis.

Annex 5

TSC Summary – Review of Class 1 and 2 System Platforms and Pre-Developed Complex Components[10]

Note this information has been imported from a TSC report (Ref. 30) and the formatting of the TSC report has been retained.

[10] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 5

A Annex: TSC Task Summary - Review of Class 1 and 2 System Platforms and Pre-Developed Complex Components

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of Class 1&2 System Platforms and Pre-Developed Complex Components (TSC Task 15) for the UK EPR reactor design.

This review follows on from the review of Pre-Developed Class 1 System Platforms carried out in a preliminary activity (TSC Task 5).

The aim of the review has been:

- To determine the adequacy and sufficiency of the evidence provided by the Requesting Party (EDF Energy and Areva NP, hereafter referred to as EDF and AREVA) to support claims and arguments of the application of appropriate standards and guidance to the production of the platform.

  This has included review of the evidence to support further claims and argumentation presented by EDF and AREVA relating to the conformance of specific Control & Instrumentation platforms to selected Safety Assessment Principles (SAPs). The SAPs considered relate to necessary characteristics of such platforms to fulfil C&I requirements. Eleven SAPs have been considered in the timescales of the review (EQU.1 - Qualification procedures, EDR.1 - Failure to safety, EDR.2 - Redundancy, diversity and segregation, EDR.3 - Common cause failure, ESS.1 - Requirement for safety systems, ESS.21 - Reliability, ESS.23 - Allowance for unavailability of equipment , ESS.27 - Computer based safety systems, ESR.3 - Provision of controls, ESR.5 - Standards for computer based equipment, ESS.15 - Alteration of configuration, operational logic or associated data).

- To determine from the evidence provided by the Requesting Party that the functionality and performance of the TELEPERM XS platform are adequate and sufficient for deployment in a Class 1 system through a focused review of:

  - Deterministic behaviour of the TELEPERM XS platform by considering:

    - Avoidance of internal and external interference;
    - Avoidance of concurrent interactions including asynchronous interrupts;
    - Predictability of execution and communication;
    - Fully defined states and modes of operation;
    - Static Memory Management.

  - Self Checking and Fault Management of the TELEPERM XS platform by considering:

    - Existence and definition of Memory Tests;
    - Existence and definition Processor Instruction Tests;

Annex 5

  - Detection of random hardware failures and subsequent action;
  - Detection of erroneous software behaviour and subsequent action;
  - Detection of data transmission corruption/errors and subsequent action;
  - Detection of discovery program over run and subsequent action;
  - Determination of validity of inputs.

- Gain confidence that the Requesting Party has adequate evidence to support claims and arguments of the application of appropriate standards and guidance to the production of the Non Computerised Safety System;

- Gain confidence that the methodology used for the qualification of the smart devices used in nuclear safety function is adequate.

The task has reviewed samples of platform-related evidence presented by EDF and AREVA via:

- the claims-argument-evidence table that provides the RP's basis of the demonstration of SAP conformance;

- responses to Technical Queries;

- responses to actions from meetings involving EDF and AREVA, HSE/NII and the TSC; and

- responses to technical observations raised by the preliminary activity known as Task 5, including platform-related observations in the HSE/NII Step 2 and 3 reports.

The C&I architecture has been modified significantly since the definition that was presented by EDF and AREVA in Step 3 in response to Regulatory Issue RI-UKEPR-02. The proposed addition of the Non-Computerised Safety System has resulted in reduced reliability claims for the primary (TELEPERM XS) and secondary (SPPA_T2000) protection systems (1E^{-4} pfd and 1E^{-2} pfd respectively[11]) which has been recorded in Section 2 of the attachment to EDF and AREVA letter EPR00180R. The scope of the Step 4 Task 15 review therefore covers the Teleperm XS (including the Qualified Display System) version 3.5.3, SPPA-T2000 version S5 and Non Computerised Safety System (NCSS) platforms. The scope of the review also covers smart devices as pre-developed components.

A total of 57 detailed observations resulting from the review have been raised. These technical observations have been designated TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher – 11 of these observations have been designated TO1 and 46 of these observations have been designated TO2.

By analysing the detailed observations a set of high level areas for improvement was recognised. The following sections provide details on the technical observations raised during the review.

[11] ONR note: Throughout these annexes the TSC uses the words reliability or reliabilities generically when quoting claim limits which are specified by EDF and AREVA as probability of failure on demand (pfd) figures.

Annex 5

Some Technical Observations raised during the review were subsumed by other Technical Observations or resolved before this report was issued. These Technical Observations are:

- **T15.TO2.04 has been subsumed by T15.TO2.02;**
- **T15.TO2.20, 21 & 23 have been subsumed by T15.TO2.19; and**
- **T15.TO2.56 has been resolved as a further review of the sampled evidence which was applicable to SAP EDR.2 addressed the technical observation.**

Annex 5

T15.TO2.01 - Response to Task 5 Report Observations

The TSC report *Task 5 Pre-Developed Class 1 System Platforms Review for UK EPR Reactor S.P1440.54.15, Issue 1.4* identified 38 Technical Observations which were also recorded in Technical Query TQ-EPR-571. EDF and AREVA has not provided a formal response to this TQ within the timescales of this review.

The TSC has performed a review of the 38 Technical observations and it is the opinion of the TSC that 9 of these observations have not been addressed through evidence seen during the Task 15 review.

a) EPR.T5.7 - The *ISTec report ISTec Assessment of application of tools for TELEPERM XS, ISTec - A – 1085. Rev. 0, June 2006* documents the ISTec assessment of the tools that are part of the TELEPERM XS platform. This has led to a number of points for which the designer or future operator/licensee is requested to address:

   i. Some tools were not assessed by ISTec in detail (e.g. code generators) because they were type-tested by GRS. However clauses 13 and 14.2 of IEC 60880:2006 require that the defence in depth principles should be considered in the development, selection and use of tools. For these tools the only protection provided against failures is their type testing.

      The designer or future operator/licensee is requested to justify that the qualification of these tools is adequate, and why other protections (e.g. validation of their outputs) are not considered.

   ii. The argument for the adequacy of the SPACE editor is that its output can be verified by another tool, and that it has a considerable amount of operational experience. While this could be an acceptable argument, it is only valid if it can be assured that the output is verified.

      The designer or future operator/licensee is requested to demonstrate how the output from the SPACE editor is verified when it is used in the development of specific applications as required by IEC 60880:2006, clause 14.2 (limits of applicability of tools).

   iii. Some tools were developed in accordance with internal assurance procedures. The designer or future operator/licensee is requested to justify that the internal assurance procedures meet the requirements of IEC 60880.

   iv. For several tools (e.g. hwparams, swparams), it is stated that they are only used for documentation purposes, and hence do not have a safety impact. The designer or future operator/licensee is requested to justify how documentation generated by such tools has no safety impact as required by IEC 60880, clause 14.2 (limits of applicability of tools).

   v. For some tools, it is stated that they are not suitable, or have restricted use, for verification tasks. (e.g. cpuload, netload, rediff). The designer or future operator/licensee is requested to demonstrate that tools stated as not suitable for, or have restricted use for verification tasks, are not used for such purposes as required by IEC 60880, clause 14.2 (limits of applicability of tools).

b) EPR.T5.8 - Section 6 of the *United States Nuclear Regulatory Commission Safety Evaluation by the Office of Nuclear Reactor Regulation Siemens Power Corporation Topical Report EMF-2110 (NP), "Teleperm XS: A digital Reactor Protection System" Project No. 702. Dated 5th May 2000* report identifies a number of conditions that need to be satisfied when using the TELEPERM XS in specific applications.

Annex 5

The designer or future operator/licensee is requested demonstrate that the 17 actions recorded in *Section 6.0 Plant-Specific Items* of the report *United States Nuclear Regulatory Commission Safety Evaluation by the Office of Nuclear Reactor Regulation Siemens Power Corporation Topical Report EMF-2110 (NP), "Teleperm XS: A digital Reactor Protection System" Project No. 702. Dated 5th May 2000* have been addressed for the UK EPR.

c) EPR.T5.11 - The information available to the reviewer does not describe the relationship between the safety and software lifecycles. Also, there is no description of organisational team structure and roles with respect to approvals and independence.

The designer or future operator/licensee is requested to:

1. Demonstrate that processes are in place to manage the interface and interactions of the safety and software lifecycles, and that these processes have been adhered to; and

2. Justify that the processes meet the requirements of clause 5.4 of IEC 60880, and clause 6 of IEC 61513.

d) EPR.T5.18 - Section 3.2.2 *"Integration and System Test"* of *"TELEPERM XS: A digital Reactor Protection system EMF-2110 (NP)(A) Revision 1" states the* following:

> *"The test was done using the test field with the original hardware and software of the first large TELEPERM XS application. This application was the limitation and control system for the Nuclear Power Plant in Untersweser".*

The designer or future operator/licensee is requested to justify that the testing evidence gained using the test field based on the limitation and control system for the Nuclear Power Plant in Untersweser is applicable when its use is claimed for the UK EPR.

e) EPR.T5.21 - There is insufficient information to demonstrate that requirements of clause 14 of IEC 60880 have been satisfied for qualification of the compiler as the qualification evidence only cites service history. The designer or future operator/licensee is requested to demonstrate that the compilers used for the TELEPERM XS platform are suitable for the development of Class 1 systems.

f) EPR.T5.26 - The designer or future operator/licensee is requested to demonstrate that conformance with the standard KTA 3503 satisfies the requirements of IEC 60987 for manufacturing.

g) EPR.T5.28 - With regard to the Common Position of Seven European Nuclear Regulators and Authorised Support Organisations, Revision 2007, chapter 1.1 (Safety Demonstration), there is no clear evidence provided to indicate that a Safety Plan for TELEPERM XS was produced to address topics such as:

- organisational arrangements;
- demonstration that system/software/hardware requirements satisfy safety requirements;
- independence of those undertaking the safety demonstration activities; and
- safety demonstration strategy

Annex 5

The designer or future operator/licensee is requested to demonstrate that the requirements of this chapter have been satisfied.

h) EPR.T5.31 - With regard to the Common Position of Seven European Nuclear Regulators and Authorised Support Organisations, Revision 2007, chapter 1.5 (Tools).

The designer or future operator/licensee is requested to demonstrate that faults cannot be introduced/not detected by the TELEPERM XS development and verification tools, or that adequate measures are established to detect the introduction of potential tool-introduced faults.

i) EPR.T5.34 - The information given in the TELEPERM XS documentation *TELEPERM XS: A Digital Reactor Protection System, EMF-2110 (NP)(A), Revision 1* does not present evidence in accordance with the requirements of clause 6 “System Safety Life Cycle” (and its sub-clauses) of IEC 61513:2001.

The designer or future operator/licensee is requested to demonstrate how the TELEPERM XS satisfies requirements of clause 6 “System Safety Life Cycle” (and its sub-clauses) of IEC 61513.

T15.TO1.02 - TELEPERM XS Platform - Justification for the use of Programmable Complex Electronic Components in Class 1 C&I Systems

a) The designer or future operator/licensee is requested to justify the use of programmable complex electronic components in the TELEPERM XS components that are part of Class 1 C&I systems. The justification should identify the standards, guidance and criteria that are used to demonstrate that the components are fit for purpose, and the evidence of their application. Note: a provisional development standard for programmable complex electronic components and a process for its application has been identified in EDF and AREVA letter *Response to TATS action 36-I&C5 Explanation of the Basis for the Qualification of the CEC - EPR00741N.*

b) The designer or future operator/licensee is requested to complete a Programmable Complex Electronic Component Checklist S.P1440.074.013 Issue 2.2.2 for the TELEPERM XS SVE2 and ESCC2 components.

T15.TO1.03 - TELEPERM XS Platform – Scope of Application of Programmable Complex Electronic Components/Configware Campaign

The review activity addressed EDF and AREVA’s explanation of the basis of Qualification of Programmable Complex Electronic Components. A review of EDF and AREVA letter *Response to TATS action 36-I&C5 Explanation of the Basis for the Qualification of the CEC - EPR00741N* was performed*.*

The designer or future operator/licensee is requested to ensure that the Complex Electronic Components/Configware campaign stated in EDF and AREVA letter *Response to TATS action 36-I&C5 Explanation of the Basis for the Qualification of the CEC - EPR00741N* is applied for all TELEPERM XS modules that contain such components that are being used on UK-EPR.

TELEPERM XS Platform - General Process Areas for Improvement

The review of the TELEPERM XS Platform against International Nuclear Standards highlighted several areas for improvement that the designer or future operator/licensee is requested to address.

Annex 5

T15.TO2.05 - A TELEPERM XS IEC 60987 conformance matrix has not been made available within the timescales of the review. The designer or future operator/licensee is requested to demonstrate conformance with IEC 60987. This demonstration is to cover all TELEPERM XS hardware components that will be used on the UK EPR.

T15.TO2.06 – The Teleperm XS IEC 60880 conformance matrix for TELEPERM XS platform software has not been made available within the time scales of this review. The designer or future operator/licensee is requested to demonstrate conformance with IEC 60880.

T15.TO2.07 - The scope of static analysis to be applied to the TELEPERM XS platform software has not been defined within the timescales of this review. The designer or future operator/licensee is requested to define fully the level of static analysis to be applied to the TELEPERM XS platform software components used for the UK EPR.

T15.TO2.08 – Section 2 of the *Software Tests, TXS-4.1en, Revision A* states the following for module tests:

> *'A white-box test of a piece of software, usually performed by the implementer as a smoke test (quick test of basic functionality) and/or verification of software at the deepest level (normally inside the software development environment)'.*

From this it is understood that software development involves informal testing and debugging. However, clause 8.2.3.1 of IEC 60880:2006 requires module testing to be a formal verification activity and *Software Tests, TXS-4.1en, Revision A* suggests a degree of informality, with a lack of specific test criteria to be satisfied at this level. A Technical Query was raised concerning this but no response was received during the timescales of this review. The designer or future operator/licensee is requested to ensure evidence is produced that demonstrates that clause 8.2.3.1 of IEC 60880 is satisfied for module testing.

T15.TO2.09 - No conformance statement for TELEPERM XS platform development against the requirements of IEC 61513 has been provided in the timescales of this review. The designer or future operator/licensee is requested to demonstrate conformance with IEC 61513 for the TELEPERM XS platform development.

T15.TO2.10 - Insufficient information on the TELEPERM XS software platform aspects of installation and operation has been provided in the timescales of this review. There is an expectation from IEC 60880 clause 12 for an Installation/Commissioning Plan/Procedure to be in place for installing and commissioning a given release of the software for initial and/or modification purposes. The Installation/Commissioning Plan/Procedure should address:

1. Security processes (including any bypasses required for installation);
2. Verification processes (to check the validity/integrity of the installed software).

The designer or future operator/licensee is requested to ensure evidence on the Installation and Operational aspects of the TELEPERM XS software platform is produced in conformance with IEC 60880 clause 12.

Annex 5

T15.TO2.11 - TELEPERM XS Platform – Software Tools

The review of the TELEPERM XS platform included a review of tools used to develop the platform software and tools developed to support the production of TELEPERM XS based applications.

Insufficient information has been provided in the timescale of the review on the TELEPERM XS software development process for new software tool selection and strategy for tool upgrade and replacement.

The designer or future operator/licensee is requested to ensure evidence of process for new software tool selection and strategy for tool upgrade and replacement is available.

TELEPERM XS Platform - Requirements Management, Traceability and Document Hierarchy

The review of the TELEPERM XS platform identified several technical observations with respect to Requirements Management, Requirements Traceability and Documentation Hierarchy.

EDF and AREVA presented a current process improvement programme which addresses Requirements Management, Requirements Traceability and Documentation Hierarchy.

T15.TO2.12 - TELEPERM XS safety requirements should be explicitly identified and provide clear traceability to the tests and test results that demonstrate that they have been met. The designer or future operator/licensee is requested to ensure a process is implemented on the UK-EPR which manages safety requirements and their traceability to test case/procedure and test results. The designer or future operator/licensee is also requested to demonstrate adequacy of the process.

T15.TO2.13 - A TELEPERM XS Platform requirement specification should be produced from which hardware and software requirements can be derived. The designer or future operator/licensee is requested to ensure a process is implemented on the UK-EPR that identifies the production of a Requirements Specification from which hardware and software requirements can be derived. The designer or future operator/licensee is also requested to demonstrate adequacy of the process.

T15.TO2.14 - There is area for improvement in the traceability from TELEPERM XS Platform requirements to test case/procedure to test results. The designer or future operator/licensee is requested to ensure a process is implemented on the UK-EPR to manage requirements and their traceability to test case/procedure and test results. The designer or future operator/licensee is also requested to demonstrate adequacy of the process.

T15.TO2.15 - There should be clear traceability from requirements into all levels of test, specifically to TELEPERM XS Platform Integration Tests. The designer or future operator/licensee is requested to ensure a process is implemented on the UK-EPR to manage requirements and their traceability to TELEPERM XS Platform Integration test case/procedure and test results. The designer or future operator/licensee is also requested to demonstrate adequacy of the process.

T15.TO2.16 - All documents used as inputs to platform test activities should be clearly identified within the documentation hierarchy and also in the applicable quality plans. The designer or future operator/licensee is requested to ensure a process is implemented on the UK-EPR to manage requirements and a definition of the documentation hierarchy that demonstrate requirements traceability through the Teleperm XS lifecycle data. The designer or future operator/licensee is also requested to demonstrate adequacy of the process.

Annex 5

T15.TO2.17 - TELEPERM XS Platform - Use of Formal Methods to Identify Failure Modes

IEC 60987:2007 clause 5.3 has an expectation that Mean Time Between Failure for revealed and un-revealed failures are specified as system platform requirements. The reviewed TELEPERM XS components user manuals *(Teleperm XS User Manual SPAM1 Programmable analogue signal processing module (6FK5327-8AA00) TXS-2601-76-V1.1 and Teleperm XS User Manual SVE2 processing module (6FK5206-8AA/-8AE/-8BA/-8BE) TXS-1020-76-V3.0)* present Failure In Time and make a claim that the Failure In Time values are based on comparable components.

The designer or future operator/licensee is requested to:

- Justify how Failure In Time relates to Mean Time Between Failure for revealed and un-revealed failures;

- Justify how Failure In Time values can be based on Failure In Time values of comparable products.

T15.TO1.18 - TELEPERM XS Platform - Role of the External Independent Assessor in Software Production Excellence and Independence Confidence Building Measures

EDF document *RI-UKEPR-002 Answer to Action A1.5 – Production Excellence and Independent Confidence Building for EPR UK safety I&C, ENSECC090137 Revision B* section 3.1 identifies that the external independent assessment of the TELEPERM XS platform software is part of their Independent Confidence Building Measures. However during the review meetings on 3, 4 & 5 Aug and 30th Sept 2010 it was indicated that parts of the External Independent Assessor's activities were being used as part of the platform software Production Excellence argument, specifically:

- Managerial Independence of Verification activity (IEC 60880 clause 8.1.2);

- Independence of Developers and Verifiers (IEC 60880 clause 8.1.1);

- The timing of the independent verification activities within the overall software development lifecycle (production excellence) as presented in Figure 3 of IEC 60880 (IEC 60880 clause 8.1.12 & 8.1.13).

The designer or future operator/licensee is requested to:

1. Clearly identify the role of the External Independent Assessor as being part of Software Production Excellence or Software Independent Confidence Building Measures (it cannot meet the needs of both);

2. If the role of the External Independent Assessor is identified as part of the Software Independent Confidence Building Measures then the designer or future operator/licensee is requested to:

    a. Identify compensating measures to fulfil the requirements of IEC 60880 clauses 8.1.1, 8.1.2, 8.1.12 & 8.1.13;

    b. Investigate the reasonable practicality of enhancing the current software verification process for new and modified software so that it meets the requirements of IEC 60880 clauses

Annex 5

8.1.1, 8.1.2, 8.1.12 & 8.1.13 or provide justification that the existing arrangements meet the requirements of IEC 60880 clauses 8.1.1, 8.1.2, 8.1.12 & 8.1.13.

T15.TO1.19 - TELEPERM XS Platform - Role of the External Independent Assessor in Hardware Development and Verification Activities

EDF document *RI-UKEPR-002 Answer to Action A1.5 – Production Excellence and Independent Confidence Building for EPR UK safety I&C, ENSECC090137 Revision B* section 3.1 identifies that the external independent assessment of the TELEPERM XS platform hardware is part of their Independent Confidence Building Measures. However during the review meetings on 3, 4 & 5 Aug and 30th Sept 2010 it was indicated that parts of the External Independent Assessor's activities were being used as part of the platform hardware development and verification argument, specifically:

- Independence of Verification activity (IEC 60987 clause 7.3.1);
- Timing of verification activities (IEC 60987 clause 7.1.1).

The designer or future operator/licensee is requested to:

1 Clearly identify the role of the External Independent Assessor as being part of hardware development and verification or hardware independent assessment (it cannot meet the needs of both);

2 If the role of the External Independent Assessor is identified as part of the hardware independent assessment then the designer or future operator/licensee is requested to:

  a Identify compensating measures to fulfil the requirements of IEC 60987 clauses 7.1.1 & 7.3.1;

  b Investigate the reasonable practicality of enhancing the current hardware verification process for new and modified software so that it meets the requirements of IEC 60987 clauses 7.1.1 & 7.3.1.

TELEPERM XS Platform - Software Module and Integration Test Independence

T15.TO2.22 - TELEPERM XS platform Software Module and Integration Test independence does not meet the objectives of IEC 60880 clause 8.1.2 i.e. they may be in the same team, therefore not managerially independent. The designer or future operator/licensee is requested to justify that the current arrangements for the Software Production Excellence Verification and Validation activities meet the requirements of IEC 60880 clause 8.1.2. If this is not achievable the designer or future operator/licensee is requested to identify appropriate compensating measures.

TELEPERM XS Platform - Systematic Formal Checks of Hardware Lifecycle Data Items

T15.TO2.24 - Areva documents *Summary Qualification Report for SVE2 - 8BA/BE and SBU1/SKO1 - 8BA, NLTCG/2007/en/0039, Rev C, TXS-PrÜfspezifikation: TypprÜfung der FUTIS I/O Komponenten SAI, SAO, SDI, SDO, SGPIO. NGLTD/2005/de/0230 Rev A,* and *Documentation of theoretical and practical testing according to KTA 3503 of the Overvoltage barrier modules SOBx-y, ID-No's 6FK5325-8AA01 … -8AA05 from the system TELEPERM XS of the company AREVA NP GmbH, TÜV Rheinland, 968/K 138.00/06* identify the hardware lifecycle documents subject to theoretical test by Technischer

Annex 5

Überwachungsverein, and a general statement is made in these reports about whether each document is as expected or not. The documents identified are consistent to those required by *Safety Standards of the Nuclear Safety Standards Commission (KTA) - Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System - KTA 3503 (11/2005)* however it is not possible to determine if all lifecycle data has been subject to systematic formal checks. The designer or future operator/licensee is requested to ensure systematic formal checks have been applied to all hardware lifecycle data items. If this is not achievable the designer or future operator/licensee is requested to identify appropriate compensating measures.

TELEPERM XS Platform – Review Approach and Criteria of the Independent Assessor

T15.TO2.25 - The Technischer Überwachungsverein test type reports for TELEPERM XS components indicate that reviews were performed but no details on how reviews were conducted and the criteria used for review are identified. The designer or future operator/licensee is requested to justify and make available details of Technischer Überwachungsverein's review approach and criteria.

TELEPERM XS Platform - Claims Made Against the Use of KTA3503

During the review Hardware Qualification was addressed. TELEPERM XS Platform hardware components are qualified against German Nuclear standard *Safety Standards of the Nuclear Safety Standards Commission (KTA) - Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System - KTA 3503 (11/2005)*, however it was noted that inappropriate claims were being made against the standard with respect to its scope and its application of IEC 60780.

T15.TO2.26 - *Safety Standards of the Nuclear Safety Standards Commission (KTA) - Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System - KTA 3503 (11/2005)* only refers to IEC 60780 as informative and does not directly respond to it, so no claim can be made that IEC 60780 has been applied. The designer or future operator/licensee is requested not to quote *Safety Standards of the Nuclear Safety Standards Commission (KTA) - Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System - KTA 3503 (11/2005)* in response to making claims against IEC 60780 unless this is appropriately justified.

T15.TO2.27 - *Safety Standards of the Nuclear Safety Standards Commission (KTA) - Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System - KTA 3503 (11/2005)* is a standard for performing Type Testing and is not a standard covering the full development lifecycle, so no claim against Areva's full hardware development lifecycle can be made by citing *Safety Standards of the Nuclear Safety Standards Commission (KTA) - Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System - KTA 3503 (11/2005)*. The designer or future operator/licensee is requested not to quote *Safety Standards of the Nuclear Safety Standards Commission (KTA) - Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System - KTA 3503 (11/2005)* in response to claims made against the full development lifecycle of the TELEPERM XS unless this is appropriately justified.

TELEPERM XS Platform - Qualification

During the review Hardware Qualification of the TELEPERM XS was addressed and several technical observations were made.

Annex 5

T15.TO2.28 - Review of EDF and AREVA documents *Compliance of the TXS Hardware Design and Engineering Process with IEC60987 Ed 2 NLTC-G/2008/en/0053, Revision A* and *Overview of approach for TXS hardware qualification NLTC-G/2007/en/0072, Revision A* provided no information how Qualified Target Life (as identified in IEC 60987 clause 6.2.5) is addressed for the TELEPERM XS platform hardware. The designer or future operator/licensee is requested to demonstrate that their hardware qualification process addresses Qualified Life.

T15.TO2.29 - From the evidence sampled no evidence could be found that specified the Qualified Life (as required by IEC 60780 Section 4) for the TELEPERM XS platform hardware. The designer or future operator/licensee is requested to demonstrate that the hardware qualification process addresses Qualified Life.

T15.TO2.30 - EDF and AREVA use a standard approach to equipment qualification that is presented in document *Teleperm XS General Specification for Equipment Qualification of I&C Components of Class 1E for mild environment NLTD-G/2008/en/0229 Rev C*. A review of Summary Qualification Reports provided for components SVE2, SOB and SDIx (*Summary Qualification Report for SVE2 - 8BA/BE and SBU1/SKO1 -8BA, NLTCG/2007/en/0039 Rev C, Summary Qualification Report: Qualification of the Overvoltage Barrier Modules SOB1-24, SOB1-48, SOB2-24, SOB2-48, SOB3 and SOB31-24. NLTC-G/2007/en/0014, Rev A and Summary Qualification Report for the binary input modules SDI1-24, SDI2-24, SDI1-48 and binary output modules SDO1-24, SDO1-48, NLTC-G/2007/en/0028, Rev B respectively*) could not determine if this standard approach has been applied. For UK-EPR the designer or future operator/licensee is requested to justify that an adequate qualification process has been applied to the applicable TELEPERM XS components.

T15.TO2.31 - The standard approach to equipment qualification that is presented in document *Teleperm XS General Specification for Equipment Qualification of I&C Components of Class 1E for mild environment NLTD-G/2008/en/0229 Rev C* provides no guidance on Pre-Ageing as identified in IEC 60780 Clause 5.3.3. The designer or future operator/licensee is requested to ensure the hardware qualification process addresses Pre-Ageing.

T15.TO2.32 - The Summary Qualification Reports provided for SVE2, SOB and SDIx (*Summary Qualification Report for SVE2 - 8BA/BE and SBU1/SKO1 -8BA, NLTCG/2007/en/0039 Rev C, Summary Qualification Report: Qualification of the Overvoltage Barrier Modules SOB1-24, SOB1-48, SOB2-24, SOB2-48, SOB3 and SOB31-24. NLTC-G/2007/en/0014, Rev A and Summary Qualification Report for the binary input modules SDI1-24, SDI2-24, SDI1-48 and binary output modules SDO1-24, SDO1-48, NLTC-G/2007/en/0028, Rev B respectively*) do not appear to identify if pre-ageing as identified in IEC 60780 Clause 5.3.3 has been addressed or justification provided as to why pre-aging is not appropriate. The designer or future operator/licensee is requested to demonstrate that Pre-Aging has been applied prior to the qualification of parts of the TELEPERM XS platform where it is appropriate.

TELEPERM XS Platform - Frequency of Reporting of Self Test Results

As part of the review activity a deep sampling of evidence specific to TELEPERM XS Platform self test was performed and several technical observations relating to self test were made.

T15.TO2.33 - The designer or future operator/licensee is requested to demonstrate that the frequency of the TELEPERM XS memory checks are performed at a sufficient rate to detect and report memory failures in a timely manner.

Annex 5

T15.TO2.34 - The designer or future operator/licensee is requested to demonstrate that for TELEPERM XS on a cycle overrun, the fault condition is communicated in a manner that allows appropriate corrective/mitigating actions to be performed.

T15.TO2.35 - The designer or future operator/licensee is requested to demonstrate that for TELEPERM XS on failure to complete self test, the fault condition is communicated in a manner that allows appropriate corrective/mitigating actions to be performed.

T15.TO2.36 - TELEPERM XS Platform – Estimation of Processor Utilisation

As part of the review, determining the processor utilisation of TELEPERM XS platform software was considered. Although evidence exists to demonstrate that processor utilisation of the TELEPERM XS platform software has been measured using specialist TELEPERM XS platform tools, no evidence had been provided reporting the timescales of this review to demonstrate that worst case timing scenarios had been used.

For TELEPERM XS the designer or future operator/licensee is requested to demonstrate that worst case timing scenarios have been used when determining processor utilisation of the TELEPERM XS platform software.

T15.TO2.37 - TELEPERM XS Platform – Fault and Change Management

During the review activity, the Fault and Change Management System applied to the TELEPERM XS Platform was reviewed. The TELEPERM XS Platform Fault/Change Management activities are controlled using the open source tool “Request Tracker” that enforces a Fault/Change Management Lifecycle and its use and application appears appropriate. However there is no detailed documented approach to Fault/Change Management which will allow each phase of the Fault/Change Management Lifecycle to be performed in a consistent and repeatable way.

The designer or future operator/licensee is requested to ensure a detailed TELEPERM XS Platform Fault/Change Management process that can be applied consistently and in a repeatable way is implemented, and which should also include a systematic approach to impact analysis and regression testing.

T15.TO1.38 - SPPA T2000 Platform – Adequacy of Testing and Test Evidence

EDF and AREVA have indicated (in response to Technical Query TQ-EPR-1133) that EDF, Areva and Siemens are issuing a report describing the strategy, principles and coverage of the tests performed for AS620B Automation System and particularly for the System Software due to concerns raised by Autorité Sûreté Nucléaire (French Nuclear Safety Authority).

The designer or future operator/licensee is requested ensure the areas for improvement identified in the report are addressed and ensure the requirements for production excellence of a Class 2 system (at the integrity level used for the UK-EPR) have been met.

T15.TO1.39 - SPPA T2000 Platform - Evidence on the Application of IEC 60987

Evidence on the application of IEC 60987 (including IEC 60780) to SPPA-T2000 hardware development has not been provided within the timescales of this review. The designer or future

Annex 5

operator/licensee is requested to demonstrate conformance with IEC 60987 (including IEC 60780) for SPPA-T2000 hardware development for existing hardware and any newly developed hardware.

SPPA T2000 Platform - Production Excellence

The sample based review of the SPPA T2000 platform identified several areas for improvement on production excellence:

T15.TO2.40 - SPPA-T2000 hardware development process or lifecycle data was not provided in the timescales of this review. The designer or future operator/licensee is requested to justify the adequacy of the SPPA-T2000 hardware development process and lifecycle data.

T15.TO2.41 - SPPA-T2000 Qualification does not address or justify the omission of Accident Radiation, Accident Thermodynamics and Post Accident Conditions tests. The designer or future operator/licensee is requested to ensure that test coverage includes such tests or justify why they are not applicable.

T15.TO2.42 - The SPPA-T2000 Production Excellence strategy has been provided in *UKEPR EPR control and instrumentation (C&I) Actions from Level 4/Level 3 meeting in response to action 33-I&C-6 Letter ND(NII) EPR 00609N*. This production excellence strategy identifies a pre-developed software process review and also states that it has not been performed. The designer or future operator/licensee is requested to perform this review for the UK-EPR.

T15.TO2.43 - The *FA3 standard instrumentation and control system qualification synthesis evaluation report PELL-F DC 52 Rev A* identified a number of test failures. The designer or future operator/licensee is requested to demonstrate/confirm that the modifications made to address these failures are included in the UK-EPR build standard and that the tests on the new UK-EPR standard will be conducted in accordance with IEC61513.

T15.TO2.44 - The IEC 61513 conformance statement presented in section 4 of *IEC 61513 and 62138 justification for SAS, Siemens Energy Sector Document DN 2.2.24 Version 3.0 BP* appears to present a combined conformance statement for the SPPA-T2000 platform and the SAS Application which doesn't clearly differentiate between the two. The designer or future operator/licensee is requested to provide IEC 61513 conformance evidence that clearly differentiates between the SPPA-T2000 platform and Safety Automation System application.

SPPA T2000 Platform – Changing from Version S5

T15.TO1.45 SPPA T2000 - Changing from Version S5

The review of the SPPA-T2000 platform was performed on version S5; however it is believed that an alternative version may be used for UK-EPR.

Should an alternative version of the SPPA-T2000 platform be used for UK-EPR, the designer or future operator/licensee is requested to produce the following:

- A formal change proposal to modify the UK EPR baseline to the alternative version of SPPA-T2000;
- A Basis of Safety Case that as a minimum addresses:

Annex 5

- How the designer or future operator/licensee will assure at least the same level of platform reliability as that achieved by version S5;
- A comprehensive impact assessment of the delta between SPPA-T2000 S5 and the alternative version on the rest of the C&I architecture.

Review of other Platforms

T15.TO1.46 - Basis of Safety Case for Non Computerised Safety System Platform

Evidence on standards, guidance and criteria that are to be used to demonstrate that the Non Computerised Safety System platform is fit for purpose has not been provided within the timescales of this review.

The designer or future operator/licensee is requested to produce a Basis of Safety Case to demonstrate the adequacy of the safety of the platform used for Non Computerised Safety System.

T15.TO1.47 - Basis of Safety Case for Qualified Display System Platform

Evidence on standards, guidance and criteria that are to be used to demonstrate that the Qualified Display System platform is fit for purpose has not been provided within the timescales of this review.

The designer or future operator/licensee is requested to supply a Basis of Safety Case to demonstrate the adequacy of the safety of the Qualified Display System platform.

T15.TO1.48 - Qualification Method for Smart Devices

It was planned to review EDF and AREVA's position paper that describes the process used for qualification of the smart devices with a reliability claim of 10^{-2} pfd and which also defines complementary measures to be considered for the qualification process of smart devices with a reliability claim of 10^{-3} pfd. However the position paper was not provided by EDF and AREVA within the timescales of this review.

The designer or future operator/licensee is requested to define the methodology used for the qualification of the smart devices used in nuclear safety functions.

Claims Argument Evidence

A review of the TELEPERM XS and SPPA T2000 evidence which had been identified as part of the Claims Argument Evidence that demonstrates satisfaction of the Safety Assessment Principles was performed. The primary aim of the review was to determine if the evidence cited in *Claims-Argument-Evidences trail for satisfaction of SAPs relevant to I&C PELL-F DC 9 Rev C* supported the claims and arguments.

The following technical observations were made:

T15.TO2.49 - For SAP EDR.1 *Self Test Coverage Analysis SIE QU633 version 7* does not present a system level reliability study for the T2000 platform which is requested to support the fail safe argument. The reliability study is presented in *Reliability Analysis SPPA-T2000 SIE QU627 revision 4.0*. The designer or future operator/licensee is requested to cite the *Reliability Analysis SPPA-T2000*

Annex 5

SIE QU627 revision 4.0 in the version of the claims-argument-evidence that is referenced from the UK EPR pre-construction safety report.

T15.TO2.50 - For SAP EDR.1 the Failure Modes and Effects Analysis for the SDI1-24 Digital Input Module Report (*SDIx Failure Mode and effect analysis (FMEA) NLTCG2008EN1013 Rev B*) as used in the TELEPERM XS shows that there are a number of potential failures that cannot be detected. The designer or future operator/licensee is requested to demonstrate that this level of risk is acceptable.

T15.TO2.51- For SAP EDR.3 the TELEPERM XS Probabilistic Safety Analysis should be referenced by the *Claims-Argument-Evidences trail for satisfaction of SAPs relevant to I&C PELL-F DC 9 Rev C*; The designer or future operator/licensee is requested to include this reference for this SAP in the version of the claims-argument-evidence that is referenced from the UK EPR pre-construction safety report.

T15.TO2.52 - For SAP ESS.23 *Chapter 18.2.4 of the Pre Construction Safety Report PRINCIPLES OF NORMAL OPERATION - Core Unloading* is cited as evidence; this doesn not appear relevant to this SAP. The designer or future operator/licensee is requested to explain the relevance of this reference to this SAP.

T15.TO2.53 - For SAP ESS.27 the evidence *Test Certificate - TXSDRVGEN-0707-02* is cited. The designer or future operator/licensee is requested to update the Claims, Argument and Evidence trail to clarify the purpose of this evidence.

T15.TO2.54 - For SAP EDR.3 the evidence *Protection System, Reliability and availability study NEPS-F DC 29* is cited however it is understood that this document will be superseded by Failure Mode Effects Analysis calculations. The designer or future operator/licensee is requested to update the Claims, Argument and Evidence trail for this SAP to ensure it refers to the document.

T15.TO1.55 - For SAP EDR.2 the cited evidence *SPPA-T2000 reliability analysis for the T2000 SIE QU627 revision 4.0* platform is only hardware based and does not take into account systematic software failure of the platform software. The designer or future operator/licensee is requested to include systematic software failure in the SPPA-T2000 reliability analysis for UK-EPR.

T15.TO2.57 - For SAP EDR.3 the cited evidence *Common Cause Failure Analysis of FA3 I&C Architecture H-P1A-2007-02803-FR May 2009* Section 1 states that the method is qualitative in nature. However it is understood that the results of the CCF analysis are used as inputs to reliability calculations. The designer or future operator/licensee is requested to justify how the results of a qualitative CCF analysis can be used in reliability calculations.

T15.TO2.58 - For SAP EDR.3 the cited evidence *Analysis of the digital CCF within systems supporting F1A safety-class functions (PS) in the instrumentation & control architecture of the FA3 EPR, ENSECC080054 Rev A1* does not address the potential for CCF within TELEPERM XS itself. Although the shared use of software is addressed, there is no discussion on the potential for digital hardware components as a source of CCF. The designer or future operator/licensee is requested to review the potential for CCF of digital hardware components within TELEPERM XS platform itself, and include the evidence in the Claims, Argument and Evidence trail.

T15.TO2.59 - For SAP ESS.27 the response to TATS action 33 I&C 6 which is recorded in *Appendix 1 Production Excellence and Independent Confidence Building Measures strategy for systems supporing F1B function* of EDF and AREVA letter *EPR00609N* should be cited as evidence of Design Production

Annex 5

Excellence for pre-existing T2000 software. The designer or future operator/licensee is requested to update the Claims, Argument and Evidence trail for this SAP as appropriate.

T15.TO2.60 - For SAP ESS.27 and ESR.5 the software re-use argument presented in *IEC 61513 and 62138 justification for SAS, Siemens Energy Sector Document DN 2.2.24 Version 3.0 BPE* should address all class 2 hardware components of the SPPA-T2000 platform that contain dedicated devices with embedded software, or if no such software exists a positive statement saying so should be made. The designer or future operator/licensee is requested to update the Claims, Argument and Evidence trail for this SAP as appropriate.

T15.TO2.61 - For SAP ESS.15 The argument in the Claims Argument Evidence Trail presents the principles for the security procedures that will be used to control access to the SPPA Engineering System. However no argument is presented regarding measures to ensure that the Engineering System cannot cause unintended interference with the class 2 Safety Automation System during plant operation. The designer or future operator/licensee is requested to implement measures that ensure the Engineering System cannot cause unintended interference with the class 2 Safety Automation System during plant operation.

T15.TO2.62 – Some Failure Modes and Effects Analysis for TELEPERM XS components have been provided e.g. *Failure modes, failure effect and failure detection SVE2, NLTC-G/2008/en/1010* and *SDIx Failure Mode and effect analysis (FMEA) NLTCG2008EN1013 Rev B*. The designer or future operator/licensee is requested to include Failure Modes and Effects Analysis for all TELEPERM XS components applicable to the UK-EPR in the CAE trail.

Review of the actions identified in United States Nuclear Regulatory Commission Safety Evaluation Report “Teleperm XS: A digital Reactor Protection System”

The TSC Task 15 review considered the observation raised in paragraph 39 of the *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.* Paragraph 39 states:

> *“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.”*

The report *United States Nuclear Regulatory Commission Safety Evaluation by the Office of Nuclear Reactor Regulation Siemens Power Corporation Topical Report EMF-2110 (NP), “Teleperm XS: A digital Reactor Protection System” Project No. 702. Dated 5th May 2000* identifies 17 actions, 4 of which (1, 12, 13 and 17) have been investigated during this review as they aligned with some of the review activities performed under TSC Task 15. The remaining 13 actions have been reviewed by other TSC tasks. The review identified 8 TSC Task 15 technical observations that relate to the 4 Nuclear Regulatory Commission actions. The associated TSC Task 15 observations are:

- T15.TO2.12;
- T15.TO2.13;
- T15.TO2.14;

Annex 5

- T15.TO2.30;
- T15.TO2.31;
- T15.TO2.32;
- T15.TO2.33;
- T15.TO2.58.

In conclusion it is the opinion of the TSC that from the evidence sampled that:

For the TELEPERM XS platform version 3.5.3:

- The review performed to determine the adequacy and sufficiency of the samples of evidence provided by the Requesting Party to support claims and arguments of the application of appropriate standards and guidance to the production of the platform identified four major areas for improvement regarding:
  - Justification for the use of Programmable Complex Electronic Components in TELEPERM XS modules for deployment in Class 1 C&I Systems;
  - Role of the External Independent Assessor in Software Production Excellence and Independence Confidence Building Measures;
  - Role of the External Independent Assessor in Hardware Development and Verification Activities;
  - Provision of a Basis of Safety Case for Qualified Display System Platform.
- The review performed to determine from the samples of the evidence provided by the Requesting Party that the functionality and performance of the TELEPERM XS platform are adequate and sufficient for deployment in a Class 1 system (through a focused review of Deterministic Behaviour, Self Checking and Fault Management) identified no major areas of improvement.

From the evidence sampled and subject to successful resolution of all technical observations related to the TELEPERM XS platform no evidence was found to indicate that the TELEPERM XS platform version 3.5.3 is not adequate and sufficient for deployment in a Class 1 system.

For the SPPA-T2000 version S5:

- The review performed to determine the adequacy and sufficiency of the samples of evidence provided by the Requesting Party to support claims and arguments of the application of appropriate standards and guidance to the production of the platform identified three major areas for improvement regarding:
  - Adequacy of Testing and Test Evidence;
  - Evidence of the application of IEC 60987 to hardware development of the SPPA-T2000;
  - Potential change from SPPA-T2000 version S5 for UK EPR.

From the evidence sampled and subject to successful resolution of all technical observations related to the SPPA-T2000 platform no evidence was found to indicate that the SPPA-T2000 platform version S5 is not adequate and sufficient for deployment in a Class 2 system. However it should be noted that

Annex 5

should a different version of SPPA-T2000 be used on UK EPR then the designer or future operator/licensee is requested to demonstrate that the selected version is adequate and sufficient for deployment in a Class 2 system.

For the NCSS only the functional and safety requirements and diversity criteria were available during the timescales of the review and these were addressed by TSC Task 20 that reviewed the responses to Regulatory Issue RI-UKEPR-002 actions A1.2 and A1.3. No opinion on the NCSS platform can be formed until the standards, guidance and criteria used for platform production have been demonstrated as adequate and sufficient for deployment in a Class 2 system.

For Smart Devices, no opinion can be formed until details of the methodology used for the qualification of the smart devices used in safety functions has been provided and reviewed.

Annex 6

TSC Summary – Review of C&I Safety and Safety-Related Systems[12]

Note this information has been imported from a TSC report (Ref. 31) and the formatting of the TSC report has been retained.

[12] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 6

A Annex: TSC Task Summary - Review of C&I Safety and Safety-Related Systems

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of Safety and Safety-Related Systems for UK EPR for the UK EPR reactor design.

This review follows on from the review of process-related claims and argumentation carried out in a preliminary activity (TSC Task 6). The aim of the review has been to gain confidence that the Requesting Party (Electricité de France SA and Areva NP SAS, hereafter referred to as "EDF and AREVA") have adequate evidence to demonstrate that appropriate standards have been conformed to in the development of Safety and Safety-Related Systems for UK EPR, and the principles of production excellence and independent confidence building measures have been applied in the development of the software in Class 1 systems. This has included a review of samples of the evidence to support further claims and argumentation presented by EDF and AREVA relating to relevant Safety Assessment Principles (SAPs) and international nuclear standards. Due cognisance has been taken of selected Technical Assessment Guides (TAGs).

The task has also reviewed samples of the evidence presented by EDF and AREVA via:

- the claims-argument-evidence table that provides the RP's basis of the demonstration of SAP conformance;
- responses to Technical Queries;
- responses to actions from meetings involving EDF and AREVA, HSE/NII and the TSC
- and responses to technical observations raised during the preliminary activity, including system-related observations in the HSE/NII GDA Step 2 and 3 reports.

The systems that were originally within the scope of the task were the Protection System (PS), the Safety Information and Control System (SICS), the Safety Automation System (SAS) and the Process Automation System (PAS). One further system was added to the architecture as part of the response to Regulatory Issue RI-UKEPR-02 – the Non-Computerised Safety System (NCSS) – but evidence relating to the safety demonstration of this system has not been presented in the timeframe of this review. The inclusion of the Qualified Display System (QDS) has been proposed for addition to the C&I architecture. However the details of the implementation of this system, including provision of a safety demonstration, through a Basis of Safety Case (Safety Plan, Safety Deliverables, Schedule and argument that demonstrates the deliverables meet the requirements of the applicable standards and SAPs), has not been presented in the timeframe of this review.

The scope of the evidence that is specific to the UK EPR is defined by EDF and AREVA in *"UK EPR CONTROL AND INSTRUMENTATION (C&I) – SCOPE OF GDA"* (letter ND (NII) EPR00686N). As some UK EPR evidence, including function block diagrams, was not available within the timeframe of this review, some of the reviews (e.g. design documents, PS function block diagrams) were based on evidence from the Flamanville 3 (FA3) C&I system. EDF and AREVA have indicated that improvements to the processes for requirements definition and traceability used in the development of FA3 have already been identified. Not all of the UK EPR evidence that has been declared in scope and was to be considered within the selected sample has been provided within the timescale of this review.

The observations in the HSE/NII reports for GDA Steps 2 and 3 have been apportioned for review to tasks 14 through 18.

Annex 6

Of the 7 observations in the Step 2 report that were apportioned to this task, 1 is considered by the TSC to be resolved. Some progress has been made on the other 6 observations. Outstanding points are covered by the following Technical Observations (TOs) and potential GDA Issue (pGI) which have been raised in relation to them: T16.TO1.02, T16.TO1.03, T16.TO2.18, T16.TO2.22, T16.TO2.26, pGI-UKEPR-C&I.07.02[13]. The original Step 2 observations are adequately addressed by these TOs and pGI.

Only one observation of the Step 3 report (in paragraph 39) was apportioned to this task. It states that the actions identified in the safety evaluation report produced by United States Nuclear Regulatory Commission (US NRC) will be considered during the Step 4 assessment. The Task 16 review of samples of the evidence provided by EDF and AREVA has led to the following conclusions for these US NRC actions:

- **Action 2**: Verification and Validation, and configuration management activities have been considered as part of the Task 16 review. Further evidence is needed to demonstrate that the activities are conformant to nuclear standards (See T16.TO1.01). Based on the sampled evidence reviewed there are some areas for improvement with V&V activities (See T16.TO2.19). Based on the sampled evidence, no areas for improvement have been identified with system configuration management activities.

- **Action 9**: The Fault Schedule (PEPR-F DC 4 B) includes a worksheet which shows which functions reduce the risk from anticipated transients without scram (ATWS). However, it does not identify diverse means for providing the protection (See T16.TO2.21).

- **Action 17**: EDF and AREVA has improved the process for managing traceability data. However, a method document that defines how traceability data is managed has yet to be produced (T16.TO2.15).

The original Step 3 actions are adequately addressed by the referenced TOs.

Regarding standards conformance, selected IEC standards have provided a reference for this part of the review. For the PS, EDF and AREVA has committed to provide analyses which demonstrate compliance with specific IEC standards (i.e. General Requirements for Systems IEC 61513:2001, Class 1 and 2 Hardware Requirements for Computer Based Systems IEC 60987:2007 and Software Requirements for Systems Performing Category A Functions IEC 60880:2006) but the delivery dates are too late for consideration in this review (see T16.TO1.01). In the absence of such analyses, samples of other project evidence, such as quality plans have been reviewed against the requirements of the standards. Based on the evidence sampled, no major areas for improvement in standards conformance for the Protection System have been identified. However a number of detailed technical observations have been raised.

Regarding independent confidence building measures (as specified in ESS.27), for the PS software, quality assessments of system documents are performed by EDF independent units (e.g. SEPTEN and CEIDRE). Also, on-site commissioning tests that exercise all C&I equipment and systems are to be carried out by EDF and AREVA. Additionally, EDF and AREVA has committed to:

[13] ND note: GI-UKEPR-CI-06.A2 is the issued version of the provisional GDA Issue (pGI).

Annex 6

- produce a feasibility study on static analysis of the UK EPR Protection System software, and the qualification of the TELEPERM XS development tools, including the automatic code generator and C compiler and
- carry out a minimum of 5000 tests on the TELELEPRM XS PS Test Division, and to carry out a review of the reasonable practicability of carrying out additional tests (up to 50,000) within the PS implementation programme. Research will be undertaken into the feasibility of implementing statistical testing on simulation of the PS using the simulator (SIVAT).

For the SAS and PAS the evidence for compliance with IEC 61513:2001 and IEC 62138:2004 was presented through various quality plans. Based on the evidence sampled, no major areas for improvement in standards conformance for the SAS and PAS have been identified. However a number of detailed technical observations have been raised with respect to identification of evidence to substantiate the compliance claims. EDF and AREVA has committed to provide an analysis which demonstrates compliance with IEC 60987:2007 but have declared this to be out of scope of GDA.

Regarding demonstration of compliance with the selected SAPs via the claims-argument-evidence information, no major areas for improvement have been identified. However a number of detailed technical observations have been raised.

A total of 34 technical observations have been raised from this review. These technical observations have been designated TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher – 3 of these have been designated TO1 and the remainder have been designated TO2.

The TO1 technical observations are:

1. **T16.TO1.01** - The designer or future operator/licensee is requested to demonstrate that the processes to develop the Protection System (PS) are compliant with:

   - IEC 61513:2001
   - IEC 60880:2006
   - IEC 60987:2007

   Regarding IEC 61513: 2001, it is noted that table 7 of the System Quality Plan (SQP) (NLE-F DM 10007, Revision D) provides a top level mapping between clauses in the standard and process steps defined by the SQP. Although informative, it does not provide sufficient detail to confirm that all aspects of each clause, as specified by detailed sub-clauses, are satisfied. The designer or future operator/licensee is requested therefore to ensure that the analysis addresses the detailed sub-clauses.

2. **T16.TO1.02** - The designer or future operator/licensee is requested to demonstrate the safety of the Non-Computerised Safety System, through a Basis of Safety Case (Safety Plan, Safety Deliverables, Schedule and argument that demonstrates the deliverables meet the requirements of the applicable standards and SAPs), to include evidence that the processes to develop the equipment will be compliant with appropriate standards including:

   - IEC 61513:2001

Annex 6

- IEC 60987:2007

3. **T16.TO1.03** - The designer or future operator/licensee is requested to demonstrate the safety of the Class 1 displays, through a Basis of Safety Case (Safety Plan, Safety Deliverables, Schedule and argument that demonstrates the deliverables meet the requirements of the applicable standards and SAPs), to include evidence that the processes to develop the application and the equipment will be compliant with appropriate standards such as:

   - IEC 61513:2001
   - IEC 60880:2006
   - IEC 60987:2007

The TO2 technical observations applicable to the Protection System are:

1. **T16.TO2.10** - Table 2 of the SQP (NLE-F DM 10007, Issue D) defines the engineering documents that are to be produced. The scoping letter (Scope of UK EPR Instrumentation & Control Design for GDA, ND (NII) EPR00686N, 22 December 2010) states the development phase 'System Specification' is within scope of GDA. However, the following documents which are produced by that phase have not been provided:

   - D-01.3: Master Test Plan
   - D-01.4: Protection System - System Requirements Specification
   - D-01.5: System Qualification Plan
   - D-01.9: System Configuration Management Plan
   - D02.3: Protection System - System Functional Design Description

   The designer or future operator/licensee is requested to ensure UK EPR versions of the above documents are produced.

2. **T16.TO2.11** - In the absence of provided compliance analyses to demonstrate the satisfaction of the requirements of IEC 60987:2007 for the protection system, conformance has been considered by the review of samples of other project evidence, such as quality plans and a number of detailed points have been raised.

   The designer or future operator/licensee is requested to address the following points related to project quality plans:

   a. Clause 5.3.6 requires maintenance requirements to be specified. There is no indication in the provided evidence of how this requirement is satisfied.

   b. Clause, 5.4.4 requires that hardware requirements identify prohibited construction materials or production processes. There is no indication in the provided evidence of how this requirement is satisfied.

3. **T16.TO2.12** - Table 8 of a previous version of the quality plan (NLE-F DC 113, Issue C) identified the Method Documents which are relevant to individual process steps. Table 8 of the UK EPR

Annex 6

quality plan (NLE-F DM 10007, Issue D) only lists Method Documents but does not indicate which process step they are applicable to.

It therefore cannot be confirmed that all process steps have an associated Method Document.

The designer or future operator/licensee is requested to demonstrate that all process steps have adequate detailed procedures, which provide the necessary rules and guidelines to be followed when the process steps are being undertaken.

4. **T16.TO2.13** - Guidelines for the Verification of TELEPERM XS Application Software Items (NLE-F, DM 10022) is under development.

   The designer or future operator/licensee is requested to review this document and confirm its adequacy.

5. **T16.TO2.14** - The user manual for developing TELEPERM XS-based applications is entitled 'TELEPERM XS User Manuals, Engineering System SPACE. TXS-2100-76-V4.0'.

   The following areas for improvement have been identified in relation to this document:

   a. There is no reference to the user manual from the System Quality Plan (SQP) for TXS C&I applications (NLE-F DM 10007, Revision D). The designer or future operator/licensee is requested to demonstrate that due account is taken of the manual in the development of TELEPERM XS based applications.

   b. It is noted that the manual specifically refers to version 3.4.x of the Core Software. The Technical Support Contractor understands that the core software is at a later release (3.5.x).

      The designer or future operator/licensee is requested to demonstrate that development of UK EPR TELEPERM XS-based applications is based on a version of the TELEPERM XS User Manual which is applicable to the version of TELEPERM XS that is selected for the UK EPR.

6. **T16.TO2.15** - The process to manage traceability data from requirements through design and implementation, and to Verification and Validation (V&V) is still under development, and no traceability data has been provided for the UK EPR.

   The designer or future operator/licensee is requested to:

   a. Ensure a method document that defines how traceability data is managed is produced.

   b. Ensure evidence of comprehensive traceability from input requirements through to System Requirements, software and hardware requirements, design and implementation, and V&V evidence is produced.

7. **T16.TO2.16** - IEC 60880:2006, clause 12.4.2 requires training plans to be developed. This is not addressed by the System Quality Plan (SQP) (NLE-F DM 10007, Issue D). EDF and AREVA have stated that production of training plans is outside the scope of the SQP. The Overall C&I System Quality Plan (NLN-F DC 132, Rev A) has been inspected and this does not address Training Plans.

   The designer or future operator/licensee is requested to ensure that the requirement to produce Training Plans is in scope of an appropriate controlling document such as a quality plan.

Annex 6

8. **T16.TO2.17** - The following areas for improvement regarding the use of TELEPERM XS development and verification tools have been identified:

   a. An observation was raised as part of a preliminary activity known as Task 6 concerning the potential risk of faults being introduced through the use of TELEPERM XS tools.

      The response was, in summary, that the qualification of tools is addressed as part of the development of the TELEPERM XS platform.

      However, the response does not address the original observation, which is over how the tools are used and whether or not the development process includes measures which mitigate faults which might be introduced through their use (e.g. verification of tool outputs). So risks associated with tool usage are specific to the process used to develop applications, and the generic argument that the tools have been qualified is insufficient.

      The designer or future operator/licensee is requested to demonstrate that:

      - The way tools are used to develop and verify applications has been analysed to mitigate potential faults that might be introduced.

      - Restrictions on the way tools should be used are considered and addressed in the development process.

   b. The 'CASSIS'[14] tool is used during testing to identify discrepancies between expected and actual results, which are subsequently analysed manually. This indicates that the V&V process is dependent on the integrity of this tool.

      The designer or future operator/licensee is requested to demonstrate that the CASSIS tool is of adequate integrity for the verification of Class 1 applications.

   c. The SPYCE tool performs syntactic checks of the SPACE Database.

      The designer or future operator/licensee is requested to demonstrate that the SPYCE tool is of adequate integrity for its use in verifying the SPACE database.

9. **T16.TO2.18** – Regarding error detection and management within the Protection System, if a function block detects that one of its inputs is out of range, the output is set to an extreme value, but the corresponding fault flag is not set. Therefore when the output is used as an input to a subsequent function block it would not be aware that an error had occurred.

   The designer or future operator/licensee is requested to ensure errors are handled appropriately (e.g. errors detected inside function blocks are communicated to subsequent function blocks, and managed in subsequent function blocks.)

10. **T16.TO2.19** – The following areas for improvement have been identified regarding testing of the Protection System:

    a. Test coverage is in the form of requirements coverage. It is demonstrated within test specifications (D-03.2), which provide traceability between test cases and functions defined by document D-02.3.

       However, there is no structural coverage information to explain how the paths in the following documents are tested:

[14] ONR note: CASSIS is a Functional test coverage tool.

Annex 6

- D-21.1: I&C Function Specification
- D-22.1: Function Diagrams (i.e. Specification and Coding Environment (SPACE) Diagrams)

The designer or future operator/licensee is requested to ensure adequate structural test coverage at the function block level is recorded in an auditable form.

b. Some testing is performed using the Simulation Based Validation Tool (SIVAT). The Technical Support Contractor has noted that the object code tested on the simulator will be different from that executed on the target, because different compilers are used.

EDF and AREVA have explained that for individual function blocks this would not be an issue, as the entire function block library will have been tested on the target as part of the TELEPERM XS development, and delivered as object code (as opposed to being recompiled for the application). However, the application will contain calls into the function block library, and the object code for these calls tested on SIVAT will be different from the target object code.

The designer or future operator/licensee is requested to demonstrate that the testing of the object code of the Protection System, either via the verification and validation process or via the statistical testing activity, achieves adequate coverage (e.g. statements, branches and path segments) of the object code of the executable application program.

11. **T16.TO2.20** - The C&I TXS Cabinets Qualification Program (NLZ-F DC 3, Revision C) has been reviewed and a number of areas for improvement have been identified. The designer or future operator/licensee is requested to address the following observations:

    a. It appears from the System Quality Plan (SQP) (NLE-F DM 10007, Issue D) that the System Requirements Specification encapsulates the Performance Specification; however there is insufficient provided information to determine if it addresses the requirements of clause 5.2 of IEC 60987.

    b. Section 7 of the TXS Cabinets Qualification Program states that tests will be performed across a range of environmental conditions, by reference to ‘Design and Construction Rules for Electrical Components of Nuclear Islands, December 2005’ (RCC-E). However exposure to radiation and chemicals are not addressed (as required by IEC 60780 clause 5.3.1.5.)

    c. Clause 5.3.2 of IEC 60780:1998 states that tests for accident conditions should be performed, including earthquake, cumulated irradiation doses, injection of saturated steam. Section 7.5.2 of the qualification plan addresses seismic tests, but no tests were presented for other accident conditions.

12. **T16.TO2.21** - This concern was originally raised in paragraph 39 of the observations that relate to C&I Class 1 and more important Class 2 systems, that are raised in the HSE/NII report for GDA Step 3 C&I assessment of the UK EPR design.

    The Fault Schedule (PEPR-F DC 4 B) includes a worksheet which shows which functions reducing the risk from anticipated transients without scram (ATWS). However, it does not identify diverse means for providing the protection.

Annex 6

The designer or future operator/licensee is requested to demonstrate that the TXS system is diverse from the system for reducing the risk from anticipated transients without scram (ATWS).

13. **T16.TO2.01** - The designer or future operator/licensee is requested to address the following observations which have arisen from the review of the Claims/Argument/Evidence (CAE) information presented by EDF and AREVA to support conformance to SAP EQU.1 (Equipment qualification):

    a. The argument states that qualification procedures will address actuators, sensors and essential services. However, qualification of these items is not addressed by the referenced evidence (NLE-F DC 113 "TXS based I&C System Quality Plan, NLZ-F DC 3 "I&C TXS cabinets Qualification Program").

    The designer or future operator/licensee is requested to update the CAE to demonstrate that adequate qualification procedures are established for actuators, sensors and essential services.

    b. The CAE refers to the TXS based C&I System Quality Plan as NLE-F DC 113, but that document has been superseded by NLE-F DM 10007.

    The designer or future operator/licensee is requested to:

    - Update the CAE to refer to NLE-F DM 10007 rather than NLE-F DC 113.
    - Review the CAE, and update if necessary, to ensure that it includes correct document references.

    c. The CAE does not address qualification of the TXS components.

    The designer or future operator/licensee is requested to update the CAE to demonstrate that the TXS components have been adequately qualified.

    d. The designer or future operator/licensee to note that a number of areas for improvement relating to TELEPERM XS equipment qualification were identified as a result of the review of evidence against standards, and those points are applicable to the CAE presented for SAP EQU.1. (See T16.TO2.20 above).

    The designer or future operator/licensee is requested to update the CAE for EQU.1 to address the areas for improvement reflected in T16.TO2.20.

    e. RCC-E defines the French design and construction rules for electrical components of nuclear islands, and EDF and AREVA have claimed compliance with these rules. In particular, NLZ-F DC 3 "I&C TXS cabinets Qualification Program" indicates that various chapters within RCC-E will be satisfied (e.g. B2400, B2500, B2600). However, a number of other chapters (e.g. B2240, B2300 and B3500) also contain requirements related to equipment qualification, but these chapters are not discussed in the evidence.

    The designer or future operator/licensee is requested to review the CAE, and update it to ensure it fully addresses the requirements of RCC-E.

    f. RCC-E chapters B5000 and B6000 include qualification requirements for equipment in *'ambience family 1 and 2'* respectively. The evidence does not state which family the cabinets belong to, nor does it confirm that the appropriate requirements are satisfied.

Annex 6

The designer or future operator/licensee is requested to update the CAE to state which '*ambience family*' the cabinets belong to, and demonstrate that the appropriate requirements are satisfied.

14. **T16.TO2.02** - This TO was raised in error in an early draft of the report, and was subsequently removed.

15. **T16.TO2.03** - The designer or future operator/licensee is requested to address the following observations which have arisen from the review of the Protection System CAE information presented by EDF and AREVA to support conformance to SAP EDR.2 (Design for Reliability - Redundancy, diversity and segregation), and update the CAE information:

    a. The referenced evidence (Protection System Detailed Specification file, NLE-F DC 38) has been superseded by NLN-F DC 193, Rev A (Protection System-System description).

    The designer or future operator/licensee is requested to:

    - Update the CAE to refer to NLN-F DC 193 rather than NLE-F DC 38.

    - Review the CAE, and update if necessary, to ensure that it includes correct document references.

    b. Section 4.2 of NLE-F DC 249, Revision C, ("TELEPERM XS based systems Concept for Electrical Separation") states that the technical solutions are temporary, and the analysis is in progress. Completeness of the analysis for the UK EPR needs to be confirmed.

    The designer or future operator/licensee is requested to update the CAE to demonstrate that an analysis of the UK EPR architecture has been performed.

    c. Appendix A of NLE-F DC 249, Revision C identifies the signal exchanges and states whether segregation between systems, through separation or decoupling, is implemented for each. The following points are noted:

    - For some signal exchanges it is concluded that there is no need for separation or decoupling, but no justification is provided.

    - Not all signal exchanges between modules of the Protection System are addressed e.g. it does not address Remote Acquisition Unit / Acquisition and Processing Unit, Acquisition and Processing Unit / Actuator Logic Unit

    The designer or future operator/licensee is requested to update the CAE to demonstrate adequacy of segregation of all signal exchanges between modules of the Protection System. This should include justifications for those cases where there is no separation or decoupling.

    d. The evidence does not address physical separation of cables as required by RCC-E, chapter D7300.

    The designer or future operator/licensee is requested to update the CAE to demonstrate adequacy of separation of cables, as required by RCC-E, chapter D7300.

16. **T16.TO2.04** - The designer or future operator/licensee is requested to address the following observations which have arisen from the review of the Protection System CAE information

Annex 6

presented by EDF and AREVA to support conformance to SAP EDR.3 (Design for Reliability - Common Cause Failure (CCF)), and update the CAE information:

a. Section 1 of H-P1A-2007-02803-FR (“I&C Electrical Systems Project: Common Cause Failure Analysis of FA3 I&C Architecture”) explains that the analysis only considers designs of digital components or systems as sources of CCF. The justification is that other sources of CCF are taken into account in the design of the system. However, there is no reference to an analysis of Common Cause Failure of non digital aspects of the system (e.g. electrical power.)

   The designer or future operator/licensee is requested to update the CAE to demonstrate that an adequate Common Cause Failure analysis has been performed on non digital aspects of the system.

b. Section 1 of H-P1A-2007-02803-FR states that the method for CCF analysis is qualitative in nature. However it is understood that the results of the Common Cause Failure analysis are used as inputs to reliability calculations. Clarification is needed on how the Common Cause Failure analysis supports the reliability calculations.

   The designer or future operator/licensee is requested to update the CAE to clarify how the qualitative nature of the Common Cause Failure analysis supports the reliability calculations.

c. The potential for Common Cause Failure within TELEPERM XS itself is not fully addressed, in that although the shared use of software is considered, there is no discussion on the potential for digital hardware components as a source of Common Cause Failure.

   The designer or future operator/licensee is requested to update the CAE to demonstrate that adequate consideration has been given to the potential for digital hardware components as a source of Common Cause Failure.

d. The argument states that the shared use of subroutines within TXS is addressed in the "non-specific processing part" of the C&I compact model used in the Probabilistic Safety Assessment (PSA). This is documented in section 4.3.14.3 of the PSA (NEPS-F DC 355) which supports the argument. The PSA should therefore be referenced from the argument.

   The designer or future operator/licensee is requested to update the CAE to include the PSA as part of the argument.

e. Section 4.4 of ENSECC080054 (“Analysis of Digital Common Cause Failures of E1A (PS) Class Level 1 Systems of FA3 I&C Architecture”) states that network bandwidth between divisions is a potential source of Common Cause Failure. It goes on to describe mechanisms within TXS which ensure that saturation of one network cannot affect others. However this only addresses networks within a division, and not across divisions. Further evidence is needed to demonstrate cross division networks have been analysed as potential sources of Common Cause Failure.

   The designer or future operator/licensee is requested to update the CAE to demonstrate that adequate consideration has been given to the potential for networks between divisions as sources of Common Cause Failure.

f. The independence of the networks within a division has been investigated (by the Technical Support Contractor) by considering the architecture as described in the PS System Description, NLN-F DC 193. It is noted not all networks within the Protection

Annex 6

System are considered within the analysis (e.g. Remote Acquisition Unit / Acquisition and Processing Unit; Acquisition and Processing Unit/ Actuator Logic Unit). The analysis should be updated to consider all networks.

The designer or future operator/licensee is requested to update the CAE to demonstrate that the CCF analysis addresses all networks within the Protection System.

g. The argument states that shared use of hardware / equipment (cabinets, cabling, piping, power etc); Sensors; Actuators are addressed by the evidence. However, the referenced evidence does not address these.

   The designer or future operator/licensee is requested to update the CAE to demonstrate that CCF analysis addresses all hardware / equipment (cabinets, cabling, piping, power etc), Sensors and Actuators.

17. T16.TO2.05 - The designer or future operator/licensee is requested to address the following observations which have arisen from the review of the Protection System CAE information presented by EDF and AREVA to support conformance to SAP EMT.7 (Maintenance, Inspection and Testing - Functional Testing), and update the CAE information:

a. The CAE refers to NLE-F DC 38 (PS Detailed Specification File) which is a Flamanville 3 document. The evidence needs to be updated for UK EPR.

   The designer or future operator/licensee is requested to update the CAE to address the UK EPR architecture.

b. It is noted that the test approach for safety functions is performed in discrete stages, e.g. verify that sensor data is acquired by the Protection System; verify that trip signals from the Actuator Logic Unit activate Reactor Trip, through the use of test signals.

   This approach does not seem to be consistent with the requirements of the SAP and RCC-E Chapter C3323, which imply that complete functions should be tested.

   The designer or future operator/licensee is requested to update the CAE to demonstrate that complete functions are tested, as required by the SAP and RCC-E Chapter C3323.

c. RCC-E chapter C3322 states ‘W*hen a trip parameter is computed from several variables, the contribution of each variable shall be verified individually, with the other variables adjusted to within their operating range at a nominal or at a preset value*.’ The evidence referenced in the CAE trail does not demonstrate that this requirement is satisfied.

   The designer or future operator/licensee is requested to update the CAE to demonstrate that the requirements of RCC-E chapter C3322, concerning the contribution of individual variables to trip parameter calculations, are satisfied.

d. Chapter C3323 of RCC-E states that test signals shall be superimposed on normal signals (thus perturbing the measured variable), or by using a substitute input signal. There is no provided evidence of this principle being applied.

   The designer or future operator/licensee is requested to update the CAE to demonstrate that the requirements of RCC-E chapter C3323, concerning the imposition of test signals on normal signals, are satisfied.

e. Chapter C3322 of RCC-E states that testing of response times is not needed if it can be checked during plant operation or during routine testing, and if it can be demonstrated that changes in response time beyond reasonable limits are accompanied by detectable

Annex 6

deviations in performance characteristics. This requirement has not been addressed in the CAE information for conformance to EMT.7.

The designer or future operator/licensee is requested to update the CAE to demonstrate that the requirements of RCC-E chapter C3322 regarding the testing of response times are satisfied.

f. Clause 4 IEC 60671:2007 states that failure modes not revealed by self-supervision, shall either be shown not to affect the safety function, or shall be covered by periodic testing. There is no analysis provided, or referred to that demonstrates that periodic testing addresses all failure modes which are not addressed by self-monitoring.

The designer or future operator/licensee is requested to update the CAE to demonstrate that periodic testing addresses all failure modes which are not addressed by self-monitoring, as required by Clause 4 IEC 60671:2007.

g. A number of detailed observations related to the completeness of test definitions, and definition of pass/fail criteria have been identified with the tests listed below.

- Section 2.2.4 states SICS Reactor Trip manual command is not represented since the implementation of the command is not fixed
- Test Principle 3 - step 2 says verify that the test has been correctly performed, without saying how or by providing pass/fail criteria.
- Test Principle 6 (Diesel Standing Order) is not defined.
- Test Principle 11 (analog and digital indicators) indicates that principles have not been defined
- Test Principle 15 (Parameterisation, Test/Diagnosis, Disable Keys) – it is stated that these are tested when used, however no justification is provided. The concern is how it can be confirmed that the functions will be available when required.
- Test Principle 16 'The test is a spot check' suggesting a degree of informality.

The designer or future operator/licensee is requested to update the tests identified above to ensure that they are completely and formally defined.

18. **T16.TO2.06** - The designer or future operator/licensee is requested to address the following observations which have arisen from the review of the Protection System CAE information presented by EDF and AREVA to support conformance to SAP ESS.18 (Safety Systems - Failure Independence), and update the CAE information.

a. Section 4.2 of NLE-F DC 249, Revision C, (“TELEPERM XS based systems Concept for Electrical Separation”) states that the technical solutions for separation are temporary, and the analysis of compliance with RCC-E is in progress. Completeness of the analysis for the UK EPR needs to be confirmed.

The designer or future operator/licensee is requested to update the CAE to demonstrate that an analysis of the UK EPR architecture has been performed.

Annex 6

b. Appendix A of NLE-F DC 249, Revision C identifies the signal exchanges and states whether segregation between systems, through separation or decoupling, is implemented for each. The following points are noted:

   - For some signal exchanges it is concluded that there is no need for separation or decoupling, but no justification is provided.
   - Not all signal exchanges between modules of the Protection System are addressed.

   The designer or future operator/licensee is requested to update the CAE to demonstrate the adequacy of segregation of all signal exchanges between modules of the Protection System. This should include justifications for those cases where there is no separation or decoupling.

c. The referenced evidence does not address separation between modules of the PS, and between cables associated with the PS.

   The designer or future operator/licensee is requested to update the CAE to demonstrate adequacy of separation between modules of the PS and between cables associated with the PS. This should include justifications for those cases where there is no separation or decoupling.

d. The referenced evidence does not address the potential for faults with the Service Unit causing the disabling of the PS (e.g. an invalid input from the service unit to the PS).

   The designer or future operator/licensee is requested to update the CAE to demonstrate that potential faults with the Service Unit cannot cause the PS to be disabled.

e. The inclusion of the Qualified Display System (QDS) has been proposed for addition to the PS, however no details have been provided in the Step 4 GDA timeframe. If the QDS is included in the PS then the CAE trail will have to be updated to demonstrate that any faults it causes cannot disable the PS.

   If the QDS is included within the PS architecture the designer or future operator/licensee is requested to update the CAE to demonstrate that potential faults with the QDS cannot disable the PS.

19. T16.TO2.07 - The areas for improvement described in Technical Observation T16.TO2.18 above (concerning error detection and management) are applicable to ESS.21 (Safety Systems – Reliability).

    The designer or future operator/licensee is requested to update the CAE for ESS.21 to address the areas for improvement presented in T16.TO2.18.

20. T16.TO2.08 - The designer or future operator/licensee is requested to address the following point which has arisen from the review of the Protection System CAE information presented by EDF and AREVA to support conformance to SAP ESS.23 (Safety Systems - Allowance for unavailability of equipment), and update the CAE information.

    a. The argument does not refer to the 4-train architecture, which would appear to contribute to the satisfaction of this SAP.

       The designer or future operator/licensee is requested to consider the appropriateness of the 4-train architecture in the context of this SAP and update the CAE accordingly

Annex 6

b. The only evidence referred to from the CAE is to chapter 18.2.4 of the PCSR which is not related to this SAP.

The designer or future operator/licensee is requested to update the CAE to demonstrate that the requirements of ESS.23 are satisfied.

21. **T16.TO2.09** - The designer or future operator/licensee is requested to address the following observations which have arisen from the review of the Protection System CAE information presented by EDF and AREVA to support conformance to SAP ESS.27 (Safety Systems - Computer-based safety systems), and update the CAE information.

a. The CAE refers to the TELEPERM XS based C&I System Quality Plan as NLE-F DC 113, but that document has been superseded by NLE-F DM 10007. The designer or future operator/licensee is requested to:

- Update the CAE to refer to NLE-F DM 10007 rather than NLE-F DC 113.
- Review the CAE, and update if necessary, to ensure that it includes correct document references.

b. Technical Observations T16.TO1.01 and T16.TO2.12 through T16.TO2.19 are also applicable to this SAP. The designer or future operator/licensee is requested to update the CAE for ESS.27 to address the points recorded in T16.TO1.01 and T16.TO2.12 through T16.TO2.19.

c. Regarding Independent Confidence Building Measures, EDF and AREVA have committed to carry out a minimum of 5000 tests on the TELEPERM XS PS Test Division, and to carry out a review of the reasonable practicability of carrying out additional tests (up to 50,000) within the PS implementation programme. Research will be undertaken into the feasibility of implementing statistical testing on simulation of the PS using the simulator (SIVAT). They have also committed to produce a feasibility study on static analysis of the UK EPR Protection System software, and qualification of the TELEPERM XS development tools, including the automatic code generator and C compiler. This concern is being tracked through pGI-UKEPR-C&I.03.01[15]. However the measures described above are not recorded in the CAE.

The designer or future operator/licensee is requested to update the CAE to include the above information on Independence Confidence Building Measures.

d. The CAE leads to document NLE-F DC 222 - Protection System, Severe Accident I&C, Reactor Control Surveillance and Limitation System V&V and Test Plan as evidence of independent confidence building measures. However, the document describes processes which are required by IEC 60880, and do not represent Independent Confidence Building Measures (i.e. in addition to that required by IEC 60880).

The designer or future operator/licensee is requested review the appropriateness of NLE-F DC 222 in the CAE trail for this SAP, and update the CAE to explain its relevance to Independent Confidence Building Measures.

22. **T16.TO2.33** - The designer or future operator/licensee is requested to demonstrate that adequate measures are in place to address the potential design and implementation issues

[15] ND note: GI-UKEPR-CI-02 is the issued version of the provisional GDA Issue (pGI).

Annex 6

concerned with Calculated Trips, which are captured in ‘*Programmable Calculated Trips – WPD Notes & Checklist* S.P1440.74.11’, which is based on requirements and guidance identified in:

- IEC 61513:2001
- IEC 60880:2006
- IEC 61888:2002
- Trip Parameter Acceptance Criteria for Safety Analysis of CANDU Nuclear Power Plants, Canadian Nuclear Safety Commission Regulatory Guide G-144
- IEEE Standard 754 on Floating Point Numbers and Guidance material
- Relevant Safety Assessment Principles

The TO2 technical observations which are applicable to the Safety Automation System (SAS) and the Process Automation System (PAS) are:

23. **T16.TO2.22** – The designer or future operator/licensee is requested to address the following points which have arisen from the review of the SAS/PAS CAE for SAP EDR.1 and update the CAE information:

    a. The CAE states that SIE QU633 provides a system level reliability study. However the study is not provided in SIE QU633.

    The designer or future operator/licensee is requested to update the CAE to demonstrate that SAS/PAS system level reliability study has been performed.

    b. The CAE claims that SIE QU 627 provides an FMEA of SPPA-T2000 based C&I systems (i.e. SAS, PAS and PICS). However, SIE QU 627 is the reliability analysis of the SPPA-T2000 platform and the document does not contain an FMEA.

    The designer or future operator/licensee is requested to update the CAE to demonstrate that an FMEA of the SPPA-T2000 has been performed.

24. **T16.TO2.23** - The designer or future operator/licensee is requested to address the following point which has arisen from the review of the SAS/PAS CAE for SAP EDR.2, and update the CAE information:

    The CAE claims that SIE QU 627 provides a reliability analysis for the SPPA-T2000 based C&I systems, i.e. SAS and PAS. However, the analysis addresses hardware only and does not take into account systematic software failures of the application software.

    The designer or future operator/licensee is requested to update the CAE to provide evidence of a reliability analysis for the SPPA-T2000 based C&I systems, i.e. SAS and PAS that includes consideration of systematic software failures.

25. **T16.TO2.24** - The designer or future operator/licensee is requested to address the following points which have arisen from the review of the SAS/PAS CAE for SAP EDR.3, and update the CAE information:

    a. The CCF analysis only applies to the SAS (not PAS).

Annex 6

The designer or future operator/licensee is requested to update the CAE to demonstrate that a CCF analysis of the PAS has been performed.

b. The analysis only addresses digital aspects of the SAS system, and there is no reference to an analysis of Common Cause Failure of non digital aspects of the system (e.g. electrical power.) Further evidence is needed to confirm that an adequate Common Cause Failure analysis has been performed on non digital aspects of the system.

   The designer or future operator/licensee is requested to update the CAE to demonstrate that an adequate Common Cause Failure analysis has been performed on non digital aspects of the SAS system.

26. **T16.TO2.25** - The designer or future operator/licensee is requested to address the following point has arisen from the review of the SAS/PAS CAE for SAP EQU.1, and update the CAE information:

    The quality plan for SPPA based systems does not address qualification, as required by IEC 61513:2001, clause 6.4, and RCC-E chapter C5800.

    The designer or future operator/licensee is requested to update the CAE to demonstrate that the requirements for qualification, as specified by IEC 61513:2001 clause 6.4, and RCC-E chapter C5800 are satisfied.

27. **T16.TO2.26** - The designer or future operator/licensee is requested to address the following points which have arisen from the review of the SAS/PAS CAE for SAP EMT.7, and update the CAE information:

    a. QU633 describes the periodic test between SICS and PAS/SAS at a high level of abstraction at the platform level. However, there is insufficient provided evidence to demonstrate how overlapping periodic test and self test ensures that the functionality of the complete safety-related function from sensor to actuator is provided.

       The designer or future operator/licensee is requested to update the CAE to demonstrate that overlapping periodic test and self test ensures that the functionality of the complete safety-related function from sensor to actuator is tested.

    b. Observation O14 from the HSE/NII Step 3 assessment requested a description of how SAP EMT.7 is satisfied for “F2 C&I not in continuous operation”. This has not been addressed in the CAE information.

       The designer or future operator/licensee is requested to update the CAE to demonstrate how SAP EMT.7 is satisfied for “F2 C&I not in continuous operation”.

    c. It is noted that the argument states ‘*For SAS, PAS and PICS Overlapping periodic testing and self-testing ensure that the functionality of the complete system (and its components) from sensor to actuator is provided.’*. However, the evidence does not address the PICS.

       The designer or future operator/licensee is requested to update the CAE to demonstrate that overlapping periodic testing and self-testing ensure that the functionality of the PICS is provided.

28. **T16.TO2.27** - The designer or future operator/licensee is requested to address the following point which has arisen from the review of the SAS/PAS CAE for SAP ESR.5, and update the CAE information:

Annex 6

The referenced evidence, DN 2.2.24, is specific to SAS. Confirmation is required that corresponding information is established for the PAS.

The designer or future operator/licensee is requested to update the CAE to confirm that DN 2.2.24 is applicable to the PAS, or if not, to update the CAE to demonstrate that the PAS is compliant with IEC 61513 and 62138

29. **T16.TO2.28** - Evidence has been sought, from the Areva and Siemens quality plans (NLF-F DC 82 Rev C, PD110, Issue 1.0), to confirm that the requirements of IEC 61513:2001 are satisfied for Class 2 and 3 systems. For some clauses the provided evidence does not provide this confirmation.

    The designer or future operator/licensee is requested to demonstrate that the following requirements are satisfied:

    a. 6.1.2 *System Specification* - both quality plans state that this is beyond their scope.
    b. 6.1.6 *System Installation* - NLF-F DC 82 states that it is applied but also states that it is not addressed by this plan.
    c. For each of the following sub-clauses NLF-F DC 82 states that the clause is applied, but does not provide or refer to supporting evidence:
        - 6.2.5 - *System Installation Plan*
        - 6.2.6 - *System Operation Plan*
        - 6.2.7 - *System Maintenance Plan*
    d. Clause 6.4 – *Qualification* - both documents state that the clause is applied, but do not provide or refer to supporting evidence.

30. **T16.TO2.29** - Evidence has been sought, from System Specification File SY710 to confirm that the requirements of IEC 62138:2004 Clauses 5.3 and 6.3 *Software Requirements* Specification are satisfied. It can be seen that the document does address the requirements of the clauses, however it includes requirements for the SPPA T2000 Platform and the SAS application.

    The designer or future operator/licensee is requested to indicate which aspects of System *Specification* File SY710 are applicable to each of the platform and the SAS application.

31. **T16.TO2.30** - Evidence has been sought, from the Areva and Siemens quality plans (NLF-F DC 82 Rev C, PD110, Issue 1.0), to confirm that the requirements of IEC 62138:2004, Clause 5.8 & 6.8 – *Installation of Software on Site* is satisfied for Class 2 and 3 systems.

    NLF-F DC 82 states that the clause is applied, but does not provide or refer to supporting evidence.

    The designer or future operator/licensee is requested to demonstrate that the above clause is satisfied.

32. **T16.TO2.31** - No evidence on the application of IEC 60987:2007 to the SPPA T2000 applications has been provided.

Annex 6

The designer or future operator/licensee is requested to demonstrate that the requirements of IEC 60987:2007 have been satisfied for SPPA-T2000 based systems on UK EPR.

The TO2 observation which is applicable to the Safety Information and Control System (SICS) is:

33. **T16.TO2.32** - The designer or future operator/licensee is requested to demonstrate that the following standards have been satisfied in the development and production of the Safety Information and Control System.
    - IEC 61513:2001
    - IEC 60987:2007
    - IEC 60780:1998

Conclusion of Task Review

For the PS, based on the sampled evidence, and subject to satisfactory resolution of the technical observations, there is no evidence to indicate that the requirements of relevant standards are not satisfied. There is some evidence of independent confidence building measures for the PS, however some areas for improvement have been identified.

For the NCSS and QDS, a demonstration of safety has not been provided.

For the SAS and PAS, based on the sampled evidence, and subject to satisfactory resolution of the technical observations, there is no evidence to indicate that requirements of relevant standards are not satisfied.

For the SICS, the review was limited to confirming that the equipment has been developed and qualified to appropriate nuclear hardware standards. This limited review is justified on the fact that the SICS is based on conventional technology i.e. it consists of a set of conventional controls and displays (push buttons, light indicators, analogue displays, recorders etc.). Insufficient information has been provided in the period of this review for it to be confirmed that the SICS has been developed and qualified to appropriate standards.

Annex 7

TSC Summary – Review of the C&I Architecture for Safety Capability[16]

Note this information has been imported from a TSC report (Ref. 32) and the formatting of the TSC report has been retained.

[16] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 7

A Annex: TSC Task Summary - Review of the C&I Architecture for Safety Capability

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of the C&I Architecture for safety capability (TSC Task 17) for the UK EPR reactor design.

This review follows on from the review of architecture-related claims and argumentation carried out in a preliminary activity (TSC Task 7), relating to:

a) defence in depth and failure mode management including common cause failure.
b) independence and diversity;
c) provision for automatic and manual safety actuation;
d) appropriateness of equipment type/class.

The aim of the review has been to gain confidence that the Requesting Party (EDF Energy and Areva NP, hereafter referred to as EDF and AREVA) has adequate evidence to support these architecture-related claims and argumentation. The review has included consideration of evidence to support further claims and argumentation presented by EDF and AREVA relating to conformance of the C&I architecture to 19 selected Safety Assessment Principles (SAPs). The review has taken due cognisance of selected HSE Technical Assessment Guidelines (TAGs) and international nuclear safety standards. The task has reviewed architecture-related evidence presented by EDF and AREVA via:

- the claims-argument-evidence table that provides the basis of the demonstration of SAP conformance;
- responses to Technical Queries;
- responses to actions from meetings involving EDF and AREVA, HSE/NII and the TSC;
- and responses to technical observations raised during Step 3, including architecture-related observations in the HSE/NII GDA Step 2 and Step 3 reports.

In addition, the task has reviewed changes to the UK EPR C&I architecture that have occurred since the end of Step 3 of the GDA process.

The scope of the evidence that is specific to UK EPR is defined by EDF and AREVA in *"UK EPR CONTROL AND INSTRUMENTATION (C&I) – SCOPE OF GDA"* (letter ND(NII)EPR00686N). The structures, systems and components (SSCs) that comprise the C&I architecture is consistent with this scoping letter. The main SSCs that were reviewed in the architecture review are as follows: Teleperm XS platform and its hosted systems (Protection System, Reactor Control, Surveillance and Limitation System, and Severe Accident I&C system); SPPA-T2000 platform and its hosted systems (Safety Automation System, RRC-B Safety Automation System, Process Automation System, and Process Information and Control System); Safety Information and Control System; Priority and Actuation Control System; Process Instrumentation Preprocessing System; class 1 network; class 2 network (SAS bus); and class 3 networks (Plant bus and Terminal bus). In addition, two further SSCs have been added to the C&I architecture in response to Regulatory Issue RI-UKEPR-002 – the Non-Computerised Safety System and the class 1 displays and controls interface with the Protection System – but evidence relating to these additional SSCs has not been developed in the timeframe of this review.

The C&I architecture has been modified significantly since the definition that was presented by EDF and AREVA in the April 2008 version of the Pre-Construction Safety Report (PCSR): The addition of the Non-Computerised Safety System has resulted in reduced reliability claims for the primary and secondary protection systems; several systems now have higher classification; a new class 2 network has been introduced for use by the secondary protection system; a new system has been added to

Annex 7

respond to certain types of severe accident; the interfaces with the Protection System have been changed so as to avoid inputs from lower-classified systems; class 1 controls and displays have been introduced in the Main Control Room and the Remote Shutdown Station.

A total of 27 technical observations resulting from the Task 17 review remain unresolved at the end of the review period. These observations have been designated as TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher – 8 of these observations have been designated as TO1 and 19 of these observations have been designated as TO2. Note that where a gap in the numbering sequence exists, this is due to the resolution of an observation that had been allocated this number.

Technical Observations designated TO1

The eight TO1 technical observations are as follows:

T17.TO1.01 - The categorisation and classification scheme in NEPS-F DC 557 does not conform to IEC 61226:2009 and UK expectations. The designer or future operator/licensee is requested to:

a. update the categorisation and classification scheme (eg. as defined in NEPS-F DC 557) with all appropriate IEC 61226:2009 clauses and use this to re-classify the C&I systems.

b. state explicitly the claim limits for each class in the categorisation and classification scheme so as to reflect the following:
For non-computer based systems, including systems with complex electronics such as Complex Programmable Logic Devices[17]:
- Class 1 1E-5 ≤ probability-of-failure-on-demand (pfd) < 1E-3
- Class 2 1E-3 ≤ pfd < 1E-2
- Class 3 1E-2 ≤ pfd ≤ 1E-1
For computer-based systems:
- Class 1 1E-4 ≤ pfd < 1E-2
- Class 2 1E-2 ≤ pfd
- Class 3 1E-1 ≤ pfd
For high demand or continuous modes of operation then the pfd is replaced by a frequency (f) of failure per year but the figures remain the same.

c. identify how the time following each fault at which, or the period throughout which, the main and diverse lines of defence will be called upon to operate, is taken into account in the classification and categorisation scheme.

T17.TO1.02 - With regard to the Fault Schedule in PEPR-F DC 4 rev B, the designer or future operator/licensee is requested to:

a. update the Fault Schedule to identify the C&I systems that are involved in each safety function.

[17] ND note: Depen ding on the degree of complexity, and the use of software techniques and tools the computer-based system limits may need to be applied.

Annex 7

b. confirm that the Fault Schedule is consistent with the Probabilistic Safety Assessment in its identification of all diverse lines of defence needed to meet the required risk mitigations, especially for infrequent events with high consequence.

Document ECECC080669 rev B "*Architecture of instrumentation and control system EPR FA 3: design principles and defence-in-depth*" states that the allocation of RRC-A functions is performed on a case-by-case basis, taking into account independence requirements (of the C&I system providing the defence from the initiating event). However, it was not possible to locate any results of this case-by-case analysis that shows that in all cases, each C&I safety and safety-related system is independent of, and invulnerable to, any fault that the system is claimed to act against. The designer or future operator/licensee is requested to:

c. substantiate the claim that each C&I safety and safety-related system is independent of, and invulnerable to, any fault that the system is claimed to act against.

T17.TO1.04 - The designer or future operator/licensee is requested to update the specification of the Protection System for UK EPR (NLN-F DC 193 rev A) to include the commitments to avoid networked (hardwired connections justified on a case-by-case basis) communication into the Protection System from lower classified systems.

T17.TO1.11 - The designer or future operator/licensee is requested to update the pre-construction safety report and identified references to:

a. capture the claims-argument-evidence information in PELL-F DC 9;

b. include the modifications to the architecture for UK EPR that have been committed to since November 2009. The update to include all commitments captured in the following documents:
   i. letter EPR00180R;
   ii. letter EPR00607N;
   iii. response to TQ-EPR-1003.

T17.TO1.14 - The designer or future operator/licensee is requested to update the pre-construction safety report to define the controls and displays to be provided by the class 1 extension to the Process Information and Control System, in the Main Control Room and in the Remote Shutdown Station, including whether the implementation of this class 1 extension will use the Qualified Display System or not.

T17.TO1.15 - The designer or future operator/licensee is requested to update the pre-construction safety report, and supporting documents such as "*Sizing of SICS*" (document ECEF021068 rev C), to ensure an adequate scope of parameters are defined for display using Class 1 equipment (e.g. by comparison with the category 1 safety parameters as defined by U.S. NRC Regulatory Guide 1.97 Revision 3 - May 1983). The designer or future operator/licensee is also requested to investigate the practicability of using a class 1 origin instead of a lower class origin for such safety parameters (when this is available).

T17.TO1.24 - The technology to be used for the implementation of the Non-Computerised Safety System is declared by EDF and AREVA to be out of scope of Step 4 of GDA, and as a result, its impact on the C&I architecture, and justification of its reliability claim, could not be reviewed. The designer or future operator/licensee is requested to address this by provision of a safety demonstration through a Basis of Safety Case for the NCSS, when the supplier and technology for NCSS have been selected.

T17.TO1.25 - The designer or future operator/licensee is requested to incorporate the commitment made in letter EPR00180R into the safety case submission, regarding the disconnection of the Teleperm XS Service Unit during plant operation, to mitigate the risk that it could cause unintended interference to the operation of the class 1 part of the Protection System.

Technical Observations designated TO2

The nineteen TO2 technical observations are as follows:

T17.TO2.03 - The designer or future operator/licensee is requested to address the results of its review of the use of class 3 systems in the diverse line of defence for category A functions.

T17.TO2.05 - The designer or future operator/licensee is requested to address the following areas for improvement regarding the self-test function of Teleperm XS:

a. If there is repeated cycle overrun by the software application and/or service task, which causes the self-test function not to execute, this may not be detected for one hour before an alarm is raised. The designer or future operator/licensee is requested to substantiate the claim that safety is not compromised if the self-tests do not execute for one hour.

b. Table 1 in "*TXS Self-monitoring and fail-safe behaviour*" (document NLTC-G 2008 EN 0079 rev B) identifies some components that are not self-tested during cyclic operation without providing justification. The designer or future operator/licensee is requested to identify the full set of Teleperm XS platform components used by the Protection System that are not subject to self-test, and to justify why this does not compromise safety.

T17.TO2.06 - The designer or future operator/licensee is requested to address the following areas for improvement regarding the self-test function of the SPPA-T2000 platform:

a. to ensure that the fail-safe states of the SPPA-T2000 modules analysed in "*Self test coverage analysis*" (document SIE QU633 v5.0) are well-defined and documented.

b. to demonstrate full coverage of the SPPA-T2000 modules/components by self-test, and the justification for any absence of self-test.

c. to address the effects on safety of application software or service unit processing overrun that denies execution of the self-test software.

T17.TO2.07 - The designer or future operator/licensee is requested to ensure that Failure Modes and Effects Analyses have been completed for class 1 C&I components and systems, in particular:

a. Process Instrumentation Preprocessing System

b. Priority and Actuation Control System (PACS), plus addressing the results of the Reliability study for the actuation equipment for the Flamanville 3 reactor (FA3), including the PACS switchgear, due mid 2011. If the FA3 study is not directly applicable to the UK EPR then an appropriate reliability study should be completed for the UK EPR.

Annex 7

c. Reactor Trip equipment, including trip breakers and trip contactors.

T17.TO2.08 - The designer or future operator/licensee is requested to demonstrate the single failure criterion via functional and/or system-level redundancy for the class 1 Safety Information and Control System (SICS) controls/displays, and class 1 Priority and Actuation Control System/actuator (PACS) equipment, in particular for the following cases:

a. for SICS equipment that is shared across all four divisions, for example, the equipment that issues an order that is distributed to all four divisions;

b. for PACS/actuator equipment that is shared by multiple lines of defence for the same Postulated Initiating Event.

T17.TO2.09 - The designer or future operator/licensee is requested to demonstrate the single failure criterion for:

a. a single failure that disables an entire division performing an Engineered Safeguard Action function, such as a loss of common power supply at division level, when the function is implemented in only two divisions, and when the other instance of the Engineered Safeguard Action function is disabled due to maintenance.

b. consequential failures of C&I systems and their supporting equipment (cabinets, power, networks etc), as required by SAP EDR.4 paragraph 175.

T17.TO2.10 - The designer or future operator/licensee is requested to justify the allocation of manual actuation over automatic actuation for each safety and safety-related I&C function for UK EPR.

T17.TO2.13 - The selection of the technology and supplier for the Turbine Control system for UK EPR is out of scope of Step 4 of GDA. The designer or future operator/licensee is requested to ensure a safety demonstration is produced for the Turbine Control system when the supplier and technology have been selected.

T17.TO2.16 - The designer or future operator/licensee is requested to demonstrate that the manual controls in the Remote Shutdown Station, and the Terminal Bus, will be usable when the Main Control Room becomes uninhabitable. In particular, a response from EDF and AREVA has stated that a design study is in progress for the Flamanville 3 reactor, to address a technical solution for avoiding spurious commands being sent from the operator workstation in the Main Control Room whilst uninhabitable, potentially causing overload of the Terminal Bus (which may disable the operator workstation in the Remote Shutdown Station). The designer or future operator/licensee is requested to address the results of this study for UK EPR.

T17.TO2.17 - The designer or future operator/licensee is requested to update the safety case submission to record which Protection System functions use internal diverse detection, and which do not, and for those that do not, to include the justifications.

T17.TO2.18 - The review of the adequacy of the frequency of periodic testing of class 1 equipment is out of scope for Step 4 of GDA. The designer or future operator/licensee is requested to update the safety demonstration to include this information.

Annex 7

T17.TO2.19 - The designer or future operator/licensee is requested to demonstrate the adequacy of the monitoring of class 1 actuators used by the Protection System and by category A Safety Information and Control System functions.

T17.TO2.20 - The review of the Operating Technical Specification for each C&I system to examine whether it defines either a grace period for repair or a fail-safe operating mode, and to examine if the grace period is exceeded, whether a fail-safe action is required by the operator, is out of scope for Step 4 of GDA. The designer or future operator/licensee is requested to update the safety demonstration to include this information.

T17.TO2.21 - The adequacy of the controls provided by C&I systems to maintain variables within specified ranges, is out of scope of GDA. Likewise, the definition of Temporary Operating Modes that allow online modification of plant variables via the Service Unit is out of scope of GDA. The designer or future operator/licensee is requested to update the safety demonstration to include this information.

T17.TO2.22 - The design of communications systems that enable information and instructions to be transmitted between locations, and that provide external communications with auxiliary services and such other organisations as may be required, is out of scope of GDA. The designer or future operator/licensee is requested to update the safety demonstration to include this information.

T17.TO2.23 - Some types of external hazard are out of scope of GDA because they are site-dependent, and hence the risk assessment requires site-specific data. The designer or future operator/licensee is requested to update the safety demonstration to include this information.

T17.TO2.26 - Document ECECC100744 rev A “Plant I&C requirement specification” applicable to UK EPR does not contain the C&I functional requirements, and instead refers to a document that defines the classification scheme. The designer or future operator/licensee is requested to update the safety case submission to identify the set of C&I functional requirements.

T17.TO2.27 - The presentation by EDF and AREVA in response to action 43-I&C-6 states that the relay logic in the Priority and Actuation Control System always prioritises signals from the Protection System over signals from the Non Computerised Safety System (NCSS), and over signals from the SPPA-T2000 Safety Automation System (SAS), Process Automation System (PAS), and Process Information and Control System (PICS). The designer or future operator/licensee is requested to:

a. demonstrate that the effect of a fault in the Protection System that attempts to set "Protection Order On" when "Protection Order Off" is also set cannot inhibit or impede orders from NCSS, SAS, PAS or PICS;

b. demonstrate that it is never the case (or fully justify each case as being appropriate) that a Protection System signal that is part of a category B (or lower) function can cause a signal from SAS, PAS, PICS, or NCSS that is part of a category A function for the same actuator, to be inhibited or impeded, due to this prioritisation. The demonstration to include consideration of Protection System failures such that operation of any category A function by backup systems is not frustrated by such failures.

T17.TO2.28 - Within the Probabilistic Safety Assessment model, the Process instrumentation Preprocessing System (PIPS) is included in the sensor modelling, and the Priority and Actuation Control System (PACS) is included in the actuator modelling. The designer or future operator/licensee is requested to review the reasonable practicability of modelling the PIPS and PACS systems separately from the sensors and actuators, in order to make explicit:

Annex 7

a. the occurrence of any potential common cause failures in these systems and their modules;

b. the need for diversity if reliability claims for modules in these systems exceed acceptable limits.

A number of further observations that relate to the C&I architecture have arisen from the review of the responses to RI-UKEPR-002 and are documented in "*Review of Responses to Regulatory Issue RI-UKEPR-002 - Task 20*".

Conclusion of Task Review

With regard to the architecture-related observations in the HSE/NII GDA Step 3 report, the following conclusions are reached:

a) "*Protection systems reliability claims difficult if not impossible to substantiate*" has been resolved by the commitment in letter EPR00180R to reduce the reliability claims as a result of introduction of the Non-Computerised Safety System;

b) "*Independence between the safety (Class 1) and safety related systems (Class 2/3) appears to be significantly compromised*" has been resolved by changes to class 1 system interfaces with lower-classified systems;

c) "*No Class 1 manual controls or indications either in the Main Control Room or Remote Shutdown Station*" has been resolved by the class 1 extension to the Process Information and Control System;

d) "*EPR function categories / equipment class assignments do not appear to align with UK expectations as defined in BS IEC 61226:2005*" has been progressed and outstanding points are covered by technical observation T17.TO1.01 and potential GDA Issues PGI-UKEPR-C&I-02 and PGI-UKEPR-CC.01[18];

e) "*lack of overall specification of the C&I architecture*" has partially been resolved, and the outstanding point (absence of functional requirements for C&I) has been covered by technical observation T17.TO2.26;

f) "*absence of key information in the PCSR*" has been progressed and outstanding points are covered by technical observation T17.TO1.11 and potential GDA Issue PGI-UKEPR-C&I-04[19].

Of the 19 SAPs that have been reviewed by Task 17, only two (ESS.1 and ESS.2) have no associated technical observation. Nevertheless, in view of the fact that written commitments have been made by EDF and AREVA to resolve the topics in the identified TO1 observations, which have also been captured in the set of potential GDA Issues, it is the opinion of the TSC that an acceptable way forward has been achieved for the major architecture-related elements of the C&I design to meet the intent of the appropriate SAPs, TAGs and IEC standards.

[18] ND note: GI -UKEPR-CC-01 is the issued version of the provisional GDA Issues (pGI) that is addressing the concern identified here.

[19] ND note: GI-UKEPR-CI-03 is the issued version of the provisional GDA Issue (pGI).

Annex 8

TSC Summary – Review of the Diversity of those Systems Contributing to the Implementation of Category A Functions[20]

Note this information has been imported from a TSC report (Ref. 33) and the formatting of the TSC report has been retained.

[20] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 8

A Annex: TSC Task Summary - Review of the Diversity of those systems Contributing to the Implementation of Category A Functions

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of the diversity of those systems contributing to the implementation of category A functions (TSC Task 18) for the UK EPR reactor design.

The use of various forms of diversity within systems performing protection functions is important to minimise the risk of simultaneous failure on demand of those systems.

This review follows on from the review of diversity claims and argumentation carried out in a preliminary activity (TSC Task 8), relating to:

a) equipment diversity (including diversity of platform);
b) diversity of verification and validation;
c) diversity of physical location (segregation);
d) software diversity;
e) functional / data / signal diversity;
f) diversity of design / development;
g) diversity of specification.

The aim of the review has been to gain confidence that the Requesting Party (EDF Energy and Areva NP, hereafter referred to as EDF and AREVA) has adequate evidence to support these diversity claims and arguments. This has included review of the evidence to support further claims and argumentation presented by EDF and AREVA relating to the conformance of specific C&I protection systems to selected Safety Assessment Principles (SAPs) that relate to diversity.

Five SAPs have been considered during the review (EDR.2 - Redundancy, Diversity and Segregation, EDR.3 – Common Cause Failures, EDR.4 - Single Failure Criterion, ESS.18 - Failure Independence, and ERC.2 - Shutdown Systems). The review has taken due cognisance of selected HSE Technical Assessment Guides (TAGs) and international nuclear safety standards. The task has also reviewed evidence presented by EDF and AREVA via:

- the claims-argument-evidence table that provides the basis of the demonstration of SAP conformance;
- responses to Technical Queries;
- responses to actions from meetings involving EDF and AREVA, HSE/NII and the TSC;
- and responses to technical observations raised during the preliminary activity, including diversity-related observations in the HSE/NII GDA Step 2 and Step 3 reports.

In addition, the task has reviewed diversity-related changes to the UK EPR C&I architecture that have occurred since the end of Step 3 of the GDA process.

The scope of the evidence that is specific to UK EPR is defined by EDF and AREVA in *"UK EPR CONTROL AND INSTRUMENTATION (C&I) – SCOPE OF GDA"* (letter ND(NII)EPR00686N). The review of the diversity of those systems contributing to the implementation of category A functions is consistent with this scoping letter. The main systems that were reviewed in the diversity review are as follows: Protection System (hosted on the Teleperm XS platform); Safety Automation System and Process Automation System (hosted on the SPPA-T2000 platform); and the Non-Computerised Safety System

Annex 8

(NCSS), which has been added to the C&I architecture since Step 3 of GDA in response to Regulatory Issue RI-UKEPR-002.

A total of 11 technical observations resulting from the review remain unresolved at the end of the review period. These technical observations have been designated as TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher – 5 of these observations have been designated as TO1 and 6 of these observations have been designated as TO2. Note that where a gap in the numbering sequence exists, this is due to the resolution of an observation that had been allocated this number.

<u>Technical Observations designated TO1</u>

The five TO1 technical observations are:

T18.TO1.01 - The designer or future operator/licensee is requested to update the Pre-Construction Safety Report (PCSR) to capture the claims-argument-evidence information, and to reflect the diversity-related changes that result from the modifications to the architecture for UK EPR that have been committed to by EDF and AREVA since June 2009.

T18.TO1.02 - The designer or future operator/licensee is requested to provide detailed substantiation for the reliability claims and classification of all C&I components used by more than one system important to safety, and potentially by more than one line of defence, for example, common use of sensors, the Process instrumentation Preprocessing System, actuators, and the Priority and Actuator Control System, by the protection systems for the same Postulated Initiating Event. In addition:

a. the substantiation should consider the potential for common mode failure as a result of use of such common components;
b. where the required reliability of a device or system exceeds expected claim limits for this type of equipment, the designer or future operator/licensee is requested to present a solution that employs diversity to reduce the reliability claims within the claim limits.

T18.TO1.03 - The technology to be used for the implementation of the Non-Computerised Safety System is out of scope of GDA Step 4, and as a result, its diversity from that of the computerised platforms, and justification of its reliability claim, could not be assessed. The designer or future operator/licensee is requested to address this by provision of a safety demonstration through a Basis of Safety Case for the diversity aspects of the NCSS when the supplier and technology for NCSS have been selected.

T18.TO1.04 - Version S5 of the SPPA-T2000 platform is believed to be obsolete. Should a different version be selected for UK EPR, the designer or future operator/licensee is requested to substantiate the diversity claim between Teleperm XS and the new version. This substantiation to cover, amongst others, diversity of the technology (including hardware and software components, communication protocol, and supplier etc.) of the class 1 Profibus network in Teleperm XS, and the technology of the class 2 Profibus DP network in the AS 620B Automation System in the SPPA-T2000. The designer or future operator/licensee is also requested to present a full diversity analysis between the UK EPR version of SPPA-T2000 and the technology selected for the Non-Computerised Safety System.

T18.TO1.05 - The designer or future operator/licensee is requested to address in the safety case submission, the commitment in the response to Technical Query 368 observation 3 – “*Areva/EDF will*

Annex 8

avoid use of, for a given initiating event, the same type of smart equipment in multiple lines of defence."

Technical Observations designated TO2

The six TO2 technical observations are:

T18.TO2.01 - The designer or future operator/licensee is requested to include in the safety case submission the analysis of the effect of the loss of one or more divisions on the Protection System (PS) category A functions that need to exchange information across all divisions, and to justify why this does not compromise the safety aspects of these category A functions.

T18.TO2.03 - The designer or future operator/licensee is requested to update the Fault Schedule to identify the C&I systems that are involved in each safety function, and the required risk reductions.

T18.TO2.06 - There are two independent mechanisms for shutdown – reactor trip and extra boration – and both are claimed to be actuated by the diverse protection systems Protection System (PS) and Safety Automation System (SAS). Whilst there is evidence that PS and SAS implement diverse Reactor Trip functions, the designer or future operator/licensee is requested to demonstrate adequate diversity and common mode failure analysis for:

a. the equipment used by PS to actuate boration, compared to the equipment used by SAS to actuate boration;

b. the equipment used by either PS or SAS to actuate reactor trip, compared to the equipment used by that system to actuate boration.

T18.TO2.07 - Document "*TELEPERM XS based systems - Concept for Electrical Separation*" (NLE-F DC 249 rev C) specifies the requirements and technological solutions for electrical separation between Teleperm XS equipment and other technology equipment for the Flamanville 3 reactor. For each solution, evidence is provided to demonstrate compliance with the appropriate clause in the French Nuclear Standard "*RCC-E*", except for two solutions in section 4.2, which are noted as temporary solutions, with RCC-E compliance being "under analysis". These relate to the electrical signals that are output from, or input to Teleperm XS computers, using an overvoltage barrier module to provide protection. The designer or future operator/licensee is requested to demonstrate for these two cases that a solution that complies with RCC-E has been designed for UK EPR.

T18.TO2.08 - SAP ERC.2 paragraph 445 relates to, for example, situations where the control rods fail to insert on a Reactor Trip signal from the Protection System. In this situation an Anticipated Transient Without Scram (ATWS) signal is initiated by the C&I to actuate the Extra Boration System (EBS) and Safety Injection System (SIS) to inject borated water. The designer or future operator/licensee is requested to address this scenario in the claims-argument-evidence entry for SAP ERC.2.

T18.TO2.09 - Regarding diversity of specification:

a. The requirements specifications of the Teleperm XS and the SPPA-T2000 platforms were not made available during the timescales of the review. Hence a diversity analysis of these specifications could not be carried out. The designer or future operator/licensee is requested

Annex 8

to demonstrate adequate diversity in the method of specifying the requirements of Teleperm XS and SPPA-T2000.

b. The requirements for diverse systems such as the Protection System (PS) and the Safety Automation System (SAS) are each expressed using high-level function block diagrams. The designer or future operator/licensee is requested to demonstrate adequate diversity in the method of specifying the requirements of PS and SAS.

A number of further observations that relate to diversity aspects of the C&I architecture have arisen from the review of the responses to Regulatory Issue RI-UKEPR-002 and are documented in "*Review of Responses to Regulatory Issue RI-UKEPR-002 - Task 20*" - these observations are prefixed by "T20" and their significance is documented in the aforementioned Task 20 report. Reference is also made to observations raised by the review of C&I architecture that are documented in "*Step 4 Report for Task 17: Review of C&I Architecture for UK EPR*"– these observations are prefixed by "T17".

<u>Conclusion of Task Review</u>

With regard to the seven aspects of diversity that were covered by the review, the following conclusions are reached:

a) equipment diversity (including diversity of platform) – the most significant observation is for the designer or future operator/licensee to provide detailed substantiation for the reliability claims and classification of all C&I components used by more than one system important to safety, and potentially by more than one line of defence (T18.TO1.02);
b) diversity of verification and validation – the most significant observation is for the designer or future operator/licensee to justify diversity between Teleperm XS and SPPA/T2000 on verification / validation tools, methods and teams (T20.A1.3.4 (TO2));
c) diversity of physical location (segregation) – the most significant observation is for the designer or future operator/licensee to update the specification of the Protection System to include the commitments made by EDF and AREVA regarding inputs to the Protection System from lower class systems, and from the Teleperm XS Service Unit (T17.TO1.04 and T17.TO1.25);
d) software diversity – the most significant observation is for the designer or future operator/licensee to justify diversity between Teleperm XS and SPPA/T2000 on software development tools, methods and programming environment (T20.A1.3.4 (TO2));
e) functional / data / signal diversity – the most significant observation is for the designer or future operator/licensee to provide detailed substantiation for the reliability claims and classification of sensors (including Smart sensors) and sensor conditioning modules used by more than one system important to safety, and potentially by more than one line of defence (T18.TO1.02 and T18.TO1.05);
f) diversity of design / development – the most significant observation is for the designer or future operator/licensee to justify diversity between Teleperm XS and SPPA/T2000 on design / development tools, methods and programming environment (T20.A1.3.4 (TO2));
g) diversity of specification – observations were raised requesting the designer or future operator/licensee to demonstrate adequate diversity in the method of specifying the requirements of Teleperm XS compared to SPPA-T2000, and the requirements of the Protection System compared to the Safety Automation System (T18.TO2.09).

A further conclusion is that there is the need to repeat aspects of these diversity reviews when the technology and supplier for the Non-Computerised Safety System has been selected (T18.TO1.03), and when the version of the SPPA-T2000 platform for UK EPR has been finalised (T18.TO1.04).

Annex 8

With regard to the four main diversity-related observations in the HSE/NII GDA Step 3 report, the following conclusions are reached:

a) "*excessive reliability claim for the diverse protection systems taken together*" has been resolved by the commitment in letter EPR00180R to reduce the reliability claims as a result of introduction of the Non-Computerised Safety System;

b) "*lack of evidence of platform diversity*" has been progressed and outstanding points are covered by the following observations: T20.A1.3.4 (TO2), T18.TO1.03, T18.TO1.04, and T18.TO2.09, and by potential GDA Issue PGI-UKEPR-C&I-07 action 1[21];

c) "*lack of evidence of diversity within systems in the same safety group when high reliability is needed*" has been progressed and outstanding points are covered by observation T18.TO1.02, and potential GDA Issue PGI-UKEPR-C&I-07 action 9[22];

d) "*absence of key information in the PCSR*" has been progressed and outstanding points are covered by observation T18.TO1.01, and potential GDA Issue PGI-UKEPR-C&I-04[23].

Of the five SAPs considered in the Task 18 review, all have associated technical observations. Nevertheless, the diversity-related changes that have been introduced into the C&I architecture since GDA Step 3 have resulted in each of these five SAPs being addressed in principle.

It is the opinion of the TSC that an acceptable way forward has been achieved for the major diversity-related elements of the C&I design to meet the intent of the appropriate SAPs, TAGs and IEC standards, subject to successful resolution of the observations arising from this review, and the applicable potential GDA Issues.

[21] ND note: GI-UKEPR-CI-06.A1 is the issued version of the provisional GDA Issue (pGI).

[22] ND note: GI-UKEPR-CI-06.A9 is the issued version of the provisional GDA Issue (pGI).

[23] ND note: GI-UKEPR-CI-03 is the issued version of the provisional GDA Issue (pGI).

Annex 8

Review of Responses to Regulatory Issue RI-UKEPR-002 – TSC Summary[24]

Note this information has been imported from a TSC report (Ref. 34) and the formatting of the TSC report has been retained.

[24] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 8

A Annex: TSC Task Summary: Review of Responses to Regulatory Issue RI-UKEPR-002

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of the responses by EDF and AREVA to the actions in Regulatory Issue RI-UKEPR-002 (TSC Task 20) within the action plan defined in letter ND(NII) EPR00459R.

The Regulatory Issue RI-UKEPR-002 was closed by HSE/NII in November 2010 via letter EPR0700266N.

However there remain open technical observations from the TSC Task 20 review, some of which have been covered by actions within Potential GDA Issues that relate to C&I for UK EPR. This Annex lists the 19 open technical observations that resulted from the Task 20 review. Each technical observation has been identified throughout the Task 20 review period using a unique identifier that is of the form "*T20.<action number within RI-UKEPR-002>.<index>*". Each technical observation has also been designated as "*TO1*" or "*TO2*" by the TSC depending on its significance, of which TO1 is the higher. The Task 20 open technical observations are listed below, and have been grouped according to the subject matter of the following TSC Tasks:

a) TSC Task 14, which has reviewed the Quality Assurance arrangements and procedures that are defined by EDF-CNEN and Areva NP Quality Management Systems, and that relate to the lifecycle of class 1, 2 and 3 C&I systems;
b) TSC Task 15, which has reviewed the evidence to support the classification of the class 1 and 2 pre-developed components of the C&I architecture, in particular the Teleperm XS, and SPPA-T2000 platforms;
c) TSC Task 16, which has reviewed the evidence to support the classification of the class 1 and 2 C&I systems important to safety, in particular the Protection System and the Safety Automation System;
d) TSC Task 17, which has reviewed the C&I architecture for safety capability;
e) TSC Task 18, which has reviewed the evidence to support the diversity claims and argumentation of those C&I systems contributing to the implementation of category A functions.

Note that where a gap in the indexing sequence exists in the technical observation identifiers, this is due to the resolution of a technical observation that had been allocated this index during the Task 20 review period.

Applicable to all TSC Tasks

T20.A1.2.4 – designation TO1 - The selection of the supplier and technology to be used for the Non Computerised Safety System (NCSS) platform has not yet been made, and hence the review of the suitability of the technology, and of the lifecycle processes to develop class 2 NCSS application functions, to meet reliability claims, safety requirements and diversity criteria, has not been possible. The designer or future operator/licensee is requested to address this by provision of a safety demonstration through a Basis of Safety Case for the NCSS, when the supplier and technology for NCSS have been selected.

Annex 8

Task 15 (Pre-Developed Components)

T20.A1.4.1 – designation TO1 - The designer or future operator/licensee is requested to:

a) justify the class 1 software reliability claim for Teleperm XS and the Protection System, based on the Production Excellence and Independent Confidence Building argument.

b) demonstrate compliance with IEC 60987 for the development, verification and qualification of the SPPA-T2000 platform hardware.

c) align the reliability claims for the Reactor Control, Surveillance and Limitation System, and the Severe Accident Instrumentation & Control System, that are defined by the Compact Model for the UK EPR PSA (section 4.2.1 of NEPS-F DC 576 rev A) with the claim limits for computer-based systems in observation T17.TO1.01, in particular:

d) - Class 2 1E-2 ≤ pfd

e) - Class 3 1E-1 ≤ pfd

T20.A1.5.2 – designation TO1 - The designer or future operator/licensee is requested to demonstrate compliance of Teleperm XS lifecycle processes with IEC 60880 and IEC 60987.

T20.A1.5.5 – designation TO1 - The designer or future operator/licensee is requested to justify the use of programmable complex electronic components within the Teleperm XS modules that are components of UK EPR class 1 systems. The justification should identify the standards, guidance and criteria that are used to demonstrate that the components are fit for purpose, and provide evidence of their application.

Task 16 (Systems Important to Safety)

T20.A1.4.3 – designation TO2 - The designer or future operator/licensee is requested to justify the differences between instances of the Protection System across the four divisions, and the argument for how this does not compromise redundancy or overall reliability.

T20.A1.5.1 – designation TO1 - The designer or future operator/licensee is requested to address the following areas for improvement that resulted from the review of production excellence and independent confidence building measures for the Protection System in document ENSECC090137 Rev B:

a) lack of mention of the use of formal methods, and the limitations of the PolySpace tool for static analysis (no formal proof capability);

b) the need for a detailed investigation into the reasonable practicability of increasing the number of statistical tests that are executed in the target environment from 5000 during the site licensing phase, and the need to provide a plan of all activities required to implement the statistical tests;

c) lack of mention of qualification of the development tool-chain for class 1 application development, and in particular, validation of the compiler.

T20.A2.2.3 – designation TO2 – The specification of the Protection System for UK EPR in document NLN-F DC 193 rev A contains a note that suggests that it does not fully reflect the UK EPR solution and that this specification will only be completed during the site license phase. The designer or future

Annex 8

operator/licensee is requested to present a clear statement on the parts of the Protection System specification that are to be considered as complete for UK EPR, as documented in NLN-F DC 193 Rev A.

Task 17 (C&I Architecture)

T20.A1.3.5 – designation TO1 - The designer or future operator/licensee is requested to justify the reliability claims of the Priority and Actuator Control System and Reactor Trip equipment when either is shared by more than one line of defence for the same Postulated Initiating Event.

T20.A2.2.1 – designation TO1 - The designer or future operator/licensee is requested to address the following commitments made in the response to TQ-EPR-1003 regarding one-way communication from the Protection System to lower-classified systems:

a) Signal from Safety Automation System (SAS) / Process Automation System (PAS) to the Protection System (PS) for the periodic test of the Emergency Feed Water System pump (EFWP) – "*A solution to inhibit this signal when no periodic test is being performed will be implemented. The detailed solution will be defined during the detailed design phase (outside the scope of GDA)*".

b) For all signals from SAS/PAS to PS – "*A final confirmatory analysis, based on the final list of exchanged signals, will be performed during the detailed design phase outside the scope of GDA.*"

c) "*The alarms from the Reactor Control, Surveillance and Limitation System to the Safety Information & Control System will be implemented by a separate connection without interface with the Protection System.*"

d) "*A separate connection from the Severe Accident Instrumentation and Control System (SA I&C) to the Process Information & Control System will be implemented in the UK EPR in order to remove all connections from the SA I&C to the Protection System.*"

e) "*…the TELEPERM XS gateway GW1 and the network to the Monitoring and Service Interface will be implemented with E1A TELEPERM XS components.*"

f) Analysis of hard-wired connections from the Non Computerised Safety System to PS.

It is noted that there may be detailed implementation issues which cannot be fully addressed under GDA.

T20.A2.3.2 – designation TO1 - The designer or future operator/licensee is requested to demonstrate non-interference in the operation of a higher class system by the operation of a lower class system, for all cases where C&I systems of different classification are connected and can operate as part of the same safety function. The demonstration to address communication from the class 3 Process Information & Control System (PICS), via class 3 networks, to the class 2 Safety Automation System (SAS).

T20.A2.3.4 – designation TO2 - The designer or future operator/licensee is requested to demonstrate that electrical separation is implemented for each I&C system hosted by the SPPA-T2000 platform.

Annex 8

T20.A3.6 – designation TO1 – EDF and AREVA has indicated in letter EPR00607N that the intention for UK EPR is to implement a class 1 Qualified Display System (QDS) for the class 1 displays and controls sent to the Protection System, in both the Main Control Room (MCR) and the Remote Shutdown Station (RSS). The designer or future operator/licensee is requested to:

a) produce detailed substantiation of the Class 1 control and display facilities in the MCR and RSS, noting the strong preference of HSE/NII for these to be the same for MCR and RSS, and for these to include manual Reactor Trip and Engineered Safeguard Action controls, as well as Permissives and Resets for the Protection System;

b) justify any class 1 controls and displays provided by the Safety Information & Control System (SICS) in the MCR, that are not supported by the QDS in the RSS, especially relating to SICS controls sent to the Safety Automation System and the Non Computerised Safety System;

c) produce a Basis of Safety Case for the Class 1 control and display system (QDS);

d) produce a justification in terms of the functional coverage of the QDS (the response to include consideration of US Nuclear Regulatory Commission Regulatory Guide 1.97 Revision 3).

T20.A4.6.2 – designation TO1 - The designer or future operator/licensee is requested to consider whether the Process Automation System (PAS) implements any of the main reactor controls, and if so, to justify why category B is not the appropriate categorisation of these functions, and why class 2 is not the appropriate classification of the PAS system.

T20.A5.4 – designation TO2 - The designer or future operator/licensee is requested to demonstrate that performance tests that verify end-to-end response times from sensor data acquisition through to sending an actuation order, have been executed without failure for the Protection System and Safety Automation System safety and safety-related functions on the Flamanville 3 reference implementation.

T20.A5.5 – designation TO2 - The designer or future operator/licensee is requested to demonstrate, for those functions important to safety which use the Class 3 Terminal bus and/or Plant bus, that end-to-end response time requirements are achievable by design.

Task 18 (Diversity)

T20.A1.2.3 – designation TO1 - The designer or future operator/licensee is requested to address the following review comments in a revision of the Non Computerised Safety System (NCSS) diversity requirements specification.

a) Please clarify how analysis of Common Cause Failure (CCF) as a result of shared sensors, or shared use of signal conditioning systems (PIPS), or shared use of actuators, by more than one of the protection systems, is taken into account in the Probabilistic Safety Assessment (PSA). In this context, note that the claim limit for hardware-based systems as defined by the SAPs and TAGs is 1E-5 pfd.

b) There are a number of entries where it is stated “no diversity requirement”. Please ensure that the reasons for there being no diversity requirement is explained and justified in the document. For example, it is necessary to ensure relevant IEC 61513 clauses are addressed (e.g. design and test diversity) and in particular the I&C system tests which are part of verification and validation would appear to require diversity.

Annex 8

c) Please clarify why there is no diversity requirement for the NCSS maintenance processes, particularly relating to outage maintenance.

d) Please clarify whether diversity level Ed=3 / Hd=3 applies to the V&V for the NCSS platform (compared to that of the Teleperm XS and SPPA-T2000 platforms) and if so, to reflect this in the document. Also please clarify the role of third party certification organisations such as TÜV.

e) Please explain why the risk of error introduction by the use of common testing tools and/or a common test environment between NCSS and the Protection System (or Safety Automation System) is not a concern.

f) Please explain how the risk of CCF due to the use of common basic components (such as capacitors and resistors) is addressed and factored into the PSA.

T20.A1.3.1 – designation TO1 - The designer or future operator/licensee is requested to:

a) substantiate the probabilistic claims for any sensor, and any module of the sensor conditioning and decoupling system (PIPS), that is used by more than one system important to safety, and potentially by more than one line of defence. Where probabilistic claims exceed claim limits for such devices that are defined by HSE/NII, the designer or future operator/licensee is requested to present a solution that employs diversity to reduce the reliability claims within the claim limits.

b) align the reliability claim for non-class-1 instrumentation in the UK EPR PSA, as given in the Compact Model (section 4.1 of document NEPS-F DC 576 rev A), with the claim limits stated in observation T17.TO1.01b, in particular:

c) - Class 2 1E-3 ≤ pfd < 1E-2

d) - Class 3 1E-2 ≤ pfd ≤ 1E-1.

T20.A1.3.4 – designation TO2 - The designer or future operator/licensee is requested to justify diversity between Teleperm XS and SPPA-T2000 platforms, on tools, methods and programming environment. This is also to address independence of Teleperm XS and SPPA-T2000 teams.

T20.A1.4.2 – designation TO1 - The designer or future operator/licensee is requested to demonstrate the reliability of the protection systems when taken in combination. If multiplication of probability-of-failure-on-demand values is used, then the adequacy of independence and diversity needs to be established.

Conclusion of Task Review

Although Regulatory Issue RI-UKEPR-002 has been closed, the designer or future operator/licensee is requested to respond to the technical observations resulting from the Task 20 review. It is noted that in some cases, this may be achieved via resolution of actions in the Potential GDA Issues raised by HSE/NII that relate to C&I.

Annex 9

TSC Summary – Review of Responses to Regulatory Issue RI-UKEPR-002[25]

Note this information has been imported from a TSC report (Ref. 34) and the formatting of the TSC report has been retained.

[25] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 9

A Annex: TSC Task Summary - Review of Responses to Regulatory Issue RI-UKEPR-002

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of the responses by EDF and AREVA to the actions in Regulatory Issue RI-UKEPR-002 (TSC Task 20) within the action plan defined in letter ND(NII) EPR00459R.

The Regulatory Issue RI-UKEPR-002 was closed by HSE/NII in November 2010 via letter EPR0700266N.

However there remain open technical observations from the TSC Task 20 review, some of which have been covered by actions within Potential GDA Issues that relate to C&I for UK EPR. This Annex lists the 19 open technical observations that resulted from the Task 20 review. Each technical observation has been identified throughout the Task 20 review period using a unique identifier that is of the form "*T20.<action number within RI-UKEPR-002>.<index>*". Each technical observation has also been designated as "*TO1*" or "*TO2*" by the TSC depending on its significance, of which TO1 is the higher. The Task 20 open technical observations are listed below, and have been grouped according to the subject matter of the following TSC Tasks:

f) TSC Task 14, which has reviewed the Quality Assurance arrangements and procedures that are defined by EDF-CNEN and Areva NP Quality Management Systems, and that relate to the lifecycle of class 1, 2 and 3 C&I systems;

g) TSC Task 15, which has reviewed the evidence to support the classification of the class 1 and 2 pre-developed components of the C&I architecture, in particular the Teleperm XS, and SPPA-T2000 platforms;

h) TSC Task 16, which has reviewed the evidence to support the classification of the class 1 and 2 C&I systems important to safety, in particular the Protection System and the Safety Automation System;

i) TSC Task 17, which has reviewed the C&I architecture for safety capability;

j) TSC Task 18, which has reviewed the evidence to support the diversity claims and argumentation of those C&I systems contributing to the implementation of category A functions.

Note that where a gap in the indexing sequence exists in the technical observation identifiers, this is due to the resolution of a technical observation that had been allocated this index during the Task 20 review period.

Applicable to all TSC Tasks

T20.A1.2.4 – designation TO1 - The selection of the supplier and technology to be used for the Non Computerised Safety System (NCSS) platform has not yet been made, and hence the review of the suitability of the technology, and of the lifecycle processes to develop class 2 NCSS application functions, to meet reliability claims, safety requirements and diversity criteria, has not been possible. The designer or future operator/licensee is requested to address this by provision of a safety demonstration through a Basis of Safety Case for the NCSS, when the supplier and technology for NCSS have been selected.

Annex 9

Task 15 (Pre-Developed Components)

T20.A1.4.1 – designation TO1 - The designer or future operator/licensee is requested to:

- **f) justify the class 1 software reliability claim for Teleperm XS and the Protection System, based on the Production Excellence and Independent Confidence Building argument.**
- **g) demonstrate compliance with IEC 60987 for the development, verification and qualification of the SPPA-T2000 platform hardware.**
- **h) align the reliability claims for the Reactor Control, Surveillance and Limitation System, and the Severe Accident Instrumentation & Control System, that are defined by the Compact Model for the UK EPR PSA (section 4.2.1 of NEPS-F DC 576 rev A) with the claim limits for computer-based systems in observation T17.TO1.01, in particular:**
- **i) - Class 2 1E-2 ≤ pfd**
- **j) - Class 3 1E-1 ≤ pfd**

T20.A1.5.2 – designation TO1 - The designer or future operator/licensee is requested to demonstrate compliance of Teleperm XS lifecycle processes with IEC 60880 and IEC 60987.

T20.A1.5.5 – designation TO1 - The designer or future operator/licensee is requested to justify the use of programmable complex electronic components within the Teleperm XS modules that are components of UK EPR class 1 systems. The justification should identify the standards, guidance and criteria that are used to demonstrate that the components are fit for purpose, and provide evidence of their application.

Task 16 (Systems Important to Safety)

T20.A1.4.3 – designation TO2 - The designer or future operator/licensee is requested to justify the differences between instances of the Protection System across the four divisions, and the argument for how this does not compromise redundancy or overall reliability.

T20.A1.5.1 – designation TO1 - The designer or future operator/licensee is requested to address the following areas for improvement that resulted from the review of production excellence and independent confidence building measures for the Protection System in document ENSECC090137 Rev B:

- **d) lack of mention of the use of formal methods, and the limitations of the PolySpace tool for static analysis (no formal proof capability);**
- **e) the need for a detailed investigation into the reasonable practicability of increasing the number of statistical tests that are executed in the target environment from 5000 during the site licensing phase, and the need to provide a plan of all activities required to implement the statistical tests;**
- **f) lack of mention of qualification of the development tool-chain for class 1 application development, and in particular, validation of the compiler.**

T20.A2.2.3 – designation TO2 – The specification of the Protection System for UK EPR in document NLN-F DC 193 rev A contains a note that suggests that it does not fully reflect the UK EPR solution and that this specification will only be completed during the site license phase. The designer or future

Annex 9

operator/licensee is requested to present a clear statement on the parts of the Protection System specification that are to be considered as complete for UK EPR, as documented in NLN-F DC 193 Rev A.

Task 17 (C&I Architecture)

T20.A1.3.5 – designation TO1 - The designer or future operator/licensee is requested to justify the reliability claims of the Priority and Actuator Control System and Reactor Trip equipment when either is shared by more than one line of defence for the same Postulated Initiating Event.

T20.A2.2.1 – designation TO1 - The designer or future operator/licensee is requested to address the following commitments made in the response to TQ-EPR-1003 regarding one-way communication from the Protection System to lower-classified systems:

g) Signal from Safety Automation System (SAS) / Process Automation System (PAS) to the Protection System (PS) for the periodic test of the Emergency Feed Water System pump (EFWP) – "*A solution to inhibit this signal when no periodic test is being performed will be implemented. The detailed solution will be defined during the detailed design phase (outside the scope of GDA)*".

h) For all signals from SAS/PAS to PS – "*A final confirmatory analysis, based on the final list of exchanged signals, will be performed during the detailed design phase outside the scope of GDA.*"

i) "*The alarms from the Reactor Control, Surveillance and Limitation System to the Safety Information & Control System will be implemented by a separate connection without interface with the Protection System.*"

j) "*A separate connection from the Severe Accident Instrumentation and Control System (SA I&C) to the Process Information & Control System will be implemented in the UK EPR in order to remove all connections from the SA I&C to the Protection System.*"

k) "*…the TELEPERM XS gateway GW1 and the network to the Monitoring and Service Interface will be implemented with E1A TELEPERM XS components.*"

l) Analysis of hard-wired connections from the Non Computerised Safety System to PS.

It is noted that there may be detailed implementation issues which cannot be fully addressed under GDA.

T20.A2.3.2 – designation TO1 - The designer or future operator/licensee is requested to demonstrate non-interference in the operation of a higher class system by the operation of a lower class system, for all cases where C&I systems of different classification are connected and can operate as part of the same safety function. The demonstration to address communication from the class 3 Process Information & Control System (PICS), via class 3 networks, to the class 2 Safety Automation System (SAS).

T20.A2.3.4 – designation TO2 - The designer or future operator/licensee is requested to demonstrate that electrical separation is implemented for each I&C system hosted by the SPPA-T2000 platform.

Annex 9

T20.A3.6 – designation TO1 – EDF and AREVA has indicated in letter EPR00607N that the intention for UK EPR is to implement a class 1 Qualified Display System (QDS) for the class 1 displays and controls sent to the Protection System, in both the Main Control Room (MCR) and the Remote Shutdown Station (RSS). The designer or future operator/licensee is requested to:

e) produce detailed substantiation of the Class 1 control and display facilities in the MCR and RSS, noting the strong preference of HSE/NII for these to be the same for MCR and RSS, and for these to include manual Reactor Trip and Engineered Safeguard Action controls, as well as Permissives and Resets for the Protection System;

f) justify any class 1 controls and displays provided by the Safety Information & Control System (SICS) in the MCR, that are not supported by the QDS in the RSS, especially relating to SICS controls sent to the Safety Automation System and the Non Computerised Safety System;

g) produce a Basis of Safety Case for the Class 1 control and display system (QDS);

h) produce a justification in terms of the functional coverage of the QDS (the response to include consideration of US Nuclear Regulatory Commission Regulatory Guide 1.97 Revision 3).

T20.A4.6.2 – designation TO1 - The designer or future operator/licensee is requested to consider whether the Process Automation System (PAS) implements any of the main reactor controls, and if so, to justify why category B is not the appropriate categorisation of these functions, and why class 2 is not the appropriate classification of the PAS system.

T20.A5.4 – designation TO2 - The designer or future operator/licensee is requested to demonstrate that performance tests that verify end-to-end response times from sensor data acquisition through to sending an actuation order, have been executed without failure for the Protection System and Safety Automation System safety and safety-related functions on the Flamanville 3 reference implementation.

T20.A5.5 – designation TO2 - The designer or future operator/licensee is requested to demonstrate, for those functions important to safety which use the Class 3 Terminal bus and/or Plant bus, that end-to-end response time requirements are achievable by design.

Task 18 (Diversity)

T20.A1.2.3 – designation TO1 - The designer or future operator/licensee is requested to address the following review comments in a revision of the Non Computerised Safety System (NCSS) diversity requirements specification.

g) Please clarify how analysis of Common Cause Failure (CCF) as a result of shared sensors, or shared use of signal conditioning systems (PIPS), or shared use of actuators, by more than one of the protection systems, is taken into account in the Probabilistic Safety Assessment (PSA). In this context, note that the claim limit for hardware-based systems as defined by the SAPs and TAGs is 1E-5 pfd.

h) There are a number of entries where it is stated “no diversity requirement”. Please ensure that the reasons for there being no diversity requirement is explained and justified in the document. For example, it is necessary to ensure relevant IEC 61513 clauses are addressed (e.g. design and test diversity) and in particular the I&C system tests which are part of verification and validation would appear to require diversity.

Annex 9

i) Please clarify why there is no diversity requirement for the NCSS maintenance processes, particularly relating to outage maintenance.

j) Please clarify whether diversity level Ed=3 / Hd=3 applies to the V&V for the NCSS platform (compared to that of the Teleperm XS and SPPA-T2000 platforms) and if so, to reflect this in the document. Also please clarify the role of third party certification organisations such as TÜV.

k) Please explain why the risk of error introduction by the use of common testing tools and/or a common test environment between NCSS and the Protection System (or Safety Automation System) is not a concern.

l) Please explain how the risk of CCF due to the use of common basic components (such as capacitors and resistors) is addressed and factored into the PSA.

T20.A1.3.1 – designation TO1 - The designer or future operator/licensee is requested to:

e) substantiate the probabilistic claims for any sensor, and any module of the sensor conditioning and decoupling system (PIPS), that is used by more than one system important to safety, and potentially by more than one line of defence. Where probabilistic claims exceed claim limits for such devices that are defined by HSE/NII, the designer or future operator/licensee is requested to present a solution that employs diversity to reduce the reliability claims within the claim limits.

f) align the reliability claim for non-class-1 instrumentation in the UK EPR PSA, as given in the Compact Model (section 4.1 of document NEPS-F DC 576 rev A), with the claim limits stated in observation T17.TO1.01b, in particular:

g)- Class 2 1E-3 ≤ pfd < 1E-2

h)- Class 3 1E-2 ≤ pfd ≤ 1E-1.

T20.A1.3.4 – designation TO2 - The designer or future operator/licensee is requested to justify diversity between Teleperm XS and SPPA-T2000 platforms, on tools, methods and programming environment. This is also to address independence of Teleperm XS and SPPA-T2000 teams.

T20.A1.4.2 – designation TO1 - The designer or future operator/licensee is requested to demonstrate the reliability of the protection systems when taken in combination. If multiplication of probability-of-failure-on-demand values is used, then the adequacy of independence and diversity needs to be established.

Conclusion of Task Review

Although Regulatory Issue RI-UKEPR-002 has been closed, the designer or future operator/licensee is requested to respond to the technical observations resulting from the Task 20 review. It is noted that in some cases, this may be achieved via resolution of actions in the Potential GDA Issues raised by HSE/NII that relate to C&I.

Annex 10

EDF and AREVA Final Deliverables in Response to the C&I GDA Issues

GDA issue	GDA issue action	Document title and reference number / description if not evident from title	Revision	TRIM reference
		GDA Issue CI-01		
CI-01	A1	*Justification note for NCSS platform selection*: PTI DC 5	Rev. A	2011/348047
CI-01	A1	*Outline of Basis of Safety Case of Non-Computerized Safety System*: PEL-F/11.0309	24/10/11	2011/559493
CI-01	A1	*List of contents of NCSS Basis of Safety Case*: PTLI 12.1060	Rev. A	2012/262204
CI-01	A1	*Non-Computerised Safety System - Basis of Safety Case*: PTL-F DC 5	Rev. A	2012/309805
CI-01	A1	NCSS - BSC Requirements Traceability Matrix	03/08/12	2012/309800
CI-01	A1	*Unicorn Project - Platform Quality Plan*: TA-2057230	Rev. D	2012/264201
CI-01	A1	*NCSS Quality Plan*: TA-2061589	Rev. C	2012/271260
CI-01	A1	*NCSS System Verification and Validation Plan*: TA-2065953	Ind. C	2012/304887
CI-01	A1	*UNICORN Project Justification of Platform reliability & Response Time on a typical automatic function*: TA-2082935	Ind. B	2012/300352
CI-01	A1	*UNICORN Project Justification of Reliability Allocation*: TA-2096900	Ind. A	2012/300353
CI-01	A1	*NCSS platform specification*: TA-2060143	Rev. C	2012/234904
CI-01	A1	*UNICORN Project Module Common Requirements Specification*: TA-2084059	Ind. A	2012/306921
CI-01	A1	*UNICORN Project Module Specification SCAT NTA-228830*: TA-2080785	Ind. A	2012/306884
CI-01	A1	*UNICORN Project Module Specification VOPER NTA-228831*: TA-2080787	Ind. A	2012/306889
CI-01	A1	*UNICORN Project Module Specification AVACT NTA-228835*: TA-2080788	Ind. A	2012/306907
CI-01	A1	*Design of the NCSS System – Principles of Selection of Actuators Orders and Information for Operation*: ECECC100555	Rev. B	2012/261606

Annex 10

GDA issue	GDA issue action	Document title and reference number / description if not evident from title	Revision	TRIM reference
CI-01	A1	*UNICORN Project platform qualification programme*: TA-2073805	Ind. D	2012/300350
CI-01	A1	*NCSS System Specification*: TA-2062484	Ind. C	2012/271215
CI-01	A1	*C&I back up system*: UKEPR-CMF-014	Rev. B	2011/86065
CI-01	A1	*Safety Requirements for Non-Computerised Safety System (NCSS)*: NEPS-F DC 555	Rev. D	2012/243802
CI-01	A1	*EPR UK Functional Requirements on Non-Computerised Safety I&C Functions*: NEPR-F DC 551	Rev. C	2012/284449
CI-01	A1	*Comparison of the NCSS functions and SAS diversified functions*: PEPR-F.12.1062	Rev. 1	2012/343682
CI-01	A1	*EPR UK – Functional Justification of the Non-Computerised Safety System Design*: PEPR-F DC 105	Rev. A	2012/284451
CI-01	A1	*Requirements for Non-Computerised I&C Platform*: PTI DC 2	Rev. E	2012/180475
CI-01	A1	*Non Computerized Safety System - Diversity Criteria*: PELL-F DC 11	Rev. C	2012/343776
GDA Issue CI-02				
CI-02	A1	*Programme of Statistical Testing Activities*: ECECC111521	Rev. B	2012/241333
CI-02	A1	*Proposal for Research Programme on Simulation-Based Statistical Testing*: ECECC111572	Rev. B	2012/241363
CI-02	A1	*Feasibility study into the use of MALPAS for UK EPR*: 5094205-rep-01	Ver 3.0	2012/241187
CI-02	A1	*Feasibility Study into Compiler Validation for Teleperm XS*: 5098073-rep-02	Ver 4.0	2012/241308
CI-02	A1	*UK EPR Protection System - scope and programme of work to address functional static analysis and compiler validation*: ENSECC110123	Rev. B	2012/241312
CI-02	A1	*UK EPR Protection System - Overall Scope of Independent Confidence Building Measures*: ENSECC110173	Rev. B	2012/261811
GDA Issue CI-03				
CI-03	A1	*UKEPR GDA I&C System CAE Document*: 16626-709-000-RPT-0028	Issue 3	2012/263127
CI-03	A1	*Update of Claims-Argument-Evidences trail for satisfaction of SAPs relevant to I&C*: 16626-709-000-RPT-0031	Issue 2	2012/262241

Annex 10

GDA issue	GDA issue action	Document title and reference number / description if not evident from title	Revision	TRIM reference
GDA Issue CI-04				
CI-04	A1	*Lifecycle approach to qualify Smart Devices in nuclear safety applications*: ENSECC110106	Rev. B	2012/138921
CI-04	A1	*EMPHASIS Tool Evaluation*: ENSECC110110	Rev. B	2012/114491
CI-04	A1	*Justification of smart devices for nuclear safety applications*: ENSECC110102	Rev. B	2012/216195
CI-04	A1	*UK EPR Smart Devices - Trial Applications*: ECECC111184	Rev. B	2012/61878
CI-04	A1	*Summary Qualification Report for* … [Digital chart recorder]: ECECC121091	Rev. A	2012/261696
CI-04	A1	*Qualification Plan for* … [Digital chart recorder]: ECECC111779	Rev. A	2012/77840
CI-04	A1	*SICS chart recorder - Requirements Identification File*: ECECC120095	Rev. B	2012/261700
CI-04	A1	*SICS chart recorder - Equipment Identification File*: ECECC120096	Rev. B	2012/261702
CI-04	A1	*Report on software assessment of … series electronic chart recorders*: ECECC121090	Rev. A	2012/261695
CI-04	A1	*Emphasis assessment database* [Digital chart recorder]: ECECC121338	Rev. A	2012/294001
CI-04	A1	*Operational Experience Report* [Digital chart recorder]: ECECC120781 (Not sampled)	Rev. A	2012/294007
CI-04	A1	*GDA – EPR UK – Report of the audit held on the 15th and 16th of February, 2012, in … premises, in …, concerning the software development of the recorder …*: EDESFR120956 (Not sampled)	Rev. A	2012/293996
CI-04	A1	*Electromagnetic Interference (EMI) qualification report for* … [Digital chart] *recorders*: TR90725-06N-1 (Not sampled)	Rev. 2	2012/293989
CI-04	A1	*Seismic qualification report for* … [Digital chart] *recorders*: TR90725-06N (Not sampled)	Rev. 2	2012/293984
CI-04	A1	*Test report for Software/Firmware Validation of* … [Digital chart] *recorders*: TR90725-06N-2 (Not sampled)	Rev. 2	2012/293985
CI-04	A1	*Engineering Assessment Report for the substantiation of the* … [Digital chart recorder] *for use in Safety applications*: RP_DES-CAP_SYST_00377 (Not sampled)	Rev. A	2012/294032
CI-04	A1	*CINIF EMPHASIS Phase 2 DXA_Daqstation YHQ* (Not sampled)	Rev. 2	2012/294037

Annex 10

GDA issue	GDA issue action	Document title and reference number / description if not evident from title	Revision	TRIM reference
CI-04	A1	*CINIF EMPHASIS Phase 3 DXA_Daqstation YHQ* (Not sampled)	Rev. 2	2012/294036
CI-04	A1	*Progress Report on Class 1 Smart Device Trial Assessment*: ECECC121403	Rev. A	2012/309902
CI-04	A1	*Summary Qualification Report for STT1 Temperature Transmitter*: ECECC121337	Rev. A	2012/309900
CI-04	A1	*Software Assessment Report for STT1 Temperature Transmitter*: ECECC121336	Rev. A	2012/309897
CI-04	A1	*Standard Temperature Transmitter - Requirements Identification File*: ECECC121334	Rev. A	2012/447358
CI-04	A1	*Standard Temperature Transmitter - Equipment Identification File*: ECECC121335	Rev. A	2012/447359
CI-04	A1	*Assessment Plan for Class1 Smart Device Trial*: ECECC121333 (Not sampled)	Rev. A	2012/339486
		GDA Issue CI-05		
CI-05	A1	*Stage 1 Design Change Proposal (description and rationale)*: UKEPR-CMF-029	31/05/11	2011/306576
CI-05	A1	*Impact study of the change from SPPA T2000 S5 to S7 – CMF Stage 2*: PEL-F/11-0245	Rev. B	2011/479490
CI-05	A1	*Outline of Basis of Safety Case for the SPPA-T2000 Based I&C Systems (SAS, PAS, SAS RRC-B, PICS and Plant Bus) and SPPA-T2000 platform*: PEL-F/11.0353	21/12/11	2011/648745
CI-05	A1	*List of contents of the Basis of Safety Case of SPPA-T2000*: PEL-F/12.0152	Rev. A	2012/262203
CI-05	A1	Basis of Safety Case Requirements Traceability Matrix	Ver. 1	2012/263166
CI-05	A1	*Self test coverage analysis*: Ev1-Key CI 3b (Not sampled)	Rev. 0	2011/648743
CI-05	A1	*Basis of Safety Case of SPPA-T2000*: PEL-F DC 13	Rev. A	2012/263148
CI-05	A1	*Software Identification File*: QU004A (Not sampled)	Rev. 0.2	2012/280617
CI-05	A1	*Hardware Identification File*: QU021 (Not sampled)	Rev. 0.2	2012/280622
CI-05	A1	*System Specification File*: QU014	Rev. 0.1	2012/280618
CI-05	A1	*IEC 62138 conformity for Class 2*: QU042	Rev. 0.1	2012/280625

Annex 10

GDA issue	GDA issue action	Document title and reference number / description if not evident from title	Revision	TRIM reference
CI-05	A1	*IEC 62138 conformity for Class 3*: QU041	Rev. 0.2	2012/280624
CI-05	A1	*Module dependability analysis for SPPA-T2000(S7)AS620B and SPPAT2000 OM690 components/Safety parameter determination approach*: QU019	Rev. 0.0	2012/280621
CI-05	A1	*Reliability Analysis SPPA-T2000/S7*: QU018	Rev. 0.0	2012/280620
CI-05	A1	*Definition of the predictability model of SPPA-T2000/S7*: QU017	Rev. 0.2	2012/280619
CI-05	A1	*Self test coverage analysis*: QU003 (Not sampled)	Rev. 0.1	2012/280613
		GDA Issue CI-06 Action 1		
CI-06	A1	*Methodology and Organization for Diversity Management between I&C Platforms and I&C Systems*: PTL-F DM 1	Rev. B	2012/243631
CI-06	A1	*RS/PTL Organisation Note For I&C Platforms Diversity Management*: PTL-F DC 4	Rev. A	2012/244350
CI-06	A1	*Diversity Criteria Between Protection System and Safety Automation System*: PTL-F DC 3	Rev. B	2012/343777
CI-06	A1	*Overall Approach to Diversity of UK EPR I&C Systems*: ECECC121713	Rev. A	2012/337777
CI-06	A1	*Exclusion of CCF between SPPA T2000(S7) and TELEPERM XS by using diversity (Taishan project diversity document)*: NLTC-G/2009/en/0018	Rev. B	2012/325926
CI-06	A1	*Current Diversity Analysis between SPPAT2000(S7) and TELEPERM XS – Corrective action plan*: PTI12.1071 Rev. A	Rev. A	2012/381535
CI-06	A1	*Key Elements for Diversity Management Methodology Improvement*: PTI/12.1072 Rev. A	Rev. A	2012/381536
CI-06	A1	*Justification of diversity between I&C systems implemented in I&C platforms*: PELZ-F DC 2	Rev. B	2012/410350
		GDA Issue CI-06 Action 2		
CI-06	A2	*Teleperm XS I&C System Compliance Analysis With IEC 60880*: PEL-F DC 9	Rev. A	2012/251141
CI-06	A2	*Teleperm XS I&C Systems Compliance Analysis With IEC 60987*: PEL-F DC 10	Rev. A	2012/251142
CI-06	A2	*Teleperm XS I&C System Compliance Analysis With IEC 61513*: PEL-F DC 8	Rev. A	2012/251140
CI-06	A2	*Compliance Analysis with IEC 60880 – Platform Part*: PTLD-G/2010/en/0383	Rev. A	2012/290977

Annex 10

GDA issue	GDA issue action	Document title and reference number / description if not evident from title	Revision	TRIM reference
CI-06	A2	*Compliance Analysis with IEC 60987 – Platform Part*: NLTC-G/2008/en/0053 (Not sampled)	Rev. A	2012/290975
CI-06	A2	*Compliance Analysis with IEC 61513 – Platform Part*: PTLC-G/2010/en/0047	Rev. B	2012/290976
CI-06	A2	*Justification of PS Reliability*: PELL-F DC 233	Rev. B	2012/237452
CI-06	A2	*PS Reliability, Availability and Maintenance Studies*: NEPS-F DC 29 BPE	Rev. G	2012/124449
CI-06	A2	*SVE2 Failure mode, failure effects and failure detection (FMEA)*: NLTC-G/2008/en/0039 (Not sampled)	Rev. D	2012/124471
CI-06	A2	*SAI1 Failure mode and effect analysis (FMEA)*: NLTC-G/2008/en/0056 (Not sampled)	Rev. F	2012/124480
CI-06	A2	*SDIx Failure mode and effect analysis (FMEA)*: NLTC-G/2008/en/0049 (Not sampled)	Rev. F	2012/124472
CI-06	A2	*SGPIO1 Failure mode and effect analysis (FMEA)*: NLTC-G/2008/en/0062 (Not sampled)	Rev. D	2012/124483
CI-06	A2	*SAO1 Failure mode and effect analysis (FMEA)*: NLTC-G/2008/en/0058 (Not sampled)	Rev. F	2012/124481
CI-06	A2	*SDO1 Failure mode (FMEA)*: NLTC-G/2008/en/0006 (Not sampled)	Rev. E	2012/124463
CI-06	A2	*SL22 and SLM2 failure modes (FMEA)*: NLTC-G/2007/en/0071 (Not sampled)	Rev. C	2012/124460
CI-06	A2	*SDM1 Failure modes and effect analysis (FMEA)*: NLTC-G/2008/en/0014 (Not sampled)	Rev. B	2012/124469
CI-06	A2	*SOBx-y Failure modes and effect analysis (FMEA)*: NLTC-G/2008/en/0008 (Not sampled)	Rev. B	2012/124465
CI-06	A2	*Subrack with power supply, fans and backplane - failure mode and effect analysis*: NLTC-G/2008/en/0054 (Not sampled)	Rev. C	2012/124474
CI-06	A2	*PS (incl. RPI sw) / RCSL / SA I&C / PIPS Teleperm XS I&C System Engineering Quality Plan*: PEL-F DC 7	Rev. A	2012/263128
CI-06	A2	*TXS I&C Systems Verification and Validation plan*: PELV-F DC 28	Rev. A	2012/263542
CI-06	A2	*Protection System. Failure Mode and Effect Analysis - System Level*: NLN-F DC 83	Rev. D	2011/621856
CI-06	A2	*Independence of the Class 1 Protection System (PS), the Safety Automation System (SAS) and the Non-Computerised Safety System (NCSS)*: ECECC111963	Rev. C	2012/307164
CI-06	A2	*Generic rule for the electrical isolation of EPR Instrumentation and Control Systems*: ECECC111058	Rev. B	2012/231930

Annex 10

GDA issue	GDA issue action	Document title and reference number / description if not evident from title	Revision	TRIM reference
CI-06	A2	*TELEPERM XS based systems Concept for Electrical Separation*: NLE-F DC 249	Rev. E	2012/3466
CI-06	A2	*Meeting report regarding TELEPERM XS, Concept for Electrical Separation*: RFP47142REC	19/08/09	2012/3457
		GDA Issue CI-06 Action 3		
CI-06	A3	*UK EPR Guideline for Application of Production Excellence and Independent Confidence Building*: ECECC111134	Rev. C	2012/298715
CI-06	A3	*Justification for Production Excellence and Independent Confidence Building Measures used for Teleperm XS Based Systems*: ECECC111557	Rev. B	2012/290717
CI-06	A3	*Justification for Production Excellence and Independent Confidence Building Measures used for SPPA-T2000 Based Systems*: ECECC120398	Rev. B	2012/336458
		GDA Issue CI-06 Action 4		
CI-06	A4	*Protection System- System Description (Pilot Study)*: NLN-F DC 193	Rev. C	2012/186993
CI-06	A4	*Analysis of the non disturbance of the Protection System by lower classified signals coming from systems in interface*: PELL-F DC 252	Rev. A	2012/186996
		GDA Issue CI-06 Action 5		
CI-06	A5	*RO-UKEPR-082 – Full response to Action A6*: Letter EPR00823R	11/03/11	2011/145670
CI-06	A5	*Appendix A Independence of the PICS and the SAS*: ECECC121458	Rev. A	2012/304938
		GDA Issue CI-06 Action 6		
CI-06	A6	*Class 1 Control and Display Facilities in the Main Control Room and the Remote Shutdown Station*: ECECC111829	Rev. B	2012/308513
CI-06	A6	*Outline of content of the Basis of Safety Case for the Protection System Operator Terminal*: ECECC111181	Rev. A	2011/436271
CI-06	A6	*Contents List and Traceability Matrix of: ECECC120489A - PSOT Basis of safety Case*: ECECC111271	Rev. A	2012/262200
CI-06	A6	*Protection System Operator Terminal Basis of Safety Case*: ECECC120489	Rev. A	2012/215687
CI-06	A6	*PSOT Requirements Specification - Feasibility Study*: ECECC110951	Rev. A	2012/282102
CI-06	A6	*See CI06 A2: PS (incl. RPI sw) / RCSL / SA I&C / PIPS Teleperm XS I&C System Engineering Quality Plan*: PEL-F DC 7 (Not sampled)	Rev. A	2012/263128

Annex 10

GDA issue	GDA issue action	Document title and reference number / description if not evident from title	Revision	TRIM reference
CI-06	A6	*See CI06 A2: TXS I&C Systems Verification and Validation plan*: PELV-F DC 28 (Not sampled)	Rev. A	2012/263542
CI-06	A6	*SysQAP QDS System Quality Assurance*: NLS-F DC 10067	Rev. B	2012/392222
CI-06	A6	*SysVVP QDS Software Verification and Validation Plan*: NFLS DC 177 (Not sampled)	Rev. E	2012/401102
CI-06	A6	*SysCMP QDS System Configuration Management Plan*: NFLS DC 186	Rev. E	2012/307078
CI-06	A6	*PSOT BSC Supporting docs QDS System Software Development rules, recommendations and guidelines*: NFLS DC 119	Rev. C	2012/392221
CI-06	A6	*QDS Operation Principles*: NLS-F DC 10143 (Not sampled)	Rev. B	2012/282105
CI-06	A6	*Oasis Concepts and Tools*: NFLS DC 165	Rev. C	2012/282104
CI-06	A6	*Protection System- System Description (Pilot Study)*: NLN-F DC 193	Rev. C	2012/186993
CI-06	A6	*PSOT Functional Scope*: ECECC120711	Rev. A	2012/271172
		GDA Issue CI-06 Action 7		
CI-06	A7	TQ-EPR-1486 Availability of SICS controls.	Full	2011/619286
		GDA Issue CI-06 Action 8		
CI-06	A8	*UK EPR: Justification of time response end to end on Terminal Bus Plant Bus*: ECECC111368	Rev. B	2012/322568
		GDA Issue CI-06 Action 9		
CI-06	A9	*Diversity Criteria For Sensors & Conditioning*: PELL-F DC 82	Rev. C	2012/424866
CI-06	A9	*Diversity criteria definition for Priority Actuation Control (PAC) module*: ECECC120443	Rev. B	2012/315332
CI-06	A9	*Diversity implementation Plan for Priority Actuation Control (PAC) module*: ECESN120472	Rev. A	2012/319795
CI-06	A9	*UKEPR Basis of Substantiation for the Reliability Claims for the PACS Modules*: ECECC121662	Rev. A	2012/336366
CI-06	A9	*Interfaces Entre Systemes de Controle Commande et Cellules Actionneurs HTA et BT (Annex 1 PACS diagram type 1 SM)*: ECEMA071141	Ind. A	2012/336358

Annex 10

GDA issue	GDA issue action	Document title and reference number / description if not evident from title	Revision	TRIM reference
CI-06	A9	*Interfaces Entre Systemes de Controle Commande et Cellules Actionneurs HTA et BT (Annex 2 PACS diagram type 2 SM)*: ECEMA071141	Ind. A	2012/336363
CI-06	A9	*Diversity Implementation Plan For Sensors & Conditioning*: PELA-F DC 3	Rev. C	2012/425767
CI-06	A9	*UK GDA – Allocation of sensors and conditioning when 3 lines of defence are involved*: PEPS-F DC 148	Rev. A	2012/411783
CI-06	A9	*Functional Analysis For Sensors' Common Cause Failure*: PEPR-F DC 83	Rev. C	2012/425768
CI-06	A9	*EXAR 8.0 Ausfallraten-Prognose*: EK31 4.529A	29/03/12	2012/138513
CI-06	A9	*Phase Model for the Development of 1E-Qualified I&C Hardware Components*: FAW NLL-G-132	Rev. A	2012/138516
CI-06	A9	*Qualification of the Binary Signal Conditioning module SBC1 6FK5326-8AA00*: NLTCG 2007 en 0032	Rev. C	2012/138521
CI-06	A9	*Qualification of the standard-signal multiplier module SNV1-2.5 6FK5250-8AA01 ES02 and SNV1-10 6FK5250-8AA02 ES01*: NLTCG 2007 en 0051	Rev. A	2012/138529
CI-06	A9	*SNV1 Failure mode and effects analysis (FMEA)*: NLTCG 2008 en 0043	Rev. D	2012/138534
CI-06	A9	*Failure modes and effects analysis (FMEA) for SBC1*: NLTCG 2008 en 0059	Rev. D	2012/138540
CI-06	A9	*Ausfallratenberechnung zur Baugruppe Binärsignalaufbereitung SBC1 6FK5326-8AA00*: NLTDG 2006 de 0174	Rev. A	2012/138542
CI-06	A9	*UK EPR GDA - Basis of Substantiation for the Reliability Claims for Sensors and Conditioning Modules*: PELA-F DC 7	Rev. B	2012/391227
CI-06	A9	*Field failure rate calculation and statistics of Teleperm XS; Status 2011-06-30*: PTLDG 2011 en 0302	Rev. A	2012/138779
CI-06	A9	*General approach to Failure Rate calculation and FMEA of TXS-modules*: PTLSCG 2012 en 0010	Rev. A	2012/138782
CI-06	A9	*Architecture of instrumentation and control system UK EPR: design principles and defence-in-depth*: ECECC100831	Rev. B	2012/396558
CI-06	A9	*Engineering and Projects Organisation EPR overall I&C design process*: PELA-F 12.1004	Rev. B	2012/310148
CI-06	A9	*UK EPR GDA - Classification of I&C system features*: ECEF091489	Rev. E	2012/417591
CI-06	A9	*Definition of I&C architecture design requirements in the UK context*: ECECC120414	Rev. A	2012/314765
GDA Issue CC-01 Action 6				

Annex 10

GDA issue	GDA issue action	Document title and reference number / description if not evident from title	Revision	TRIM reference
CC-01	A6	*Safety Principles Applied to the UK EPR I&C Architecture in terms of the Requirements for Diversity and Independence*: PEPS-F DC 90	Rev. C	2012/342262
CC-01	A6	*Methodology for Classification of Structures, Systems, Safety Features and Components*: NEPS-F DC 557	Rev. D	2012/424300
CC-01	A6	*Engineering and Projects Organisation*: PELA-F 12.1004	13/02/12	2012/82826
CC-01	A6	*UK EPR Generic Design Assessment – Classification of I&C Safety Features*: ECEF091489	Rev. E	2012/417591
CC-01	A6	*Definition of I&C architecture design requirements in the UK context*: ECECC120414	Rev. A	2012/314765
GDA Issue CC-02 Action 6				
CC-02	A6	IEC61513 ed. 2001 §6.1.1 Mapping to FA3 PS documentation	02/07/12	2012/262140
CC-02	A6	*UK GDA - Response to TQ-EPR-1624 : Elements of protection system – Primary/Secondary (P/S) related*: PEPRF.12.1121	09/08/12	2012/317566
CC-02	A6	*UKEPR: SAS IEC 61513 System Requirement Specification (SRS) Equivalence*: ECECC121435	Rev. A	2012/320333
CC-02	A6	*SRS Equivalence Justification Note for PAS and PACS*: ECECC121609	Rev. A	2012/320334
CC-02	A6	*RCSL detailed specification*: NLP-G/2006/en/1007	Rev. G	2011/85726
CC-02	A6	*Severe Accident I&C Detailed Specification File*: NLE-F DC 106	Rev. C	2011/92832
CC-02	A6	*Process Instrumentation Pre-Processing System Detailed Specification*: NLE-F DC 173	Rev. C	2011/92833
CC-02	A6	*C&I backup system*: UKEPR-CMF-014	Stage 3	2012/468227
CC-02	A6	*Communication of PS with other systems*: UKEPR-CMF-015	Stage 3	2012/468230
CC-02	A6	*Class 1 Information and Controls in MCR and RSS (QDS)*: UKEPR-CMF-026	Stage 3	2012/465606
CC-02	A6	*Safety Information and Control System Class Upgrade (class 1)*: UKEPR-CMF-27	Stage 3	2012/451034
CC-02	A6	*Impact Analysis for Change SPPA-T2000 platform version from S5 to S7*: UKEPR-CMF-029	Stage 3	2012/465609
CC-02	A6	*Functional Scope Allocation Of Main Reactor Controls*: UKEPR-CMF-40	Stage 3	2012/465616

Annex 10

GDA issue	GDA issue action	Document title and reference number / description if not evident from title	Revision	TRIM reference
CC-02	A6	*Classification of maintenance and testing tools of C&I systems - Periodic test and maintenance functions on C&I systems shall be categorised one category below the function impacted by the maintenance or the periodic test*: UKEPR-CMF-60	Stage 3	2012/459377
CC-02	A6	*Classification of the RodPilot - Rod pilot to be Class 2 in accordance with UK EPR classification methodology*: UKEPR-CMF-61	Stage 3	2012/459376
CC-02	A6	*Qualification of SMART devices in UK context - SMART devices have to follow the agreed UK EPR qualification program*: UKEPR-CMF-62	Stage 3	2012/459375
CC-02	A6	*Independent confidence building measures (ICBMs) on software based C&I systems*: UKEPR-CMF-63	Stage 3	2012/459372
CC-02	A6	*C&I diversity on sensors and sensor conditioning*: UKEPR-CMF-64	Stage 3	2012/468248
CC-02	A6	*C&I diversity on PAC modules*: UKEPR-CMF-65	Stage 3	2012/468250
CC-02	A6	*Protection System Reference Configuration*: UKEPR-CMF-66	Stage 3	2012/459369
CC-02	A6	*Addition of secondary side (VVP) pressure measurements*: UKEPR-CMF-67	Stage 3	2012/468254
CC-02	A6	*Non Computerised Safety System (NCSS) Design Improvement*: UKEPR-CMF-68	Stage 3	2012/468256
CC-02	A6	*C&I - Reference Configuration*: UKEPR-CMF-81	Stage 3	2012/468314
CC-02	A6	*Design principles of the Instrumentation and Control systems* PCSR Chapter 7.1: UKEPR-0002-071	Issue 4	2012/425069
CC-02	A6	*General architecture of the Instrumentation and Control systems* PCSR Chapter 7.2: UKEPR-0002-072	Issue 4	2012/433581
CC-02	A6	*Class 1 Instrumentation and Control systems* PCSR Chapter 7.3: UKEPR-0002-073	Issue 4	2012/433586
CC-02	A6	*Class 2 instrumentation and control systems* PCSR Chapter 7.4: UKEPR-0002-074	Issue 4	2012/425072
CC-02	A6	*Class 3 Instrumentation and Control Systems* PCSR Chapter 7.5: UKEPR-0002-711	Issue 1	2012/425076
CC-02	A6	*Instrumentation* PCSR Chapter 7.6: UKEPR-0002-075	Issue 4	2012/425078
CC-02	A6	*I&C tools, development process and substantiation* PCSR Chapter 7.7: UKEPR-0002-076	Issue 4	2012/433590
CC-02	A6	*Human Factors* PCSR Chapter 18.1: UKEPR-0002-181	Issue 6	2012/450492

Annex 10

GDA issue	GDA issue action	Document title and reference number / description if not evident from title	Revision	TRIM reference
CC-02	A6	*Classification of structures, equipment and systems* PCSR Chapter 3.2: UKEPR-0002-032	Issue 4	2012/450462

Annex 11

TSC Summary **–** GDA Issue **GI-UKEPR-CI-01** – Design Information for the Non-Computerised Safety System (NCSS) Required[26]

Note this information has been imported from a TSC report (Ref. 74) and the formatting of the TSC report has been retained.

[26] Note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 11

Annex: TSC task summary - GDA Issue **GI-UKEPR-CI-01** – Design Information for the Non-Computerised Safety System (NCSS) Required

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of submissions presented by EDF and AREVA to address resolution of GDA Issue GI-UKEPR-CI-01, "Detail of the Non- Computerised Safety System (NCSS) design has not been made available within GDA. EDF and AREVA have provided a commitment that the NCSS will be implemented in diverse technology to the computer based protection systems. A Basis of Safety Case for the NCSS is required for GDA". The following text is an extract from the TSC report Ref. 74.

The aim of this review was to consider the submissions in line with the Actions as identified in the Resolution Plan and to advise HSE/ONR on their adequacy, or otherwise, to support HSE/ONR decisions on the close out of the Actions, and hence the GDA Issue. GI-UKEPR-CI-01 consists of a single Action supported by eleven main submissions that are defined in the Resolution Plan, plus six further submissions that were defined during the GDA Closure phase. From review of each submission, Technical Clarifications and Observations were raised, as required, in order to achieve resolution of the GDA Issue.

The submissions address the following topics:

- NCSS functional and safety requirements for the system and platform;
- NCSS system definition and sample module specifications;
- NCSS diversity criteria and diversity justification;
- NCSS justification of reliability;
- NCSS Basis of Safety Case (BSC);
- sample plans (for example, quality, qualification, verification and validation) that support the NCSS BSC.

The submissions were reviewed against the clauses of IEC standards and ONR guidance documents where applicable, and where none apply, the competence and experience of the reviewer was used as the basis for review.

Following the TSC review of EDF and AREVA's response to the Technical Clarifications and Observations and related amendments to submitted documents, any open TSC Observations are captured in the corresponding GDA Issue report (this document) and are also highlighted to ONR.

<u>Closed Technical Clarifications and Observations</u>

Nineteen Technical Observations and requests for Clarification raised by the reviews of the submissions in support of resolution of GI-UKEPR-02 were closed during the GDA Closure phase. The topics are summarised below:

1) The Basis of Safety Case for the NCSS was supplied and reviewed, and the structure and content has been demonstrated to be adequate for the purposes of resolving the GDA Issue.
2) The classification of the NCSS has been agreed as Class 2, and the categorisation of the functions that it performs has been agreed as spanning Categories A, B and C.

Annex 11

3) The diversity criteria for the NCSS have been defined, and preliminary conformance with the criteria (i.e. given the current phase of the development of the NCSS system and UNICORN platform) has been demonstrated via the NCSS system specification, NCSS platform requirements, and NCSS quality plans. The conformance demonstration should be completed once the design is finalised.

4) The NCSS architecture satisfies the Single Failure Criterion.

5) The NCSS is independent of the other protection systems (i.e. the Class 1 Protection System and Class 2 Safety Automation System).

6) The mechanisms by which fail-safe operation of the NCSS will be achieved have been defined.

7) The current design of the NCSS does not utilise complex hardware, such as FPGAs[27], to carry out the safety functions.

8) The Basis of Safety Case states that the design and implementation of the NCSS system and its platform will comply with appropriate international standards, and lists these explicitly. The list includes IEC standards 61513, 61226, 60780, 60987, 62340, and 62138 (the latter is for Class 3 software, which is not part of the protective functions).

9) The interfaces for the NCSS manual controls and indications, and for the actuators via the switchgear, have been defined.

In addition, all Technical Observations that were raised during Step 4 of the GDA process, that are cited as providing further information in action A1 of GDA Issue GI-UKEPR-CI-01, have been closed as a result of the reviews of the documents submitted during the GDA Closure phase.

Open Observations

The observations raised by the reviews of the submissions that relate to the NCSS Basis of Safety Case (BSC), and that remain open at the end of the GDA Closure phase are summarised below. The open points to be addressed are:

1) Several areas for improvement have been identified in relation to the content of the BSC for the NCSS (for example, the document should explain how manual resets of all NCSS automatic functions are implemented so as to conform with Safety Assessment Principle (SAP) ESS.14).

2) The BSC for the NCSS states that compliance analyses will be developed to demonstrate coverage of applicable clauses in IEC standards 61226, 61513, 60709, 60780 and 62138 (for Class 3 software-based modules). The BSC should address the production of a compliance analysis for an appropriate hardware standard (noting that the scope of IEC 60987 is for computer-based systems and that the generic IEC 61508 standard may be more applicable) or justify this omission.

3) A demonstration of adequacy of the diversity of the NCSS platform, compared to the two computerised C&I platforms, should be produced and documented at the detailed design level.

4) The NCSS functional requirements definition should be completed with detailed design information.

5) Some potential areas for improvement in the operator interface have been identified for consideration, such as: the addition of actuator check-backs; confirmation of manual

[27] ONR note: FPGA is an abbreviation of Field Programmable Gate Array.

Annex 11

push-button command actions; and detection and resolution of inconsistencies in switch settings for NCSS / Normal modes of operation (i.e. with the computer based protection systems in service).

6) A demonstration of compliance with SAP EMT.7 should be produced with regard to in-service functional testing that proves the complete system, including redundancies.

7) A demonstration that the NCSS platform conforms to all applicable NCSS requirements should be produced.

8) A justification of the NCSS manual command architecture (single or dual chain) should be produced.

9) The reliability and response time analysis is preliminary, and should be completed when the detailed design information is available. A demonstration that the response times and accuracy requirements are achievable by design should be presented.

10) The effects of power failure on the fail-safe state of modules that are configured as "*energised-to-actuate*", and the plant impact, should be analysed.

11) Conformance to NCSS platform requirements should be demonstrated for each of the platform modules.

12) The NCSS platform is expected to undergo significant development to meet its requirements for UK EPR, and hence the Configuration Management Plans should define adequate change control processes and regression testing methods.

<u>Conclusions of the Review</u>

For GDA Issue GI-UKEPR-CI-01, based on the sampled evidence, there is no evidence to indicate that the Basis of Safety Case for the NCSS has not been adequately defined and agreed to the level required to conclude the GDA Closure review.

The open observations are not considered to be at a level of significance that would prevent closure of the GDA Issue. It is judged appropriate that these open observations be addressed during the Nuclear Site Licensing activity.

Annex 11

GI-UKEPR-CI-01 OPEN TECHNICAL OBSERVATIONS

GICI01.TO2.18 – The user documentation from the supplier of the gateway and datalogger modules, that describes their configuration options and procedures, should be included in the list of inputs to task E.19 "*To configure software components*", as defined in section 4.3.3 of the NCSS Quality Plan TA-2061589 rev C.

GICI01.TO2.19 – With regard to the verification and validation of the NCSS system and UNICORN platform, the following observations are raised:

a) the system verification and validation plan should demonstrate conformance with IEC 61513:2011 clause 6.2.6, by setting out the precise principles to be followed by the test plans to achieve adequate coverage of representative plant conditions;

b) the system verification and validation plan should demonstrate conformance with IEC 61513:2011 clause 6.3.5 a) by demonstrating that all configurations of the NCSS that are required for system validation are defined;

c) the platform quality plan should require adequate regression testing of engineering and test tools after a version change;

d) the NCSS System Qualification Plan (or other document(s) in the NCSS suite of plans defined in the NCSS Quality Plan) should demonstrate compliance at system level with all relevant clauses related to 'plans' from IEC 61513 and IEC 60987.

GICI01.TO2.20 – In order to improve the safety-related information for the SICS operators on the fault-free operation of the NCSS when there is total loss of the computerised systems, NCSS indications relating to "*Partial triggers*", "*Voting Results*", and "*Discrepancy on outputs of automatic functions compared to Permissives*" should be displayed on the SICS if it is reasonably practicable to do so, in accord with NCSS safety requirement RS30040-S.

GICI01.TO2.21 – The following observations arose as a result of the review of the UNICORN Project Platform Specification, TA-2060143 rev C:

a) Section 2.2.3 states that no actuator check-backs are systematically sent to the NCSS display on SICS for operator information, in contrast to the SPPA-T2000 which displays these check-backs systematically on PICS. Please document the justification for this design decision in the context of the loss of both computerised platforms (including PICS).

b) Section 2.2.3 also states that "*As manual commands are not permanently established (use of push button in MCR) they can be maintained either by the operator maintaining his pressure on the button or thanks to a pulse function…*". Please document the process that ensures that the operator is made aware that the manual command has been actioned to mitigate the risk, for example, that the operator does not maintain pressure on the button for a sufficient period of time.

c) Section 6.1 states that "*the object of the PT [Periodic Test] is not to make sure that all the electronic devices are 100% operational…*". Please document the explanation for why the lack of full coverage is not a concern and in particular, in relation to periodic testing of all safety-related NCSS equipment (i.e. in the context of conformance to SAP EMT.7, which requires in-service functional testing to prove the complete system). The explanation to cover the case in which a latent fault in redundant equipment remains

Annex 11

undetected by periodic testing until the equipment exhibiting that fault is required to deliver a safety function.

d) Section 10 provides a compliance matrix against the NCSS requirements in PTI DC 2 revision E. Five of these requirements are identified as being "Not Compliant" for the UNICORN platform (NCP16.1, NCP21.1, SYS3.3. SYS5.2 and LOG1.2). Please document the justification for why each of these non-compliances is considered to be acceptable.

GICI01.TO2.23 – The following observation arose from the review of "*Design of the NCSS System – Principles of selection of actuator orders and information for operators" -* ECECC100555 rev B:

The footnote in Section 4, and the summary of mode selection in Section 4.5, state that there are four switches in the SICS that control selection of NCSS-mode/Normal-mode, one for each division. The safety case should clarify if the intent of the design is for all four switches to be set to the same mode at any given time, or whether the intent is to support a mixed-mode working where some divisions are in Normal mode and others are in NCSS mode.

If the intent of the design is for all four switches to be set to the same mode, the safety case should address the consequences of the switch settings being erroneously set differently. If instead the intent of the design is to support mixed-mode working, the safety case should address the consequences of this operating mode on the HMI operator interface on the SICS and on the PSIS, with respect to the NCSS manual controls and indications that are active, and those that are not active.

GICI01.TO2.24 – In accordance with clause 4.3.3 of IEC60987:2007 '*Nuclear Power Plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*', the Platform Quality Plan TA-2057230 should describe the organisation, management and execution of the following quality related activities:

iii. 4.3.3 g) – control of test equipment.
iv. 4.3.3 h) – control of hardware handling/storage/shipping.

GICI01.TO2.25 – The explanation provided in the response to TQ-EPR-1580 point c) that relates to why failure of the Protection System cannot block NCSS manual and automatic commands at the switchgear is based on the fail-safe state of PS outputs being zero, which inhibits its orders:

"*In case of Total Loss of Computerised I&C (TLIC), it is required that NCSS orders are sent to actuators. This effectively happens because:*

> *- given the PS failsafe features, PS outputs are set to 0 (1 is used to send orders), then orders sent by NCSS (i.e. 1) can be transmitted to actuators ("OR GATE" between PS & NCSS orders).*"

The explanation above should be incorporated into the safety case documentation.

GICI01.TO2.26 – In the context of the architecture for processing NCSS manual commands, please ensure that:

a) the NCSS System Specification is updated to record the final decision as to whether the NCSS architecture defines a single or a dual chain of processing for manual commands;

Annex 11

b) the justification of this choice, in the context of the reliability and availability targets for the NCSS manual commands, is presented in the NCSS safety case.

GICI01.TO2.27 – The following observations that arose from the review of the UNICORN Platform Qualification Plan - TA-2073805 rev D – should be addressed:

a) The specific configuration of the UNICORN platform that is chosen as the Prototype (as defined in Section 2.4.1) should be justified as being representative of the UK EPR NCSS configurations, as committed in the response to Level 3 meeting action GI 1-I&C-6.

b) Entries marked as "*later*" or "*TBD*" in Section 6.3, relating to the qualification test conditions and applicable criteria, should be completed with the actual information.

c) Requirement NCP4.1.16 in document PTI DC 2 rev E, which relates to the independence of the platform qualification team from those conducting platform qualification for Teleperm XS and SPPA-T2000, is marked as "Out of scope" in Table 7 in Section 7 of TA-2073805 rev D. The comment cross-refers to the UNICORN Platform Specification requirements document TA-2060143 rev C, but this document also states in its compliance matrix in Table 76 of Section 10 that NCP4.1.16 is "Out of scope". The means by which UNICORN platform diversity requirements such as NCP4.1.16 are to be met should be stated in appropriate UNICORN planning documents.

GICI01.TO2.28 – The following observations that arose from the review of the *UNICORN Project Justification of Platform Reliability & Response Time on a Typical Automatic Function* - TA-2082935 rev B – should be addressed:

a) Ensure that the POWER BLOCK module is incorporated into the reliability analysis as soon as the cabinet power arrangement is designed, and analyse the effects of power failure on the fail-safe state of the AVACT module in the "*energised-to-actuate*" configuration, and other modules that are energised-to-actuate, such as the alarm management module and the Cabinet Monitoring Unit, that need to report faults to the operators.

b) Ensure that demonstration of satisfying requirement NCP16.1 in PTI DC 2 rev E - "*Portion of non detected dangerous failures should be as low as reasonably possible and not exceed 50 FIT*" - is presented for all dangerous failures of the UNICORN platform modules that carry out safety functions (for example, those failures marked as "*DG*" in the "*cat FM*" column in Table 5 in Appendix 1).

c) Section 2.2.8.1 gives the assumptions upon which the reliability analysis is based, including β factors of which have been "…*chosen for their consistency with the state of the art*". A justification of the applicability of the selected β factors should be documented.

d) TA-2082935 rev B analyses the frequency of spurious actuation of the "typical" NCSS function, and compares this frequency with the target rate for the NCSS Reactor Trip function (not exceeding 10^{-6} per hour). The target rate for NCSS spurious actuation of ESFAS functions should also be stated, and should be used in the analysis of the actual NCSS functions.

e) The final safety, availability, and response time analyses for all NCSS functions, including manual functions and ESFAS functions (see point d) above), should be presented in an update to TA-2082935, as committed in Section 2.1.6 of revision B.

Annex 11

f) TA-2082935 rev B does not analyse the effect on the reliability of the system of a division being unavailable due to maintenance. The effect of division unavailability on system reliability should be analysed, and any consequences for operational constraints stated.

GICI01.TO2.29 – The following observations that arose from the reviews of the sample of UNICORN module specifications that were provided during GDA, should be addressed:

a) If a complex electronic device, such as an FPGA, is used in a UNICORN module that performs a safety function then the justification of production excellence should include a demonstration of conformance to an appropriate standard, for example, IEC 62566.

b) Each UNICORN module specification should contain a completed conformity matrix that traces between the requirements in the module specification and those in the UNICORN Platform Specification TA-2060143, with justifications documented for any non-conformities.

GICI01.TO2.30 – The following observations that arose from the review of the NCSS Basis of Safety Case, PTL-F DC 5 rev A, should be addressed:

a) In section 1.1.5, the use of a test connector system within each division is presented as the means of connecting the NCSS Test Bench for periodic testing. The justification that the test connector system cannot unintentionally frustrate the operation of the NCSS functions during non-periodic-test-mode (normal) operation should be presented.

b) Section 1.1.5 states that end-to-end periodic testing is not practicable, and hence a series of partial tests that overlap will be used instead. The justification for why end-to-end testing that exercises all parts of the system (including redundant parts) is not reasonably practicable should be presented in the Basis of Safety Case.

c) Section 2.2.4 refers to the “*ISIP*” and the “*IWC*” devices for operator interface. If these are the same as the “*PSIS*” and “*PIPO*” respectively, which have been used in other submissions, then the safety case submissions should be made consistent in the naming of such devices.

d) Sections 2.2.5.2 and 2.2.5.3 state that the response time and accuracy requirements will be fully defined in later versions of the NCSS functional requirements NEPR-F DC 551 revision C. A demonstration that the response times and accuracy requirements are achievable by design should be presented.

e) In Appendix B, the deliverable Es44 is titled “*compliance analysis / matrices against the Standards*” and the deliverables for UNIC-10-12 is titled “*Specification Conformity Matrix – Platform Level*”. Section 4.2 mentions five standards: IEC 61226, IEC 61513, IEC 60709, IEC 62138 and IEC 60780 in connection with Production Excellence – however, the safety case should state precisely those standards for which NCSS/UNICORN compliance matrices will be produced, and should address the production of a compliance analysis for an appropriate hardware standard (noting that the scope of IEC 60987 is for computer-based systems and that the generic IEC 61508 standard may be more applicable) or justify this omission.

f) For claim 3c, the argument to support the Single Failure Criterion with respect to systematic failures states that it is based on “*organisational measures*”. The safety case should explain what these measures consist of, and how they are implemented.

g) Section 4.2.3 Table 5 presents the Independent Confidence Building Measures (ICBM) for Class 3 software-based systems. The entries for “*Certification of compliance with quality standards*” and “*Commissioning tests on site*” do not show any ICBM defined

Annex 11

since the activity is performed as part of the Production Excellence leg. In such cases, the guidelines document ECECC111134 rev C Section 7 recommends, for example, an independent review of the supplier's evidence, and a justification for the selected approach. The safety case should explain how this guidance is to be implemented.

h) The list of all projected evidence documents in Appendix B should include all output documents from the ICBM activities listed in Table 5 of Section 4.2.3 (see also point g) above).

i) Section 1.2.3.2 should describe how the module design tools that are listed, contribute to the activities of the module development lifecycle.

j) Appendix B shows the Configuration Management Plans UNIC-01-04 (platform) and PM.04.1 (system) to be not yet available. These plans should define adequate change control processes and regression testing methods.

k) The NCSS BSC traceability matrix for the second entry under Section 3.2 "*Validation of the implementation*" states that there is "*no COTS*". The safety case should include justifications for the use of PCs and other pre-existing programmable equipment (including any embedded pre-developed firmware or software) within modules such as the Class 3 Gateway and Datalogger.

l) The SAP Compliance Analysis matrix in Appendix A states that SAP ESS.14 is applicable to NCSS. This SAP states that "*Safety System actions and associated alarms should not be self-resetting*" and hence the expectation is that <u>all automatic</u> functions, once triggered, will maintain their state until reset manually. The Basis of Safety Case should contain, or should refer to, a description of, and justification for, the adequacy of the reset function in relation to conformance with ESS.14; for example, the following points should be addressed:

- The entry for ESS.14 in Appendix A states that claims 3a and 5c provide justification of conformance to this SAP. The arguments and evidence to support these claims (especially 5c) in section 3.1 should address manual reset of all triggered automatic functions.
- The document should explain how manual resets of all automatic functions are implemented in all three modes of operation (PICS, SICS and NCSS).
- The NCSS functional requirements definition in NEPR-F DC 551 rev C states in Section 2.3.1 that "*<u>Some</u> functions order shall be memorised in the I&C systems, meaning that the actuation signals sent to the actuators shall be maintained until a manual reset is performed by the operator.*" Please document the explanation for how the term "*Some functions*" conforms with SAP ESS.14 expectation that this will apply to <u>all</u> automatic functions, once triggered.

m) Section 1.2.2.2.6 states that the AVACT module output is configured by the use of jumpers, and Section 6.1 of TA-2080788 rev A (AVACT module specification) requires that "*Configuration and parameters selection shall be performed with straps on the rear connector instead using PCB jumpers*". The Basis of Safety Case should include a justification of the suitability of using jumpers to configure modules versus other methods (such as soldered links), supported by an analysis of the consequences and detectability of a module being inserted into the system with an incorrect, incomplete, excluded configuration, or no configuration.

n) The Basis of Safety Case should reference submission TA-2096900 rev A "Justification of Reliability Allocation" that was provided during GDA in support of document TA-2082935 rev B "Justification of Platform Reliability & Response Time on a typical automatic function", which is reference [Ep36].

Annex 11

GICI01.TO2.31 – A demonstration of adequacy of the diversity of the UNICORN platform, compared to the two computerised C&I platforms, should be documented at the detailed design level (including modules and components) that is consistent with the diversity methodology that is defined in document PTL-F DM 1 rev B.

GICI01.TO2.32 – The following actions in the table in PEPR-F.12.1062 rev 1 "*Comparison of the NCSS functions and SAS diversified functions*" do not have entries for the corresponding NCSS functions, and the "*Comments*" column states that they are "*not analysed in the frame of NCSS yet*":

- VIV [MSIV] closure;
- VDA [MSRT] setpoint increase.

The analysis of the required NCSS contribution to these actions should be carried out.

GICI01.TO2.33 – NEPS-F DC 555 rev D should be updated to reflect the changes introduced in PEPS-F DC 90 rev C that affect the NCSS. The updates to address the following:

a) The section titled "Interpretation" for requirement RS10080-DD in PEPS-F DC 90 rev C has been updated to reflect that the backup line needs to manage certain PIEs in the frequency range $10^{-3}/r.y < f < 10^{-2}/r.y$, based on PSA expert judgement. This should be reflected in Section 3.1 of an update to NEPS-F DC 555 rev D.

b) The text of requirement RS10010-FS in PEPS-F DC 90 rev C has been modified such that the principle of fail-safe design applies to all safety systems and components, which includes the NCSS. This should be reflected in Section 3 of an update to NEPS-F DC 555 rev D.

GICI01.TO2.34 – In order to conform to clause 6.2.1 d) of IEC 61513:2001 '*Nuclear Power Plants – Instrumentation and control for systems important to safety – General requirements for systems*', the Platform Quality Plan TA-2057230 should describe the "identification of personnel/organisations responsible for QA activities and tasks, including assurance of independence".

Annex 12

TSC Summary – GDA Issue **GI-UKEPR-CI-02** - Protection System Independent Confidence Building Measures[28]

Note this information has been imported from a TSC report (Ref. 75) and the formatting of the TSC report has been retained.

[28] Note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 12

Annex: TSC task summary - GDA Issue **GI-UKEPR-CI-02** – Protection System Independent Confidence Building Measures

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of submissions presented by EDF and AREVA to address resolution of GDA Issue GI-UKEPR-CI-02, "the programme of Independent Confidence Building Measures (ICBMs) to support the safety case for the Teleperm XS Protection System to be fully defined and agreed". The following text is an extract from the TSC report Ref. 75. All references to NSL in the following text should be interpreted as a reference to the SSP.

The aim of this review was to consider the submissions in line with the Actions as identified in the Resolution Plan and to advise HSE/ONR on their adequacy, or otherwise, to support close out of the Actions, and hence the GDA Issue. GI-UKEPR-CI-02 consists of a single Action supported by six submissions that are defined in the Resolution Plan (two of which were combined within a single document ENSECC110123), plus two further submissions ("Feasibility Study into the use of MALPAS for UK EPR" and "Spurious actuation challenging category A functions") that were defined during the GDA Closure phase. From review of each submission, Technical Clarifications and Observations were raised, as required, in order to achieve resolution of the GDA Issue.

The submissions were reviewed against the clauses of IEC standards and ONR guidance documents where applicable, and where none apply, the competence and experience of the reviewer was used as the basis for review.

Following the TSC review of the Requesting Party's response to the Technical Clarifications and Observations and related amendments to submitted documents, any open TSC Observations are captured in this report and are also highlighted to ONR.

<u>Closed Technical Clarifications and Observations</u>

Fourteen Technical Observations and requests for Clarification raised by the reviews of the submissions in support of resolution of GI-UKEPR-02 were closed during the GDA Closure phase. The topics are summarised below.

1) For Statistical Testing, the following way forward was agreed:
    a) Testing of the code for all four divisions of the PS will be carried out in the test environment, with a statistically significant number of tests being carried out on one of these divisions.
    b) Testing of the full four-division PS by the use of simulation will be investigated if the results of the single division simulation are successful.
    c) The scope of Statistical Testing will cover execution of Category A and B
    d) Protection System Operator Terminal (PSOT) HMI to the extent needed to support the statistical testing of these functions.
    e) There will be no open tickets that result from failures in the Statistical Testing run which apply to the version of the PS that is used for the start of operation of the plant.
2) For Static Analysis using MALPAS, the following way forward was agreed:
    a) The scope of Compliance Analysis will cover the code of the:

Annex 12

- PS core application;
- Teleperm XS modules that are part of the PS implementation;
- PS interface units;
- Function Block libraries used by the PS;
- Firmware within I/O and communication modules.

b) Integrity checking, plus functional analysis by reverse engineering, will be used for the RTECONF configuration module.

c) There will be no open tickets that result from failures in Static Analysis which apply to the version of the PS that is used for the start of operation of the plant.

3) For Static Analysis of concurrency within the Teleperm XS kernel, the approach of using the SPIN tool was considered to be feasible.

4) For compilation tool validation via Source-to-Code Comparison (SCC) using MALPAS, the following way forward was agreed:

a) The scope of SCC will cover the compilation system tools used to build the:

- PS core application;
- Teleperm XS modules that are part of the PS implementation;
- Function Block libraries used by the PS;
- Firmware within I/O and communication modules.

b) SCC will be applied to the PS Interface Units application code if the level of automation achieved in the SCC process for the PS core is sufficiently high; however if a significant amount of manual effort is found to be necessary, this will not be reasonably practicable and a justification for adequacy of the toolset as used on the interface unit application code will be provided.

c) There will be no open tickets that result from failures in SCC which apply to the version of the PS that is used for the start of operation of the plant.

5) The reliability claim for the PS Interface Units is 10^{-3} pfd. A set of studies will be carried out in NSL to identify the most effective approach to justify why these units cannot unintentionally interfere with execution of the core PS functions.

Open Observations

The observations raised by the reviews of the submissions that relate to the ICBM elements, and that remain open at the end of the GDA Closure phase are summarised below. The open points to be addressed are:

i. For the Statistical Testing programme:

a) a demonstration of independence of the supplier of the Test System and the testing programme, from the suppliers of the PS and platform;

b) achievement of a statistically valid coverage of the full operational demand space for PS Category A functions.

ii. For the Static Analysis programme:

a) a demonstration that the implementation of the PS satisfies the assumptions used in the static analysis, e.g. no execution of Test Mode software.

Annex 12

iii. For Static Analysis of dynamic execution:

   a) a full definition of the approach to concurrency analysis of Teleperm XS system software, addressing the points that have been identified by the feasibility analysis of the use of the SPIN tool as requiring further work to achieve resolution, for example, validation of the concurrency model against the actual concurrency implemented by the Teleperm XS target code;

   b) a review of whether a concurrency analysis of the execution of the firmware embedded in the I/O and SL22 communication modules is necessary;

   c) incorporation of the guidelines in ECECC111134 rev C relating to performance analysis and testing into the ICBM activities.

iv. For the Source-to-Code Comparison (SCC) programme:

   a) the application of the ALARP assessment of the reasonable practicability of performing SCC on the PS Interface Units application code, based on the cost of the manual effort involved compared to the benefit of increased confidence in the toolset.

v. Should SCC be determined to be not reasonably practicable to be performed on the PS Interface Units application code, the following further studies will be carried out:

   a) assess technical solutions, such as hardware Command Validation Boxes, to eliminate spurious actuation from the Interface Units by design;

   b) perform a case-by-case analysis of each spurious signal to identify whether it could impact the operation of a Category A function, and if so, to identify options to detect this occurrence, and to put in place operational procedures to respond to such events.

vi. A demonstration of independence where organisations are involved in both specification/procurement and in ICBM activities, specifically NNB and EDF CNEN.

<u>Conclusions of the Review</u>

For GDA Issue GI-UKEPR-CI-02, based on the sampled evidence, there is no evidence to indicate that the programme of ICBMs to support the safety case for the Teleperm XS PS has not been adequately defined, and agreed to the level necessary to conclude the GDA Closure review.

The open observations (TOs) are not considered to be at a level of significance that would prevent closure of the GDA Issue. It is judged appropriate that these open observations be addressed during the Nuclear Site Licensing activity.

Annex 12

GI-UKEPR-CI-02 OPEN TECHNICAL OBSERVATIONS

GICI02.TO2.15 – The following observations arose from the review of the UK EPR Programme of statistical testing activities, ECECC111521 revision B:

a) With regard to the supplier of the Test System, and of the supplier of the specification of the testing programme, please justify the process that ensures and preserves adequate independence of these suppliers from the PS and Teleperm XS production teams, in the context of the "*strong support from AREVA*" that is stated in Section 6.1.

b) With regard to the transient selection strategy that is described in Section 6.4, which is stated to be subject to confirmation, please ensure that the chosen strategy achieves statistically valid coverage of the full operational demand space for PS Category A functions, unless it is justified that this is not reasonably practicable and/or other approaches are justified as providing significant advantage(s).

GICI02.TO2.16 – The static analysis performed as an ICBM on the PS code is based on an assumption that the system does not execute Test Mode software in operational mode. The safety case should explain the measures taken to ensure that this assumption holds, by demonstrating that the implementation of the PS ensures that every exit path out of code executed in Test Mode terminates with a Reset of the processor.

GICI02.TO2.17 – The approach to concurrency analysis of Teleperm XS system software, as proposed in Section 4.3 of ENSECC110123 revision B, should address the following points:

1. The PROMELA model must accurately take into account the effect of multi-processors on the concurrent behaviour of the Teleperm XS code.
2. The PROMELA model must be validated to be an accurate representation of the actual concurrency interactions in the source code of the Teleperm XS task set, including identification of all shared variables in the code, independent of the concurrency information that is contained in the Teleperm XS specification.
3. In addition to providing the results of application of the SPIN model checker to the validated PROMELA model, the demonstration of adequacy of the concurrency implementation in the safety case should:

   i. include the text provided by EDF and AREVA in the responses to points g) and h) of observation GICI02.TQ.02 in TQ-EPR-1518, as follows:

      "g) The approach retains for the Teleperm XS to avoid unbounded priority inversion, absence of deadlocks and the adequacy of CPU[29] time allocation is the following:

      Main design principle: static priority for tasks.

      - *Under normal operation only 3 tasks are active: cyclic task (RTE[30]) with highest priority, service task with medium priority and self-test task with lowest priority.*
      - *Coordination and mutual exclusion is achieved by semaphores and event flags. These services are provided by the TXS operating system*

[29] ONR note: CPU is an abbreviation of Central Processing Unit.

[30] ONR note: RTE is an abbreviation of Run Time Environment.

Annex 12

component Micros. Their correct function was tested in Micros' component test.

- *In addition to these services, interrupts are disabled by tasks to protect short term critical sections (< 1ms).*

Design and tests with respect to real time issues / concurrency.

- *Self-test: all tests which disable interrupts are designed to be bounded/limited (< 1ms). Meeting this 1ms-limit is checked in the test of the self-test component.*
- *No dynamic allocation of memory resources takes place. So deadlock situations due to depletion of resources can be excluded by principle.*
- *Interrupts: There are no process-dependent Interrupts. During normal, error-free runtime the cyclic task of a CPU is only interrupted by the timer interrupt (every 1 ms, handled by Micros timer-interrupt-handler and scheduler).*
- *RTE Mutex (Semaphore): The service task locking times of the RTE mutex are measured and documented. The locking times are sufficiently small, so that an interference with the timely start of the RTE cycle is avoided.*
- *An event flag is used by the RTE cyclic task to signal the service task that a new command message is available for processing. The correct execution of service commands and thus the correct use of the event flag is indirectly tested by many tests which issue service commands.*
- *Explicit tests of service commands also exist: For example, the current RTE test specification contains test cases (RTE version 3.6.2, test cases "ServiceNoInfluenceInOperation" and ""CheckCyclicOperationSingle), which check if service commands do not interfere with the execution of the RTE cyclic task.*

CPU time allocation

- *In TXS, all safety I&C functions (actuation path consisting of FBs, FDGs, communication, and I/O) are executed within the RTE's cyclic task. This task has the highest priority, so task starvation cannot occur. The system platform supports adequate allocation of this task's CPU times during I&C engineering and provides a method for empirical verification of adequacy during test bay by measuring actual computing time (c.f. answer to TQ-EPR-1001). This way, it will be shown (for each CPU) that the cyclic task finishes in time, guaranteeing the I&C system's designed response time. The system software's design (automatic path functionality in task with highest static priority) ensures that a starvation of the lower-priority tasks does not degrade the system's safety function(s). In addition, the TXS system platform offers two means which limit the impact of task starvation (of the lower-priority tasks) and to allow for designing a system such that this starvation is avoided:*

  a) Allocation of sufficient resources by allowing enough time. The time required for cyclic self-test task and service task per RTE cycle can be set aside as an extra reserve margin when designing the I&C system's actuation path.

  b) Restricting the change of parameters to one division at a time. This is done by locking the respective release in all but one divisions.

Annex 12

h) It is not proposed to perform any analysis of the asynchronous communication between processors.

The asynchronous aspects of the PS design may result in some variation in the order in which divisions set trip/actuation outputs. Specifically, the processing cycles of the SVE2 function processors in a TXS I&C system are not synchronized. Due to the absence of synchronization, function processors receiving data messages from other processors have to consider the situation when a new message has not been received before the start of the current processing cycle. In this case, the runtime environment of the CPUs does not wait for a message to be received, but implements a message age monitoring function. In case a new input message has not been received at the start of cycle, the message data available from the previous cycle are used for a second time for input to the current processing cycle.

This may result in different results being calculated by each division for a short period of time during a transient, but the phenomenon will only occur for a short period of time during plant transients and will then settle down so that the outputs from each division are consistent. This behaviour is considered in the worst case system response time calculation scheme."

ii. document the responses to the following specific questions raised in point g) of in TQ-EPR-1573:

a) "*Under normal operation only 3 tasks are active*" – please identify if any further tasks are active when not in normal operation and if so, how these additional tasks interact with the three tasks executing in normal operational mode.

b) "*all tests which disable interrupts are designed to be bounded/limited (< 1 ms)*" – please include the analysis that demonstrates the acceptability of disabling interrupts for this length of time for short term critical sections, which should be defined and justified including the acceptability of the frequency of execution of such interrupt-disabled critical regions.

c) "*During normal, error-free runtime, the cyclic task of a CPU is only interrupted by the timer interrupt*" – please include information on interrupts that may occur in other operational modes (e.g. accident modes) including justification as to why their use is acceptable.

d) "*The locking times are sufficiently small*" – please include the analysis to demonstrate that deadlock caused by nested Mutex locking cannot occur.

e) "*The current RTE test specification contains test cases… which check if service commands do not interfere with the execution of the RTE cyclic task*." – please include information on whether there is static analysis to demonstrate non-interference by design, as well as the demonstration by test.

f) "*The RTE's cyclic task … has the highest priority, so task starvation cannot occur*." – please include the analysis that demonstrates that the highest priority task cannot be blocked for unacceptably long periods whilst waiting to lock a Mutex that is locked by a low-priority task. Please also include the analysis that demonstrates that any task starvation that does occur in the service task or the self-test task cannot compromise the integrity of the safety functions.

g) Explanation of how cycle overrun is handled by the Teleperm XS executive – please include a justification for why the execution of the protective

Annex 12

safety functions of the PS cannot be frustrated by any CPU time overrun of the periodic processing cycle.

h) The response to TQ-EPR-1607 point a) states "*The system can tolerate data not being updated on one cycle and then re-uses the previous data. … If the data still has not been updated after more than one cycle, the receiver then applies the error processing that is appropriate for the situation*". If the PS Interface Units, at 10^{-3} pfd, fail to provide updated data to the PS Core for two consecutive cycles, please include an explanation for what is "*the error processing that is appropriate for the situation*" and how this error processing may affect the PS Core automatic functions. If the PS Core automatic functions can be frustrated by absence of updated input data for more than one cycle, please include the justification for why this does not reduce the reliability claim of the PS Core automatic functions.

4. The resolution of points 1 and 2 above should be captured in updates to appropriate documentation such as the PE and ICBM Guidelines for UK EPR in section C.3 of ECECC111134 rev C, and the justifications of adequacy of ICBM approaches for all UK EPR Class 1 computerised C&I systems.

GICI02.TO2.18 – The following observation arose from the review of document ENSECC110123 revision B:

The response to point d) of TQ-EPR-1518 relating to the justification of adequacy of the Smart difference tool has not been incorporated into the submission. The document should be updated to include the text provided in the TQ response, in particular:

- unintended aliasing is detected via a check in the De-locator;
- the list of properties of compilation, linking and locating that apply to unchanged source code modules, which form the basis of the differences check by the Smart difference tool.

GICI02.TO2.19 – The following points arose from the review of ENSECC110173 revision B Section 4.4:

a) Section 4.4 presents NNB Design Authority (DA) as having overall responsibility for the assurance of the ICBM activities. The means by which NNB DA assures that the scope, specification, and resolution of all ICBM activities have been satisfactorily addressed for the PS, should be presented in the safety case.

b) Section 4.4 states that NNB DA report separately from the NNB Delivery organisation, and that this independence demonstrates compliance with SAP ESS.27 and TAG 046. Evidence to support this argument of independence between NNB DA and NNB Delivery should be presented in the safety case.

c) The response to TQ-EPR-1561 point b) states *"The ICBM surveillance activity in CNEN uses different staff from those involved in specification and procurement."* but this independence is not demonstrated in ENSECC110173 revision B Section 4.4. The adequacy of independence between the EDF CNEN I&C staff that are involved in specification and/or procurement of the PS, and the EDF CNEN I&C staff that are involved in the PS ICBM activities, should be demonstrated in the safety case.

GICI02.TO2.20 – The need for a concurrency analysis of the execution of the firmware embedded in the I/O and SL22 communication modules should be reviewed. If there are

Annex 12

concurrent processes, including interrupt handlers, an ICBM approach should be developed, taking into account current research on this topic, for example, the CINIF ARMS study, or a full justification should be documented as to why such an approach is not proposed.

GICI02.TO2.21 – The change in the requirements specification of function blocks in relation to the setting of the error attribute on outputs as a result of software exceptions, such as numeric overflow, that occur during the computation part, should be applied to the UK EPR implementation. Please document this in the safety case, and please ensure that the safety case contains the full definition of this change, based on the summary in the response to point d) in TQ-EPR-1607, namely:

- "*the new/current general function block requirement specification requires that if output signals are not trustworthy, they shall carry the error attribute, and signals without error attribute are trustworthy.*"
- "*The application has to implement the fail-safe behaviour based on the error attribute concept.*"
- "*the TXS System Platform supports implementing fail-safe behaviour by providing function blocks which adequately deal with the error attribute. For example, the function block for 2-out-of-4 voting switches to 2-out-of-3 voting if one signal carries the error attribute. Additionally, many function blocks which may "produce" errors can be connected to a matching monitoring signal decoder, which can be used to further investigate and handle the error condition on application level.*"

Please also ensure that the safety case fully defines the fail-safe behaviour for each application function when the error attribute is set, as per the second bullet above.

GICI02.TO2.22 – The guidelines for the application of PE and ICBMs, ECECC111134 revision C, include "*Performance analysis and testing*" in the minimum set of ICBMs for a Class 1 system at both 10^{-3} and 10^{-4} pfd, which is expanded upon in Section C9 of the same submission. This guidance should be considered for incorporation into the ICBMs to be applied to the 10^{-3} and 10^{-4} pfd modules of the PS, (e.g. as defined in ENSECC110173 revision B,) in line with the minimum set of measures defined in Table 2 of ECECC111134.

GICI02.TO2.23 – The safety case to include the results of the ALARP assessment of the reasonable practicability of performing Source-to-Code Comparison on the PS Interface Units application code, based on the cost of the manual effort involved compared to the benefit of increased confidence in the toolset.

GICI02.TO2.24 – The PS and safety case documentation should be updated to record the analysis (contained in the response to TQ-EPR-1607 point a1) of unintended interference from the PS Interface Units to the PS Core, covering Electrical, Physical and Communication means of interference.

GICI02.TO2.25 – The safety case should include the results of the studies identified in ECECC121715 rev A, to be undertaken during NSL, of mitigations for plausible, but spurious operation and service commands sent by the PS interface (including the operators, PSOT, Data Interface (DI) units, and Monitoring and Service Interface (MSI) units) to the PS Core, that may impact operation of Category A functions.

Annex 12

The safety case should document the justification for the selected approach and the impact of this approach on the detailed design for UK EPR.

Annex 13

TSC Summary – GDA Issue **GI-UKEPR-CI-03** – Claims, Arguments, Evidence Trail[31]

Note this information has been imported from a TSC report (Ref. 76) and the formatting of the TSC report has been retained.

[31] Note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 13

Annex: TSC task summary - GDA Issue **GI-UKEPR-CI-03** – Claims, Arguments, Evidence Trail

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of submissions presented by EDF and AREVA to address resolution of GDA Issue GI-UKEPR-CI-03, relating to the revision and improvement of the Claims, Arguments & Evidence (CAE) Trail documentation. The following text is an extract from the TSC report Ref. 76. All references to NSL in the following text should be interpreted as a reference to the SSP.

The aim of this review was to consider the submissions in line with the Actions as identified in the Resolution Plan and to advise HSE/ONR on their adequacy, or otherwise, to support HSE/ONR decisions on the close out of the Actions, and hence the GDA Issue. GI-UKEPR-CI-03 consists of a single Action; this is divided into two sub-actions (A1.a and A1.b) each supported by a single submission. From review of each submission, queries and observations were raised, as required, in order to facilitate convergence between ONR and EDF and AREVA.

The PCSR CAE trail previously supplied by EDF and AREVA after the end of Step 4, included in the Resolution Plan, was reviewed by the TSC for adequacy, i.e.:

a. Document 16626-709-000-RPT-0003 Issue 1 *"PCSR I&C Claims, Arguments and Evidence (CAE) Final"*, supplied by EDF and AREVA under cover letter ND(NII)EPR00851R.

The updated CAE trails as defined by the Resolution Plan sub-actions, supplied by EDF and AREVA, were reviewed for adequacy, i.e.:

a. 16626-709-000-RPT-0028 Issue 3 - UKEPR GDA I&C System CAE Document (A1.a);
b. 16626-709-000-RPT-0031 Issue 2 - Update of Claims-Argument-Evidences trail for satisfaction of SAPs relevant to I&C (A1.b).

Following the TSC review of the Requesting Party's response to the Technical Clarifications and Observations and related amendments to submitted documents, any TSC observations were captured in the corresponding TSC GDA Issue report and were also highlighted to ONR.

Closed Technical Clarifications and Observations

One Technical Observation raised by the reviews of the submissions in support of resolution of GI-UKEPR-CI-03 was closed during the GDA Closure phase. The resolution is summarised below.

> From the review during the GDA Closure Phase of the initial PCSR CAE Trail , 16626-709-000-RPT-0003 Issue 1, provided at the end of Step 4, further improvements were agreed to the structure and content of the PCSR CAE Trail report to be addressed in future updates. An update to this report, 16626-709-000-RPT-0028 Issue 3 - UKEPR GDA I&C System CAE Document, was provided. The review of the latter document confirmed that the agreed structure and content had been adequately addressed.

Open Observations

Annex 13

The observations raised by the reviews of the submissions that relate to the CAE Trail documents, and that remain open at the end of the GDA Closure phase are summarised below. The open points to be addressed are:

a. For the PCSR CAE Report:

   Update the report to improve the description of the process used to derive Key Claims, describe the V&V of the Key Claims and improve the references to the claims made in the PCSR.

b. For the SAP Conformance CAE Report:

   i. Ensure that all SAP conformance CAE trails address all specific requirements of each SAP and that they are supported by the Argument and Evidence;

   ii. Acknowledging the 'live' nature of this document at this stage of the design, continuous review of the applicability and accuracy of the cited evidence should be undertaken as final detailed design documentation becomes available, and the document should be updated taking cognisance of the comments in the Technical Observations in this report raised by the review of those SAP CAE Trails sampled by the TSC during GDA Closure.

<u>Conclusions of the Review</u>

For GDA Issue GI-UKEPR-CI-03, based on the sampled evidence, there is no evidence to indicate that the revision and improvement in the CAE trail documentation has not been adequately achieved, and agreed to the level necessary to conclude the GDA Closure review.

The five open observations are not considered to be at a level of significance that would prevent closure of the GDA Issue. It is judged appropriate that these open observations be addressed during the Nuclear Site Licensing activity.

Annex 13

GI-UKEPR-CI-03 OPEN TECHNICAL OBSERVATIONS

GICI03.TO2.01 – The following observations arose from the review of the UKEPR GDA I &C System CAE Document, 16626-709-000-RPT-0028 Issue 3:

a. A further update of 16626-709-000-RPT-0028 Issue 3 should include the description of the process to derive the High Level and Key Claims, including their verification and validation activities, as provided in Appendix A to EPR01327N that explained matters raised in TQ-EPR-1482.

b. With regards to the links from Appendix C to the PCSR Chapter 7, the links to the sections of the PCSR that should be addressing the claim should be sufficiently focused and the content of the referenced section should address the intent of the claim. For example;

   Claim 4a states –

   The requirement for I&C systems important to safety and their functional requirements are determined.

   The link to the PCSR is only to Chapter 7.1, §0.1. The link only points to the three 'High Level' requirements for the C&I systems, not the individual system functional requirements or their determination, and there is no link to where the 'requirement for C&I systems' is addressed in the PCSR

   Either better PCSR referencing or amended PCSR wording should be used.

c. With regards to cited evidence to support the Claim and Argument, the evidence cited should contain the information / justification claimed in the tables in Appendix C. For example:

   Claim 3c –

   The Argument states that '*The Basis of Safety Case for the SPPA-T2000 (GI-UKEPR-CI.05 task T4) will address the Single Failure Criterion specifically for the SAS.'*. A search of the BoSC[32] revealed that SFC is not addressed at all, for platform or systems. Also, the Future Evidence references the SPPA-T2000 (S7) BoSC and specifically Section 3.3 addressing SFC. There is no Section 3.3 in the BoSC.

   Additionally, the cited Evidence should be at a sufficiently low level (e.g. at document section / sub section level) to provide the detailed information to support the Claim (e.g. explicit citing of standards compliance documents as evidence should be identified in support of High Level Claim 1 and Claim 1c)).

GICI03.TO2.02 – The following specific observations arose from the review of sampled CAE Tables in Appendix C of the UKEPR GDA I&C System CAE Document, 16626-709-000-RPT-0028 Issue 3:

a. Claim 1c) – The Argument and cited Evidence should specifically address and reference standards compliance for the C&I platforms and systems.

b. Claim 3c) – With respect to provision of future evidence documentation it should be identified that:

   1. BoSCs address the Single Failure Criterion,

[32] ONR note: BoSC is an abbreviation of Basis of Safety Case.

Annex 13

2. The System Description Documents for each C&I system address the Single Failure Criterion,

c. Claim 4a) – The Argument should clearly define how and where requirements for C&I systems and their functional requirements are determined; there is currently only cross-reference to claim 4b for Plant Transients. Also, with respect to provision of future evidence documentation it should be identified that:

1. The functional requirement documents, as per the example given for the 'non-computerised I&C functions', 'NEPR-F DC 551', will be available for all C&I system,
2. The System Description Documents for each C&I system 'define the I&C systems and their functional requirements', as claimed, or an equivalent document identified (e.g. a System Requirements Specification) that addresses functional requirements,

The System Design Manuals include the 'functional requirements that define the controls required for the plant systems to 'maintain plant variables within specified ranges'' as stated in the 'Argument', and for each C&I system all applicable SDMs are identified in the CAE trail as Evidence.

GICI03.TO2.03 – The following observations on the identification of appropriate evidence arose from the review of sampled SAP CAE Trails in Appendix 1 and the RP's 'Response' to TOs in Appendix 2 of the Update of Claims-Argument-Evidences trail for satisfaction of SAPs relevant to I&C, 16626-709-000-RPT-0031 Issue 2. However, these provide examples only and a review of applicability and accuracy of all cited evidence should be checked once final detailed design documentation is available:

a. EDR.2 – T15.TO1.55 – The RP's 'Response' to this TO implies inclusion of the SPPA-T2000 S7 Basis of Safety Case as evidence but this has not been included.

b. ESS.21 – T13.TO2.12 - QU627 "Reliability Analysis SPPA–T2000" is cited as providing module dependability analysis and system reliability analysis. However, the BoSC references to QU018 as the "Reliability Analysis SPPA-T2000 S7" and QU019 as the "Module dependability analysis for SPPA-T2000 S7...". The CAE for this SAP should reference the correct analysis documents, or a distinction made between use of S5 and S7 references.

c. ESS.21 – T17.TO2.19 -This TO related to the demonstration of the adequacy of the monitoring of Class 1 actuators used by the PS. The RP's 'Response' to this TO is to include ECECC111829 Rev A "Class 1 control and display facilities in the Main Control Room and the Remote Shutdown Station" as evidence against the PACS in support of 'revealing internal faults'. However, ECECC111829 does not reference monitoring Class 1 actuators and does not refer to the PACS at any point. The reason for including this document as evidence should be clarified.

d. ESS.27 – T13.TO2.14 – This TO related to the removal of Hardware qualification in a demonstration of conformance with a software related SAP; however, the reference to compliance with hardware design and engineering processes is still included.

e. EKP.5 – T13.TO2.20 - PEPS-F DC 90 defines the safety principles to be applied including for Defence in Depth and ECEF091489 rev D, that supports PEPS-F DC 90, identifies the allocation of functions to I&C systems. These documents should be cited as evidence in future updates to this document.

f. ESS.11 – T13.TO2.26 - The RP's 'Resolution' for this TO suggests inclusion of ECEF021069 "Sizing of the SICS" as evidence for the SICS; this has not been included.

Annex 13

g. General – The evidence / documents, identified as part of the CAE trails is not always the most recent or that used to support safety arguments made elsewhere. A means of maintenance and configuration control of the CAE trails is necessary.

GICI03.TO2.04 – The following observation on the adequacy of CAE trails to supp ort the demonstration of SAP c onformance arose from the review of sampled SAP CAE Trails in Appendix 1 and the RP's 'Response' to TOs in Appendix 2 of th e Update of Claims-Argument-Evidences trail for satisfaction of SAPs relevant to I&C, 16626-709-000-RPT-0031 Issue 2:

a. ESR.10 – T13.TO2.37 – ESR.10 states '*Faults in control systems and other safety-related instrumentation should not cause an excessive frequency of demands on a safety system*'. This TO related to improving the argument and evidence to demonstrate that control system failures will not cause excessive demands on safety systems. However:

   i. There is no mention in the argument of controls systems such, as PAS and RCSL, (although they are mentioned in the evidence) of how failure of these systems may make demands on safety systems, and that these demands are not excessive.

   ii. There is still a reference to 'NEPR-F DC 172, "Functional Description of P/S Limitation and Operator Aid I&C Function", that provides an example description, from the FA3 Project, of the limitation functions to be implemented in the RCSL to respond to disturbances in the primary and secondary systems'. This is more about normal plant transient control covered by ESR.9, where this reference is, correctly, cited. The applicability of NEPR-F DC 172 to ESR.10 (e.g. as a result of control system failures generating plant transients) should be clarified.

GICI03.TO2.05 - From th e review of Tech nical Observations cited by ONR in GDA Issu e GI-UKEPR-CI-03 it was found that T18.TO2.08 relating to the CAE for SAP ERC.2 paragraph 445 has not been addressed. The CAE for ERC.2 paragraph 445 should be updated during NSL in line with the requirements of T18.TO2.08.

Annex 14

TSC Summary – GDA Issue **GI-UKEPR-CI-04** – Smart Devices[33]

Note this information has been imported from a TSC report (Ref. 77) and the formatting of the TSC report has been retained.

[33] Note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 14

Annex: TSC task summary - GDA Issue **GI-UKEPR-CI-04** – Smart Devices

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of submissions presented by EDF and AREVA to address resolution of GDA Issue GI-UKEPR-CI-04, relating to the definition of a methodology for the qualification of Smart Devices for use in the implementation of nuclear safety functions. The following text is an extract from the TSC report Ref. 77. All reference to NSL in the following text should be interpreted as a reference to the SSP.

The aim of this review was to consider the submissions in line with the Actions as identified in the Resolution Plan and to advise HSE/ONR on their adequacy, or otherwise, to support HSE/ONR decisions on the close out of the Actions, and hence the GDA Issue. GI-UKEPR-CI-04 consists of a single Action supported by six main submissions. From review of each submission, Technical Clarifications and Observations were raised as required in order to reach convergence between ONR and EDF and AREVA (i.e. the submissions are adequate for the purpose of closing out the GDA Issue but there may be open observations that should be addressed during Nuclear Site Licensing (NSL)).

The proposed methodology for qualifying Smart Devices as defined by the Resolution Plan and described in the documents listed below, were reviewed against the clauses of the applicable documents; *Licensing of safety critical software for nuclear reactors; Common position of seven European nuclear regulators and authorised technical support organisations,* and the *Smart Sensors and Actuators Checklist* produced by the TSC in Phase 1 Step 4. The following documents were reviewed:

b. *ENSECC110106 "Lifecycle approach to qualify Smart Devices used in nuclear safety applications";*

c. *ENSECC110110 "EMPHASIS Tool Evaluation";*

d. *ENSECC110102 "Justification of smart devices for nuclear safety applications".*

The examples of the implementation of the methodology as defined by the Resolution Plan, and the documents listed below, were also reviewed against the methodology documents and the clauses of applicable documents identified above. The following were reviewed:

a. *ECECC111184 "UK EPR Smart Devices – Trial Applications";*

b. *ECECC121091 "Summary Qualification Report … " and supporting documents;*

c. *ECECC121403 "Progress Report on Class 1 Smart Device Trial Assessment" and supporting documents.*

An interim version of the Class 2 Trial Application Progress Report was submitted along with supporting documents, including; Requirements Identification File, Equipment Identification File and Qualification Plan. These were not included in the Resolution Plan as defined deliverables but they are referenced from the identified deliverables as outputs from the process and inputs to the final deliverable for the Class 2 Trial Application. They were reviewed to identify potential concerns early in the application of the justification methodology.

Following the TSC review of the Requesting Party's response to the Technical Clarifications and Observations and related amendments to submitted documents, any TSC observations were captured in the corresponding TSC GDA Issue report and were also highlighted to ONR.

<u>Closed Clarifications and Observations</u>

Annex 14

The responses to nineteen of the Technical Observations and Requests for Clarification raised by the reviews of the submissions in support of resolution of GI-UKEPR-CI-04 were considered to be sufficient and adequate to allow these to be 'Closed' during the GDA Closure phase. The related topics are summarised below.

a. For the SMART Device qualification methodology documentation:

   i. Documentation was updated to clarify use of standards, roles of organisations, modification process, use of pre-existing devices and classification and reliability requirements;

   ii. Documentation was updated to clarify use of the EMPHASIS tool and the applicable question set;

   iii. The scope of the trial application of the SMART device qualification methodology was improved and trial application deliverables clarified;

   iv. A consistent approach was confirmed and hardware qualification requirements clarified;

   v. Source code access requirements and 'prior-use' arguments were defined;

   vi. Class 1, 2 and 3 SIL levels were aligned with the requirements of IEC 61508 and TAG046;

b. For the Class 2 SMART Device trial application submission documents:

   i. The Equipment Identification File was updated to clearly cover the requirements placed on it by ENSECC110106;

   ii. The Requirements Identification File was updated to address unspecified behaviours and demonstrate these are not exhibited.

<u>Open Observations</u>

These observations were raised by the reviews of the submissions that relate to the SMART Device qualification methodology and its trial application for Class 1 and 2 devices, and are summarised below.

a. For the Class 2 SMART Device trial application submission documents:

   i. The Summary Qualification Report should address more specifically the Hardware Qualification Step 6, include more specific detail in the SIL2 justification, and align proven in use arguments with relevant standards;

   ii. The Software Assessment Report should identify and reference documented evidence of software testing;

   iii. All Techniques & Measures required by Annex A to ENSECC110102 should be addressed;

   iv. Future use of the EMPHASIS tool database should have adequate and appropriate Evaluator comments.

b. For the Class 1 SMART Device trial application submission documents:

   i. The Requirements Identification File should address exact parameterisation functionality and identify the process for verifying correct parameter transfer;

   ii. The Summary Qualification Report should address more specifically the Hardware Qualification Step 6 and clearly identify that the qualification is based on the specific UK EPR methodology developed in response to GDA Issue GI-UKEPR-CI-04 and not Flamanville 3;

Annex 14

iii. All Techniques & Measures required by Annex A to ENSECC110102 should be addressed;

iv. Future use of the EMPHASIS tool database should have adequate and appropriate Evaluator comments.

Conclusions of the Review

For GDA Issue GI-UKEPR-CI-04, based on the sampled evidence, there is no evidenc e to indicate that the definition of a methodology for the qualification of Smart Devices for use in the implementation of nuclear safety functions has not been adequately defined, and agreed to the level required to conclude the GDA Closure review.

The six open observations are not considered to be at a level of significance that would prevent closure of the GDA Issue. It is judged appropriate that these open observations be addressed during the Nuclear Site Licensing activity.

Annex 14

GI-UKEPR-CI-04 OPEN TECHNICAL OBSERVATIONS

GICI04.TO2.03 – The following observations arose from the review of the Class 2 Smart Device Qualification Trial Appli cation documents; ECECC121091 Rev A, ECECC12 1090 Rev A, ECECC120095 Rev B and ECECC120096 Rev B:

a. The Smart Device qualification process, summarised in the Summary Qualification Report, should address all Steps, including Hardware Qualification (Step 6) and deliver all outputs from these steps in accordance with the methodology.

b. The Summary Qualification Report should include a level of specific detail to demonstrate a SIL2 justification has been made (e.g. actual reliability data against the SIL2 requirement, static / complexity analysis undertaken and the results, tools used for such and the justification of these tools).

c. EDF had only 'limited access' to source code. The process (ENSECC110102B Appendix C) requires statistical testing if source code is not obtained. The full implementation of the methodology should ensure that a lack of full source code access leads to applicable additional testing in accordance with Appendix C, and provides justification where this is not practicable.

d. Section 6.2 of the SQR sets out a CAE format for ICBM; this provides Claims and Arguments followed by a 'summary of evidence'. The 'evidence' should identify which Claim it supports.

e. In the Software Assessment Report EMPHASIS review under 'Phase 4 – Software', it is stated;

   i. 'The software was extensively tested, and documented to a satisfactory degree.'

   The full impl ementation of the method ology should clearly identify and refe rence the documented evidence of this extensive software testing.

f. Under section 6.3 'OPEX' it is stated that 'Calculations of reliability show that DX1000 failure rates are consistent with a 10-2/SIL 2 product'. Proven in use should meet the requirements of IEC61508 clause 7.4.10.1-7, and this should be justified.

g. Appendix A to ENSECC110102B describes certain techniques and measures that '*should be considered for inclusion as ICBMs and should in any case be offered as part of the justification if pre-existing evidence for them is available*' and also states that '*If these techniques are not to be performed as ICBMs, the reasons for their exclusion should be documented*'. The full implementation of the methodology should ensure that the Techniques and Measures are addressed in the Summary Qualification Report as required by Appendix A to ENSECC110102.

h. The Requirements Identification File should be updated to fully reflect the requirements of the application, including interactions with the environment and personnel, taking into account IEC 61513:2011 clause 6.2.3.2 relating to requirements for pre-existing components.

i. The review of the EDF EMPHASIS V1.2 database file identified instances where there was no detailed Evaluator's comment to confirm the specifics of the Question had been addressed or simply 'OK' was inserted. Future use of the EMPHASIS Assessment Tool should ensure adequate and appropriate Evaluator comments are included to confirm and support the evaluation of an 'adequate' response.

GICI04.TO2.04 – The following observations arose from the review of the Class 1 Smart Device Qualification Trial Application Requirements Identification File, ECECC121334 Rev A:

Annex 14

a. The exact parameterisation functionality should be explicitly defined and the requirement for non-interference with the safety function of the device needs to be addressed,

b. There should be a requirement in the RIF[34] to verify that the correct parameters have been transferred,

c. The RIF should include the requirement that the parameterisation process is designed to be resistant to inadvertent changes, such as memory loss and resets caused by power loss and restoration.

d. The operating environment section, section 3.2, should address the correct device.

GICI04.TO2.05 – The following observations arose from the review of the Class 1 Smart Device Qualification Trial Application Summary Qualification Report, ECECC121337 Rev A:

a. The SQR concentrates on Step 7 of the Smart Device justification methodology (software assessment PE/CM/ICBM) with no reference to Step 6 (hardware assessment). The SQR should identify how each Step of the Smart Device qualification lifecycle has been addressed.

b. There appear to be errors in the referencing in the report. The referencing to supporting documents should be reviewed for accuracy and amended where necessary.

c. The SQR states that qualification is based on the existing process in use for FA3 rather than that derived in response to GI-UKEPR-CI-04. The SQR should be clear on exactly what qualification process has been used.

GICI04.TO2.06 – The following observations arose from the review of the Class 1 Smart Device Qualification Trial Application Software Assessment Report, ECECC121336 Rev A:

a. In the extract of Phase 4 (Software) Main Questions where the ‘Final decision’ on the answer was ‘Adequate’, there is no ‘Evaluation commentary’ to explain what the auditor saw and to show that this clearly demonstrated that all points of the question had been answered. The ‘Evaluation commentary’ should be completed in sufficient detail to demonstrate that the question has been answered correctly and that all aspects of the question have been addressed.

b. Appendix A to ENSECC110102B describes certain techniques and measures that ‘*should be considered for inclusion as ICBMs and should in any case be offered as part of the justification if pre-existing evidence for them is available*’ and also states that ‘*If these techniques are not to be performed as ICBMs, the reasons for their exclusion should be documented*’. The full implementation of the methodology should ensure that the Techniques and Measures are addressed in the Summary Qualification Report as required by Appendix A to ENSECC110102.

GICI04.TO2.07 – The following observations arose from the review of the response to TATS action GI 14-I&C-4 relating to the safety effect of parameterisation:

a. Where Commercial Off The Shelf (COTS) software and Software of Unknown Pedigree (SOUP) etc. is incorporated into a Smart Device, justification should be produced that this software is fit for its intended purpose. The justification to include the techniques

[34] ONR note: RIF is an abbreviation of Requirements Identification File.

Annex 14

and measures used in its development, and the independent confidence building measures used.

b. Where it is claimed that COTS or SOUP etc. included in a Smart Device does not perform a safety function and therefore does not need to be justified to appropriate safety standards, then a full justification should be produced that it cannot unintentionally interfere with software that performs a safety function. The justification to include the potential for such software to be executed inadvertently, for memory to be corrupted (including program storage areas), and for its execution to fail to terminate when commanded, etc.

c. A justification should be produced that the process for the loading and read back of parameters in a Smart Device has adequate integrity. The justification to include the potential for the incorrect translation of data values, the incorrect positioning of values in the parameterisation memory, and incorrect parameterisation caused by e.g. version changes.

The above approach to the use and justification of COTS and SOUP should be included in the methodology for the justification of both Class 1 and Class 2 Smart Devices for use in nuclear safety applications, e.g. ENSECC110102.

GICI04.TO2.08 – The following observations arose from the review of the Class 1 Smart Device Qualification Trial Application documents; ECECC121337 Rev A, ECECC12 1336 Rev A, ECECC121334 Rev A and ECECC121335 Rev A:

a. The GDA submission for the trial application of the Class1 Smart Device qualification methodology represents an interim assessment based on available data and has identified a number of gaps, weaknesses and further work/analysis to be completed before a full conclusion can be drawn. The full and final suite of Class 1 Smart Device qualification documentation and supporting evidence, for the STT1 Temperature Transmitter should be reviewed when available during NSL.

Further updates to the documents and the review of them should take account of observations GICI04.TO2.04, GICI04.TO2.05, GICI04.TO2.06 and GICI04.TO2.07.

Annex 15

TSC Summary **–** GDA Issue **GI-UKEPR-CI-05 –** Obsolescence of the SPPA T2000 Platform[35]

Note this information has been imported from a TSC report (Ref. 78) and the formatting of the TSC report has been retained.

[35] Note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 15

Annex: TSC task summary - GDA Issue **GI-UKEPR-CI-05** - Obsolescence of the SPPA T2000 Platform

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of submissions presented by EDF and AREVA to address resolution of GDA Issue GI-UKEPR-CI-05, "definition of the platform that will be provided for the UK EPR and submission of a Basis of Safety Case that fully addresses the change from the SPPA T2000 (Siemens S5 based) to the proposed system". The following text is an extract from the TSC report Ref. 78. All references to NSL in the following text should be interpreted as a reference to the SSP.

The aim of this review was to consider the submissions in line with the Actions as identified in the Resolution Plan and to advise HSE/ONR on their adequacy, or otherwise, to support HSE/ONR decisions on the close out of the Actions, and hence the GDA Issue. GI-UKEPR-CI-05 consists of a single Action supported by five main submissions. From review of each submission, Technical Clarifications and Observations were raised, as required, in order to reach convergence between ONR and EDF and AREVA (i.e. the submissions are adequate for the purpose of closing out the GDA Issue but there may be open observations that should be addressed during Nuclear Site Licensing (NSL)).

The submissions were reviewed against the clauses of IEC standards and ONR guidance documents where applicable, and where none apply, the competence and experience of the reviewer was used as the basis for review.

Following the TSC review of the Requesting Party's response to the Technical Clarifications and Observations and related amendments to submitted documents; any TSC observations are captured in the corresponding TSC GDA Issue report and are also highlighted to ONR.

The following Change Management Forms for this design change were reviewed by ONR:

1. *"Change Management Form 29 - SPPA T2000 S7*
   Stage 1 Design Change Proposal (description and rationale)";
2. *"Change Management Form 29 – SPPA T2000 S7*
   Stage 2 Impact Study (Impact analysis)".

The Basis of Safety Case (BoSC) for the change from the SPPA T2000 version S5 platform to the replacement version S7 platform, and other supporting documentation, as identified in the Resolution Plan, were reviewed against the list of criteria specified by HSE/ONR in the GDA Issue Action, and in the context of the selected SAPs and other applicable documents. The BoSc related documents reviewed were:

1. *"Outline of Basis of Safety Case for the SPPA-T2000 based I&C systems (SAS, PAS, SAS RRC-B, PICS and Plant Bus) and SPPA-T2000 platform" – PEL-F/11.0353;*
2. *"Basis of Safety Case for the change from SPPA T2000 S5 to S7" – PEL-F DC13 Revision A;*

The document *"Justification that the SPPA T2000 S7 platform and TXS platform are suitably diverse to support the reliability claims made for combinations of systems using the two platforms",* originally cited in the Resolution Plan, was removed by EDF and AREVA, as proposed in letter EPR01111N, and agreed by ONR via letter EPR70414N. The intent was that this would be replaced with a document on Platform Diversity, *'Justification of diversity between I&C platforms – PTL-F DC 2 rev A'*. PTL-F DC 2 rev A was not submitted during GDA as highlighted by EDF and AREVA in letter EPR 01315N, and has been replaced by two submissions as agreed with ONR at a Technical Meeting on 9 August 2012:

Annex 15

1. NLTC-G/2009/en/0018 rev B "*Exclusion of CCF between SPPA T2000(S7) and TELEPERM XS by using diversity*", the existing platform diversity analysis between Teleperm XS and SPPA-T2000/S7 that was developed for the Taishan project;
2. PTI12.1071 rev A "*Current Diversity Analysis between SPPA-T2000(S7) and TELEPERM XS - Corrective action plan*", a document that presents the diversity issues highlighted in the above document and proposed corrective actions.

These submissions were reviewed under GDA Issue GI-UKEPR-CI-06 Action A1*.*

A sample (six of nine) of the detailed evidence documents provided by EDF and AREVA in support of the BoSC, in addition to the documents identified in the Resolution Plan, was reviewed against the claims and arguments presented in the BoSC. The sample was sufficient for the TSC to form an opinion on the adequacy of the justification for the change from the SPPA T2000 version S5 platform to the replacement version S7 platform.

Closed Technical Clarifications and Observations

One Technical Observation was raised after a review of the Outline of the BoSC submission in support of resolution of GDA Issue GI-UKEPR-CI-05. Points raised included the scope of the BoSC (it appeared to be focussing on justifying the S7, not the change from S5 to S7), inconsistencies between the expected BoSC format and that proposed, and deficiencies in the proposed BoSC content. These were resolved during the GDA Closure phase, as summarised below.

EDF and AREVA made a number of commitments which were subsequently incorporated into the BoSC by:

a. ensuring the BoSC focused on changes from the SPPA-T2000 S5 platform to the S7 platform.
b. following the original format proposed by EDF and AREVA in letter EPR00852R, ONR requirements set out in letter EPR70302R, and the BoSC content guidance in the Appendix to TQ-EPR-1507; and
c. identifying how all requirements / expectations had been captured in the BoSC using a traceability matrix.

The two Technical Observations from Step 4 identified in the GDA Issue were also closed on the basis of the content of the submissions provided as part of the execution of the Resolution Plan.

Open Observations

The observations raised by the reviews of the Basis of Safety Case for the change from SPPA-T2000 S5 to S7 and the documents submitted in support of it, that remain open at the end of the GDA Closure phase are summarised below.

a. For the Basis of Safety Case:
    i. Due to the dispersed nature of the safety demonstration, the structure of the BoSC should be rationalised or the location of the key elements of the safety demonstration identified in the introduction.
    ii. The rationale for the identification of the requirements and selection of the SAPs should be given.
    iii. Demonstration should be included that hardware development conforms to safety principles and standards.
    iv. Detailed consideration should be included of the changes in engineering tools.

Annex 15

v. A ‘Conclusion’ that pulls together the safety demonstration and the Impact analysis to adequately demonstrate the basis of the safety case for the change from S5 to S7 should be included.

b. For supporting documents:

i. Standards compliance justifications should; have complete and accurate referencing to evidence documentation, address the specific requirements of each point of the clause, and explain how the evidence demonstrates that the requirements of the clause are met.

ii. Reliability and Dependability analyses should; identify how assumptions are validated and accounted for in calculations, ensure all modules are addressed or explain any omissions, and due to redacted information it should be identified that there is an auditable trail leading to the conclusions.

iii. For the System Specification File, it should be identified that the UKEPR System Specification contains the equivalent information as provided in the FA3 System Specification, and that descriptions of modules CP443-1 and IM616 address firmware.

Conclusions of the Review

For GDA Issue GI-UKEPR-CI-05, based on the sampled evidence, there is no evidence to indicate that the definition of the change of the SPPA T2000 platform from Siemens S5 to S7 for the UK EPR and production of a Basis of Safety Case addressing the change has not been adequately achieved, and agreed to the level necessary to conclude the GDA Closure review.

The six open observations are not considered to be at a level of significance that would prevent closure of the GDA Issue. It is judged appropriate that these open observations be addressed during the Nuclear Site Licensing activity.

Annex 15

GI-UKEPR-CI-05 OPEN TECHNICAL OBSERVATIONS

GICI05.TO2.01 – The following observations arose from the review of IEC 62138 Justification for AS620B, (UK EPR-QU 042, Rev 0.1):

a. There are a number of clauses for which the justification for compliance is just a reference to documents, and frequently these documents are referred to simply by title without specific document references. Complete and accurate referencing to evidence documentation should be included in the compliance analysis.

b. The justification for compliance with the clauses does not always address the specific requirements within each point of the clause. Also, where evidence of clause compliance is via a reference to an evidence document there is no accompanying explanation as to how the evidence document demonstrates that the requirements of the clause are met. The justification for clause compliance should address all clause requirements and clearly explain how each of these requirements is met by reference to the pertinent section / paragraph of the evidence document.

c. There are occasions where the justification for clause compliance is claimed to address software in a number of systems/sub-systems, e.g. AP system software (APSSW) / IM616 / FUM. However, the justification refers to a set of documents that appear to relate to specific software, for example, to the APSSW only. The justification for clause compliance should address all software cited against the clause (e.g. AP System Software (APSSW)/ IM616 / FUM, and SIMATIC S7 operating system (S7-OS) / CP 443-1 / CP 443-5), that each is covered by the evidence and an explanation of how this evidence demonstrates compliance for each software cited.

Further details and specific examples of the general points above can be found in Annex F, 'Supplement to GICI05.TO2.01', of GDA Issue GI-UKEPR-CI05 TSC report 39075/38099R.

GICI05.TO2.02 – The following observations arose from the review of 'IEC 62138 Justification for OM690', (UK EPR-QU 041, Rev 0.2):

a. The description of the quality system indicates it to be appropriate in terms of scope and its procedures are referenced in the compliance statements. However, the quality system should be examined for completeness and the adequacy of the procedures confirmed, e.g. by inspection, and documented. Evidence of their use should be identified in UK EPR-QU041 to support the safety case.

b. The link between the descriptive information in the clause introduction and the individual clause requirements should be made explicit in the responses provided for the individual sub-clause items and not be by inference; the compliance document UK EPR-QU041 should be improved to support the safety case.

c. The descriptions and compliance statements refer to supporting evidence, e.g. process inputs and outputs, in generic terms as 'specifications', 'design papers', 'logs' and 'test reports' for all phases of the development lifecycle / standard clauses. The 'referencing' of this information should be in sufficient detail to allow the items to be identified. Similarly, references such as F-PRI06 and F-O4207 should be given in full. The compliance document UK EPR-QU041 should be improved to support the safety case.

d. The evidence supporting compliance is in the form of head documents, e.g. QU036, specific references, e.g. F-PRI06 and F-O4207, and generic descriptions, e.g. 'design papers'. This evidence should be examined for completeness and adequacy, e.g. by inspection, and the outcome documented.

Annex 15

GICI05.TO2.03 – The following observations arose from the review of Reliability Analysis SPPA-T2000/S7, (UK EPR-QU018, Rev 0.1):

a. The reference numbers for the dependability analyses have been redacted from the document. It should be identified that the Reliability Analysis (UK EPR-QU 018, Rev 0.1) and Dependability Analysis (EPR-QU019, Rev 0.1) are consistent with each other.

b. The Basis of Safety Case of SPPA-T2000 (BoSC) (PEL-F DC 13, Rev A) identifies modules XU and CM104; however, these are not considered in the Reliability Analysis. The reasons for excluding these modules from the analysis should be identified in the Basis of Safety Case document

c. Section 2.1.5 presents a number of assumptions: e.g. the ambient temperature for the calculations is 40^0C; 3 out of 4 Operator Working Places run the plant. There is no indication of how these assumptions are validated or accounted for in higher level calculations i.e. reliability calculations based on the analysis presented in the document.

   The basis for these assumptions should be identified in the Basis of Safety Case.

   The assumptions that relate to plant conditions and equipment availability / repair times should be captured in operating procedures.

d. Much of the detail of the analysis and calculations and the results have been redacted from the document such that it is not possible to confirm if there has been an auditable trail leading to the conclusions and that the results support the claims made in the BoSC.

   An auditable trail leading to the conclusions that the details of the analysis and the results support the claims made in the BoSC should be identified in the BoSC e.g. by inspection of the unredacted documentation.

GICI05.TO2.04 – The following observations arose from the review of Module dependability analysis for SPPA T2000 (S7) AS620B / SPPA-T2000 – OM components Safety parameter determination approach, (UK EPR-QU019, Rev 0):

a. Section 3.3 presents an assumption that the ambient temperature for the calculations is 40^0C. There is no indication of how this assumption is validated or accounted for in higher level calculations, i.e. reliability calculations based on the analysis presented in the document.

   The basis for this assumption should be identified in the Basis of Safety Case.

   The assumption should be captured in operating procedures.

b. Section 4 identifies the modules for which the analysis has been performed and a table includes a reference to the reports for each module. It is noted that there is no reference for the XU and CM104 modules, which are identified in the BoSC.

   The reasons for excluding these modules from the analysis should be identified in the Basis of Safety Case document.

c. The redaction of the dependability analysis is such that it is not possible to confirm if there has been an auditable trail leading to the conclusions and that the results support the claims made in the BoSC (via QU018).

   An auditable trail leading to the conclusions that the details of the analysis and the results support the claims made in the BoSC should be identified in the BoSC e.g. by inspection of the unredacted documentation.

Annex 15

GICI05.TO2.05 – The following observations arose from the review of System Specification File (DSS), (UK EPR-QU014, Rev 0.1):

a. Not all of the annexes have been provided for review as they contain Siemens protected information. Therefore, the review included consideration of the corresponding FA3 System Specification (SY710, Version: BPE 6.0).

   The UK EPR System Specification should:

   i. contain the equivalent information as that provided in the FA3 System Specification (as claimed in note 4 to Table 18 of the BoSC).

   ii. reflect the changes to the architecture described in the Basis of Safety Case (BoSC).

b. Annex 4 of the FA3 System Specification provides a detailed description of interfaces and annexes 7 and 8 give information on diagnostics and interlocking of control panels. The location of the equivalent information in the UK EPR System Specification should be identified.

   Detailed definitions of interfaces, equivalent to those documented in Annexes 4, 7 and 8 of the FA 3 System Specification should be identified in the UK EPR System Specification.

c. Sections 2.3 and 2.4 of the FA3 System Specification provide details of how the AP open and closed loop control functions are implemented. Equivalent descriptions should be produced for the UK EPR System Specification.

d. The description of Automation Processor System Software in the FA3 System Specification indicates that it performs redundancy functions, but this is not shown in the description of the equivalent software in the BoSC.

   As the BoSC does not refer to redundancy functions performed by the AP system software the BoSC should identify the reasons why this approach has been adopted.

e. The descriptions in the UK EPR System Specification of modules CP443-1 and IM616 should address firmware.[36]

GICI05.TO2.06 – The following observations arose following the review of the Basis of Safety Case for the change from SPPA T2000 S5 to S7 (PEL-F DC13 Rev A), and a sample of its supporting references, against the BoSC contents structure and completed Traceability Matrix (PEL-F 12 0152) and the requirements of GI-UKEPR-05:

a. The document review and the traceability matrix PEL-F 12 0152 shows the identification of ‘requirements / design principles / standards’ is dispersed across the document including sections 2 and 3. Similarly, the ‘safety demonstration’ can be found in a number of sections of the document including sections 3, 4 and 5. The document structure should be rationalised, e.g. to follow that proposed by the RP, or the location of the key elements, i.e. the ‘requirements / design principles / standards’ and the ‘safety demonstration’ and their role should be identified in the introduction.

b. The origin of the claims made under the six key claim headings is not immediately apparent. A rationale for the identification of the requirements in 2.1.1 to 2.1.5 should be given.

[36] ONR Note: EDF and AREVA have clarified that dedicated documents will be provided to describe the hardware and software architecture of SPPA-T2000 components.

Annex 15

c. The control of development at the highest level is not visible particularly that for the hardware. Additional information should be identified for hardware development to show it conforms to the safety principles and standards at each step of the development and deployment.

d. The adequacy of the identified test reports should be confirmed during NSL once they are available.

e. The means by which the applicable SAPs were selected, or excluded, e.g. EDR.4 for Single Failure Criterion, is not apparent. A rationale for SAP selection should be identified.

f. The analysis in the BoSC does not appear to consider, in detail, changes to the engineering tools including the introduction of the S7 code converter and ES-S7 server to load the AS620B system identified in section 1. This should be included directly or by reference to supporting documentation (annex 4 of BoSC reference [3] and the testing identified in BoSC reference [42] may be relevant in this respect).

g. The BoSC should contain a ‘Conclusion’ that pulls together the safety demonstration and impact assessment to show that all aspects have been identified and considered, e.g. by reference to the impact analysis conducted under CMF029 Stage 2, and to demonstrate adequacy of the change from SPPA-T2000 platform version S5 to S7.

h. The means by which complex components including programmable hardware, e.g. ASICs and FPGAs, are developed and included in the equipment should be identified.

Observations GICI05.TO2.01. 02. 03, 04 a nd 05 and also GICI06.A8.T O2.06 should be addressed in conjunction with GICI05.TO2.06.

Annex 16

TSC Summary – GDA Issue **GI-UKEPR-CI-06** – Issues arising from Regulatory Issue RI02[37]

Note this information has been imported from a TSC report (Ref. 79) and the formatting of the TSC report has been retained.

[37] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 16

Annex: TSC task summary - GDA Issue **GI-UKEPR-CI-06** – Issues arising from Regulatory Issue RI02

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of submissions presented by EDF and AREVA to address resolution of GDA Issue GI-UKEPR-CI-06, issues arising from Regulatory Issue RI 02. The following text is an extract from the TSC report Ref. 79. All references to NSL in the following text should be interpreted as a reference to the SSP.

The aim of this review was to consider the submissions in line with the Actions as identified in the Resolution Plan and to advise HSE/ONR on their adequacy, or otherwise, to support close out of the Actions, and hence the GDA Issue. GI-UKEPR-CI-06 consists of nine Actions supported by twenty-five submissions defined in the Resolution Plan, plus thirty-three submissions provided in Step 4 of GDA, and thirty-six additional submissions provided in the GDA Closure phase. From review of each submission, Technical Clarifications and Observations were raised, as required, in order to achieve resolution of the GDA Issue.

The submissions were reviewed against the clauses of IEC standards and ONR guidance documents where applicable, and where none apply, the competence and experience of the reviewer was used as the basis for review.

Following the TSC review of the Requesting Party's response to the Technical Clarifications and Observations and related amendments to submitted documents, any open TSC Observations are captured in this report and are also highlighted to ONR.

Closed Technical Clarifications and Observations

Forty-seven Technical Clarifications and Observations raised by the reviews of the submissions in support of resolution of the nine actions in GI-UKEPR-CI-06 were closed during the GDA Closure phase. An overall summary of the related topics is provided below.

Action A1 - A way forward was agreed for the definition of the methodology that is to be applied to diversity and independence management of the three C&I protection systems and their platforms. In addition, convergence (i.e. adequacy for the purpose of closing out the GDA Issue, but there may be open observations that should be addressed during Nuclear Site Licensing (NSL)) has been reached on the diversity criteria to be applied to various aspects of the design, development and deployment of these systems.

Action A2 - The approach to hardware reliability and Production Excellence (PE) demonstration of software of the Protection System (PS) and its platform has been converged upon. Convergence has been reached on the approaches for conducting the reliability analysis of SPPA-T2000/S7-based C&I systems, and of the NCSS and its platform (UNICORN).

Action A3 - Convergence was reached on the guidelines for the application of PE activities and Independent Confidence Building Measures (ICBMs) to computer-based systems important to safety. A way forward was agreed for the justification of PE activities and ICBMs for TELEPERM XS-based systems, and for SPPA-T2000/S7-based systems, based on these guidelines.

Action A4 - The architectural changes relating to the commitment made in GDA Step 4 to eliminate, where reasonably practicable, inputs to the PS from lower classified systems, have been captured in revision C of the PS System Description. The justifications of non-disturbance of PS functions via hardwired connections have also been reviewed, and convergence on these justifications was reached.

Action A5 - A demonstration has been reviewed that potential erroneous behaviour of the Class 3 SPPA-T2000 systems and equipment, resulting in challenges to the Safety Automation

Annex 16

System (SAS), cannot interfere with the SAS automatic safety functions. Convergence on the acceptability of the results has been reached.

Action A6 – Convergence has been reached on the definition of the Class 1 controls and indications, at the level of the generic design, in both the Main Control Room and the Remote Shutdown Station. Convergence has also been reached on the Basis of Safety Case for the Class 1 Protection System Operator Terminal (PSOT).

Action A7 - A justification was provided and accepted, as to why having the Safety Instrumentation and Control System controls inactive until needed (when there is failure of the Process Instrumentation and Control System), is preferable to having them active during normal operation.

Action A8 - A way forward has been agreed with regard to the demonstration that end-to-end response time requirements are achievable for the UK EPR implementation, based on a review of performance improvements that are identified to meet the requirements of the reference implementation (Flamanville 3).

Action A9 - Convergence has been reached on the criteria used to assess adequacy of diversity for sensors, conditioning modules, and the Priority Actuation Control (PAC) system. Convergence has also been reached on the basis of substantiation of the probabilistic claims, and the approach to implementing the required diversity, for sensors, conditioning modules, PAC modules, and other C&I actuation components.

<u>Open Observations</u>

Forty-six Technical Observations raised by the reviews of the submissions in support of resolution of the nine actions in GI-UKEPR-CI-06 remain open at the end of the GDA Closure phase. An overall summary of the related topics is provided below.

Action A1 – A full diversity justification between the Teleperm XS and SPPA-T2000/ S7 platforms that is applicable to UK EPR, using the methodology agreed during GDA, should be implemented and documented. The definition of the diversity management methodology should be refined and completed, as committed during the GDA process, and evidence should be produced to demonstrate that this methodology is being carried out throughout the UK EPR C&I system lifecycle.

Action A2 - Further evidence should be included in the compliance analyses to demonstrate conformance with specific clauses of IEC 61513, IEC 60880, and IEC 60987, for the PS and associated Teleperm XS modules to be used for UK EPR, and to demonstrate that the PS design target reliability is met for all of its functions. A detailed justification should be included in the safety case to support the reliability claim of 10-2 pfy/ pfd for systems based on the SPPA-T2000/S7 platform. A detailed justification should be included in the safety case to support the reliability claim of 10-3 pfy/pfd for the UNICORN platform modules used to implement the NCSS system for UK EPR. The results of further independence-related, and common cause failure-related, analyses that have been identified as to be performed during Nuclear Site Licensing should be included in the safety case.

Action A3 - The PE/ICBM guidelines should ensure that a demonstration is produced to show that each tool is fit for its purpose at the classification level at which it is applied, and that a demonstration of adequacy that is commensurate with a system's classification is produced for all aspects of the dynamic behaviour of a system and its platform. The safety case for ICBMs applicable to the SPPA-T 2000/S7 software should identify the criteria used to select the key software elements for code review, and should justify and define fully the approach to be used for both C code and assembler code. The safety case should also demonstrate that the test platform used for the dynamic testing of SPPA- T2000/S7 software that is performed as an ICBM, is sufficiently representative of the target execution environment.

Action A4 - The safety case should record a generic rule that defines the minimum classification requirements for maintenance and periodic testing equipment, tools and components. The

Annex 16

safety case should also record the results of the completion of the analysis into the effect on the PS safety functions of potential spurious orders from lower-classified systems via hard wired links.

Action A5 - The justification of the failure independence that mitigates the propagation of errors between C&I systems hosted on the SPPA-T2000 platform, based on version S7 technology rather than version S5 technology, should be included in the safety case. The definition of the functional and safety interlocks that prevent the operation of spurious actions that are inappropriate to the current state of the plant, should be included in the safety case. The analysis of the potential transmission of a spurious, but plausible, order from the Process Information and Control System to the SAS, should be completed, and its effect on the SAS safety functions should be assessed and documented.

Action A6 - Some areas for improvement in the PSOT Requirements Specification and Basis of Safety Case have been identified. The plant probabilistic safety analysis should include the reliability and functionality of the PSOT system to demonstrate that UK EPR safety targets are met. The approach to the ICBMs to be applied to the PSOT system for static analysis of the source code, and for demonstrating the adequacy of the development tools, and for demonstrating the adequacy of the dynamic behaviour, should be fully defined. The adequacy of all complex electronic components, or smart devices, that are used in either the Safety Information and Control System or the PSOT should be justified (see SAPs ESS.21 and ESS.27). Conformance with appropriate IEC standards should be fully demonstrated for the Qualified Display System hardware and software.

Action A7 – No open observations.

Action A8 - Analysis of the applicability to UK EPR of the results of the potential performance improvements to be identified for the Flamanville 3 project should be carried out, and changes integrated into the UK EPR C&I design where appropriate. A full justification should be documented in the safety case that end-to-end response time requirements for C&I functions on the SPPA-T2000/S7 platform are achievable under worst case (avalanche) conditions. Analysis should be carried out of the effect of any increases in times within the predictability model for SPPA-T2000/S7, compared to version S5, on the safety functions carried out by the systems important to safety that execute on this platform.

Action A9 - Comprehensive diversity implementation plans should be produced, both for sensors and conditioning modules, and for PAC modules, that demonstrate conformance with the applicable diversity methodologies that were agreed in the GDA process, including consideration of the impact of maintenance and common mode failure on the ability of any safety system to perform its safety role. Evidence that is relevant to the UK EPR implementation should be presented in the safety case to substantiate that the reliability claims are met for the actual sensors, conditioning modules, and PAC modules that are used in the C&I architecture. The C&I requirements should be reviewed to ensure that all of the ONR Safety Assessment Principles and their related guidance paragraphs that are identified as being applicable to C&I, have been fully addressed. The allocation of structures, systems and components should be reviewed to ensure full conformance with the categorisation and classification scheme.

Conclusions of the Review

For GDA Issue GI-UKEPR-CI-06, based on the sampled evidence, there is no evidence to indicate that the adequacy of the documents submitted to support the intent set out in the Resolution Plan for each of the nine actions, and ultimately the GDA Issue resolution, has not been demonstrated and agreed to the level required to conclude the GDA Closure review.

The open observations are not considered to be at a level of significance that would prevent closure of the GDA Issue. It is judged appropriate that these open observations be addressed during the Nuclear Site Licensing activities.

Annex 16

GI-UKEPR-CI-06 OPEN TECHNICAL OBSERVATIONS

Action A1

GICI06.A1.TO2.04 – The following observations that arose from the reviews of NLTC-G/2009/en/0018 rev B and PTI12.1071 rev A should be addressed in relation to the justification of diversity between the versions of Teleperm XS and SPPA-T2000/S7 that are to be deployed for UK EPR:

a) A full diversity justification between Teleperm XS and SPPA-T2000/S7 should be developed and documented in the UK EPR safety case, that demonstrates how all platform-related diversity criteria in document PTL-F DC 3 are satisfied, and that documents the results of following the diversity methodology process that is defined in document PTL-F DM 1.

b) The design diversity justification should include evidence to support the claim that the development tools, methods and processes used on the two platforms are fully independent and diverse, covering for example:

- the SPACE and ES680 tools generating the automation software;
- the HMI software tools such as Simatic Touch Panels and ES685 tools used to generate the OM690 software.[38]

c) The human diversity justification should include evidence to support the claim of organisational independence between the divisions of Siemens that are involved in the development, manufacture and maintenance of the two platforms, including the use of sub-contractors. For example, the justification should demonstrate the independence between Siemens Fürth and Siemens Erlangen for the manufacture of the binary and analog I/O modules, and between Siemens Karlsruhe and Siemens Erlangen for the manufacture of the processor boards and subracks.

d) The equipment diversity justification should include evidence to support the diversity claim for corresponding components in the two platforms that each originate within:

- Siemens, for example, the TXS backplane bus compared to the backplane bus used for communication in FUM subracks;
- Infineon, for example, the binary and analog I/O controllers.

The equipment diversity justification should also address context of use, and development tools employed, for these components.

e) The equipment diversity justification should confirm that the ASPC2 Profibus controller is not used in the version of SPPA-T2000 that is used for UK EPR, as committed in Section 3 of PTI12.1071 rev A.

f) The equipment diversity justification should confirm that the AMPRO firmware package is not used in the SL22 controller in the version of Teleperm XS that is used for UK EPR, as committed in Section 3 of PTI12.1071 rev A.

g) The equipment diversity justification should confirm that the "OLMAS" ASIC is not used in the version of SPPA-T2000 that is used for UK EPR, as committed in Section 4 of PTI12.1071 rev A. The justification to identify requirement constraints applicable to UK EPR for:

[38] ONR Note: EDF and AREVA have clarified that there are no Simatic touch panels in the UK EPR C&I architecture and confirmed that the diversity requirement is between the safety (SICS) and operational (PICS and PSOT) displays.

Annex 16

- non-use of the AV42 priority management module;
- a maximum of 4 FUM racks associated with an AP for the SAS cabinets.

h) The software diversity justification should include evidence that the MICROS and S7-OS operating systems cannot sustain a systematic Common Cause Failure due to the effects of peak loading and avalanche conditions, that may cause, for example, repeated cycle overrun.

i) The timescale for delivery of the computerised and non-computerised platform diversity justifications should be specified, and should be consistent with the commitment in letter EPR01412N – *"prior to programme milestone 'First Safety Concrete'"*.

GICI06.A1.TO2.05 – Section 11.6.3 of NLTC-G/2009/en/0018 rev B states for SPPA-T2000/S7 that on-line replacement of function blocks and on-line modification to the application call table is possible for the Taishan implementation. The safety case for UK EPR should include a justification that such on-line actions are controlled, see SAP ESS 15, and cannot frustrate the execution of a safety function by the SAS during normal operation.

GICI06.A1.TO2.06 – The documents PTL-F DC 3 rev B and PTL-F DM 1 rev B should be updated to incorporate the following commitments made in the response to TQ-EPR-1628, and in submission PTI/12.1072 rev A:

a) Response to TQ-EPR-1628 point b) states: "*The definition of "main component' and the degree of diversity required [for each grade of complex component] will be precisely detailed in the revision C of the methodology for diversity justification PTL-F DM 1 in the frame of the NSL*." These definitions should include <u>all</u> the corresponding information provided in the TQ response for this point.

b) Response to TQ-EPR-1628 point b) also states: "*The revision B of PTL-F DC 3 – Diversity criteria between PS and SAS, will define the term "main component*". However, only a subset of the text provided in the TQ response has been included in PTL-F DC 3 rev B, and this text is embedded within the definition of Ed=1.5, rather than in a "Definitions" section. The full definition of the term *"main component*", as provided in the response to TQ-EPR-1628 point b), should be included in a "Definitions" section in PTL-F DC 3.

c) Response to TQ-EPR-1628 point g) states: "*The detailed description of the management of software diversity will be provided in the revision C of the document PTL-F DM 1.*" And this commitment is repeated in the response to TQ-EPR-1628 point h). This detailed description should be included in PTL-F DM 1 revision C.

d) PTL-F DM 1 revision C should define the completed and improved diversity management methodology, as committed in Section 1 of PTI/12.1072 rev A, and should incorporate the refinements to the methodology that are defined in PTI/12.1072 rev A, as stated in Section 3 of that document.

e) PTL-F DM 1 revision C should address the following points that arose from the review of PTI/12.1072 rev A:

   i. In Section 2.1 of PTI/12.1072 rev A, the introductory text for Category 2 "*Interfaces*" covers electrical/optical conversion, network switches and gateways as examples of interface equipment, but these are not covered by sub-categories 2.1 ("*Signal diffusion*") and 2.2 ("*Decoupling measures / signal isolation*"). Please ensure that the sub-categories cover all types of interface equipment.

   ii. In Table 3 in Section 2.4.2 of PTI/12.1072 rev A, the "*necessary conditions to fulfil the diversity criteria*" sub-section includes "*Description of the module architecture*

Annex 16

and design" but this does not include software-related attributes. To support the performance of the software diversity analysis, the template forms in Appendix A and B should include entries to record and compare software-related attributes, such as design process, programming language, operating system, and runtime environment.

iii. Section 2.3.2 of PTL-F DM 1 rev B presents two alternative cases for Step 2, that addresses the diversity methodology for electronic components, which differ depending on the overall reliability claim. The "comparison" template form in Appendix B of PTI/12.1072 rev A should identify the overall reliability claim, e.g. above or below 10^{-6} pfd, and should require a more extensive comparison process for modules with a reliability claim better than 10^{-6} pfd, to match the requirement in Step 2 Case b) in PTL-F DM 1 rev B.

iv. Section 2.3 of PTI/12.1072 rev A states "*To ensure the exhaustiveness of the diversity analysis additional verifications are performed not only within a sub-category but transversely (as described in step 3 of the methodology in [PTL-F DM 1 rev B])*". The process for identifying the use of a common complex component in diverse platforms (potentially making use of the checklist in Appendix B of PTI/12.1072 rev A), and for performing the subsequent common cause failure analysis, should be described in an update to PTL-F DM 1 rev B.

f) PTL-F DM 1 revision C should define the criteria for a module or component to be classified as being "*simple*" – the term being used, for example, in Section 2.3.2 of PTL-F DM 1 rev B, and referred to in Section 4.2.4 of PELA-F DC 7 rev B.

GICI06.A1.TO2.07 – The following observations that arose from the review of ECECC121713 rev A, and Appendix A of letter EPR01412N, should be addressed:

a) Section 3.2.2.1 of ECECC121713 rev A states that "*there are no specific requirements for RCSL and PAS to be diverse from each other*", which is consistent with PEPS-F DC 90 rev C. However, Section 2.4 of Chapter 7.1, of the March 2011 version of the PCSR places a diversity-related design constraint on the allocation of "*functions where a failure of a system could be the initiating event and therefore the allocation of subsequent levels of defence has to be on a diverse platform."* This PCSR section cites an example of allocating an RRC-A function that addresses a fault sequence that could be initiated by the failure of a control or safety system, e.g. the PAS, to a system that is implemented on a diverse platform, e.g. the RCSL. This diversity-related design constraint should be stated explicitly in the safety principles applicable to diversity and defence-in-depth for UK EPR C&I Systems, or other appropriate safety case document.

b) A detailed justification of the diversity between SICS and PICS/PSOT should be developed and documented in the safety case, as committed in Section 3.2.4 of ECECC121713 rev A.

c) A final diversity compliance report that addresses system-level diversity for the C&I protection systems should be carried out and documented in the safety case when the detailed design is complete, as committed in Section 3.3 of ECECC121713 rev A.

d) The list of TELEPERM XS C&I platform components in Section 3.4 of ECECC121713 rev A should include the Profibus networks, and the section should clarify that platform diversity analysis includes the communication equipment/firmware/protocols associated with each platform.

e) An assessment of actuator components to identify any embedded or associated C&I components, other than the PAC modules, should be carried out and documented in the safety case when the detailed design is complete, and appropriate diversity criteria, implementation plans and substantiations should be developed and documented,

Annex 16

including in relation to any smart equipment that may be used, as committed in Section 3.6 of ECECC121713 rev A. The assessment should include reliability and diversity analyses for Reactor Trip equipment used by the protection systems, for example, reactor trip breakers and reactor trip contactors.

f) Arguments and evidence for fail-safe operation of the SAS and NCSS Class 2 systems, to support the claim of meeting requirement RS10010-FS as defined by PEPS-F DC 90 rev C, should be developed and documented, as noted in Appendix A of ECECC121713 rev A : "*will be provided in a later revision of this document*".

g) Evidence to support the claim that diversity requirements are actively managed throughout the system lifecycle, as described in ECECC121713, should be included in the safety case.

h) Please ensure that all information on diversity lifecycle phases and management that is contained in Appendix A of letter EPR01412N, is captured in an update to ECECC121713 rev A, for example:

- the text in the section headed "*Contract Specifications*" in EPR01412N is not fully incorporated into ECECC121713 rev A;
- the commitment to deliver the C&I diversity justifications prior to programme milestone "*First Safety Concrete*", in the section headed "*Diversity Justification*", is not incorporated in ECECC121713 rev A;
- the summary provided in the section headed "*Summary of Diversity Management Measures*" is not fully incorporated into Section 4 "*Conclusions*" of ECECC121713 rev A.

GICI06.A1.TO2.08

1. The textual definitions of the requirements for corresponding diversity criteria categories and levels are inconsistent across PELL-F DC 11 rev C (NCSS), PTL-F DC 3 rev B (PS/SAS), PELL-F DC 82 rev B (sensors/conditioning) and ECECC120443 rev B (PAC module). The use of the same mnemonic but with different definitions is potentially confusing, for example:

   a) Levels Dd=1 and Dd=2 in ECECC120443 rev B are associated with human diversity requirements, whereas these levels in PELL-F DC 11 rev C and PTL-F DC 3 rev B are associated with design diversity requirements.

   b) Levels Hd=1 and Hd=2 in ECECC120443 rev B are associated with human diversity of reviewers, whereas these levels in the other criteria documents are associated with human diversity of designers.

   c) Level Sgd=1 in PELL-F DC 82 rev B is broadly equivalent to level Fd=1 in PELL-F DC 11 rev C and PTL-F DC 3 rev B.

   d) Levels Sgd=2 and Sgd=3 in PELL-F DC 82 rev B correspond to levels Sgd=1 and Sgd=2 respectively in PELL-F DC 11 rev C and PTL-F DC 3 rev B.

   e) Level Swd=4 has been introduced in PELL-F DC 82 rev B, and is broadly equivalent to elements of Ed=2 in PELL-F DC 11 rev C and PTL-F DC 3 rev B.

   f) The Equipment Diversity levels for sensors in PELL-F DC 82 rev B incorporate elements of functional diversity that are defined by Functional Diversity levels in PELL-F DC 11 rev C and PTL-F DC 3 rev B.

   g) Level Ed=1 for sensors in PELL-F DC 82 rev B, and for actuators in ECECC120443 rev B allow the equipment to be supplied by the same

Annex 16

manufacturer, but this is not allowed for Ed=1 in PELL-F DC 11 rev C and PTL-F DC 3 rev B, nor for conditioning modules in PELL-F DC 82 rev B.

h) Level Ed=2 for conditioning modules in PELL-F DC 82 rev B allows the equipment to be supplied by the same manufacturer, but this is not allowed in any of the other criteria definitions for this level.

i) For levels Ed=1 and Ed=2 in PELL-F DC 82 rev B, the importance of using a different manufacturer appears to be opposite for sensors compared to conditioning modules. For sensors, Ed=1 allows same manufacturer and Ed=2 requires different manufacturer, but for conditioning modules, Ed=1 requires different manufacturer and Ed=2 allows same manufacturer.

j) Level Ed=3 requires independence of organization in PELL-F DC 11 rev C and PTL-F DC 3 rev B, but not in PELL-F DC 82 rev B.

k) Level Ed=4 has been introduced for sensors in PELL-F DC 82 rev B, which is broadly equivalent to level Ed=3 in the other criteria definitions.

l) Level Ed=1.5 is defined in PELL-F DC 11 rev C and PTL-F DC 3 rev B to address computerised systems, but not in PELL-F DC 82 rev B, despite the presence of software in conditioning modules;

The definitions of the levels for each of the C&I diversity categories that are specified in PELL-F DC 11 rev C, PTL-F DC 3 rev B, PELL-F DC 82 rev B, and ECECC120443 rev B should be reviewed to assure consistency both within each topic (e.g. sensors and conditioning modules) and across all topics (e.g. between PACS, computerised systems, non-computerised systems, and sensors and conditioning). The rationale supporting any inconsistencies in the criteria definitions for each level should be documented, for example, in the safety case or alongside the definitions.

2. For each case where the definition of a diversity criteria level is altered as a result of the review, the choice of diversity level that applies to the corresponding systems, modules or components should be reviewed to ensure that the requirements have not been weakened.

GICI06.A1.TO2.09 – The following points that arose from the review of PE LZ-F DC 2 rev B should be addressed:

a) Evidence should be included in the safety case to support the diversity claim of meeting Human Diversity level Hd=2 “*different engineering management teams with no direct communication…*” for the testing and verification activities of, for example:

- the PS and SAS, which are stated as being carried out by PELV2-F (Protection System testing and verification) and PELV3-F (Safety Automation System testing and verification) sub-divisions of the AREVA NP PELV-F division;
- the PS and NCSS, in the case that sub-divisions of AREVA TA are involved in these activities for both platforms.

The evidence should also cover the use of sub-contractors, for example, the PELR-G sub-division of AREVA.

b) In Table 21 of Section 5.6 in PTL-F DC 3 rev B, there is a diversity requirement of Swd=1 on the Verification and Validation of the PS compared to the SAS, which requires “*different computer languages and tool chain*” to be used. A diversity analysis for the software and scripting languages that comprise the tests, test environment, and test invocation for the testing and V&V activities of PS compared to SAS should be included in the safety case. The analysis to compare the Test Tools and V&V Tools

Annex 16

presented in PELZ-F DC 2, for example, ERBUS, SIVAT, RT-SIM and CASSIS compared to Labview and Tec4Function[39].

c) Evidence should be included in the safety case to support the claim that a justification of compliance with the diversity requirements is produced at the start and end of each configuration of the C&I systems, as committed in Section 8 of PELZ-F DC 2 rev B.

Action A2

GICI06.A2.TO2.06 – A justification should be produced for the use of impedance isolation devices other than the Teleperm XS *SOBx* overvoltage barrier modules, to protect against overvoltage events for signals within one division, for example, distribution of analog signals from conditioning cabinets (outputs from module SNV1), as described in Section 3.2.1 of NLE-F DC 249 rev E.

GICI06.A2.TO2.07 – The following points regarding compliance with IEC 61 513:2001 have resulted from the review of PEL-F DC 8, Revision A. Please address these so that adequate compliance with the standard is demonstrated:

a) Section 2.1 describes how the compliance analysis is effectively a plan of how the requirements will be addressed, and the final evidence will be in design documents etc (as identified in the compliance matrix). The final information should contain appropriate evidence to demonstrate that the relevant clauses have been satisfied.

b) Section 2.3 identifies three open points which should be addressed so that compliance is demonstrated. The affected clauses are:

- Open Point 1: Clause 6.1.1.1.1 a) – "*Margins between setpoints for trip functions are not addressed in the I&C documentation. These information may be available in other documentation and remain to be clarified.";*
- Open Point 2: Clause 6.1.2.2.2 b) c) – "*Compliance with IEC 60709 is required. So far, no compliance analysis with this standard has been elaborated.";*
- Open Point 3: Clause 6.2.6 c) – "*It is not clear today if the Periodic Test instructions will be elaborated by AREVA or by EDF/NNB based on AREVA elements (as it is done for FA3). Consequently, it is not clear if they are part of the Quality Plan or not.".*

c) The analysis for a number of clauses justifies compliance by identifying functional aspects of the system, and this is supported by references to:

- requirements specifications (e.g. "System Specifications", "I&C Functions Specifications); and
- other documents (e.g. "TXS operation principles" and "Concepts") (e.g. 6.1.2.3 (a), 6.1.1.1.2, 6.1.1.2.1 (a).

With the former, confidence is gained that the functionality is correctly implemented as a result of V&V activities, and the associated traceability information. With the latter, the situation is less clear as to whether or not the referenced items form part of the formal requirements definition and associated traceability path. Please include evidence to demonstrate that the functionality described in the "TXS operation principles" and

[39] ONR note: the tools ERBUS, SIVAT, RT-SIM, CASSIS, Labview and Tec4Function are not referenced in the document, but have been provided as comparison examples by the TSC.

Annex 16

"Concepts" is traceable through to its implementation and V& V in the compliance analysis.

d) Clause 6.1.2.1 (c) indicates that TXS user manuals are part of the evidence, but does not identify them explicitly. Please include explicit references to manuals, or an indication of where they are identified (e.g. in the Quality Plan) in the compliance analysis. This information is necessary so that confidence can be gained that relevant documentation on how the platform is used is available.

e) Clause 6.1.2.1 (c) addresses unused functions. The analysis claims that "*Demonstration that these functions cannot jeopardise the required functions is performed through platform qualification and system qualification (test bay)*."

This implies that non-interference by unused functions is demonstrated just by test. It does not seem practical to demonstrate non-interference solely by test. Please include further information in the compliance analysis to describe what other measures (e.g. analyses) are taken to demonstrate that unused functions have no effect on the operation of the system.

f) Clause 6.1.2.4 (b) is concerned with the containment of failure. However, the analysis just repeats the requirement, rather than explaining how the requirement is satisfied. Please include evidence in the compliance analysis to demonstrate that compliance is achieved.

g) The analysis for clause 6.1.3.1.1 (b) states: "*System Integration and Validation are performed in simulated environment and on hardware target*."

The TSC understands that only coverage testing is performed on the simulator, and functional testing is performed on the target hardware, not the simulator. The analysis should confirm that the requirements of the clause are satisfied.

h) The analyses of Clause 6.1.3.1.2 (a) and (c) state that the recommendation is addressed in the Plant Probabilistic Safety Assessment. Therefore, please produce evidence in the safety case to confirm that this clause is satisfied.

i) It is noted that for the analysis of the clauses listed below, compliance is not demonstrated because responsibility for the requirement rests with the licensee (referred to as "plant owner" in the compliance analysis):

- 6.1.7 (System Design Modification) (c) and (d)
- 6.2.7 (System Maintenance Plan) (c) and (d)
- 6.3.6.1 (System modification documentation)
- 6.4.3 (Maintaining qualification)

Compliance with these clauses should be demonstrated by the licensee.

j) No analysis has been provided for clause 6.2.1.1 (b). Please include evidence to confirm that this clause is satisfied in the compliance analysis.

k) Clause 6.2.1.2 (b) requires that "the *configuration control shall provide the facilities required to initiate a design freeze. Procedures and authority required for any further modification following a design freeze shall be defined*."' However, the analysis only addresses roles and responsibilities, and not the procedures and facilities to initiate a design freeze. Please produce information in the compliance analysis that confirms that there are adequate facilities and procedures to manage design freezes.

l) Clause 6.2.7 (System maintenance plan) (d) requires that: "*the new calibration is within defined limits (when such limits are enforced by the system, no formal constraint need be placed upon the maintenance staff*".

Annex 16

The analysis states "*The system provides a mean to implement the new calibration in the system using the service unit. However, it is assumed that the new parameters values are defined by physicist engineers using specific tools that are not part of the system. These tools ensure that the new parameter values are within the defined limits. They issue a certified parameter file that can then be implemented in the system using the System Service Tool of the Service Unit*".

The analysis therefore includes an assumption. Please include evidence to support the validity of this assumption in the compliance analysis, and produce a justification of the arrangements including for the tools.

m) Clause 6.3.1 requires that requirements are traceable and consistent with the requirements for the system. Section 5 of the Quality Plan describes how traceability is managed from the System Requirements Specification through design to implementation and test. It is also stated that traceability is verified as part of the verification of individual documents.

However, it is noted that no traceability data is established from the System Requirements Specification to its input documents (e.g. TELEPERM XS documentation, Plans for Overall I&C, Requirements for Overall I&C, Overall I&C Architecture Description). Please include evidence in the compliance analysis to demonstrate that there is complete traceability between the System Requirements Specification and its input documents.

n) Appendix A of the V&V Plan (PELV-F DC 28) lists the inputs against which the System Requirements Specification is verified. However, it only includes a subset of those listed in the QP, for instance it does not include Allocation of I&C Functions, Design Constraints for I&C systems. Please include evidence in the compliance analysis to confirm that the System Requirements Specification is verified against all of its inputs.

o) The analysis for Clause 6.4.1 (Functional and environmental qualification) states that a qualification plan is produced, but the analysis does not confirm that qualification reports are produced. Please include evidence in the compliance analysis to confirm that qualification reports are produced.

p) Clause 6.4.2 (a) includes requirements for additional qualification of interconnected systems. The response states "*Tests of interconnection between I&C systems are related to the test of the overall I&C and are thus not supposed to be performed at the level of the individual systems. However, this may happen. In that case, such tests are introduced in the Master Test Plan and detailed in the Level Test Specification*". Additionally, the response to clause 6.4.2 (b) states that the requirements for this clause are out of the scope.

There is a lack of information on how the additional tests are identified. Please produce evidence to confirm that adequate qualification of interconnected systems is performed, and include it in the compliance analysis.

q) It is noted that there are numerous other references to the Quality Plan, V&V Plan and System Configuration Management Plan, but these refer just to the documents, not to specific sections.

The compliance evidence should, where possible, reference specific sections within documents.

GICI06.A2.TO2.08 – The following points regarding compliance with IEC 60 880:2006 have resulted from the review of PEL-F DC 9, Revision A, and should be addressed so that adequate compliance with the standard has been demonstrated:

Annex 16

a) Section 2.1 describes how the compliance analysis is effectively a plan of how the requirements will be addressed, and the final evidence will be in design documents etc. The final information should contain appropriate evidence to demonstrate that the relevant clauses have been satisfied.

b) Section 2.3 identifies three open points which should be addressed in the compliance analysis so that compliance is demonstrated. The affected clauses are:

- Open Point 1: Clause 5.7.3 – "User access QDS (PSOT)";
- Open Point 2: Clause 11.2.1 – "The *availability of a representative platform to perform validation test when the system will be under operation remain to be discussed (same principle as FA3 or not)";*
- Open Point 3: Clause 11.2.7 – "*Documentation of the plan related to on-site modifications remains to be defined (in particular the responsibility shall be clarified)".*

c) The analysis for a number of clauses justifies compliance by identifying functional aspects of the system, and this is supported by references to:

- requirements specifications (e.g. "System Specifications", "I&C Functions Specifications); and
- generic documents (e.g. "TXS operation principles" and "Concepts") (e.g. 5.7.2, 6.1, 6.2, 6.3, 7.1).

With the former, confidence is gained that the functionality is correctly implemented as a result of V&V activities, and the associated traceability information. With the latter, the situation is less clear as to whether or not the referenced items form part of the formal requirements definition and associated traceability path. Please include evidence in the compliance analysis to demonstrate that the functionality described in the "TXS operation principles" and "Concepts" is traceable through to its implementation and V&V.

d) Clause 5.7.2.7 requires that '*'The design documentation shall identify and describe the functions critical for security and the security features implemented into the software.".* The references just include the System Security Plan, and should include the corresponding document which specifies the requirements. Please include evidence in the compliance analysis to demonstrate that security features are captured as formal requirements.

e) Clause 5.7.4.2 addresses provisions against hidden functions. The analysis claims that this is addressed through V&V activities. Non-interference by unused functions cannot be demonstrated just through test. Please include further information in the compliance analysis to describe what other measures (e.g. analyses) are taken to demonstrate non-interference from hidden functions.

f) The analysis of 6.1.1 identifies the System Requirements Specification (SRS) [D-01.1] as the source of software requirements. The analyses of clauses 6.1.2 and 6.1.3 identify the following documents that are derived from the SRS:

- System Specification [D-02.1];
- Concepts [D-02.2];
- System Functional Design Description [D-02.3];
- I&C functions specification [D-21.1].

It is necessary to show two-way traceability between the SRS and System Specification, Concepts, System Functional Design Description I&C functions specification.

Annex 16

Section 5 of the Quality Plan addresses traceability and states: '*Every requirement which is considered in the System Specification (step S-02) is traced from the System Requirements Specification to the System Specification Documentation (the System Specification [D-02.1] and the Concepts [D-02.2])*'.

However, it is not clear how traceability between the SRS and all the documents that constitute the System Specification is demonstrated.

The analysis should describe how traceability between all systems and software requirements is confirmed.

g) Clause 7.1.4.1 requires that '*Where pre-developed software is to be used, the capabilities of the software shall be evaluated and assessed (see 15.3) to ensure that it is suitable for the intended role*.'. The analysis only refers to the TELEPERM XS 60880 compliance evidence. However, the System Quality Plan PEL-F DC 7 rev A identifies further analyses in Step S-06 to justify the design of the system with regards to its requirements, for example, the "*Suitability Analysis*" (output [D-06.3]). Please include evidence in the compliance analysis for all analyses that provide justifications of the suitability of the TXS platform software that is used by the Protection System.

Also, any application software taken from other projects (e.g. Flamanville 3 (FA3)) should be confirmed by analysis to be suitable.

h) Clause 9.1.1 requires the preparation of a system integration plan and subsequent clauses state requirements on its content. However, the majority of the documents referenced are the outputs from V&V in support of the demonstration that adequate integration has been performed. It is therefore not clear which document will identify the sub-systems and components that are to be integrated to form the system, and what plans will be created to describe how these items will be integrated.

The compliance analysis should describe how the requirements for a system integration plan are satisfied.

i) Clause 9.3.2 requires that '*The test cases selected for system verification shall exercise all module interfaces as well as the basic operation of the modules themselves*.'.

The analysis states "*It is checked that all system inputs have been stimulated, that all outputs have been activated and the extent to which the system's internal operation has been exercised is assessed*.". This implies that the "check" just checks what has been tested rather than confirms that the internal operation has been adequately exercised. Please clarify in the compliance analysis how the internal operation of modules is fully tested.

j) Clause 10.3 requires that tests are included for all functions that affect safety. According to the V&V Plan (PELV-F DC 28), traceability from the Requirement Specifications ([D-01.4] and [D-02.1]) to the test specifications is performed through the Requirement Traceability Matrix. However, functionality is also defined in:

- Concepts [D-02.2];
- System Functional Diagrams [D-02.3]; and
- System Functional Design Description [D-02.4].

Please include evidence in the compliance analysis to demonstrate that the functionality identified in these documents has been correctly implemented.

k) The analysis of clause 10.3.4 indicates that system validation is confined to tests, with no supporting activities (e.g. the analyses defined in PEL-F DC 7 rev A for Step S-06). The compliance analysis should include all system validation activities.

Annex 16

l) Clause 11.2.1 considers the procedure for executing a software modification. The response states that "*a representative platform will be used to test the modifications and ensure the validity of the modifications*.". Please confirm in the compliance analysis that the "*representative platform*" consists of the target hardware, and it is the final object code that is tested.

m) It is noted that for the analysis of the clauses listed below, compliance is not demonstrated because responsibility for the requirement rests with the licensee (referred to as "plant owner" in the compliance analysis):

- 11.3.1 – 11.3.3: Software modification after delivery; and
- 12.4.1, 12.4.2.1, 12.4.3: Training programme/plan/system.

Compliance with these clauses should be demonstrated by the licensee.

n) Clause 14.2 includes a number of requirements related to the selection and use of tools. The analysis states "*The tools used to develop TXS systems are imposed by the TXS platform. Compliance to this requirement is ensured by the TXS platform and is shown thanks to the compliance analysis of the TXS platform to IEC60880.*". The TSC considers that this is valid up to a point, but there are some aspects of the clause that should be addressed by the application.

Please produce evidence in the compliance analysis to confirm that the corresponding observation identified in GDA Step 4 (T16.TO2.17 in Annex 6 of the ONR Step 4 report 'Step 4 Control and Instrumentation Assessment of the EDF and AREVA UK EPR Reactor' , ONR-GDA-AR-11-022 Revision 0) which is cited for further guidance in Assessment Finding AF-UKEPR-CI-027, has been addressed.

o) The analysis for Clauses 14.3.5.4 and 14.3.5.8 state "*The system provides a mean to implement new parameters in the system using the service unit. However, it is assumed that the new process parameters values are defined by physicist engineers using specific tools that are not part of the system.*".

The analyses therefore include assumptions. The licensee should demonstrate that the arrangements, including for the tools, are adequate for implementing new parameters in a Class 1 system.

p) The analysis of clause 15 only addresses Platform software. Any application software taken from other projects (e.g. FA3) should also be confirmed by analysis to be suitable.

q) It is noted that the analysis for clause 5.6.7 refers to a specific section of the System Configuration Management Plan (SCMP). It is noted that there are numerous other references to the SCMP and the Quality Plan and V&V Plan, but these refer just to the document, not to specific sections.

The compliance evidence should, where possible, reference specific sections within documents.

GICI06.A2.TO2.09 – The following points regarding compliance with IEC 60 987:2007 have resulted from the review of PEL-F DC 10, Revision A, and should be addressed so that adequate compliance with the standard has been demonstrated:

a) Section 2.1 describes how the compliance analysis is effectively a plan of how the requirements will be addressed, and the final evidence will be in design documents etc. The final information should contain appropriate evidence to demonstrate that the relevant clauses have been satisfied.

b) The analysis for a number of clauses justifies compliance by identifying functional aspects of the system, and this is supported by references to:

Annex 16

- requirements specifications (e.g. “System Specifications”, “I&C Functions Specifications); and
- other “Concepts” documents (e.g. 5.1.2, 5.2.3 (d), 5.3.7).

With the former, confidence is gained that the functionality is correctly implemented as a result of V&V activities, and the associated traceability information. With the latter, the situation is less clear as to whether or not the referenced items form part of the formal requirements definition and associated traceability path. Please include evidence in the compliance analysis to demonstrate that the functionality described in the “TXS operation principles” and “Concepts” is traceable through to its implementation and V&V.

c) There are several clauses where documents are identified but without specific section references:

- Clauses 4.3.1 (b), 4.3.3 (c)) refer to “*Quality Assurance Plan for the UK NPP*”;
- Clause 5.1.3 identifies documents ‘Guidelines for TELEPERM XS;
- Clause 5.2.3 refers to TXS Modules User Manuals.

The compliance evidence should, where possible, reference specific sections within documents.

d) Clause 5.2.3 c) requires that qualification requirements are specified. However, the analysis states that this is addressed at the platform level. This does not seem to be appropriate as there should be qualification requirements for the Protection System (PS) itself. It is noted that section 3.3 (Step S-01) of the Quality Plan states that qualification requirements are considered, but there is no indication of where they are documented. Please include evidence in the compliance analysis of satisfaction of qualification requirements for the PS.

e) The analysis of Clause 5.3.6 on reliability and availability through life is in terms of the platform. This is incomplete as some maintenance activities will be system specific. Please include further evidence in the compliance analysis to demonstrate that this clause is fully addressed, e.g. reference to Operation and Maintenance Manual D-05.1.

f) The analysis for Clause 7.3.1 (c) (Verification) refers to “*Guide for Verification of TXS application software items [NLE-F DM 10022]*”. Please clarify in the compliance analysis why a software document is used to demonstrate compliance of hardware related requirements.

g) Clause 7.4 (c) includes a requirement regarding calibration of test tools. The analysis is in terms of the “Suitability Analysis” which presumably addresses the suitability of tools in a general sense, and it is expected that test procedures would address calibration of specific instances of tools. Please confirm in the compliance analysis that calibration of tools is addressed as part of the test process.

h) The analysis of clause 7.5 identifies documents which are not listed in the references column. The list of references should be complete.

i) Clause 8 (Qualification) requires compliance with IEC 60780. The analysis states “*At system level, the qualification process will be presented through the System Qualification Plan*”. The System Qualification Plan has not been provided during the GDA phase. Please include evidence in the compliance analysis to confirm that the requirements of IEC 60780 have been satisfied.

j) Clause 10.7 addresses testing of protection against electromagnetic interference. The analysis refers only to Platform evidence. There is no indication of tests at a system level (e.g. interconnected components in and across cabinets). Please include

Annex 16

evidence in the compliance analysis to confirm that testing of the PS system has demonstrated adequate protection against electromagnetic interference.

k) It is noted that in the analysis for the following clauses, some aspects of compliance are not demonstrated because responsibility is deemed to rest with the licensee (referred to as "plant owner" in the compliance analysis):

- 11.1: Maintenance requirements; and
- 11.2: Failure data.

Compliance with these clauses should be demonstrated by the licensee.

l) It is noted that there are numerous references to the Quality Plan, V&V Plan and System Configuration Management Plan, but these refer just to the documents, not to specific sections.

The compliance evidence should, where possible, reference specific sections within documents.

GICI06.A2.TO2.11 – The safety case should demonstrate that the Protection System design target reliability[40] (1E-04 pfd) is met for all of its functions for UK EPR. The demonstration is to incorporate, where applicable, the results of the Flamanville 3 investigations into modifications to ensure that the Protection System design target is met for the three FA3 functions: "*RT on low DNBR*", "*MSRT opening on SG pressure > Max 1p*" and "*Manual EBS actuation*" in Section 7 of NEPS-F DC 29 rev G for which the design target is not currently achieved.

GICI06.A2.TO2.12 – The following points regarding compliance with IEC 61513 have resulted from the review of PTLC-G/2010/en/0047, Rev B, and should be addressed so that adequate compliance with the standard can be demonstrated:

a) The system compliance report PEL-F DC 8 identified:

- 4 sub-clauses (6.1.1.1.3, 6.1.1.2.2, 6.1.2.2.3, 6.2.2 c) to be addressed exclusively in the platform compliance evidence:

  However:

  - o 6.1.1.1.3, and 6.2.2 c) are addressed in the platform report as exclusively system related. It is noted that despite this, this report provides narrative in support of compliance for the platform.
  - o 6.1.2.2.3 is identified in this report as being applicable to both system and platform.

- 12 sub-clauses which are applicable to both system and platform.

  However, in this report only three of these (6.1.2.1, 6.1.3.1.3 & 6.4.2) are identified as being applicable to both system and platform.

Please ensure that the system and platform compliance documents are rationalised to present an accurate presentation of how compliance with IEC61513 is achieved.

b) The following points related to requirements specifications have been identified:

i. Section 6.3.1 states: '*TELEPERM XS contributes to this by providing documentation about the characteristics of hard- and software modules and their*

[40] ONR note: Specified as a probability of failure on demand.

Annex 16

generic qualification including independent assessment which eases selection of these components for the use in systems, and for the evaluation of compliance of the components' characteristics with the requirements of the individual system'.

However, the documents which define the software and hardware characteristics are not identified.

Please identify the documents which define the software and hardware characteristics in the compliance analysis and confirm that they are available.

ii. Section 6.1.1 indicates that a System Requirements specification has not been established. However, section 6.3.5 identifies system tests, and in the absence of a system requirements specification it is not clear what the tests are performed against.

Please clarify the basis for system tests in the compliance analysis.

iii. Section 6.1.2 mentions '*requirements specifications*' but does not identify these documents. Please identify the '*requirements specifications*' in the compliance analysis and confirm that they are available.

iv. Section 6.1.2.3 states that the software specification should include the specification of service and system software functions, i.e. that there should be a specification for the platform software. The response refers to '*Operation Principles and Safety Features of the TELEPERM XS System*'. However, the version of that document considered during GDA Step 4 (NGLT/2003/en/0045, revision D) was an informative document, rather than one which specifies the functions. Please identify in the compliance analysis how and where software functions are specified.

c) Section 6.1.2.1 states that the platform contains some pre-existing software and hardware components. Examples of pre-developed hardware components are identified, with a brief explanation of how they have been qualified including a reference to the approach that was adopted. However, the qualification evidence is not identified.

Please identify in the compliance analysis the evidence that demonstrates that pre-developed hardware components have been qualified and confirm that it is available.

d) The responses to parts b) and c) of clause 6.1.2.3 describe how the SPACE editor is used. It is noted that there is no reference to a manual. During the GDA Step 4 review, the TSC became aware of the manual '*Teleperm XS User Manuals – Engineering System SPACE (TXS Core Software 3.4.x)*'.

Please ensure that this manual has been updated for the latest release and is referenced in the compliance analysis.

e) Section 6.2.3 explains that generic system/integration tests were performed in 1996/1997 and tests of changes have been performed for subsequent releases (3.5.3 and 3.5.4) and a reference is included to the supporting evidence. The TSC has no concerns with this approach. However, please confirm in the compliance analysis that tests have been successfully performed for the version to be used on UK EPR.

f) Section 6.3 refers to '*user manuals'* and '*data sheets*'. However, explicit document references are not identified. Please identify in the compliance analysis the document identifiers/reference numbers.

g) The following sections indicate that requirements of the standard are achieved through assessments by ISTec and TÜV but there is no indication of the scope of their assessment, nor the assessment criteria:

Annex 16

- 6.3.3;
- 6.4.1.2.

Please include evidence in the compliance analysis to confirm that the ISTec and TÜV assessments satisfy the intent of the requirement.

h) Section 6.3.4 refers to a testing procedure but does not provided references to test documentation e.g. to specifications and reports. Please identify in the compliance analysis the test evidence resulting from the application of the referenced procedure.

i) Section 6.4.1.2 addresses qualification of pre-existing software. The following points are noted:

i. SL22: presents an argument which should be substantiated, especially on the following points:

- A claim is made that it has very good reliability.
- A claim is made on extensive testing.

No details are provided or referenced that justify the above claim s. Please include an explanation in the compliance analysis of how the a bove claims are substantiated.

ii. STT1:

- Has been 'subject to independent assessment in line with this safety standard' – please include evidence of this assessment in the compliance analysis.
- Has been 'judged as acceptable for safety applications' – please include evidence in the compliance analysis to confirm that it has been judged acceptable for Class 1 systems.

j) It is possible that changes may be made to the equipment between the date of the review and the installation of the equipment. Please identify any updated evidence, or ensure that the referenced evidence is valid, for the version of the Teleperm XS to be used on the UK EPR.

GICI06.A2.TO2.13 – The following points regarding compliance with IEC 60880 have resulted from the review of PTLD-G/2010/en/0383, Revision A and should be addressed so that adequate compliance with the standard can be demonstrated:

a) The platform compliance report provides almost complete coverage of clauses, the main exception being the treatment of normative annex B (clause 7.3.2.1) for which no compliance information is provided.

Please produce evidence of complete coverage of clauses, and ensure that evidence is identified in the compliance analysis to confirm that all clauses have been satisfied.

b) Section 0 (References) explains that many of the referenced documents apply to release 3.5.x, and provides a reference to documents which will provide the corresponding information for release 3.6.x, which is undergoing qualification.

Please ensure that all relevant documents have been established for release 3.6.x.

c) Section 5.1explains how third party assessments (process review, code reviews, and static analysis) have been performed by GRS, ISTec and TÜV but supporting evidence is not referenced.

Please identify the evidence of third party assessments in the compliance analysis.

Annex 16

d) Section 6.1 (Software Requirements) provides references to specifications which define the initial platform requirements. It goes on to explain that the requirements have subsequently been modified and evolved. This is reasonable, and of itself not a concern; however, it is not clear where the current set of requirements are documented. It is noted that although references 72 and 80 seem to represent requirements specifications for the run-time environment and MSI, they are not referenced from 6.1 and this does not appear to be a complete set of specifications, e.g. where are the function blocks specified?

It is also noted that the justification for compliance with clause 8.1.9 suggests that requirements are maintained in test plans, which does not seem to be appropriate.

Please identify the specifications for all software components in the compliance analysis, and ensure that they are available.

e) Section 7.4 states that a complete list of components of the platform is maintained in the product structure plan. However, the design documentation is not identified. Some design documents seem to be identified in the reference list e.g. 74: '*TXS Development Document Function Block*'; however, it is not clear if all the design documentation is identified, or if there is a master list from which it can be identified.

Please identify the design documentation for all software components in the compliance analysis, and ensure that it is available.

It is also noted that the identifier/reference number of the 'product structure plan' is not documented. Please include the identifier/reference number for this document in the compliance analysis.

f) It is possible that changes may be made to the equipment between the date of the review and the installation of the equipment. Please identify any updated evidence, or ensure that the referenced evidence is valid, for the version of the Teleperm XS to be used on the UK EPR.

GICI06.A2.TO2.14 – The following observations that arose from the review of ECECC111963 revision C should be addressed:

a) Please ensure that the scope of coverage of diversity addressed in the outputs of action A1 of GI-UKEPR-CI-06, combined with the scope of coverage addressed in ECECC111963 revision C, provides full coverage of all independence and Common Cause Failure challenges that relate to the three C&I protection systems PS, SAS and NCSS, and that this is documented, e.g. in the safety case. Please address any additional challenges to independence that are found not to be already covered, and demonstrate how adequate independence is achieved in these cases, e.g. in the safety case.

b) The safety case should record the results of the further independence-related analyses to be carried out during the Nuclear Site Licensing phase, that are listed in Section 9.2 of ECECC111963 revision C (summarised as follows):

- maintenance and repair arrangements IEC 62340 clause 9;
- common triggers in the operating conditions IEC 62340 clause 7.1.4;
- suitability of specific electrical isolation devices IEC 60709 clause 5.3.2;
- compliance with IEC 62340 clause 6.2.5 - validation;
- further compliance statements against applicable standards, for example, IEC 62340 clause 7.1.1; and

Annex 16

- clauses of IEC 62340 that are not directly linked to independence, including clauses 7.5, 7.6 and 8.

c) The safety case should also record the results of compliance analysis to be performed for cabling against clauses 6.2 to 6.5 of IEC 60709.

d) Please also ensure that the safety case fully defines the application of any further improvements in independence arrangements for the three protection systems PS, SAS and NCSS that are a consequence of these analyses.

GICI06.A2.TO2.15 – Compliance analysis evidence that demonstrates conformance of SPPA-T2000 version S7 with IEC 60987 and IEC 60780 should be produced during the NSL phase, as committed in Table 18 of PEL-F DC 13 rev A.

GICI06.A2.TO2.16 – Evidence of compliance with IEC60987 is documented in NLTC-G/2008/en/0053, Revision A. It is noted that the document was produced in 2008, and the platform may have changed since then. Please reference the updated evidence, or ensure that the referenced evidence in the compliance analysis is valid, for the version of the Teleperm XS to be used on the UK EPR.

Action A3

GICI06.A3.TO2.07 – The following observations that arose from the review of ECECC111134 revision C should be addressed:

a) In Section C3 "*Static Analysis*" bullet 4, reference is made to the *CodeSonar®* tool from GrammaTech as a suitable tool for verifying concurrency properties for Class 1 computerised multi-tasking systems at 10^{-3} pfd. Please ensure that the demonstration of suitability of this tool for verifying Class 1 concurrent systems is presented in the safety case; the demonstration to show how the tool conforms to the requirements in IEC 60880:2006 clause 14.3 'Requirements for tools.

b) In Section C9 "*Performance Analysis and Testing*", please ensure that the demonstration of adequacy for Class 1 systems includes consideration of analysis of dynamic memory capacity, for example, adequacy of capacity of message buffers when the message loading varies.

GICI06.A3.TO2.08 – The following points arose from the review of ECECC120398 rev B.

a) A functional analysis will be performed to identify key elements within the SPPA-T2000 software, which will then be analysed. The safety case should define and justify the criteria used to select the key software elements, and the approach to the code review of the selected elements, and should also include evidence that the analysis has been successfully performed.

b) The document states that 'C' code could be subjected to 'sample integrity checking'. However, it does not describe what 'sample integrity checking' means. The safety case should describe the approach for integrity checking of the 'C' code, and in particular should:

- describe how the analysis has been performed and justify its adequacy and
- confirm that the analysis has been performed, and issues arising have been addressed.

Annex 16

c) The response states the analysis of assembler code ‘would consist of an ‘eyeball’ review’’, which is assumed to mean a manual review without tool support. However, it does not describe what review criteria are to be applied. The safety case should:

- define and justify the criteria used to review assembler code, and
- demonstrate that the analysis has been performed and issues arising have been addressed.

d) Additional dynamic testing ICBM (using statistical testing principles) is to be performed, The safety case should demonstrate that the tests have been performed and issues arising have been addressed.

e) A representative SAS test platform is to be developed to perform the additional tests of the platform. The safety case should demonstrate that the test platform is sufficiently representative of the target system.

f) The response to TQ-EPR-1605 point g.1 implies that CNEN I&C performs the checks for accurate and correct content of documents, as opposed to quality reviews, as part of their surveillance activities. However, this is not described in ECECC120398 rev B.

The safety case should demonstrate that the checks performed by CNEN I&C include checks for accurate and correct content, or identify who does perform these checks independently of the supplier.

(Note that in the TQ response, point g) is erroneously labelled as f)).

g) Section 8 states that the surveillance level is Level 2, as defined in Section B1.2, which excludes “analysis of the results of the study”. However, it does not make clear who performs the analysis of the results.

The safety case should explain who is responsible for analysing the results of the studies referenced from section 8 of ECECC120398 rev B, and also the studies referenced from section 8 of ECECC111557 rev B.

Action A4

Technical observation GICI06.A6.TO2.08 remains open as a result of the review of NLN-F DC 193 rev C and PELL-F DC 252 rev A, as part of the combined responses to GDA Issue GI-UKEPR-CI-06 actions A4 and A6.

Action A5

GICI06.A5.TO2.03 – The response to TQ-EPR-1532 makes reference to “*functional and safety interlocks*” to prevent the operation of spurious actions that are inappropriate to the current state of the plant. The definition of these interlocks, and the operations they prevent, should be included in the safety case.

GICI06.A5.TO2.04 – The safety case for SPPA-T2000/S7 should be updated to include the justification of failure independence that mitigates the propagation of errors between C&I systems hosted on this platform, based on the S7 technology rather than the S5 technology, as committed in Section 2 of ECECC121458 rev A.

GICI06.A5.TO2.05 – Section 4.3.2.7 of document ECECC121458 rev A identified one type of potential error in communication from PICS to SAS for further analysis and assessment during NSL – the potential transmission of a spurious, but plausible, multi-division grouped command

Annex 16

from the PICS to the SAS, which could lead to erroneous operation of field equipment in all four divisions. Please ensure that the results of this analysis and assessment, and any consequential changes to the design, are recorded in the safety case.

GICI06.A5.TO2.06 – The safety case should demonstrate that the Class 2 RCSL Category B safety-related functions cannot be adversely affected by unintended interference from the Class 3 PAS, PICS, or Plant Bus , through the RCSL bi-directional gateway with the SPPA-T2000 platform.

Action A6

GICI06.A6.TO2.08 – The following observations arose from the review of NLN-F DC 193 rev C and PELL-F DC 252 rev A:

a) Please update NLN-F DC 193 rev C Section 5.4.9.2 phrase “*These buttons are available at anytime during plant operation*” to incorporate the clarification presented in point d) of TQ-EPR-1538 relating to the availability of the SICS manual controls.

b) Please document why the list of applicable standards in NLN-F DC 193 rev C Appendix A excludes IEC 62340, given that Sections 5.2.1 and 5.2.2 claim that the two internal sub-systems of the PS – sub-system A and sub-system B – are independent, and Section 5.2.2.2 provides an outline of the independence argument.

c) Please document why Figure 1 of PELL-F DC 252 rev A shows the inputs to PS from RIC/RPN as “*Class 1, 2*” when in the ensuing Table 1, these inputs are stated as being all Class 1.

d) Please update the PCSR to record the generic rule that the classification of the maintenance and periodic testing equipment, tools and components is required to be one class less (or better) than that of the system to which it applies, and that compensating measures should be developed where this is not reasonably practicable to achieve.[41]

e) Please update NLN-F DC 193 rev C section 6.5.1 Table 2 to record a classification for the PS and PSOT Service Units that conforms to the generic rule (see point d) above).

f) Please update PELL-F DC 252 rev A section 3.1.2 cases (A) and (E) to include the analysis based on the response to point c) of TQ-EPR-1611, relating to how a spurious order that causes a discrepancy in a dual-input signal communication from SAS/PAS to PS/MSI (both inputs set to the ‘1’ state) is detected, and what consequential action is taken to mitigate any challenge to the operation of a PS Category A function.

GICI06.A6.TO2.09 – The following points arose from the review of the PSOT Basis of Safety Case ECECC120489 rev A:

a) The plant probabilistic safety analysis should include the reliability and functionality of the PSOT system (i.e. to demonstrate that UK EPR safety targets are met).

b) SAPs EDR.2 (redundancy) and ESS.18 (isolation) should be added to the list of SAPs that apply to the PSOT, and conformance with these SAPs should be demonstrated in the safety case.

[41] ONR Note: EDF and AREVA have stated and ONR has confirmed that the PCSR has been updated.

Annex 16

c) Justification of adequacy for the configuration of all pre-developed equipment or firmware should:

- include qualification of "*Firmware Checking Tool*";
- address any configuration of pre-existing hardware or firmware not covered by this tool.

d) For any non-pre-developed CECs in the PSOT implementation, the justification of adequacy should demonstrate conformance with IEC 62566.

e) In the demonstration of conformance with SAP EMT.7, the following points should be addressed:

- in-service functional testing should prove the complete system;
- in-service functional testing should prove the safety-related function of each component.

f) The justification of adequacy to be produced for the "*Class G1*" tools that generate source code for Category A applications, and in particular for those tools that make use of a Java Virtual Machine, should demonstrate conformance with clauses 7.2, 14 and Appendix D of IEC 60880.

g) The approach to be adopted for static analysis of the source code of the PSOT application should be fully defined including consideration of:

- reasonable practicability of using a similar approach as is proposed for TXS module RTECONF, based on "reverse-engineering" tool from generated C code back to specification.

h) The Independent Confidence Building demonstration for the dynamic behaviour of the PSOT should address the guidelines for "*Performance analysis and testing*" in Section C9 of ECECC111134 revision C; including consideration of demonstrating that:

i. required response times can be met by design under worst-case conditions (e.g. via deterministic execution);

ii. CPU loading does not exceed a specified threshold when multiple tasks execute on a single processor under worst case conditions;

iii. network capacity is adequate under worst-case network loading;

iv. dynamic memory capacity (e.g. size of message buffers) is adequate under worst-case conditions;

i) The Independent Confidence Building demonstration for the dynamic behaviour of the PSOT should address the guidelines for tool-assisted static analysis of concurrency in Section C3 of ECECC111134 revision C, including consideration of:

- absence of deadlock, livelock and divergence;
- absence of race conditions due to ordering constraints on inputs and/or outputs.

j) Fully define ICBM compensating measures for the absence of Statistical Testing and Source-to-Code Comparison, for example:

- demonstrate conformance with the guidelines document ECECC111134 revision B - "*Tool review - to cover not only the track record of the tools but also some specific validations of the functions used in the development process*";[42]

[42] ONR Note: The underlining has been added by the TSC.

Annex 16

- perform testing using applicable elements of the GCC test suite as described in section 4.2.2.2.2.2 of ECECC120489 rev A).

k) Define all reports produced as a result of ICBM activities, and from all PSOT-related studies, and include these as evidence documents in support of the safety case.

GICI06.A6.TO2.10 – The adequacy of the Class 2 7-segment displays and digital chart recorders used as components of the SICS for displaying or recording Class 1 information sourced from the Protection System should be demonstrated. The demonstration to address the predicted hardware failure rate, as well as a justification of the software reliability. If such adequacy cannot be demonstrated, appropriate Class 1 equipment should be used to replace, or supplement, these devices.

GICI06.A6.TO2.11 – The response to bullet 6 of point a) of TQ-EPR-1563 states that "*It is foreseen to implement one check-back for each Permissive, Reset and Category A manual control [in the PSOT]*". In addition, the PSOT System Requirements Specification ECECC110951 rev A section 3.2.1 states that the PSOT shall include check-backs for Resets and Permissives (Requirement 12) and Category A manual actions (requirement 14). However, these check-backs have not been included in ECECC120711 rev A. Please review the inclusion of check-backs in the PSOT functional scope, taking into account human factors considerations.

GICI06.A6.TO2.12 – The PSOT Requirements Specification ECECC110951 revision A is labelled as a "*Feasibility Study*". If the results of the Feasibility Study (or the proposed Human Factors Engineering program) indicate that it is not feasible for certain requirements to be met by the PSOT implementation, a justification of adequacy, or else the inclusion of compensating measures, should be included in the safety case.

GICI06.A6.TO2.13 – The PSOT Requirements Specification ECECC110951 should define fully the following requirements that were incompletely defined in revision A:

a) Requirement 38 - *Architecture – SFC* – The requirement should cite an IEC standard by which the adequacy of the robustness of the PSOT data communication can be assessed. For example, IEC 61500:2009 "*Data communication in systems performing category A functions*" would be a suitable standard to cite in the requirement for this purpose.

b) Requirement 39 – *Availability* – The target loss rate for an individual PSOT workstation should be defined so as to meet the overall target of 10^{-3} pfy for the continuous use of the PSOT system. In addition, the Mean Time to Repair requirement for a PSOT workstation should be specified.

c) Requirement 41 – *Spurious Commands* – The requirement for the rate of issuance of a spurious command from the PSOT to the PS should be defined, and a justification should be produced that this rate will be achieved.

d) Requirement 46 – *Failure detection; information availability* – The requirement should state that communication between the PSOT and the SAS relating to the Lifesign/Failure status of each PSOT, shall be uni-directional from PSOT to SAS. This interface also should be shown in the figure under Requirement 53 (*Interfaces with other systems*), for example, via the Gateway to the SPPA-T2000 platform that is managed by the Data Interface module of the Protection System.

Annex 16

GICI06.A6.TO2.14 – The following points have arisen from the review of NLS-F DC 10067 rev B "QDS System Quality Assurance Plan".

a) There are many instances where Independent V&V of software is only stated as applicable to Types S and G1 and not Type G2; e.g. section 3.1.2.3.2.4. Please confirm and document that independence requirements are satisfied for all classes of software.

b) IEC 60880:2006 Clause 13 addresses '*Defences against common cause failure due to software*'. Please confirm and document that there are plans to demonstrate conformance with the requirements of IEC 60880:2006 Clause 13.

c) *Please* document how the QDS Hardware Quality Assurance arrangements conform to the requirements of IEC 60987.

GICI06.A6.TO2.15 – The following points have arisen from the review of NFL S DC 186 rev E "QDS System Configuration Management Plan":

a) IEC 60880:2006 (5.6.5) requires that it shall be possible to identify relevant versions of documentation associated with each software entity.

Section 5.3.4 and 5.3.5 of the CMP describe '*Release Report'* and '*Product Information'* but they do not indicate that all documentation is identified. Please document how relevant versions of documentation associated with each software entity are identified.

b) IEC 60880:2006 (5.6.10) requires that it shall be possible to identify all software entities affected by the implementation of a modification.

This may be addressed through '*Modification Requests*' as described in NFLS DC 186, and NLS-F DC 10067 rev A "*QDS Software Quality Assurance Plan*", however, this is not obvious. Please document how all software entities affected by the implementation of a modification can be identified.

c) IEC 60880:2006 (5.6.11) requires that access to all entities placed in CM shall be protected from unauthorised modification, and the security of the software is maintained.

NFLS DC 186, and NLS-F DC 10067 rev A "*QDS Software Quality Assurance Plan*" describe how changes have to be approved by the change control board. Section 5.2 of NFLS DC 186 describes how a '*Request Tracker'* tool is used to manage changes. It is assumed that these steps, plus the use of CM tools, including CVS, PVCS and Documentum provide the adequate protection. Please document how the referenced procedures and tools prevent unauthorised modification, and maintain the security of the software.

d) Clause 6.2.1.2 of IEC 61513:2001 includes requirements for system configuration management. NFLS DC 186 addresses some of these, however, there are some aspects which are not clearly addressed e.g.

- how hardware configurations are identified;
- how links between items in baselines, and the items from which they were developed are recorded;
- the provision of search facilities that allow links and multiple occurrences of items to be easily identified;
- how the status of controlled items and requested changes are tracked.

The requirements listed in section 6.2.1.2 of IEC 61513:2001 should be compared with those described in the document, using a traceability matrix, to demonstrate that the requirements of the standard are satisfied, and this should be documented.

Annex 16

GICI06.A6.TO2.16 – The Safety Case should explicitly record the commitment made in the response to point d) of TQ-EPR-1599, that the categorisation of a Permissive and Reset is the same as that of the protective function with which it is associated.

GICI06.A6.TO2.17[43] – The Safety Case should explain how the operators in the MCR are made aware that the setting of the SICS/PSOT inhibition and the Severe Accident Panel inhibition switches to RSS mode have become effective, i.e. that control from the RSS has become enabled, prior to evacuating the MCR.

GICI06.A6.TO2.18 – The following observations that arose from the review of NFLS DC 119 rev C should be addressed:

a) Appendix A states that compilation option "*–O2"* (which enables maximum optimisation) is to be used to compile the C source code of the QDS. A justification for why the risk of incorrect code generation associated with the use of this option is considered to be acceptable, should be documented in the safety case.

b) Appendix B presents a very high level of enforcement of the rules by manual review, rather than by the compiler or Logiscope tool. A review of additional suitably qualified tools to maximise the automatic enforcement of the rules, recommendations and guidelines should be carried out, and the results documented in the safety case.

c) A description of the manual code review process, and a justification of its adequacy (for example by use of verified checklists) should be documented in the safety case.

Action A7

No observations relating to GDA Issue GI-UKEPR-CI-06 action A7 remain open.

Action A8

GICI06.A8.TO2.04 – With regard to the demonstration that end-to-end response time requirements for UK EPR C&I functions that are hosted on SPPA-T2000 are achievable by design, the following observations are raised:

a) the results of the FA3 C&I Performance Action Plan for the SPPA-T2000/S5 platform should be reviewed in the context of the UK EPR implementation;

b) any identified design changes to FA3 C&I that are consequent on these results should be fully analysed in the context of the UK EPR implementation, and integrated into the UK EPR C&I design where appropriate;

c) a full justification should be included in the safety case that end-to-end response time requirements for C&I functions on the SPPA-T2000/S7 platform are achievable under worst case (avalanche) conditions. The justification should include the scenario of coincidence of worst-case system-generated event avalanches with worst-case transient-generated event avalanches;

d) evidence that is applicable to the UK EPR design should be included in the safety case to support the statement in Section 5.1.5 of ECECC111368 rev B that "*Processing*

[43] ONR Note: EDF and AREVA have clarified that RSS operation is selected on arrival in the RSS.

Annex 16

involving communication between APs has been shown by calculation to significantly increase maximum response times; however <u>such processing is avoided for any sensitive / important functions</u>".

GICI06.A8.TO2.06 – The following observations arose from the review of QU017 rev 0.2 "*Predictability Model of SPPA-T2000/S7"* and Section 2.2.2 "*Performance comparison*" in PEL-F DC 13 rev A "*Basis of Safety Case of SPPA-T2000/S7*":

a) The timing figures quoted in Table 11 of Section 2.2.2.5 in PEL-F DC 13 rev A for the S7 platform equate to those for "*hypothesis case A*" in QU017 rev 0.2, and make no reference to "*hypothesis case B*" values. A demonstration should be included in the safety case that this selection of hypothesis case A times for Max T_{CPU} and Max T_{CPU_TC} for UK EPR is both achievable and adequate.

b) The S7 timing for "*hypothesis case B*" in QU017 rev 0.2 is worse than that of the S5 timing for the free-cycle time frame $T_{FREE\text{-}Cycle}$ (1617ms compared to 1367ms). Should the values of Max T_{CPU} and Max T_{CPU_TC} for UK EPR need to be set to the hypothesis case B values, then a full analysis of the impact of the increase in ($T_{FREE\text{-}Cycle}$) should be carried out and documented in the safety case.

c) The S7 timing is worse than that of the S5 timing for the protection time frame ($T_{PROTECTION}$). Section 2.2.2.5 of PEL-F DC 13 rev A states that this increased time has "*no impact on safety*" – a justification for this claim should be included in the safety case.

d) If "*protection frames*" (as defined in Section 2.2.2.1 of PEL-F DC 13 rev A) are to be used in the UK EPR implementation, a full analysis of the impact of the increase in the protection time frame ($T_{PROTECTION}$) for version S7, in comparison to version S5, should be carried out and documented in the safety case.

Action A9

GICI06.A9.TO2.14 – The following observation arose from the re view of PEPS-F DC 90 re v B "*Safety Principles Applied to the UK EPR I&C Architecture in terms of the Requirements for Diversity and Independence"*:

1. The phrase "*or in case of high risk reduction claim to meet BSO*" has been added for requirements RS10020-D, RS10040-D and RS10050-D, as in the response to point q of TQ-EPR-1495. Please clarify in the document why this phrase does not also apply to requirement RS10060-DD.

GICI06.A9.TO2.16 – The following points arose fro m the revie w of docu ment ECECC120443 rev B "*Diversity criteria definition for Priority Actuation Control (PAC) module*":

a) A justification should be included in the safety case for the choice of 10^{-5} pfd as the Common Cause Failure limit for two or more redundant PACS modules, as stated in Section 4.1 of ECECC120443 rev B.

b) A justification should be included in the safety case relating to the impact on the reliability claim of 10^{-9} pfd for a "*PACS A*" and "*PACS B*" diverse group of modules (in a 2 PACS A plus 2 PACS B arrangement with 2oo4 voting) when one division is in maintenance, and its corresponding PACS module is unavailable as a result of common mode failure, and why this situation is acceptable.

Annex 16

GICI06.A9.TO2.17 – The following observation raised as part of the review of ECECC120414 rev A should be addressed:

The C&I requirements should be reviewed to ens ure that all of the SAPs and their related guidance paragraphs that are identified in ECECC120414 revision A as being applicable to C&I, have been fully addressed. For example:

a) SAP ESS.8 applies to <u>safety systems</u>, but requirements RS00050-SC point 5 and RS0090-SC that are cited as providing conformance with this SAP apply only to <u>Class 1</u> systems, which excludes the SAS and NCSS. The explicit use of "Class 1" systems in C&I requirements should be reviewed in the context of all SAPs that apply to "safety systems";

b) guidance paragraph 192 states that it should be possible to carry out these [maintenance and inspection] tests <u>without any loss of safety function</u>, whereas requirement RS00170-SRIS that is cited as providing conformance with SAP EMT.7 states that "*the subsystem shall be set to a state preferable from the plant safety point of view*";

c) guidance paragraph 146 provides an <u>order of preference</u> for the means by which a [Category A] safety function is achieved (passive measures, automatic functions, manual functions etc), whereas requirement RS00050-SC point 5 states that "*Automatic actuation of Class 1 functions shall be considered in accordance with the autonomy objectives (period of grace) of the plant*".

GICI06.A9.TO2.18 – The following observations arose from the review of ECEF091489 rev E - UK EPR GDA - Classification of I&C safety features:

1. Tables 1, 2a, 2b, 3a, 3b, 3c, 4 and 5 should be updated with the results of all reviews and analyses of categorisation, minimum classification, and system allocation that are cited in ECEF091489 rev E as to be carried out in NSL, for example:

   a) Category A safety features allocated to the SAS in the first line of protection (Table 2a) - DCL-Fs-01, DEL-Fs-01, DEL-Fs-02, DVD-Fs-01, DVL-Fs-01, DVP-Fs-02, DVP-Fs-03, DWK-Fs-08, DWK-Fs-12, and EDE-Fs-04 - should be reviewed in respect of their minimum system classification and allocation, as per Table 2a Notes (b) through (g);

   b) safety features RIS-Fs-J and RIS-Fs-Q should be reviewed in respect of system allocation and classification, as per Table 2b Notes (e) and (f);

   c) for all safety features in Tables 3a and 3b, the Safety Category column should be completed by analysis, as per Table 3a Note (x) and Table 3b Note (a);

   d) safety features ARE-Fs-A, PTR-Fs-03, PTR-Fs-14, RBS-Fs-A, RCP-Fs-F, RCV-Fs-N and RCV-Fs-O in Table 3a should be reviewed for classification and system allocation, as per Table 3a Note (a);

   e) safety features EVU-Fs-05, RCP-Fs-F and SRU-Fs-01 in Table 3a should be reviewed in respect of whether they are also needed in RRC-B (severe accident) conditions, in which case they would also be executed by the RRC-B SAS or SA I&C Class 3 system, as per Table 3a Note (e);

   f) safety features DWL-Fs-04 and EVU-Fs-06 in Table 3b should be reviewed for system allocation, as per Table 3b Note (b);

   g) all safety features in Table 3c should be reviewed for categorisation, minimum classification, and allocation, as per Table 3c Note (a);

Annex 16

h) safety features CFI-Fs-01, CRF-Fs-01, RCP-Fs-L and SEN-Fs-01 in Table 4 should be reviewed in respect of their categorisation, minimum classification, and allocation, as per Table 4 Note (a);

i) safety features DWL-Fs-01, DWL-Fs-15, EBA-Fs-09, EBA-Fs-10, EDE-Fs-05 and IAG-Fs-01 in the Severe Accident line (Table 5) should be reviewed as to whether they are allocated to the RRC-B SAS system, or to the SAS system.

2. Evidence should be produced and documented in the safety case to support the claim that the classification of the sensors and conditioning modules used to implement each of the safety features in ECEF091489 rev E is adequate with respect to the categorisation of each safety feature, including the case where a sensor or conditioning module is shared in the implementation of multiple safety features.

GICI06.A9.TO2.19 – The following observations have been raised as a result of the review of the further analysis of diversity requirements and implementation for sensors and sensor conditioning in PELA-F DC 3 rev C and PEPR-F DC 83 rev C:

a) A comprehensive sensor and conditioning diversity implementation plan should be produced that identifies the main activities to be carried out during Nuclear Site Licensing, including:

- completion of the CCF analysis of sensor and conditioning modules in PEPR-F DC 83 rev C and PELA-F DC 3 rev C, to address, for example:
    i. the diversity cases associated with conditioning modules that have not been addressed during GDA, such as the conditioning modules involved in the mitigation of faults in support functions, and faults associated with the spent fuel pool, as stated in Section 4.2.3 of PELA-F DC 3 rev C;
    ii. the adequacy of the use of “*type A*” and “*type B*” SNV1 conditioning modules, from a probabilistic point of view, in the Reactor Trip function for “*ARE [MFWS] malfunction causing an increase in feed water flow*”, as presented in Table 4 of PEPR-F DC 83 rev C, given the use of a “*type A*” SNV1 conditioning module for SG3 and SG4 SG level (Narrow Range) sensors, PRD sensors, and SG1 and SG2 SG level (Wide Range) sensors.
- completion of the analysis in Appendix B of PELA-F DC 3 rev C of all cases for which the signal diversity requirement for different parameters to be sensed by different physical effects, is not met by the reference implementation, to consider also the feasibility of using diverse sensing components to meet these requirements;
- application of the results of the functional analysis of sensor and conditioning modules CCF (previous bullet point) to determine any additional equipment diversity requirements to be met for UK EPR;
- determination of the diversity requirements to be applied to the conditioning modules associated with specific sensor pairs, as marked by “XC” in Table 6 of PELA-F DC 3 rev C;
- confirmation and demonstration that the Separation criteria not addressed during GDA are satisfied;
- confirmation of the feasibility of achieving the required equipment diversity, and identification of alternative strategies if this proves not to be reasonably practicable;
- selection of appropriate sensors and conditioning modules;

Annex 16

- demonstration of meeting the equipment diversity requirements for the selected components.

b) The diversity analysis should demonstrate that it has addressed the impact of maintenance and common mode failure on all proposed solutions.

c) Section 4.2.28.1 of PEPR-F DC 83 rev C refers to "*F1A*" and "*F1B*" classification. These terms should be altered to "*Class 1*" and "*Class 2*" respectively for UK EPR.

d) The timescale for delivery of the justification of diversity of sensors and conditioning modules should be specified, and should be consistent with the commitment in letter EPR01412N – "*prior to programme milestone 'First Safety Concrete'*".

GICI06.A9.TO2.20 – The following point arose from the review of document ECESN120472 rev A "*EPR UK - Diversity implementation plan for PAC Modules*":

a) A comprehensive PAC module diversity implementation plan should be produced that identifies the main activities to be carried out during Nuclear Site Licensing, including:

   - completion of the PAC module diversity analysis (e.g. diversity cases associated with support functions as stated at the end of Section 7.3);
   - application of the results of the final PAC module diversity analysis (previous bullet point) to determine any additional equipment diversity requirements to be met for UK EPR;
   - confirmation and demonstration that the Separation criteria that were added in ECECC120443 rev B, compared to rev A, are satisfied;
   - confirmation of the feasibility of achieving the required equipment diversity, and identification of alternative strategies if this proves not to be reasonably practicable;
   - selection of appropriate PAC modules;
   - demonstration of meeting the equipment diversity requirements for the selected modules.

b) With regard to the analysis of the effect of maintenance activity on PAC module diversity claims, as presented in letter EPR01413N, the following observations should be addressed:

   - The analysis presented in letter EPR01413N should be captured in an update to ECESN120472 rev A, or other appropriate submission in support of the safety case.
   - In the case of periodic testing of Protection System functions, which includes switching PAC relay output into "Test" mode to avoid actuation, an explanation should be documented as to how the relay is reset to its normal position to allow use by SAS and NCSS, should the Protection System fail during its maintenance activity.
   - In the case of periodic testing of the Safety Automation System functions that affect shared PAC modules, if the reliability assessments result in a need to provide these tests more frequently than only under outage conditions, please define the measures to ensure continued availability of the PAC module during this periodic testing for use in actuation by, for example, the PS or the NCSS.

c) The timescale for delivery of the justification of diversity of PACS modules should be specified, and should be consistent with the commitment in letter EPR01412N – "*prior to programme milestone 'First Safety Concrete'*".

Annex 16

GICI06.A9.TO2.21 – The following points arose from the review of document ECECC121662 rev A "*Basis of Substantiation for the Reliability Claims for the PACS Modules*":

a) The safety case should present evidence relevant to UK EPR to substantiate the reliability claims for the actual PACS modules used in the UK EPR implementation, as outlined in Section 5 of ECECC121662 rev A, including:

- demonstration of compliance with the standards listed in Section 6.1;
- demonstration of hardware qualification against the requirements of RCC-E section B and IEC 60780;
- assessment of Common Cause Failure and evidence to support substantiation of diversity claims, as outlined in Sections 7.3 and 7.4;
- evidence to support the demonstration of meeting the claims of probability of failure on demand, as outlined in Sections 8.1.5 and 8.2.2, both for single PACS modules and for combinations of PACS modules.

b) Section 4 mentions a 'further variation' beyond the type 1SM and type 2SM PACS modules without explanation. ECECC121662 should include more detailed information on what is meant by this 'further variation' and should demonstrate the adequacy of this type of module if it is used on UK EPR.

GICI06.A9.TO2.22 – The following observations that were raised from the review of PEPS-F DC 90 rev C should be addressed:

a) PEPS-F DC 90 rev C states that maintenance is "...*not superimposed on the resulting sequences*." for the diverse line of protection, in the sub-section titled "*Interpretation*" for requirement RS100100-DD in Section 4.1.3.2. A comprehensive demonstration that common mode failure of equipment during plant maintenance does not prevent any safety system (including sensors and actuators) from performing its safety role should be included in the safety case.

b) The list of applicable standards in Section 2 "*Applicable Documentation*" of PEPS-F DC 90 rev C should include NUREG/CR-6303:1994, "*Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*", to be consistent with the use of this standard in the derivation of diversity criteria, as stated in Section 2 of *Diversity Criteria between Protection System and Safety Automation System* – PTL-F DC 3 rev A.

GICI06.A9.TO2.23 – The following observations that arose from the review of ECECC100831 rev B should be addressed:

a) Section 3.4.9.3 states that the SPPA-T2000 component of the PACS implements priority management between SAS, PAS and RRC-B SAS orders, plus Class 2 and 3 actuator position surveillance. However, Figure 2 in Section 3.3 shows connections from this component to the PS, NCSS and SA I&C systems. Please review the accuracy of these connections as shown in Figure 2, and update the diagram as necessary.

b) Section 3.4.5.1 states that some elements of the functions listed for the PAS will be re-categorised as Category B functions, and will instead be implemented by a Class 2 system. This re-allocation of Category B functions is stated as "*not available in the frame of GDA*". This re-allocation should be performed, and the results recorded in an appropriate safety case submission, e.g. ECEF091489.

Annex 16

c) Section 6.6.3 states that "*These resources [on the Severe Accident Panel] … have complete independence and autonomy from all other instrumentation and control systems*" but does not provide a cross-reference to substantiate this claim. The safety case should present the argument and evidence to support this claim.

d) Section 3.2 states that the classification scheme is as defined in NEPS-F DC 557 revision C. However, the term "*F1B functions*" is still used in Section 5.1.5.1. All use of function categories and system classifications should use the terminology defined in NEPS-F DC 557 revision C.

GICI06.A9.TO2.24 – The following observation that arose from the review of P EPS-F DC 148 rev A should be addressed:

The safety case should document the evidence from the detailed design stage that demonstrates that the c onfiguration of sensor allocation bas ed on SAS and NCSS sharing sensors/conditioning modules for a given initiating event, whilst PS uses different sensors/conditioning modules, meets UK safety requ irements from a probabilistic point of view, for <u>all</u> initiating events, as committed in Section 4 of PEPS-F DC 148 rev A.

The demonstration to consider the classification of the se nsors, and of th e conditioning modules, in the context of the combi ned reliability claim when they are shared by SAS and NCSS – for example, a Class 1 sensor would be needed to meet a combined reliability claim of 10^{-5} pfd, when shared by SAS (at 10^{-2} pfd) and NCSS (at 10^{-3} pfd).

GICI06.A9.TO2.25 – The following point that arose from the review of document PELA-F DC 7 revision B should be addressed.

The safety case should present evidence relevant to UK EPR to subs tantiate the reliability claims for th e actual sensors and conditioning modules used in the UK EPR impleme ntation, both individually and whe n grouped into function blocks, as outlined in Sectio n 4.2 of PELA-F DC 7 revision B.

Annex 17

TSC Summary – GDA Issue **GI-UKEPR-CC-01 ACTION 6 -** Categorisation and Classification of Systems, Structures and Components[44]

Note this information has been imported from a TSC report (Ref. 229) and the formatting of the TSC report has been retained.

[44] Note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 17

Annex: TSC task summary - GDA Issue **GI-UKEPR-CC-01 ACTION 6** – Categorisation and Classification of Systems, Structures and Components

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of submissions presented by EDF and AREVA to address resolution of GDA Issue GI-UKEPR-CC-01 Action A6, " *Categorisation of C&I systems to be consistent with current good practice as provided by IEC61226:2009 'Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Classification'*". The following text is an extract from the TSC report Ref. 229.

The aim of this review was to consider the submissions in line with the Action as identified in the Resolution Plan and to advise HSE/ONR on their adequacy, or otherwise, to support HSE/ONR decisions on the close out of the Action, and hence the GDA Issue. GI-UKEPR-CC-01 Action A6 is supported by submission of an update to NEPS-F DC 557 Rev. C, as described in the Resolution Plan, and supporting documents submitted under GI-UKEPR-CI-06 Action A9. From review of each submission, Technical Clarifications and Observations were raised, as required, in order to reach convergence between ONR and EDF and AREVA (i.e. the submissions are adequate for the purpose of closing out the GDA Issue but there may be open observations that should be addressed during Nuclear Site Licensing (NSL)).

The documents submitted to define the classification and categorisation approach under this, and related, GDA Issues are listed below:

a. *NEPS-F DC 557 - "Classification of Structures, Systems, and Components";*

b. *PEPS-F DC 90 - "Safety Design rules for GDA UK I&C Architecture"; and*

c. *ECEF091489* – "UK EPR Generic Design Assessment – Classification of I&C Safety Features"*;*

Of these, b. and c. were submitted under GDA Issue GI-UKEPR-CI-06 Action A9; but both relate to this Action and so were reviewed in relation to Categorisation and Classification issues. Points arising from the review of PEPS-F DC 90 under this GDA Issue have been raised via Technical Observations and Clarifications under GDA Issue UKEPR-CI-06 Action A9.

Following the TSC review of EDF and AREVA's response to the Technical Clarifications and Observations and related amendments to submitted documents, any open TSC Observations relating to this GDA Issue Action are captured in the corresponding GDA Issue report (this document) or the GI-UKEPR-CI-06 A9 report and are also highlighted to ONR.

Closed Technical Clarifications and Observations

Two Technical Clarifications raised in support of resolution of GI-UKEPR-CC-01 action A6 were resolved during the GDA Closure phase. Two further technical observations and clarifications identified by this review but raised under GI-UKEPR-CI-06 A9 were resolved. The related topics are summarised below.

a. definitions upon which categorisation and classification is based have been improved and now align with definitions in international standards;

b. the requirements in relation to categorisation and classification have been clarified and meet the requirements of IEC 61226;

Annex 17

c. the process by which classification is carried out has been clarified, so that this is now shown to align with IEC 61226;

d. the probabilistic claim limits for computerised and non-computerised C&I systems described in PEPS-F DC 90 aligns with ONR's TAG 46; and

e. the majority of system classifications align with IEC 61226, demonstrating the efficacy of the categorisation and classification process. A few exceptions have been correctly identified by EDF and AREVA, and will be resolved following completion of the design.

Four Technical Observations that were raised during Step 4 of the GDA process have been closed as a result of the reviews of the documents submitted during the GDA Closure phase.

Open Observations

The observation raised by the reviews of the submissions that relates to the C&I Categorisation and Classification, and that remains open at the end of the GDA Closure phase is summarised below.

a. The reliability claim limits presented in Section 9 of NEPS-F DC 557 should be clearly defined for both non-computerised and computerised systems in line with those defined in PEPS-F DC 90.

Conclusions of the Review

For GDA Issue GI-UKEPR-CC-01 action A6, based on the sampled evidence, there is no evidence to indicate that the Categorisation of C&I systems, consistent with current good practice as provided by IEC61226:2009 'Nuclear Power Plants – Instrumentation and Control Systems Important to Safety - Classification', has not been adequately achieved, and agreed to the level necessary to conclude the GDA Closure review.

The one open observation is not considered to be at a level of significance that would prevent closure of GDA Issue GI-UKEPR-CC-01 action A.6. It is judged appropriate that this open observation be addressed during the Nuclear Site Licensing activity.

Annex 17

GI-UKEPR-CC-01 Action A6 OPEN TECHNICAL OBSERVATIONS

GICC01.A6.TO2.01 – The following observation arose from the review of the Final version of NEPS-F DC 557 revision D:

a. The reliability claims have been included in Section 9 but they do not align with those defined in PEPS-F DC 90 in that:

   i. The ‘≤’ and ‘<’ symbols are the wrong way round; therefore for non-computerised systems the claims should be:

Class 1	$10^{-5} \leq$ pfd $< 10^{-3}$
Class 2	$10^{-3} \leq$ pfd $< 10^{-2}$
Class 3	$10^{-2} \leq$ pfd $< 10^{-1}$

   ii. The claims for computerised systems should be a decade lower as stated in PEPS-F DC 90, i.e.:

   R13 Class 1 I&C system and equipment should be in the range of $10^{-4} \leq$ pfd $< 10^{-2}$.

   R14 Class 2 I&C system and equipment 10^{-2} claim limit on the pfd

   R15 Class 3 I&C system and equipment 10^{-1} claim limit on the pfd’

The reliability claims presented in Section 9 of NEPS-F DC 557 should be clearly defined for both non-computerised and computerised systems in line with those defined in PEPS-F DC 90.

Annex 18

TSC Summary – GDA Issue **GI-UKEPR-CC-02 ACTION 1** – Consolidated Final GDA Submission Including Agreed Design Change For The UK EPR™[45]

Note this information has been imported from a TSC report (Ref. 111) and the formatting of the TSC report has been retained.

[45] Note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 18

Annex: TSC task summary - GDA Issue **GI-UKEPR-CC-02 Action 1** - Consolidated Final GDA Submission Including Agreed Design Change For The UK EPR™

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of submissions presented by EDF and AREVA to address resolution of GDA Issue GI-UKEPR-CC-02, relating to the UK EPR C&I design definition. The following text is an extract from the TSC report Ref. 111.

This report summarises the TSC review of submissions presented by EDF and AREVA to address resolution of C&I aspects of GDA Issue GI-UKEPR-CC-02, Action A.1: '*fully implement its processes to manage the implementation and acceptance of amendments to documentation impacted by design changes agreed for inclusion in GDA, including any other additionally agreed design changes associated with other GDA issues Resolution Plans. This should involve the incorporation of all relevant amendments into the impacted documentation associated with design changes, including the Reference Design Configuration Document UKEPR-I-002, the PCSR and the PCER*.'; this review specifically addresses the submissions related to Action A.1 Task 5.

Under GDA Issue GI-UKEPR-CC-02 Action A.1, Task 5 requires:

Update of Design Reference:

the design reference document (UKEPR-I-002) will be updated:

- *Regular updates to reflect status of design changes (updates every 2 months or as often as necessary).*
- *An update of UKEPR-I-002 shall be produced in April 2012 to include all design changes agreed for inclusion in GDA Design Reference and new document numbers / titles and revisions for the updated SDMs.*
- *The draft final consolidated version of UKEPR-I-002 will be submitted mid-July 2012; the final version by 05/11/2012.*

This task specifically addresses the adequacy of the GDA C&I design definition. ONR undertook the review of design changes and the PCSR. The approach to be taken in relation to Task 5 C&I design definition in the *GDA Closure* phase, as an alternative to updating the Flamanville 3 (FA3) SDMs that provide the design reference as stated in document UKEPR-I-002, was discussed at a Level 4 Meeting held on 19 April 2012. The agreed deliverables against Task 5 for the design definition of the C&I systems were captured in TATS Action GI 11-I&C-3; this action states:

Design definition:

Deliverables to be produced include:

Matrix to show how each of the requirements in IEC 61513 is met for SAS and PS,

A description of the process that is followed for each of the six systems.

The aim of this review was to consider the submissions in line with TATS Action GI 11-I&C-3 to address GI-UKEPR-CC-02 A.1 Task 5 and to advise HSE/ ONR on their adequacy, or otherwise, to support close out of the Actions, and hence the C&I element of the GDA Issue. The submissions provided in support of GI-UKEPR-CC-02 A.1 Task 5 to meet the requirements of TATS Action GI 11-I&C-3 were:

Annex 18

a. *IEC61513 ed. 2001 §6.1.1 - mapping to FA3 PS documentation.*

b. *ECECC121435 rev. A, "UKEPR: SAS IEC 61513 System Requirement Specification (SRS) Equivalence.*

c. *ECECC121609 rev. A, SRS Equivalence Justification Note for PAS and PACS.*

d. *SRS equivalence justification for the non-PS TELEPERM XS based systems in the Appendix to letter EPR01360N.*

These documents were reviewed for their adequacy to define and identify design documentation to provide an equivalence demonstration for a System Requirements Specification aligned with the requirements of IEC 61513:2001 clause 6.1.1.

Following the TSC review of the Requesting Party's response to the Technical Clarifications and Observations and related amendments to submitted documents, any TSC observations are captured in the corresponding TSC GDA Issue report and are also highlighted to ONR.

Closed Technical Clarifications and Observations

One Clarification raised by the reviews of the submissions in support of resolution of GI-UKEPR-CC-02 action A.1 Task 5 was resolved during the GDA Closure phase. The clarification was a request for supply of 'NEPR-F DC 114 P/S functional description'. The response to this request stated that the document requested is not relevant to UK EPR but is for Flamanville 3 (FA3) and identified two documents previously submitted to ONR (NEPCF.10.0263 and NEPR-F DC 551) and an additional document PEPRF.12.1121.

The additional document provided by EDF and AREVA included the information sought on functional specifications to close the clarification.

Open Observations

The observations raised by the reviews of the submissions that relate to the C&I Design Definition, and that remain open at the end of the GDA Closure phase are summarised below.

a. For the Protection System (PS) mapping to IEC 61513 clause 6.1.1 it is noted:

   i. There is no single Systems Requirements Specification for FA3 that would demonstrate the structure and content for a UK EPR SRS. Therefore, the adequacy of the UK EPR SRS should be reviewed during NSL to confirm that it addresses the requirements of IEC61513 clause 6.1.1.

   ii. The PS Detailed Specification (NLE-F DC 38) provides a requirement specification; however, the FA3 requirements reviewed are not individually identified. The UK EPR Quality Plan (PEL-F-DC7) states that all requirements will be individually identified and traced for the UK EPR. A demonstration should be produced that all PS requirements for the UK EPR have been individually identified and traced.

   iii. There are some specific omissions within the documents sampled against the claimed compliance, e.g. Clause 6.1.1.3 'Boundaries and interfaces with other systems and tools' contains the requirement for coverage of "The intended location and physical constraints" that are not currently addressed. For the UK EPR SRS, it should be identified where all IEC61513 clause 6.1.1 requirements are covered.

b. For the Safety Automation Systems (SAS) mapping to IEC 61513 clause 6.1.1 it is noted:

   i. The UK EPR SAS SRS, produced during licensing, should be reviewed to verify that it addresses all the requirements of IEC 61513:2001 clause 6.1.1.

c. For the Reactor Control and Limitation System (RCSL) SRS equivalence justification it is noted:

Annex 18

i. Three potential ‘Gaps’ (as defined in TO GICC02.TO2.03) exist in the identification of supporting evidence against clauses of IEC 61513:2001 clause 6.1.1 and these should be addressed during NSL. For example, Clause 6.1.1.2.2.d. – allows Class 2 systems to be developed by techniques other than those specified in appendix B to IEC 60880; such as those of IEC62138. It should be identified whether the RCSL design techniques are covered by the TXS platform design as is stated as the case for the PS.

ii. A number of documents that were referenced in the PS SRS equivalence justification ‘*Reactor Protection System (PS) - IEC61513 ed. 2001 §6.1.1 - mapping to FA3 PS documentation*’ were not identified as references from the RCSL Detailed Specification, e.g. IT Security Plan, Concept for Failure Handling, Periodic Test Rules etc. It should be confirmed that the equivalent RCSL documents either exist or are covered by the platform level TXS documentation.

iii. The topic of precise definition of interface requirements should be addressed in more detail. An exercise should be conducted to identify and define each interface.

The above observations should also be addressed for the Severe Accident I&C (SA I&C).

Conclusions of the Review

For GDA Issue GI-UKEPR-CC-02 action A.1 Task 5, based on the review of submissions and sampled evidence, in relation to Design Definition there is no evidence to indicate that there is insufficient information to define a SRS for the UK EPR C&I systems and the information provided based on FA3 design documentation is sufficient to conclude the GDA closure review for the deliverables expected under action A1 Task 5.

The three open observations are not considered to be at a level of significance that would prevent closure of GDA Issue GI-UKEPR-CC-02 action A.1 Task 5 in respect of the C&I systems. It is judged appropriate that these open observations be addressed during the Nuclear Site Licensing activity.

Annex 18

GI-UKEPR-CC-02 OPEN TECHNICAL OBSERVATIONS

GICC02.TO2.01 – Although found to be generally acceptable as a mapping to a system requirements specification, the following observations arose from the review of 'IEC61513 ed. 2001 §6.1.1 - mapping to FA3 PS documentation', the mapping document for the PS against the requirements of IEC 61513:2001 clause 6.1.1 System Requirements Specification, provided under letter ND(NII) EPR01238N dated 29th June 2012:

a. There is no single systems requirements specification for FA3. The UK EPR Quality Plan for Teleperm XS (PEL-F-DC7) states that a Systems Requirements Specification will be produced for UK EPR (D01.1) during the site licensing process. The adequacy of this SRS should be reviewed during NSL to confirm that it addresses the requirements of IEC61513 clause 6.1.1.

b. The PS Detailed Specification (NLE-F DC 38) provides a requirement specification; however, the requirements are not individually identified. Whilst, the UK EPR Quality Plan (PEL-F-DC7) states that all requirements will be individually identified and traced for the UK EPR, there is no evidence amongst the FA3 documents sampled, and in particular NLE-F DC 38, that this is the case in terms of the design definition using the referenced documents. A demonstration should be produced that this is carried out for the UK EPR.

c. There are some specific omissions within the documents sampled against the claimed compliance against IEC 61513:2001 clause 6.1.1. It should be identified where the specific requirements listed below are covered:

   - Clause 6.1.1.3 'Boundaries and interfaces with other systems and tools', contains the requirement for coverage of "The intended location and <u>physical constraints</u>".

   - Clause 6.1.1.5 Environmental conditions; all aspects, in particular the full range of parameters and conditions required by the clause, and heat removal conditions.

   - Clause 6.1.1.1.1 (a) (1) The matrix specifically states that the documentation does not define the margins between setpoints and allowable values.

d. There are some specific omissions from the documents sampled against the claimed compliance against IEC 61513:2001 clause 6.1.1, but where the missing information was located in other (unclaimed) documents, or other (unclaimed) sections of the same document, highlighting occurrences of inadequate referencing to supporting information. Appropriate evidence should be identified, and included in the SRS, for the requirements listed below:

   - Clause 6.1.1.1.1 (a) (2). Evidence that performance requirements such as accuracy or response time are explicitly stated.
   - Clause 6.1.1.2.1. Evidence that the design of Class 1 systems includes sufficient redundancy to meet the single-failure criterion for Category A functions during operation and maintenance.
   - Clause 6.1.1.3. Evidence of the physical and functional interfaces of the system with supporting systems and equipment.

GICC02.TO2.02 – The following observation arose from the review of ECECC121435 rev. A, the mapping document for the SAS against the requirements of IEC 61513:2001 clause 6.1.1 System Requirements Specification, provided under letter ND(NII) EPR01 309N dated 10th August 2012:

The SRSs produced during NSL for UK EPR SAS and PAS should be reviewed to verify that they include all of the requirements identified in the documents referenced from

Annex 18

ECECC121435, and that all of the req uirements of IEC 61513:2001 clause 6.1.1 are covered.

GICC02.TO2.03 – The following observations arose from th e review of th e RCSL Detailed Specification, NLP-G/2006/en/1007 against the requirements of IEC 61513:2001 clause 6.1.1:

a. The following potential 'Gaps' were identified that should be addressed during the production of a System Requirements Specification in NSL;

   i. Clause 6.1.1.2.2.d. –allows Class 2 systems to be developed by techniques other than those specified in appendix B to IEC 60880; such as those of IEC62138. It should be identified whether the RCSL design techniques are covered by the TXS platform design as is stated as the case for the PS.

   ii. Clause 6.1.1.2.5.a. – The PS SRS equivalence justification note references the Service Unit specification. The RCSL Detailed Specification refers to the RCSL Service Unit at section 8.3.1 but does not reference a RCSL Service Unit specification. The RCSL Service Unit specification should be identified and confirmed to meet the requirements of IEC 61513:2001.

   iii. Clause 6.1.1.3 3rd bullet - The PS SRS equivalence justification note references 22 dedicated Interface Specification Documents. Although interfaces are seen to be discussed in sections 4 and 5.3 of the RCSL Detailed Specification, and there are references in some instances to the 'Rod Position Instrumentation Specification', 'RCSL – Concept for Signal Annunciation' and 'Excore Instrumentation System Specification', it should be specified what documents 'describe the requirements to design the interfaces' as is the stated purpose for Interface Documents in the Appendix to letter EPR01360N.

b. The following documents were not identified as references from the RCSL Detailed Specification and it should be confirmed that these documents either exist or are covered by the platform level TXS documentation:

   i. IT Security Plan.

   ii. Concept for failure handling.

   iii. Periodic test rules (as opposed to Concept for Periodic Tests that is identified),

   iv. RCSL Service Unit Specification (see above); this may be the same reference as for the PS and SA I&C (NLN-F DC 9).

   v. Operation and Maintenance Manual.

c. The topic of interfaces should be addressed in more detail. An exercise should be conducted to identify and define each interface.

The above observations should also be addressed for the SA I&C.