



UK EPR GDA PROJECT				
UK EPR	Title: Resolution Plan for GI-UKEPR-CI-06			
	RP unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 1 of 41
Approved for EDF by: A. PETIT		Approved for AREVA by: C. WOOLDRIDGE		
Name/Initials	Date	30/06/2011	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
Issues arising from RI02	C&I	SI and PSA

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

2.0 OVERVIEW OF SCOPE OF WORK

EDF and AREVA have introduced a new system called NCSS (Non Computerized Safety System) whose major requirement is diversity relative to other safety systems (the SPPA-T2000 based Safety Automation System and the TELEPERM XS based Protection System). As the supplier of the NCSS has not been defined during the step 4 of the GDA (see GI-UKEPR-CI-01), EDF and AREVA has to provide justification of the diversity, at system level and platform level, between the NCSS and each of the other safety system (SAS and PS).

The diversity between the SPPA-T2000 based I&C systems (SAS) and TELEPERM XS based I&C systems (PS) have been provided during the GDA Step 4 (see list of GDA documents already submitted). As the S5 version of the SPPA-T2000 platform will be obsolete on the timescales of UK EPR implementation (see GI-UKEPR-CI-05), the justification of the diversity with the new version of the SPPA-T2000 (S7 version) will be provided.

Responses to three actions have been provided in GDA step 4 :

- update of description of the protection system taking into account changes committed in step 4

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 2 of 41

(GI-UKEPR-CI-06.A4)

- justification of independence between PICS and SAS systems (GI-UKEPR-CI-06.A5)
- justification of the non practicability for the SICS to be in a functional state in normal operation (GI-UKEPR-CI-06.A7)

The remaining six actions will be addressed in the GI-UKEPR-CI-06 resolution plan (see more detailed justification of the scope of work below)

- The diversity between the three platforms and systems implemented using the three platforms will be justified considering the technology selected for the NCSS platform for the UKEPR and the updated version S7 for the platform SPPA/T2000. (GI-UKEPR-CI-06.A1)
- Evidence will be provided for the justification of the reliability figures considered for each of the protection systems when claimed independently and in combination (GI-UKEPR-CI-06.A2)
- Production Excellence and Independent Confidence Building Measures for the computer based systems important for safety on the UKEPR will be described and justified (GI-UKEPR-CI-06.A3). NB Independent Confidence Building Measures for the TELEPERM XS based protection system are addressed by GI-UKEPR-CI-02.
- A Basis of Safety Case will be provided for the implementation of Protection System Operator Terminal to be provided in the Main Control Room and in the Remote Shutdown Station (GI-UKEPR-CI-06.A6)
- Evidence will be provided to demonstrate that for those functions important to safety which use class 3 terminal bus and /or Plant bus, end-to-end response time requirements are achievable by design (GI-UKEPR-CI-06.A8)
- Detailed substantiation will be provided for the reliability claim of any system /component used by more than one system important for safety and potentially by more than one line of protection (GI-UKEPR-CI-06.A9)

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 3 of 41

3.0 GDA ISSUE ACTIONS AND RESOLUTION PLAN DELIVERABLES

3.1 Action GI-UKEPR-CI-06.A1

Action I/D	Action Description
GI-UKEPR-CI-06.A1	<p>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.</p> <p>One of the C&I architectural changes introduces 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.</p> <p>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.</p> <p>Where final detailed design information is not available, but which is identified has 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.</p> <p>For further guidance see also T13.TO1.04 in Annex 3, 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 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-06.A1

none

3.1.2 Planned submissions in response to GI-UKEPR-CI-06.A1

3.1.2.1 Description of Scope of Work

The response to this action of the GDA issue will provide a justification of the diversity between all the safety systems (SAS, PS, NCSS). This will cover diversity between platforms and between systems implemented on the respective platforms to demonstrate the validity of multiplicative reliability claims made for combinations of systems.

This task is linked to NCSS GI-UKEPR-CI-01.A1 and SPPA T2000 GI-UKEPR-CI-05.A1 and the work

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 4 of 41

related to the introduction of NCSS and SPPA T2000 S7 will be carried out under the respective resolution plans.

3.1.2.2 Description of Methodology to be employed

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 from 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.

The GDA and EDF/AREVA change management processes will be used to address design changes, resulting from the work carried out.

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

The response to this GDA issue is organised into activities related to platform diversity which involve updates of existing documents and subsequent activities which address diversity at the system level:

The diversity criteria for NCSS is contained in the document PELL-F DC 11. This task will confirm that the diversity criteria are met by the selected supplier for the NCSS. This activity is linked to the GI-UKEPR-CI.01 on substantiation of NCSS design. The document ECECC050092D "Justification of diversity between SPPA/T2000 and TELEPERM XS" will be updated to integrate the new version of the SPPA-T2000 platform and to confirm that diversity with TELEPERM XS is maintained. This activity is linked to the GI-UKEPR-CI.05 on obsolescence of SPPA-T2000.

Task 1 to GI-UKEPR-CI-06.A1 – Diversity of C&I systems

The justification of the diversity of C&I platforms and systems implemented on the platforms will be made by :

- updating the justification of diversity between TELEPERM XS and SPPA-T2000 platform to integrate the new version of the SPPA-T2000 (S7). Document to be provided as a result of GI-UKEPR-CI-05.A1 (task 5)
- providing a justification of diversity between systems implemented on the TELEPERM XS and SPPA-T2000 platforms including consideration of the new version of the SPPA-T2000 (S7). Document to be provided as a result of GI-UKEPR-CI-05.A1 (task 4)
- providing evidence (or arguments when evidence cannot be available in GDA) of compliance to the diversity requirements (PELL-F DC 11) for the diversity between the NCSS I&C platform and the TELEPERM XS. Document to be provided as part of the Basis of Safety Case for NCSS : GI-UKEPR-CI-01.A1 (task 3 and 4)
- providing a justification of diversity between systems implemented on the NCSS and TELEPERM XS platforms. Document to be provided as part of the Basis of Safety Case for

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 5 of 41

NCSS : GI-UKEPR-CI-01.A1 (task 3 and 4)

- providing evidence (or arguments when evidence cannot be available in GDA) of compliance to the diversity requirements (PELL-F DC 11) for the diversity between the NCSS I&C platform and the SPPA-T2000. Document to be provided as part of the Basis of Safety Case for NCSS : GI-UKEPR-CI-01.A1 (task 3 and 4)
- providing a justification of diversity between systems implemented on the NCSS and SPPA-T2000 platforms including consideration of the new version of the SPPA-T2000 (S7). Document to be provided as part of the Basis of Safety Case for NCSS : GI-UKEPR-CI-01.A1 (task 3 and 4)

3.1.2.3 Deliverable description

Submission date to ONR/EA

Justification of the diversity between SPPA T2000 S7 and TELEPERM XS platforms

31/03/2012

This justification for the diversity between SPPA T2000 S7 and TELEPERM XS platforms will be provided under GI-UKEPR-CI-05.A1 (task 5)

Justification of the diversity between systems implemented using the SPPA T2000 S7 and TELEPERM XS platforms

30/04/2012

This justification of the diversity between systems implemented using the SPPA T2000 S7 and TELEPERM XS platforms will be provided under GI-UKEPR-CI-05.A1 (task 4)

Justification of the diversity between NCSS and other I&C platforms

15/07/2012

This justification for the diversity between NCSS and other I&C platforms will be provided under GI-UKEPR-CI-01.A1 (task 3 and 4)

Justification of the diversity between systems implemented using the NCSS and other I&C platforms

15/07/2012

This justification for the diversity between systems implemented using the NCSS and other I&C platforms will be provided under GI-UKEPR-CI-01.A1 (task 3 and 4)

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 6 of 41

3.2 Action GI-UKEPR-CI-06.A2

Action I/D	Action Description
GI-UKEPR-CI-06.A2	<p>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.</p> <p>The EDF and AREVA safety case makes a claim of 1×10^{-4} probability of failure on demand (pfd) for the Class 1 Protection System (PS), 1×10^{-2} pfd for the Safety Automation System (SAS) and 1×10^{-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.</p> <p>For further guidance see also T16.TO2.21 in Annex 6, and T20.A1.4.1 and T20.A1.4.2 in Annex 9 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>

3.2.1 Deliverables already submitted to ONR/EA in response to GI-UKEPR-CI-06.A2

The documents listed below have been provided during GDA.

	Date of submission
<u>Modules reliability FMEA TELEPERM XS</u> NLTHG2008EN1001 NLTCG2008EN1002 -1004 – 1007 to 1017 ND(NII) ERP00127N <i>This document presents the failure modes of the module on a functional basis, the mechanisms that are typically used to detect malfunctions, and the quantitative assessment of the different failure modes. Processing modules, network modules, input modules and output modules are covered.</i>	30/06/2009
TELEPERM XS Engineering Procedure - Methodology for RAMS Studies. NLE-F DM 10032 Revision A. AREVA. June 2010. (E) ND(NII) EPR00459R <i>This document presents the methodology which will be used to calculate the reliability values for the Protection System, including the Probability of Failure on Demand of following functions: reactor Trip, ESFAS functions, diesel actuation and control loop.</i>	30/10/2010

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 7 of 41

TELEPERM XS Self-monitoring and fail safe behaviour.
NLTC-G/2008/en/0079

30/06/2009

ND(NII) ERP00127N

This document presents the self tests implemented in the TELEPERM XS platform.

Compliance of the TELEPERM XS platform with IEC60987 NLTC-G/2008/en/0053

08/01/2010

TQ381

This document provides the compliance analysis of the process of development of the TELEPERM XS platform with the international standard IEC60987.

System Reliability analysis SPPA-T2000 SIE QU627 Revision 5.0. Siemens. February 2009. (E)

07/06/2010

ND(NII) EPR00418N

This document provides the Mean Time Between Failure (MTBF), the average Probability of Failure on Demand (pfd), the Probability of Failure per Hour and the frequency of spurious trip rate. Following functions are considered: open and closed loop, open loop with PICS and/or SICS command.

Module reliability FMEA SIE QU626

07/06/2010

ND(NII) EPR00418N

This document describes the reliability data of each module of the SPPA-T2000 platform

Justification Report on the Independence of I&C Systems based on the SPPA T2000 Platform. ECECC080586 Revision B1. EDF. July 2009. (E)

31/07/2009

ND(NII) EPR00145N

This document justify the independence between the systems based on SPPA-T2000 platform.

Compliance of SPPA/T2000 based system with IEC61513 & IEC 62138

20/04/2010

DN 2.2.23 (compliance of PICS)

DN 2.2.24 (compliance of SAS)

TQ705

This document provides the compliance analysis of the process of development of the SAS and the PAS with the international standards IEC61513 and IEC62138.

3.2.2 Planned submissions in response to GI-UKEPR-CI-06.A2

3.2.2.1 Description of Scope of Work

The scope of this task is to provide a justification of the reliability figures used for each of the protection systems when claimed independently and in combination. The justification will cover consideration of systematic and hardware failures, and compliance with appropriate guidance and

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 8 of 41

standards.

The scope of work is split into four tasks:

- Reliability for the Class 1 Protection System (PS)
- Reliability for the Safety Automation System (SAS)
- Reliability for the Non-Computerised Safety System (NCSS)
- Independence of the Class 1 Protection System (PS), the Safety Automation System (SAS) and the Non-Computerised Safety System (NCSS)

This task is linked to NCSS GI-UKEPR-CI-01.A1 and SPPA T2000 GI-UKEPR-CI-05.A1 and a proportion of the work related to the introduction of NCSS and SPPA T2000 S7 will be carried out under the respective resolution plans.

3.2.2.2 Description of Methodology to be employed

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 from 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.

The GDA and EDF/AREVA change management processes will be used to address design changes, resulting from the work carried out.

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

The safety case makes a claim of $1 \cdot 10^{-4}$ fpd for the Class 1 Protection System (PS), $1 \cdot 10^{-2}$ fpd for the Safety Automation System (SAS) and $1 \cdot 10^{-3}$ fpd for the Non-Computerised Safety System (NCSS). The scope of these tasks is to provide a justification for each of these figures in isolation and in combination for multiplicative reliability claims.

Task 1 to GI-UKEPR-CI-06.A2 - Reliability for the Class 1 Protection System (PS)

The scope of the activity is a justification for the reliability claims made for the Class 1 Protection System (PS) in respect of compliance with standards, random failure assessment and systematic failure assessment.

Compliance of the Class 1 Protection System (PS) with standards will be assessed through a review against IEC 60880 for software and IEC 60987 for hardware. A new document will be produced to report the outcome of this assessment.

A justification of the PS reliability (HW, SW & FMEA reliability study) will be undertaken. This will cover random failure assessment, FMEA, reliability analysis and a systematic failure assessment. A new document will be produced to report the outcome of this assessment.

The programme of Independence Confidence Building Measures (ICBMs) to support the safety case for the TELEPERM XS Protection System will be addressed under GI-UKEPR-CI-02. A

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 9 of 41

justification of their adequacy to support the PS reliability claim will be provided.

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

Task 2 to GI-UKEPR-CI-06.A2 - Reliability for the Safety Automation System (SAS)

The scope of the activity is a justification for the reliability claims made for the Safety Automation System (SAS) in respect of compliance with standards, random failure assessment and systematic failure assessment.

Documents covering compliance with standards, random failure assessment and systematic failure assessment of SPPA T2000 S5 have already been provided to ONR. These are detailed in section 3.2.1 and section 3.2.2.3.

These documents specific to SPPA T2000 S5 will be subject to a review, impact analysis and update as part of the change to SPPA T2000 S7.

These activities are covered under GI-UKEPR-CI-05 – SPPA T2000 Obsolescence. The level of update and need for new documents will be determined under GI-UKEPR-CI-05.

Task 3 to GI-UKEPR-CI-06.A2 - Reliability for the Non-Computerised Safety System (NCSS)

The scope of the activity is a justification for the reliability claims made for the Non-Computerised Safety System (NCSS) in respect of compliance with standards, random failure assessment and systematic failure assessment.

These activities are covered under resolution plan GI-UKEPR-CI-01. The documents to justify the NCSS reliability will be determined under GI-UKEPR-CI-01.

Task 4 to GI-UKEPR-CI-06.A2 - Independence of the Class 1 Protection System (PS), the Safety Automation System (SAS) and the Non-Computerised Safety System (NCSS).

The scope of the activity is a justification in respect of independence and diversity for the reliability claims of up to made for combinations of the protection systems:

1*10⁻⁶ Class 1 Protection System (PS) and the Safety Automation System (SAS)

1*10⁻⁷ Class 1 Protection System (PS) and the Non-Computerised Safety System (NCSS)

1*10⁻⁵ Safety Automation System (SAS) and the Non-Computerised Safety System (NCSS)

1*10⁻⁹ Class 1 Protection System (PS), the Safety Automation System (SAS) and the Non-Computerised Safety System (NCSS).

The scope of this task is the independence of the PS, SAS and NCSS as systems in isolation from sensors and actuators. The independence of functions implemented in PS, SAS and NCSS for sensors and actuators is covered under GI-UKEPR-CI-06.A9.

An assessment of the independence between the systems will be undertaken to demonstrate that the

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 10 of 41

combined reliability claims made are supported. Justification of independence and diversity between systems is covered under the resolution plan for GI-UKEPR-CI-06.A1. This task will consider those aspects of independence between systems such as power supply, physical separation and electrical isolation not covered under GI-UKEPR-CI-06.A1 which focuses on platform diversity between systems.

A justification of the Independence of the Class 1 Protection System (PS), the Safety Automation System (SAS) and the Non-Computerised Safety System (NCSS) will be undertaken. A new document will be produced to report the outcome of this assessment.

This task will confirm that the outcome of independence and diversity assessment supports use of multiplicative reliability claims for combinations of systems.

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

Task 5 to GI-UKEPR-CI-06.A2 – Update of PCSR

The impact of the results of the reliability assessments on PCSR chapter 7 “Instrumentation and Control” will be identified and addressed. Any changes required to the PCSR will be implemented.

Draft version will be sent to ONR for comments.

3.2.2.3 Deliverable description

	Submission date to ONR/EA
Compliance with Standards (IEC 60880 and IEC 60987) of PS lifecycle (task 1) <i>This document will provide a demonstration of compliance of the PS with IEC 60880 and IEC 60987.</i>	31/03/2012
Justification of PS reliability (HW, SW & FMEA reliability study) (task 1) <i>This document will provide a justification of PS reliability covering hardware FMEA, reliability and software reliability.</i>	30/11/2011
Justification of SPPA T2000 S7 reliability (FMEA) -See GI-UKEPR-CI-05 (task 2)	30/04/2012
NCSS reliability - see GI-UKEPR-CI-01(task 3)	30/04/2012
Independence of the Class 1 Protection System (PS), the Safety Automation System (SAS) and the Non-Computerised Safety System (NCSS) (task 4) <i>This document will demonstrate that the level of independence between the Class 1 Protection System (PS), the Safety Automation System (SAS) and the Non-</i>	06/01/2012

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 11 of 41

Computerised Safety System (NCSS) is sufficient to support the reliability claims made for combinations of the systems.

Generic rule for the electrical isolation of EPR Instrumentation and Control Systems (internal connections and interfaces) ECECC100846 (task 4) 31/07/2011

This document provides Generic rules for the electrical isolation of EPR Instrumentation and Control Systems.

Update of PCSR Chapter 7: Control and Instrumentation (task 5)

Draft version 31/05/2012

Final version 21/09/2012

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 12 of 41

3.3 Action GI-UKEPR-CI-06.A3

Action I/D	Action Description
GI-UKEPR-CI-06.A3	<p>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.</p> <p>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.</p> <p>Note that the Protection System's independent confidence building measures are to be addressed under GI-UKEPR-CI-03.</p> <p>For further guidance see also T20.A1.4.1.a in Annex 9 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>

3.3.1 Deliverables already submitted to ONR/EA in response to GI-UKEPR-CI-06.A3

The documents listed below have been provided during GDA.

	Date of submission
Production excellence and independent confidence building for EPR UK safety CI, ENSECC090137 Revision B ND(NII) EPR00459R This document sets out the EDF/AREVA approach to the demonstration of the adequacy of computer based systems important to safety (CBSIS) including identification of production excellence and independent confidence building activities for each CBSIS.	30/06/2010
PE /ICBM strategy for SPPA/T2000 to justify its use for supporting F1B functions ND(NII) EPR00609N This document sets out the Production Excellence and Independent Confidence Building Measure strategy for systems supporting F1B functions.	10/11/2010

3.3.2 Planned submissions in response to GI-UKEPR-CI-06.A3

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 13 of 41

3.3.2.1 Description of Scope of Work

The scope of this task is 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.

The scope of work is split into three tasks:

- Production Excellence and Independent Confidence Building Measures Guideline for CBSIS
- Justification for Production Excellence Independent Confidence Building Measures used a for TELEPERM XS based systems
- Justification for Production Excellence and Independent Confidence Building Measures used for SPPA T2000 based systems

The approach to independent confidence building measures (PE/ICBM) for the Class 1 TELEPERM XS based Protection System (PS) is covered under GI-UKEPR-CI-02.

3.3.2.2 Description of Methodology to be employed

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 from 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.

The GDA and EDF/AREVA change management processes will be used to address design changes, resulting from the work carried out.

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

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.

Task 1 to GI-UKEPR-CI-06.A3 - Production Excellence and Independent Confidence Building Measures Guideline for CBSIS

A guidance document will be produced setting out the Production Excellence and Independent Confidence Building Measures requirements for computer based systems important to safety.

Production excellence is based on compliance with standards whilst Independent confidence

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 14 of 41

building measures are undertaken to provide a challenge to the system lifecycle, independent of the equipment supplier, and give confidence that the required functionality has been delivered to the required integrity level. Independence is required between those specifying/procuring the systems and those undertaking the Independent confidence building measures.

The class of the system, the reliability claimed and standards will be considered when setting out the requirements to demonstrate production excellence. The requirements for compensating measures to mitigate potential shortfalls in production excellence will also be discussed.

The set of candidate independent confidence building measures appropriate to different system classes and the reliability claims will be described and linked to the system class and claimed reliability.

A new document will be produced to set out the guidance for Production Excellence and Independent Confidence Building Measures.

The approach and methodology used to qualify Smart Devices for Nuclear Safety functions is covered under GI-UKEPR-CI-04 – SMART Devices.

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

Task 2 to GI-UKEPR-CI-06.A3 - Justification for Production Excellence and Independent Confidence Building Measures used a for TELEPERM XS based systems

This task will set out which activities and measures are used for the TELEPERM XS computer based systems and justify these against the guidance. TELEPERM XS based systems are PS, RSCL and SA I&C.

The development and production processes are common for systems implemented using a particular platform. The QA plan, Verification & Validation plan, processes and tools used are the same although the degree to which these are used and applied may vary dependent on the class and reliability claimed for the system.

The requirement for and degree to which activities and measures are applied will be set out and justified as appropriate for each system against the requirements for demonstrating production excellence set out in the guidance document for the applicable class of system and claimed reliability.

The Independent confidence building measures undertaken for each system will be set out and justified as appropriate against the requirements set out in the guidance document, class of system and claimed reliability.

A new document will be produced to set out the justification for the approach used for Production Excellence and Independent Confidence Building Measures for TELEPERM XS based systems.

The approach to independent confidence building measures (PE/ICBM) for the Class 1 TELEPERM XS based Protection System (PS) is covered under GI-UKEPR-CI-02.

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 15 of 41

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

Task 3 to GI-UKEPR-CI-06.A3 - Justification for Production Excellence and Independent Confidence Building Measures used for SPPA T2000 based systems

The PE/ICBM strategy for SPPA/T2000 to justify its use for supporting F1B functions was sent to ONR under cover of letter EPR00609N on 10th November 2010.

This set out the activities and measures used for the SPPA T2000 (S5) computer based systems based on SAS. The strategy will be further developed for SPPA T2000 S7 and the SPPA T2000 based systems SAS, RCC-B SAS, PAS and PICS.

The development and production processes are common for systems implemented using a particular platform. The QA plan, Verification & Validation plan, processes and tools used are the same although the degree to which these are used and applied may vary dependent on the class and reliability claimed for the system.

The requirement for and degree to which activities and measures are applied will be set out and justified as appropriate for each system against the requirements for demonstrating production excellence set out in the guidance document for the applicable class of system and claimed reliability.

The Independent confidence building measures undertaken for each system will be set out and justified as appropriate against the requirements set out in the guidance document, class of system and claimed reliability.

The specification and application of PE/ICBM related to SPPA/T2000 S7 will be addressed in the basis of safety case under resolution plan GI-UKEPR-CI-05.

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

Task 4 to GI-UKEPR-CI-06.A3 – Update of PCSR

The impact of the results of the production excellence and independent confidence building measure justifications on PCSR chapter 7 “Instrumentation and Control” will be identified and addressed. Any changes required to the PCSR will be implemented

Draft version will be sent to ONR for comments.

3.3.2.3 Deliverable description

Submission date to ONR/EA

Production Excellence and Independent Confidence Building Guideline for computer based systems important to safety (task 1)

30/09/2011

This document provides a guideline for the application of Production Excellence and Independent Confidence Building measures to I&C systems important to safety and the graded

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 16 of 41

approach determined by the system categorisation..

Justification for Production Excellence and Independent Confidence Building Measures used for TELEPERM XS based systems (task 2) 15/11/2011

This document justifies the Production Excellence and Independent Confidence Building Measures used for TELEPERM XS based systems by comparing activities and measures used against those set out in the guideline.

Justification for Production Excellence and Independent Confidence Building Measures used for SPPA T2000 based systems (task 3) 15/03/2012

This document justifies the Production Excellence and Independent Confidence Building Measures used for SPPA T2000 based systems by comparing activities and measures used against those set out in the guideline.

Update of PCSR Chapter 7: Control and Instrumentation

Draft version 31/05/2012

Final version 21/09/2012

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 17 of 41

3.4 Action GI-UKEPR-CI-06.A4

Action I/D	Action Description
GI-UKEPR-CI-06.A4	<p>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.</p> <p>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).</p> <p>For further guidance see also T17.TO1.04 in Annex 7, T20.A2.2.1 and T20.A2.2.3 in Annex 9 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>

3.4.1 Deliverables already submitted to ONR/EA in response to GI-UKEPR-CI06.A4

Following document has been provided during GDA but after the GDA Step 4 assessment phase. The document has not yet been assessed by ONR/NII.

	Date of submission
Full response to GI-UKEPR-CI-06.A4 has been provided in response to action 5 of Regulatory Observation R082. 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 (NII) EPR00790R	17/02/2011

3.4.2 Planned submissions in response to GI-UKEPR-CI06.A4

All deliverables already submitted (see 3.4.1)

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 18 of 41

3.5 Action GI-UKEPR-CI-06.A5

Action I/D	Action Description
GI-UKEPR-CI-06.A5	<p>EDF and AREVA to provide detailed substantiation of independence between PICS Class 3 and SAS Class 2 systems.</p> <p>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.</p> <p>For further guidance see also T20.A2.3.2 in Annex 9 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>

3.5.1 Deliverables already submitted to ONR/EA in response to GI-UKEPR-CI-06.A5

Following document has been provided during GDA but after the GDA Step 4 assessment phase. The document has not yet been assessed by ONR/NII.

	Date of submission
Full response to GI-UKEPR-CI.06.05 has been provided in response to action 6 of Regulatory Observation RO82: "EDF and AREVA to provide detailed substantiation of independence between PICS Class 3 and SAS Class 2 systems. (Ref RIO2 A2.3)" ND(NII) EPR00823R	11/03/2011

3.5.2 Planned submissions in response to GI-UKEPR-CI-06.A5

All deliverables already submitted (see 3.5.1)

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 19 of 41

3.6 Action GI-UKEPR-CI-06.A6

Action I/D	Action Description
GI-UKEPR-CI-06.A6	<p>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.</p> <p>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.</p> <p>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.</p> <p>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 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>

3.6.1 Deliverables already submitted to ONR/EA in response to GI-UKEPR-CI-06.A6

Following document has been provided during GDA but after the GDA Step 4 assessment phase. The document has not yet been assessed by ONR/NII.

	Date of submission
SICS Class 1 displays and controls - via TQ1130	20/01/2011
<i>The answer to TQ1130 "SICS Class 1 displays and controls" listed all PS information available on SICS. A cross comparison with NRC RG 1.97 rev 3 was provided as well as a justification for deviations and design choices.</i>	

3.6.2 Planned submissions in response to GI-UKEPR-CI-06.A6

3.6.2.1 Description of Scope of Work

The answer to this action will be divided in 2 steps:

- EDF and AREVA will provide detailed substantiation of the Class 1 control and display facilities

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 20 of 41

to be provided in the MCR and RSS.

- A Basis of Safety Case for the class 1 Protection System Operator Terminal (PSOT), will be provided as well as a justification in terms of the functional coverage of this new system. The addition of the PSOT in the MCR and the RSS covered by the GDA change process.

3.6.2.2 Description of Methodology to be employed

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 from 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.

The GDA and EDF/AREVA change management processes will be used to address design changes, resulting from the work carried out.

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

Task 1 for GI-UKEPR-CI-06.A6 – Detailed Substantiation of the class 1 control and display facilities available in the Main Control Room (MCR) and the Remote Shutdown Station (RSS)

This task will include the following activities:

- The general organisation of the MCR and the RSS in terms of equipments available to the operator and their respective role will be provided.
- The functional scope of the class 1 information and controls required in the MCR and the RSS for safely operating the plant will be written out and justified.
- Then the functional scope of the class 1 equipments available in the MCR (SICS and Protection System Operation Terminal (PSOT)) and in the RSS (PSOT) will be presented.

The draft structure of the corresponding deliverable is detailed below:

1. Introduction

- *Overview of the different control means available in the MCR and the RSS, including:*
 - *role,*
 - *class,*
 - *HMI,*
 - *technology.*
- *Operation principle in the MCR and the RSS will be recalled.*

2. Definition and justification of class 1 information and controls necessary in the MCR and the RSS for plant operation

- *Detailed functional scope of class 1 information and controls required in MCR and RSS.*

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 21 of 41

- *Justification of the class 1 functional scope.*

3. Description of class 1 information and controls available on SICS (and PIPO) in the MCR

- *Role of SICS and PIPO will be recalled.*
- *List of class 1 information and controls available on SICS (from/to the PS).*
- *Description of SICS technology arrangement will be given.*
- *SICS smart devices will be identified.*

4. Description of the class 1 information and controls available on the Protection System Operating Terminal (PSOT) in the MCR and RSS

- *Role of PSOT and integration principle in the computer-based workstations.*
- *List of information and controls available on PSOT*

Task 2 for GI-UKEPR-CI-06.A6 – PSOT Basis of Safety Case

This task will provide the basis of the safety case for the dedicated class 1 interface to be installed in the MCR and RSS (namely PSOT – Protection system Operating Terminal). The PSOT is to be based on the QDS platform from AREVA.

The general plan of the PSOT basis of safety case will be provided as an interim deliverable. The Basis of Safety Case will address the QDS platform qualification as well as its application to the UK EPR project (functional and safety requirements, specific developments...).

It will be based on input from the generic basis of safety case structure put forward for early discussion with ONR (EDF and AREVA Letter ND(NII) EPR00852R and associated ONR response letter EPR70302R).

Task 3 for GI-UKEPR-CI-06.A6 – Update of PCSR

The impact on Chapters 7 “Instrumentation and Control” and on chapter 18 “Human-Machine-Interface and Operational aspects” will be assessed and the required updates will be implemented.

Draft versions will be sent to ONR for comments.

3.6.2.3 Deliverable description

Submission date to ONR/EA

MCR and RSS description - Class 1 information and controls organisation (task 1)

31/12/2011

This document will present the class 1 information and controls systems available to the operator in the MCR (SICS and PSOT) and in the RSS (PSOT).

Outline of Basis of Safety Case for the implementation of the Protection System Operator Terminal in the MCR and the RSS (task 2)

31/08/2011

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 22 of 41

This document is an outline of the PSOT basis of safety case. It will state the points to be addressed in the final BoSC.

Protection System Operator Terminal Basis of the Safety Case and supporting documentation (task 2) 29/02/2012

This document is the Basis of Safety Case of the PSOT that includes its safety and functional requirements. PSOT safety demonstration will be addressed in this document. The PSOT is to be based on the QDS platform from AREVA.

NLN-F DC 193: Protection System – System Description (task 2) 29/02/2012

The document is the detailed specification of the reactor Protection System. The updated version integrates information about the PSOT

Update of PCSR Chapter 7 “Control and instrumentation systems”

Draft version 31/05/2012

Final version 21/09/2012

Update of PCSR Chapter 18 “Human Machine Interface and Operational aspects”

Draft version 31/05/2012

Final version 21/09/2012

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 23 of 41

3.7 Action GI-UKEPR-CI-06.A7

Action I/D	Action Description
GI-UKEPR-CI-06.A7	<p>EDF and AREVA to justify why it is not reasonably practicable for the SICS controls to be in a functional state during normal operation.</p> <p>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.</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>

3.7.1 Deliverables already submitted to ONR/EA in response to GI-UKEPR-CI-06.A7

Following document has been provided during GDA but after the GDA Step 4 assessment phase. The document has not yet been assessed by ONR/NII.

	Date of submission
Full response to GI-UKEPR-CI.06.07 has been provided in response to action 8 of Regulatory Observation RO82 :” EDF and AREVA to justify why it is not reasonably practicable for the SICS controls to be in a functional state during normal operation. (Ref RIO2 A4.2)”. Letter ND(NII) EPR00708R	07/01/2011

3.7.2 Planned submissions in response to GI-UKEPR-CI-06.A7

All deliverables already submitted (see 3.7.1)

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 24 of 41

3.8 Action GI-UKEPR-CI-06.A8

Action I/D	Action Description
GI-UKEPR-CI-06.A8	<p>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.</p> <p>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.</p> <p>For further guidance see also T20.A5.4 and T20.A5.5 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>

3.8.1 Planned submissions in response to GI-UKEPR-CI-06.A8

3.8.1.1 Description of Scope of Work

The scope of this task is 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.

The acceptability of the achieved response times will be justified by considering:

- Requirements
- Performance
 - by design
 - by test
- Acceptability

3.8.1.2 Description of Methodology to be employed

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 from 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.

The GDA and EDF/AREVA change management processes will be used to address design changes, resulting from the work carried out.

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 25 of 41

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

The object of this task is 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.

Task 1 to GI-UKEPR-CI-06.A8 – Class 3 Terminal bus and Plant bus end-to-end response times

Resolution of this issue requires discussion of the design approach to the response times for the Class 3 Terminal bus and/or Plant bus.

The scope of work covers functions important to safety that use the Class 3 plant and terminal bus. The performance requirements specified will be identified.

The extent of existing documentation covering analysis of performance will be identified together with the design basis for predictability for Class 3 systems and the minimum and maximum response times.

The response times achieved as demonstrated by testing will be set out. The acceptability of the achieved response times will be justified.

- (1) Requirements
 - a. Functions important to safety using Plant/Terminal Bus
 - b. Specified Response times
- (2) Performance
 - a. Identified by design
 - i. Requirements for Class 3 systems
 - ii. Existing documentation
 - iii. Minimum response times
 - iv. Maximum response time
 - b. Identified by test
 - i. Existing documentation
 - ii. Minimum response times
 - iii. Maximum response time
- (3) Acceptability

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 26 of 41

- a. Acceptable required response times
- b. Management of non-conformance

A new document will be produced to set out the justification for the Class 3 Terminal bus and/or Plant bus with respect to the end-to-end response time.

It is noted that the expectation is that a demonstration that required response times are achievable is by analysis and that this is then subsequently confirmed by testing.

A schedule for ONR meetings and review cycle will be defined

3.8.1.3 Deliverable description

**Submission
date to
ONR/EA**

Class 3 Terminal bus and Plant bus end-to-end response times (task 1)

30/09/2011

This document will present a summary of existing documentation covering analysis of performance together with the design basis for predictability for Class 3 systems and the minimum and maximum response times. It will also report the response times achieved as demonstrated by testing and the acceptability of those times

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 27 of 41

3.9 Action GI-UKEPR-CI-06.A9

Action I/D	Action Description
GI-UKEPR-CI-06.A9	<p>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).</p> <p>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.</p> <p>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 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>

3.9.1 Planned submissions in response to GI-UKEPR-CI-06.A9

3.9.1.1 Description of Scope of Work

The scope of this action is to justify that sufficient diversity is implemented in the I&C architecture of the UK EPR.

This action refers to the functional diversity that needs to be implemented in the I&C architecture and is related to GDA issue GI-UKEPR-FS.02. The safety principle for diversity and independence will first be set out.

Diversity criteria will be defined to justify the reliability figures for the use of the same component in the I&C architecture for the sensor, including conditioning, and PACS.

The conclusion to this action will describe how the required diversity arrangements are implemented.

The diversity of the automation part of the I&C architecture (PS/SAS/NCSS) is covered by GI-UKEPR-CI-06.A1.

3.9.1.2 Description of Methodology to be employed

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 from specialist contractors. The work will be carried out under QA arrangements established for the GDA,

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 28 of 41

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.

The GDA and EDF/AREVA change management processes will be used to address design changes, resulting from the work carried out.

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.

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

Task 1 to GI-UKEPR-CI-06.A9 - Establish and document the safety principles applied to the I&C architecture in terms of the requirements for diversity and independence

This work will establish and explain the safety principles against which the I&C architecture is designed with respect to diversity and independence. This will be a key reference for the other tasks associated with this action, as well as other actions defined under this and other GDA Issues.

Task 2 to GI-UKEPR-CI-06.A9 - Develop and document the criteria and strategy to be applied to support the selection or development of diverse sensors or modules.

If diverse components are found to be necessary they will need to be selected from the marketplace or specially developed. Criteria will be developed and documented to inform the processes of selection and/or development of diverse sensors, pre-conditioning modules, PAC modules or relays.

Task 3 to GI-UKEPR-CI-06.A9 - Implement the required diversity arrangements.

Any identified requirements for additional component diversity will be 'implemented' within GDA by either:

- Opening Change Modification Forms (CMF) where designs have already been established and need to be modified. This is likely to apply, for example, to PIPS.
- Creating specifications and rules for the selection of components where the requirements for diversity relate to components that have not yet been selected in detail. This is likely to apply to process sensors/transmitters and PAC modules or components.

Task 4 to GI-UKEPR-CI-06.A9 – Basis of substantiation for the probabilistic claims for any I&C components used by more than one system important to safety, and/or by more than one line of protection.

Taking into account any design changes implemented or required as a result of the analysis performed in previous tasks, the basis of the detailed substantiation of probabilistic claims for any I&C

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 29 of 41

components used by more than one system important to safety and/or by more than one line of protection will be provided.

Task 5 to GI-UKEPR-CI-06.A9 – Update of PCSR

Impact on chapter 7 “Instrumentation and Control” will be addressed.

Draft version will be sent to ONR for comments.

3.9.1.3 Deliverable description

Submission date to ONR/EA

Safety Design rules for GDA UK I&C Architecture (task 1)

15/08/2011

This document will clearly explain the link between the probabilistic targets of the ONR SAPs and the deterministic design of the I&C architecture, notably to illustrate the need for diversity and independence. Additionally, the safety environment and design rules related to UK GDA I&C architecture will be defined.

Diversity criteria definition for Sensor and sensor conditioning (task 2)

31/07/2011

This document will present the criteria developed to inform the processes of selection and/or development of diverse sensors and pre-conditioning modules

Diversity criteria definition for Priority Actuation Control (PAC) module (task 2)

15/03/2012

This document will present the criteria developed to inform the processes of selection and/or development of diverse PAC modules or relays

Diversity implementation plan (task 3)

30/11/2011

This document will present the plan for implementing changes required by the diversity criteria, including specifications and rules for the selection of components where the requirements for diversity relate to components that have not yet been selected

Basis of substantiation for C&I components (task 4)

15/01/2012

This document will present the basis of the detailed substantiation of probabilistic claims for any C&I components used by more than one system important to safety and/or by more than one line of protection

PCSR Chapter 7: Control and Instrumentation

Draft version

31/05/2012

Final version

21/09/2012

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 30 of 41

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			
PCSR Chapter 7: Control and Instrumentation	U	GI-UKEPR-CI-06. A2/ A3/ A6/ A9	
Draft version			31/05/2012
Final version			21/09/2012
PCSR Chapter 18 : Man Machine Interface and operational aspects	U	GI-UKEPR-CI-06.A6	
Draft version			31/05/2012
Final version			21/09/2012
GDA reference design documents (SDM in UKEPR-I-002)			
none			
Other GDA submission supporting documents			
Justification of the diversity between SPPA T2000 S7 and TELEPERM XS platforms - <i>provided under GI-UKEPR-CI-05.A1 (task 5)</i>	C	GI-UKEPR-CI-06.A1	31/03/2012
Justification of the diversity between systems implemented using the SPPA T2000 S7 and TELEPERM XS platforms- <i>provided under GI-UKEPR-CI-05.A1 (task 4)</i>	C		30/04/2012
Justification of the diversity between NCSS and other I&C platforms - <i>provided under GI-UKEPR-CI-01.A1 (task 3 and 4)</i>	C	GI-UKEPR-CI-06.A1	15/07/2012
Justification of the diversity between systems implemented using the NCSS and other I&C platforms - <i>provided under GI-UKEPR-CI-01.A1 (task 3 and 4)</i>	C		15/07/2012

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 31 of 41

Compliance with Standards (IEC 60880 and IEC 60987)	C	GI-UKEPR-CI-06.A2	31/03/2012
Justification of PS reliability (HW, SW & FMEA reliability study)	C	GI-UKEPR-CI-06.A2	30/11/2011
Justification of T2000 v7 reliability (FMEA) -See GI-UKEPR-CI-05	C	GI-UKEPR-CI-06.A2	30/04/2012
NCSS reliability - see GI-UKEPR-CI-01	C	GI-UKEPR-CI-06.A2	30/04/2012
Independence of the Class 1 Protection System (PS), the Safety Automation System (SAS) and the Non-Computerised Safety System (NCSS)	C	GI-UKEPR-CI-06.A2	06/01/2012
Generic rule for the electrical isolation of EPR Instrumentation and Control Systems (internal connections and interfaces) ECECC100846	U	GI-UKEPR-CI-06.A2	31/07/2011
Production Excellence and Independent Confidence Building Guideline for computer based systems important to safety	C	GI-UKEPR-CI-06.A3	30/09/2011
Justification for Production Excellence and Independent Confidence Building Measures used for TELEPERM XS based systems	C	GI-UKEPR-CI-06.A3	15/11/2011
Justification for Production Excellence and Independent Confidence Building Measures used for SPPA T2000 based systems	C	GI-UKEPR-CI-06.A03	15/03/2012

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 32 of 41

MCR and RSS description - Class 1 information and controls organisation	C	GI-UKEPR-CI-06.A6	31/12/2011
Contents of Basis of Safety Case for the implementation of a Class 1 control and display facilities in MCR and RSS	C	GI-UKEPR-CI-06.A6	31/08/2011
Basis of the Safety Case and supporting documentation	C	GI-UKEPR-CI-06.A6	29/02/2012
NLN-F DC 193: Protection System – System Description	C	GI-UKEPR-CI-06.A6	29/02/2012
Class 3 Terminal bus and Plant bus end-to-end response times	C	GI-UKEPR-CI-06.A8	30/09/2011
Safety Design rules for GDA UK I&C Architecture	C	GI-UKEPR-CI-06.A9	15/08/2011
Diversity criteria definition for Sensor and sensor conditioning	C	GI-UKEPR-CI-06.A9	31/07/2011
Diversity criteria definition for Priority Actuation Control (PAC) module	C	GI-UKEPR-CI-06.A9	15/03/2012
Diversity implementation plan	C	GI-UKEPR-CI-06.A9	30/11/2011

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 33 of 41

Basis of substantiation for C&I components

C

GI-UKEPR-
CI-06.A9

15/01/2012

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

Document

NLE-F DC 222 – V&V plan for TELEPERM XS systems (GI-UKERPR-CI-06.A2/A3)

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 34 of 41

5.0 JUSTIFICATION OF ADEQUACY

Action 1

The diversity justification between SPPA T2000 S7 and the TELEPERM XS 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. This work is covered under resolution plan GI-UKEPR-CI-05.

The diversity justification between NCSS and SPPA T2000 S7 and between NCSS and the TELEPERM XS 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. This work is covered under resolution plan GI-UKEPR-CI-01

TO related to this action will be addressed as follows

- T13.TO1.04 :documents provided in response to this action will be considered in the update of CAE trail (GI-UKEPR-CI-03.A1)
- T16.TO2.21 will be addressed in GI-UKEPR-CI-06.A9
- T18.TO1.03 will be addressed in GI-UKEPR-CI-01.A1
- T18.TO1.04 and T18.TO2.09 will be addressed in GI-UKEPR-CI-05
- T20.A.1.2.3 will be addressed in GI-UKEPR-CI-06.A9
- T20.A1.3.4 will be addressed in GI-UKEPR-CI-05.A1

Action 2

The reliability justification for PS, SAS and NCSS will demonstrate that the claimed reliabilities for each of the systems are achieved. The independence justification will demonstrate that the PS, SAS and NCSS systems are sufficiently independent to support the multiplicative reliability claims made for combinations of functions implemented in the systems.

The response will include consideration of systematic and hardware failures, and compliance with appropriate guidance and standards.

Compliance of the Class 1 Protection System (PS) with standards will be assessed through a review against IEC 60880 for software and IEC 60987 for hardware. A justification of the PS reliability (HW, SW & FMEA reliability study) will be undertaken. This will cover random failure assessment, FMEA, reliability analysis and a systematic failure assessment.

The programme of Independence Confidence Building Measures (ICBMs) to support the safety case for the TXS Protection System will be addressed under GI-UKEPR-CI-02.

Compliance of the Class 2 NCSS with standards will be assessed and a justification of the NCSS reliability (HW, FMEA reliability study) will be undertaken. This will cover random failure assessment, FMEA, reliability analysis and a systematic failure assessment. These activities are covered under GI-UKEPR-CI-01 – Non-Computerised Safety System.

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 35 of 41

Compliance of the Class 2 SPPA T2000 with standards will be assessed through a review against IEC 62138 for software and IEC 60987 for hardware. A justification of the SPPA T2000 reliability (HW, SW & FMEA reliability study) will be undertaken. This will cover random failure assessment, FMEA, reliability analysis and a systematic failure assessment. These activities are covered under GI-UKEPR-CI-05 – SPPA T2000 Obsolescence.

TO related to this action will be addressed as follows

- T16.TO2.21 will be addressed in GI-UKEPR-CI-06.A9
- T20.A.1.4.1 and T20.A.1.4.2 are addressed in the resolution plan of action 2

Action 3

EDF and AREVA will demonstrate Production Excellence for Computer based Systems Important to Safety and will apply Independent Confidence Building Measures to give confidence that claimed reliabilities have been achieved.

The production excellence and independent confidence building measures for the TELEPERM XS based protection system (PS) have already been transmitted during GDA. Additional independent confidence building measures for the PS are addressed by the response to GI-UKEPR-CI-02.

The demonstration of production excellence and independent confidence building measures for all Computer Based Systems Important to Safety (CBSIS) will be based on guidance derived from standards and international practice.

This includes TAG 46 which is a high level technical assessment guide addressing the UK Safety Assessment Principles applying to computer based safety systems.

It also considers the relevant guidance provided in international standards and reports including:

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

BS IEC 61226:2009. Nuclear power plants - Instrumentation and control systems important to safety – Classification of instrumentation and control functions.

IEC 60880:2006. Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions.

IEC 61513:2001. Nuclear power plants - Instrumentation and control systems important to safety – General requirements for systems.

Production excellence and independent confidence building measures appropriate to different system classes and the reliability claims will be used. This will ensure that the safety demonstration for each CBSIS is appropriate for the system class and claimed reliability.

TO related to this action will be addressed as follows

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 36 of 41

- T20.A.1.4.1 a) is addressed in the resolution plan of action 3
- T20.A1.5.1 is addressed in the resolution plan of action 3

Action 4

This action has been addressed by the transmission of revision B of the Protection System description which reflects the current design of the UK EPR I&C. Detailed justification of the few remaining Hardwired links is to be provided in NSL.

This response also addresses the following TO:

T17.TO1.04, T20.A2.2.1 and T20.A2.2.3

Action 5

Justification of independence between PICS and SAS has been provided in response to this action.

This response also addresses T20.A.2.3.2

Action 6

An overview of the current status of the class 1 information and controls available on SICS has been transmitted to ONR/NII during GDA in response to TQ1130 but after the GDA Step 4 assessment phase.

This resolution path will define and justify the UK EPR specific class 1 information and controls available on SICS (in the MCR) and on the Protection System Operating Terminal (PSOT) which is to be implemented in the MCR and the RSS (based on AREVA's QDS platform).

A preliminary list of class 1 information and controls to be implemented on SICS and PSOT will be presented and the corresponding functional coverage justified

A basis of safety case for the new class 1 system, PSOT, will be provided as a separate deliverable and will justify its functional and safety adequacy.

This resolution plan also addresses the following TO

T16.TO1.03; T17.TO1.14, T17.TO1.15, T17.TO2.16, and T20.A3.6

Action 7

Justification of the non practicability of SICS in operation when PICS is in operation has been provided in the response to this action.

Action 8

UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR-CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 37 of 41

The GDA issue deliverable will justify the design approach and response times for the Class 3 networks and their acceptability. The justification will identify the performance requirements and the demonstrations that the requirements are met. The justification will be produced in line with current guidance and standards appropriate to performance requirements and testing in safety related systems.

This response also addresses the following TO:

T20.A5.4 and T20.A5.5

Action 9

EDF and AREVA will justify and demonstrate that sufficient diversity is implemented in the I&C architecture of the UK EPR.

The potential for Common Cause Failure of I&C components will be considered in the protection system channels, in the Safety Automation System channels and in the NCSS channels from sensors to actuation signals (excluding the actuators).

Any identified potential reliability shortfall due to the use of shared or common components will be addressed.

The justifications will be produced in line with current guidance and standards appropriate to Common Cause Failure in systems important to safety.

This response also addresses the following TOs:

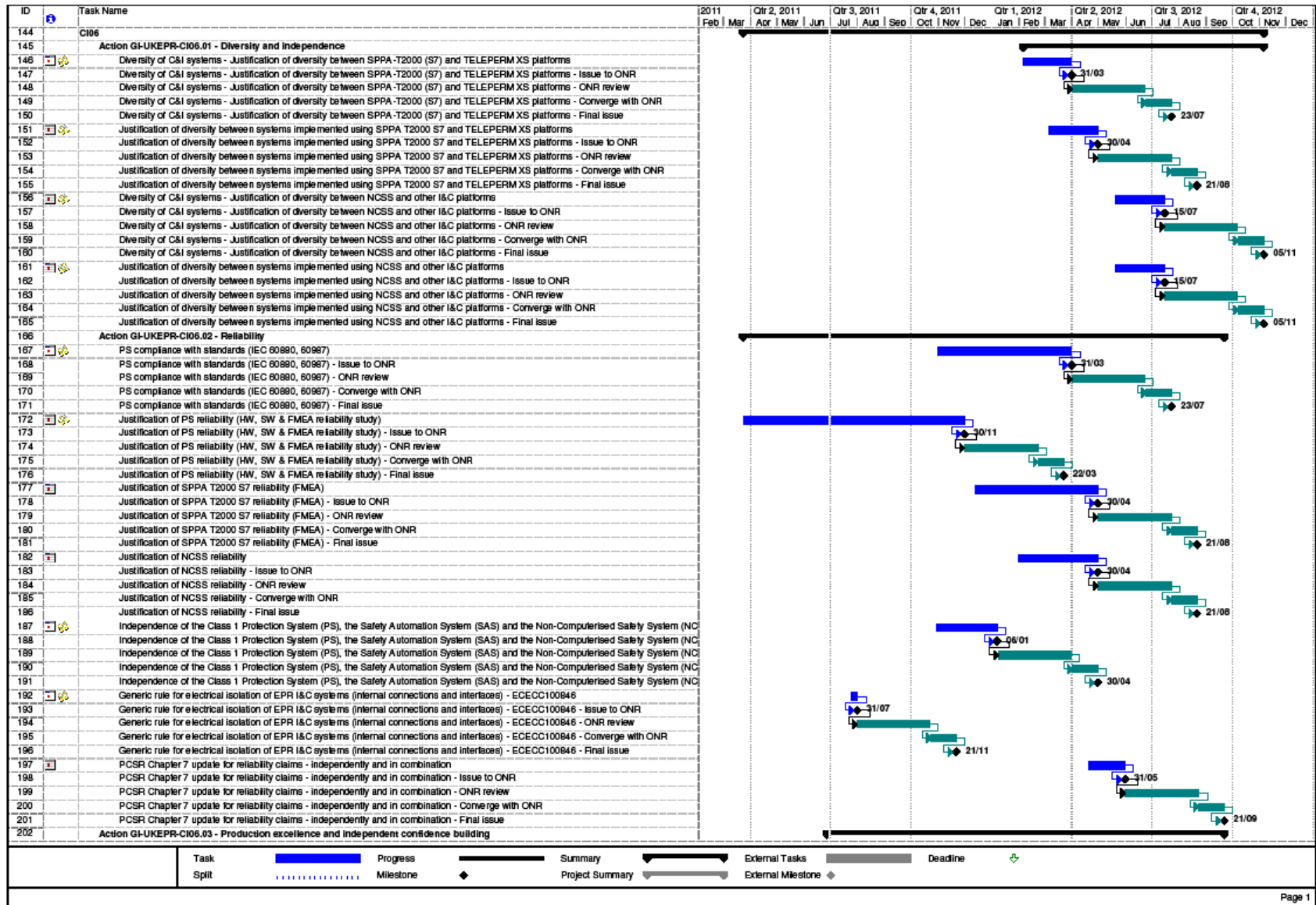
T17.TO2.07, T17.TO2.08, T18.TO1.02, T18.TO1.05, T18.TO2.06, T20.A1.3.1 a), T20.A1.3.5, and T16.T02.21.

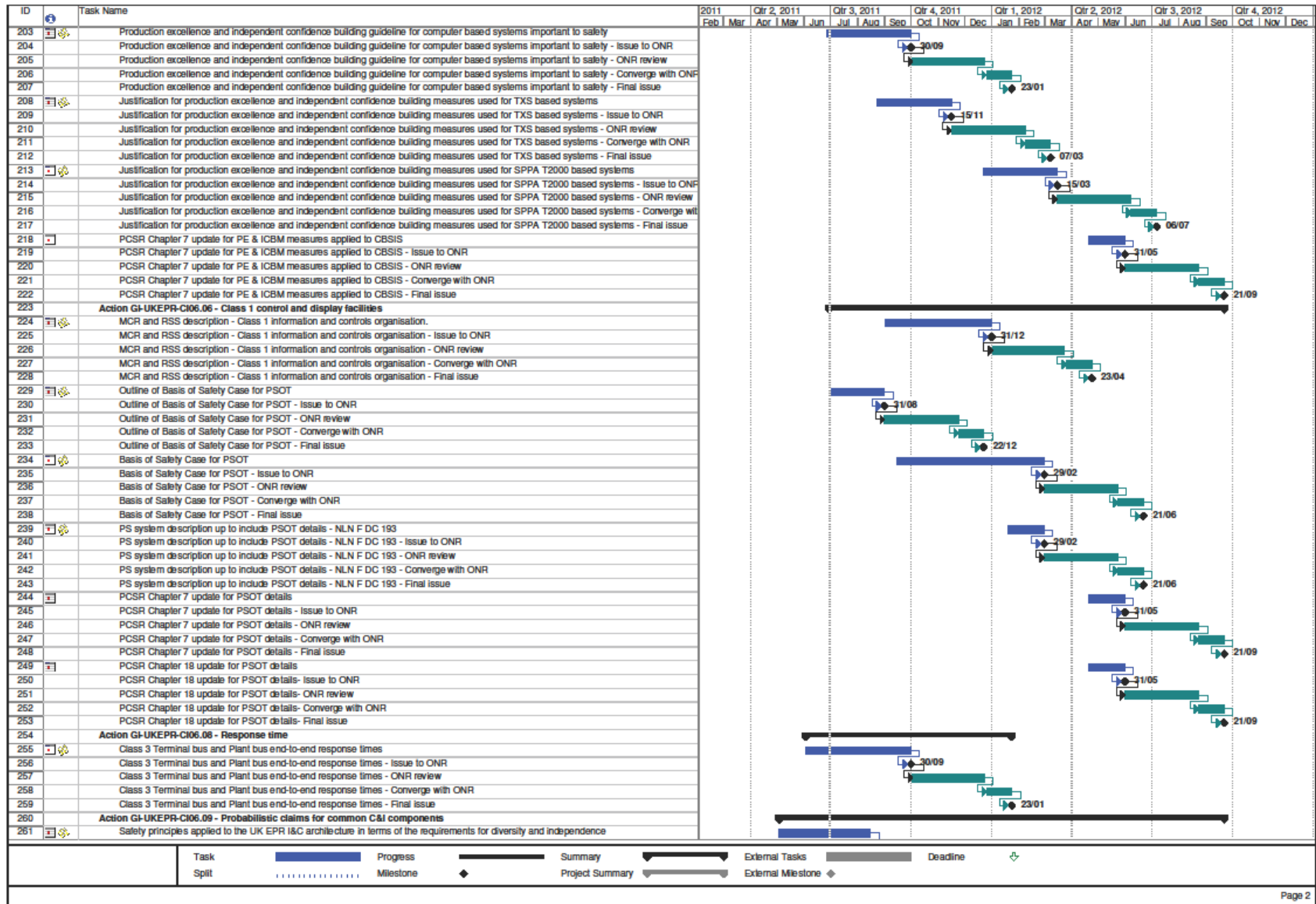
T17.TO2.28 and T20.A.1.3 1 b) are related to PSA modelling and are to be addressed in this Topic group during NSL.

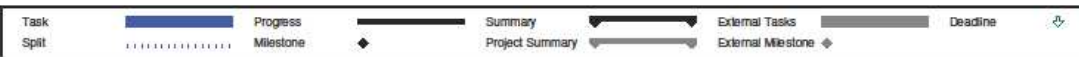
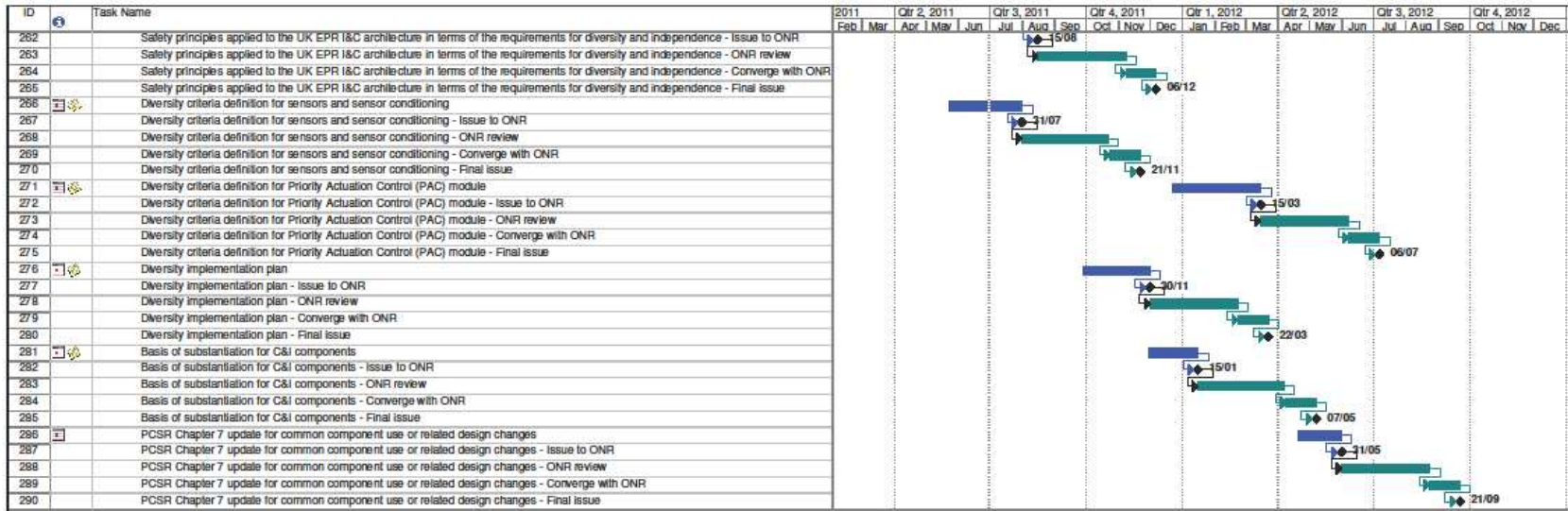
UK EPR	UK EPR GDA PROJECT			
	Title: Resolution Plan for GI-UKEPR- CI-06			
	GI unique number: GI-UKEPR-CI-06-RP	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 38 of 41

6.0 TIMETABLE AND MILESTONE PROGRAMME LEADING TO THE DELIVERABLES

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







C