



UK EPR GDA PROJECT				
UK EPR	Title: Resolution Plan for GI-UKEPR-CI-05			
	RP unique number: GI-UKEPR-CI-05-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 1 of 12
Approved for EDF by: A. PETIT Name/Initials  Date 30/06/2011		Approved for AREVA by: C. WOOLDRIDGE Name/Initials  Date 30/06/2011		

Resolution Plan Revision History

Rev.	Description of update	Date issued
0	Initial issuance	30/06/2011

1.0 GDA ISSUE

GDA Issue Title	Main Assessment Area	Related Assessment Area
Obsolescence of SPPA T2000 Platform	C&I	None

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.
------------------	--

2.0 OVERVIEW OF SCOPE OF WORK

The UK EPR I&C architecture includes systems based upon SPPA T2000. Submitted documentation is based on SPPA T2000 S5. This platform is obsolete and will not be available for UK EPR. The likely replacement platform is the SPPA T2000 S7 platform.

The scope of work is to provide a Basis of Safety Case as described in section 3.1.2.2 that fully addresses the change from the SPPA T2000 (Siemens S5 based) to the proposed replacement platform. This includes a comprehensive impact assessment for the change. A key aspect that will be addressed and justified is the diversity with TELEPERM XS platform.

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI0-5			
	GI unique number: GI-UKEPR-CI-05-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 2 of 12

3.0 GDA ISSUE ACTIONS AND RESOLUTION PLAN DELIVERABLES

3.1 Action GI-UKEPR-CI-05.01

Action I/D	Action Description
GI-UKEPR-CI-05.01	<p>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.</p> <p>A Basis of Safety Case in this context is expected, amongst others, to:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>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.</p> <p>For further guidance see also T15.T01.45 in Annex 5 and T18.TO1.04 in Annex 8 of Step 4 C&I Division 6 Assessment Report, No. 11/022 Revision A (DRAFT).</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>

3.1.1 Deliverables already submitted to ONR/EA in response to GI-UKEPR-CI-05.A1

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI0-5			
	GI unique number: GI-UKEPR-CI-05-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 3 of 12

All documents which have been provided to ONR relate to SPPA T2000 S5. Some are also relevant to SPPA T2000 S7. Task 2 will confirm which documents are relevant to SPPA T2000 S7 and where updates are required.

3.1.2 Planned submissions in response to GI-UKEPR-CI0-5.A1

3.1.2.1 Description of Scope of Work

The SPPA T2000 S7 platform will be introduced into the UK EPR I&C architecture for systems that are based upon SPPA T2000. The change from the SPPA T2000 S5 platform to the SPPA T2000 S7 platform requires justification.

The scope for the resolution plan consists of four steps:

Step 1 [Task 1 and 2] – inform ONR about the change from SPPA T2000 S5 to SPPA T2000 S7.

Step 2 [Task 3 and 4] – Establish the Basis of Safety Case for the change from SPPA T2000 S5 to SPPA T2000 S7. The Basis of Safety case will set out the activities required in order to establish the full safety case for use of SPPA T2000 S7. This includes a comprehensive impact assessment for the change to SPPA T2000 S7. The Safety Case is further described in the section 3.1.2.2. The purpose of the Safety Case is to set out the standards and the applicable safety principles, to explain how they are taken into account in the design and in the qualification programme and to justify that the design and the process of development is consistent with these requirements.

Step 3 [Task 5] - Confirm and justify diversity between SPPA T2000 S7 and TXS. This is a key aspect of the change from SPPA T2000 S5 to S7 that will be addressed.

Step 4 [Task 6] – Update PCSR and assess impact upon the GDA master submission list to ensure proper integration and consistency between the plant Safety Case and the safety Case for SPPA T2000 S7.

3.1.2.2 Description of Methodology to be employed

A Change Management Process is used to control changes made during the Generic Design Assessment (GDA) and a UK EPR GDA Change Management Form (CMF) is raised for each change. The change process has three stages; Stage 1 Design Change Proposal (description and rationale), Stage 2 Impact analysis and change categorisation, Stage 3 close out. The introduction of SPPA T2000 S7 will follow the design change process.

Justification of the change will be included in the Safety Case, the basis of which will be provided during GDA.

The Basis of Safety case will set out the overall strategy, lifecycle and QA arrangements and present a summary of the safety case for the change from SPPA T2000 S5 to S7. This includes impact analysis, design, substantiation and qualification activities and a diversity justification between SPPA T2000 S7 and the TXS based Protection based systems.

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI0-5			
	GI unique number: GI-UKEPR-CI-05-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 4 of 12

The work will be carried out by EDF/AREVA staff who have the necessary competence in Nuclear I&C design. Support will be provided as necessary from equipment suppliers and where appropriate specialist contractors. The work will be carried out under QA arrangements established for the GDA, which comply with ISO 9001.

All deliverables will be subject to co-applicant review by the requesting parties. Regular technical review meetings will be programmed to ensure that the work carried out is proceeding to plan in line with the proposed requirements and standards.

Regular review meetings will be organised with ONR and their technical support.

Task 1 to GI-UKEPR-CI-05.A1 – Confirm S7 choice - Change Management Form (CMF) stage 1

A Change Management Form stage 1 will be produced that will provide a description and rationale of the change from SPPA T2000 S5 to S7. This will confirm the change from SPPA T2000 S5 to S7.

Task 2 to GI-UKEPR-CI-05.A1 – Change Management Form stage 2 (Impact Study)

The Change Management Form stage 2 impact analysis is performed in order to define all potentially impacted documents in the UK EPR GDA submission, new documentation to be created following the change and the technical impact of the change.

An impact study will be produced to assess the impact of the change from SPPA T2000 S5 to S7. This will assess the impact of the change upon documents already provided to justify the use of SPPA T2000 S5 and determine requirements for SPPA T2000 S7.

This task will identify the documents on the submission master list that are affected.

Task 3 to GI-UKEPR-CI-05.A1 – Confirm Contents of Basis of Safety Case

The contents of the Basis of Safety Case for the change from SPPA T2000 S5 to S7 will be set out.

The Basis of Safety Case will :

- 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 I&C 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.

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI0-5			
	GI unique number: GI-UKEPR-CI-05-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 5 of 12

This activity defines in more detail the topics that will be covered in the Basis of Safety Case to address and demonstrate the suitability of the SPPA T2000 S7 platform to perform Class 2 I&C functions.

The output of this action is the list of documentation to be provided for each of the topics covered by the Basis of the Safety Case for the change from SPPA/T2000 S5 to S7 with corresponding time schedule.

The contents of the Basis of Safety Case will follow the generic model and will take account of the following topics:

- Requirements

- Standards

- Overall Life cycle

- Hardware

- Overview

- Development

- FMEA , reliability studies

- Manufacturing and repair

- Functional and Performance test

- Environmental Testing

- Software

- Overview

- Operating System

- System Software

- Development and Testing

- Verification and Validation

- FPGA , Asics

- Microcode

- Off line systems and tools

- Application development

- Assessment against Standards

- Re-use of S5 safety demonstration and impact analysis

- Independent assessment

- Quality and confidence building

- Non-perturbation of other systems

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI0-5			
	GI unique number: GI-UKEPR-CI-05-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 6 of 12

Independent confidence building measures
Programme of future work

Task 4 to GI-UKEPR-CI-05.A1 – SPPA/T2000 S7 Basis of Safety Case

The Basis of Safety Case for the change from SPPA T2000 S5 to S7 will be produced. The Basis of Safety Case will address and demonstrate the suitability of the SPPA T2000 S7 platform to perform Class 2 I&C functions and will set out the required qualification activities for the SPPA T2000 S7, when they will be carried out and how the outcome will be reported. This will include a full description of the design, design substantiation, compliance with standards, and consideration of Production Excellence and Independent Confidence Building Measures, justification of reliability and diversity.

The Basis of Safety Case will set out how a claims, argument, evidence approach will be applied to presentation of the safety case for use of SPPA T2000 S7.

More work may be required to gather and summarise the data that exists about the SPPA/T2000 S7 products, update SPPA/T2000 S5 safety demonstration submissions to reflect SPPA/T2000 S7 and to justify parts of the SPPA/T2000 S7 product that have not been previously qualified. The arrangements for undertaking these activities will be detailed together with an assessment of the SPPA/T2000 S7 products against modern nuclear sector standards, production excellence demonstration and appropriate independent confidence building measures.

Any 'gaps' will be justified on the basis of previous qualification or further activities as required.

Task 5 to GI-UKEPR-CI-05.A1 – SPPA/T2000 S7 to PS TXS Diversity

A 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 will be provided. The hardware and software components of each system will be reviewed to confirm there are no common components or features, common development history, shared production facility or other common features that may compromise the claimed reliability.

Justification of NCSS diversity with SAS SPPA T2000 S7 falls under the scope of GI-UKEPR-CI.01 as these are part of the selection criteria for NCSS.

Task 6 to GI-UKEPR-CI-05.A1 – Update of PCSR

The impact of the change from SPPA T2000 S5 to S7 on PCSR chapter 7 "Instrumentation and Control" will be identified and addressed. Any changes required to the PCSR will be implemented. Update of the GDA master submission list to ensure proper integration and consistency between the plant Safety Case and the Safety Case for SPPA T2000 S7 will be carried out if changes are identified to be required (output of task 2). Documents to be produced subsequently to GDA will be

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI0-5			
	GI unique number: GI-UKEPR-CI-05-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 7 of 12

identified in the Basis of Safety Case.

3.1.2.3 Deliverable description

**Submission
date to
ONR/EA**

<p>Change Management Form 29 - SPPA T2000 S7 (task 1) Stage 1 Design Change Proposal (description and rationale) <i>This provides a description and rationale for the change from SPPA T2000 S5 to S7.</i></p>	<p>15/06/2011¹</p>
<p>Change Management Form 29 – SPPA T2000 S7 (task 2) Stage 2 Impact Study (Impact analysis)</p> <p><i>This provides an impact study which defines all potentially impacted documents in the UK EPR GDA submission, new documentation to be created following the change from SPPA T2000 S5 to S7 and the technical impact of the change.</i></p>	<p>15/09/2011</p>
<p>Contents of Basis of Safety Case for the change from SPPA T2000 S5 to S7 (task 3)</p> <p><i>This defines in detail the topics that will covered in the Basis of Safety Case to address and demonstrate the suitability of the SPPA T2000 S7 platform to perform Class 2 I&C functions.</i></p>	<p>30/11/2011</p>
<p>Basis of Safety Case for the change from SPPA T2000 S5 to S7 (task 4)</p> <p><i>The Basis of Safety Case addresses and demonstrates the suitability of the SPPA T2000 S7 platform to perform Class 2 I&C functions and sets out the required qualification activities for the SPPA T2000 S7, when they will be carried out and how the outcome will be reported.</i></p>	<p>30/04/2012</p>
<p>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 (task 5)</p> <p><i>This provides a 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.</i></p>	<p>31/03/2012</p>

¹ This was sent on 07/06/2011 under cover letter ND(NII)EPR00872R.

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI0-5			
	GI unique number: GI-UKEPR-CI-05-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 8 of 12

Update of PCSR Chapter 7: Control and Instrumentation

Draft version 13/07/2012

Final version 05/11/2012

4.0 SUMMARY OF IMPACT ON GDA SUBMISSION DOCUMENTATION

4.1 GDA submission documents impacted by GDA Issue and scheduled to be created (C) or updated (U) within GDA

GDA Submission Documents	C/U	Related GDA Issue Action(s)	Submission Date to ONR/EA
SSER sub-chapters	U		Draft
PCSR Chapter 7: Control and Instrumentation		GI-UKEPR-CI-05.A1	13/07/2012 Final 05/11/2012
Other GDA submission supporting documents			
Change Management Form 29 SPPA T2000 S7 - Stage 1 Design Change Proposal (description and rationale)	C	GI-UKEPR-CI-05.A1	15/06/2011 ²
Change Management Form 29 SPPA T2000 S7 - Stage 2 Impact Study (Impact analysis)	C	GI-UKEPR-CI-05.A1	15/09/2011
Contents of Basis of Safety Case for the change from SPPA T2000 S5 to S7	C	GI-UKEPR-CI-05.A1	30/11/2011
Basis of Safety Case for the change from SPPA T2000 S5 to S7	C	GI-UKEPR-CI-05.A1	30/04/2012
Justification that the SPPA T2000 S7 platform and TXS platform are suitably diverse to support the reliability claims made for	C	GI-UKEPR-CI-05.A1	31/03/2012

² This was sent on 07/06/2011 under cover letter ND(NII)EPR00872R.

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI0-5			
	GI unique number: GI-UKEPR-CI-05-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 9 of 12

combinations of systems using the two platforms

4.2 GDA submission documents impacted by GDA Issue and scheduled to be updated post GDA

Document

Documents to be produced subsequently to GDA will be identified in the Basis of Safety Case.

5.0 JUSTIFICATION OF ADEQUACY

The GDA issue deliverables will provide the approach adopted to address SPPA T2000 S5 obsolescence for the UKEPR. The deliverables will include an impact analysis for the change from SPPA T2000 S5, a Basis of Safety Case setting out the design, substantiation and qualification activities and a diversity justification between SPPA T2000 S7 based and the TXS based Protection Systems.

The Basis of Safety case will set out the overall strategy, lifecycle and QA arrangements and present a summary of the safety case for the change from SPPA T2000 S5 to S7.

The Basis of Safety case will set out the activities required in order to establish the full safety case for SPPA T2000 S7. This will take account of the results of the impact analysis of the change from S5 to S7. More work may be required to gather and summarise the data that exists about the S7 products, update S5 safety demonstration submissions to reflect S7 and to justify parts of the S7 product that have not been previously qualified. The arrangements for undertaking these activities will be detailed together with an assessment of the S7 products against modern nuclear sector standards, production excellence demonstration and appropriate independent confidence building measures. Any 'gaps' will be justified on the basis of previous qualification or further activities as required.

The basis of safety case defines the safety principles and standards and justifies how these safety principles and standards will be complied with at each step of the development and deployment of SPPA T2000 S7 based systems. This will ensure that SPPA T2000 S7 based systems used for the UKEPR are compliant with appropriate standards and safety principles.

The basis of safety case will set out and justify how functional and performance requirements will be satisfied. This will ensure that SPPA T2000 S7 based systems used for the UKEPR meet their functional and performance requirements.

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI0-5			
	GI unique number: GI-UKEPR-CI-05-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 10 of 12

The basis case will set out how conformance with relevant ONR SAPs will be demonstrated to ensure that SPPA T2000 S7 based systems used for the UKEPR conform with relevant ONR SAPs.

The basis of safety case will include a full analysis of the impact of the replacement platform on the overall I&C design. This will ensure all aspects of the change are covered and that there are no detrimental effects upon the capability of the overall I&C to full fill its role and safety functions.

The basis of safety case will provide precise details of the change and demonstrate that the systems based on SPPA T2000 S7 are fit for purpose. The diversity justification between SPPA T2000 S7 and the TXS based Protection System will address and justify the key requirement that the two products as implemented support multiplicative reliability claims for combinations of functions implemented in systems using the respective products.

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-05			
	GI unique number: GI-UKEPR-CI-05-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 11 of 12

6.0 TIMETABLE AND MILESTONE PROGRAMME LEADING TO THE DELIVERABLES

Consult the following pages for the associated timetable and milestone programme.

