UK EPR	**UK EPR GDA PROJECT**			
	Title: Resolution Plan for GI-UKEPR-CI-02			
	RP unique number: **GI-UKEPR-CI-02-RP**	Revision No.: 0	Effective Date: 30/06/2011	Page No.: 1 of 14
Approved for EDF by: A. PETIT *Name/Initials* *Date* *30/06/2011*		Approved for AREVA by: C. WOOLDRIDGE *Name/Initials* C.Wooldridge *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
Protection System Independent Confidence Building Measures	C&I	None

GDA Issue	The programme of Independent Confidence Building Measures (ICBMs) to support the safety case for the TXS Protection System to be fully defined and agreed.

2.0 OVERVIEW OF SCOPE OF WORK

This work relates to the programme of Independent Confidence Building Measures to be applied to the Class 1 Protection System (PS), in particular in the areas of Statistical Testing (ST), Static Analysis and Compiler Validation.

a) Statistical Testing

There is an ONR expectation that 50000 statistically-based tests will be performed on the PS but the current project proposal is for 5000 tests to be performed on a TELEPERM XS (TXS) platform, with the possibility of performing 50000 tests on a simulator to be investigated as a research activity. Present work is to analyse the number of tests that can be performed with reasonable practicability on a TXS platform.

In order to support future activities, a research task will also be defined for the investigation of the use of TXS platform simulation techniques in future statistical testing activities.

b) Static Analysis

An initial feasibility study has indicated that the MALPAS technique is viable for use with the PS application code but further work is required to ensure the technique is scaleable and applicable to the full scope of the code.

c) Compiler Validation

A feasibility study is underway to evaluate whether Source-to-Code Comparison techniques (as used for the Sizewell B Primary Protection System) can be used to validate the compiler used for TXS. Alternative means to validate the compilers are also under investigation, but Source-to-Code Comparison is the preferred option.

The results from these studies and analyses will provide further enhancement to the Protection System safety case. Accordingly, the approaches identified above constitute specific Independent Confidence Building Measures which can effectively be applied to the UK EPR Protection System in addition to the more general measures described in GI-UKEPR-CI-06.A3.

3.0 GDA ISSUE ACTIONS AND RESOLUTION PLAN DELIVERABLES

3.1 Action GI-UKEPR-CI-02.A1

Action I/D	Action Description
GI-UKEPR-CI-02.A1	The programme of Independent Confidence Building Measures to support the safety case for the TXS Protection System to be fully defined and agreed. The proposed elements that will constitute the ICBMs are: • Statistical testing (ST) EDF and AREVA have proposed 5000 tests on the TXS equipment with the potential for 50000 on a simulator to be investigated as a research activity. ONR expects the RP to more fully define the ST approach in terms of number of tests. The RP is required to submit its analysis of the number of tests that it considers is reasonably practicable to undertake having given full consideration to any time and programme constraints. It remains ONR's expectation that 50,000 tests will be performed. ONR considers that the plant transients are sufficiently defined to allow a reasonably accurate definition of the time to undertake the tests to be established. Undertaking this analysis will give good guidance to the site specific programmes sufficiently early in the process to ensure that adequate time can be given to the statistical testing process without causing delays to the plant going into operation. In addition the RP needs to demonstrate, by the provision of a monitorable programme, that all of the activities required to implement ST have been defined and can be delivered to a timescale which allows ST to commence following completion of Factory Acceptance Testing of the PS (i.e. the final validation activity before the equipment is shipped to site). It should be noted the ICBM activities should be undertaken on the final version of the software (i.e. following the end of the software production process – see ONR TAG 46). The activities required to undertake ST are defined in a report produced by CINIF (Ref. Further development of Dynamic Testing 2 – Phase 2 (NewDDT2-3 PP/40115457/MB – Guidelines on Statistical Testing for logic or Software Elements used in Nuclear Safety Related Systems.) • Static analysis The feasibility and full extent of the application of MALPAS analysis to the Protection System application code needs to be confirmed. To date the RP has reported that it has undertaken a feasibility study which indicates that the technique is viable but the RP has stated that further work is required to ensure the technique is scaleable and applicable to the full scope of the PS application code. • Compiler validation. With regard to compiler validation, ONR is aware that the RP is considering a number of options from a Sizewell B type Source to Code Comparison to running a compiler validation test suite (along the lines of an approach developed by NPL). The ICBM approach (Scope, depth and rigour) for each of the above needs to

	be fully defined before ONR can come to a conclusion on the adequacy of the safety case for the Protection System. Currently there are too many elements that have not been fully defined and as a result further work will be required to confirm the adequacy of the proposed ICBMs, or alternative means agreed by the Regulator. For further guidance see also T16.TO2.09 in Annex 6 and T15.TO2.07, T15.TO2.18 and T15.TO2.19 in Annex 5 of Step 4 C&I Division 6 Assessment Report, No. 11/022 Revision A (Draft).

3.1.1 Deliverables already submitted to ONR/EA in response to GI-UKEPR-CI-02.A1

The documents below are relevant to this GI Action. They were submitted in response to RI-UKEPR-02 and RO-UKEPR-58.

	Date of submission
PEICBM for the UK EPR ENSECC090137B (RI-UKEPR-02.A1.5) - via ND(NII) EPR00459R *Describes current and proposed Production Excellence measures and Independent Confidence Building Measures for the Protection System and Safety Automation System*	30/06/2010
Position Paper – TELEPERM XS Functional Static Analysis Study (RI-UKEPR-02.A1.5) - via ND(NII) EPR00628N *This position paper describes the work in progress to evaluate the application of the NARPS (A study for the UK C&I Nuclear Industry Forum (CINIF)) approach to functional static analysis to the UK-EPR protection system.*	26/10/2010
Position Paper – TELEPERM XS Compiler Validation Study (RI-UKEPR-02.A1.5) - via ND(NII) EPR00685N *This position paper describes the work proposed to determine the approach to Compiler Validation for the TXS based UK-EPR protection system and allows a programme of work to be established in the context of 'independent confidence building'*	7/12/2010
Proposed approach for statistical testing for TELEPERM XS protection system for UK EPR (RO-UKEPR-58) - via ND(NII) EPR00595R *Reports the EDF/AREVA investigation of the possibility of carrying out a programme of statistical testing for the UK-EPR Protection System and following discussions with ONR determined that a testing approach using a testing of one division of hardware with three simulated divisions should be adopted together with further research to assess the practicability and limitations of testing using a simulation approach of the PS is under consideration.*	18/10/2010

3.1.2 Planned submissions in response to GI-UKEPR-CI-02.A1

3.1.2.1 Description of Scope of Work

The programme of Independent Confidence Building Measures will support the safety case for the TXS Protection System

The main elements that constitute the Independent Confidence Building Measures are statistical testing, static analysis and compiler validation. The Independent Confidence Building Measure approach (scope, depth and rigour) will be fully defined so that ONR can come to a conclusion on the adequacy of the safety case for the PS

3.1.2.2 Description of Methodology to be employed

The action is divided into several tasks as described below.

The following standards and guidelines are to be considered during performance of the tasks:

IEC 61513, IEC60880, IEC61226, IEC62138, IEC60987, NII TAG46

Documents affected (created or updated) by these tasks are listed in the following section 3.1.2.3.

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 - Statistical Testing - Definition of outline programme of statistical testing activities

This work will focus on the development of the arguments to address the number of tests that are reasonably practicable to perform, and establishing an outline programme for delivering the PS statistical testing.

The Analysis of the reasonable practicability of increasing the number of tests, will evaluate the time required to carry out a typical statistical test, as follows:

- Consider the typical plant transients to model, and length of time required to ensure Reactor Trip and appropriate Engineered Safety Features Actuation (ESFAS) have occurred (Sizewell transients modelled for PPS statistical testing will be used to inform this evaluation);

- Consider time delays within the TXS platform and Protection System (PS) functional application, which could impact test duration. Identify if time delay modifications will be required on the test platform (as was the case for Sizewell B) to allow test cases to be executed in a ‘reasonable’ timescale;

- Establish form of a typical test case, to include a ‘plant transient’ element, and ‘stable state/reset’ element;

- Review other functional aspects/performance aspects of the PS, which could have an impact on the ‘independence’ of successive tests, e.g. the use of digital filters in the system, and determine a time delay to allow the protection system to reach an established ‘stable state’ between tests;

- Determine any reset or permissive requirements required to re-establish normal stable operation at the start of each test.

The above elements will allow a ‘typical’ test case length to be established, to be used in the analysis of the number of tests possible.

An ‘outline’ design of the ‘statistical test system’ will have to be developed, to allow an estimate of the development work required to establish, a viable test system. (This will draw on the UK experience of Sizewell B and other statistical test programmes). This will need to consider the interface with the PS Test Platform, including how other PS divisions will be modelled, the design of an ORACLE, and the extent of automation of testing. The ‘conduct of statistical testing’ and the availability of sources of plant transient data will also need to be considered. Reference will be made to the CINIF report “Guidelines on Statistical Testing for logic or Software elements used in Nuclear Safety Related Systems”.

With the above information an outline programme of testing will be established based on:

- The time required to develop and commission a ‘statistical test system’;

- The time required to develop appropriate plant transient data;

- The delivery and installation of the PS Test Platform at a suitable location to support testing;

- The delivery of validated PS software, post Factory Acceptance Test;

- Estimated time required to execute 5,000 ‘typical tests’, reconciled to key hold points;

- Consideration of time required for other use of the PS Test Platform, e.g. operator training;

- Analysis to show incremental time required to carry out up to total of 50,000 tests on a ‘once-off’ basis, and reconcile to key plant hold points.

This analysis will allow investigation of the cost, time and trouble of an increase from 5000 to 50000 tests to assess and develop the arguments of ‘reasonable practicability’.

A programme will be developed to show all the activities required to implement the PS statistical testing activities.

The activities will include a justification of choice of PS Test Platform and of its ability to adequately represent all the PS divisions.

An approach to the requirements for statistical testing of subsequent software versions will be developed. This will consider the arguments of reasonable practicability and it is envisaged that a qualitative argument for restricting the number of statistical tests for future PS software builds will be developed as part of this work.

Task 2 - Statistical Testing - Scope of research task to investigate issues associated with use of simulation techniques in place of the TXS platform.

A proposal will be developed for a research task to investigate the use of PS platform simulation for statistical testing and to consider arguments to justify this approach to statistical testing as an alternative to the use of a TXS hardware platform. The proposal will define the parties to be involved – expected to be EDF R&D and Bristol University – and the basis on which the task will be managed.

Task 3- Static Analysis - Provide initial proposal of scope of PS software MALPAS analysis work and outline programme.

Activities will include, a scoping study which will consider the following issues, to allow development of an outline plan to deliver the MALPAS work:

- The extent of the TXS application code and system code associated with the Cat A reactor protection functionality to be included in the analysis. Where MALPAS analysis is not practicable or the code is outside of the Cat A reactor protection functionality, alternative ICBM approaches will be proposed. This should help with sizing the overall task, and in the generation of resource and associated cost estimates;

- Development of a resource plan to confirm the capability of the current supply chain to deliver the work. In addition, it will have to consider how the MALPAS tool and support can be maintained to provide on-going support in the future;

- Provide clarity on an optimised work programme e.g. analysis first of Function Blocks, which is expected to be the most difficult part of the overall analysis effort.

Task 4 - Compiler Validation - Feasibility report and recommended technical approach.

Tools were developed by British Energy to validate the software Build Tools used on the Sizewell B Primary Protection System (PPS), a process known as “Source to Code Comparison” (SCC). This process modelled both the source code (written in PL/M-86) and a disassembled version of the target machine code in MALPAS Intermediate Language. The MALPAS Semantic Analyser was then used to provide functional representations of small code fragments, and the Compliance Analyser used to prove that the code fragments are functionally equivalent. The SCC process was applied to all of the

PPS software, with the exception of the lower criticality Autotester modules.

A feasibility study is underway to evaluate whether Source to Code Comparison can be used to validate the compiler (and associated linker and locator) used for TXS. Based on a small use case (application) software and a small system software extract, feasibility and cost estimate (metrics) will be established for:

Step 1: Back translation = use/adaptation of BE built tools.

Step 2: Feasibility of MALPAS based semantic and compliance analysis to prove the equivalence between the C source code and the disassembled machine code

Additionally the practicability of compensatory arguments will be investigated, based on the use of a compiler validation test suite and stress testing, to provide an alternative approach if the use of Source to Code Comparison techniques are demonstrated to be not technically feasible for TXS code.

The final deliverables from the work will be a report describing the results from the feasibility study, with recommendations regarding the proposed technical approach to the work.

Task 5 - Compiler Validation - Provide an initial proposal on the scope and outline programme of work to address ‘compiler validation’.

Based on the output of Task 4 above an outline programme will be developed to identify the proposed technical scope, timescales and milestones.

Task 6 - Report of Overall Scope of TXS PS Independent Confidence Building Measures and justification of adequacy.

A report will provide an update of all the proposed Independent Confidence Building Measures for the TXS PS, including the progress made to date on the items described above and the balance of tasks that are considered to constitute Independent Confidence Building Measures as described in the output of GI-UKEPR-CI-06.A3, e.g. independent assessment of application code and of the testing programme. This report will summarise the overall position for PS Independent Confidence Building Measures and provide a justification for their adequacy.

Task 7 – Update of PCSR.

PCSR Sub-chapter 7.7 “I&C tools, development process and substantiation” will be updated taking due account of the output of the other tasks. Details of the proposed Production Excellence approach and Independent Confidence Building Measures are given in this Sub-chapter.

PCSR Sub-chapters 7.1, 7.2 and 7.3 will be reviewed and updated if required.

A draft version will be sent to ONR for comments.

3.1.2.3 Deliverable description

	Submission date to ONR/EA
Programme of statistical testing activities (task 1)	30/11/2011
This document includes statements of assumptions and pre-conditions and the outline programme for all the tasks required to develop the test system and complete a set of tests.	
Research task proposal – Use of a platform simulation approach for statistical testing of protection systems (task 2)	31/10/2011
This document defines the purpose and scope of the task, the parties to be involved – expected to be EDF R&D and Bristol University – and how the task will be managed.	
Static Analysis - scope of PS software MALPAS analysis work and outline programme (task 3)	31/10/2011
This document defines the purpose and scope of the task and the outline programme.	
Compiler Validation – Feasibility study and technical proposal (task 4)	31/08/2011
This document describes the results from the feasibility study and make recommendations regarding the proposed technical approach to the compiler validation task	
Compiler Validation - scope and programme of work to address ‘compiler validation’ (task 5)	31/10/2011
This document presents an outline programme to identify the proposed technical scope, timescales and milestones	
Protection System – Summary and justification of proposed Independent Confidence Building Measures (task 6)	31/12/2011
This document presents the summary and justification of all the proposed Independent Confidence Building Measures for the TXS PS, including progress to date and future activities	
Pre-construction safety report - Chapter 7 (task 7)	
Sub-chapter 7.7 “I&C tools, development process and substantiation” will be updated to reflect the agreed Independent Confidence Building Measures for the Protection System	
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			
Pre-construction safety report – Sub-chapter 7.7 "I&C tools, development process and substantiation"	U	GI-UKEPR-CI-02.A1	
Draft version			13/07/2012
Final version			05/11/2012
GDA reference design documents (SDM in UKEPR-I-002)			
None			
Other GDA submission supporting documents			
Programme of statistical testing activities	C	GI-UKEPR-CI-02.A1	30/11/2011
Research task proposal – Use of a platform simulation approach for statistical testing of protection systems	C	GI-UKEPR-CI-02.A1	31/10/2011
Static Analysis - scope of PS software MALPAS analysis work and outline programme	C	GI-UKEPR-CI-02.A1	31/10/2011
Compiler Validation – Feasibility study and technical proposal	C	GI-UKEPR-CI-02.A1	31/08/2011
Compiler Validation - scope and programme of work to address 'compiler validation'	C	GI-UKEPR-CI-02.A1	31/10/2011

Protection System – Summary and justification of proposed Independent Confidence Building Measures	C	GI-UKEPR-CI-02.A1	31/12/2011

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

none

5.0 JUSTIFICATION OF ADEQUACY

This scope and content of this work has been the subject of ongoing discussion with ONR during the GDA process and is informed by the guidance provided in TAG46 as well as the approach taken at Sizewell B, which is considered to be the reference for good practice in the UK.

TAG 46 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.

The work has been divided into various tasks that aim to progress, assess practicability and justify the approaches already proposed and to investigate the feasibility of the potential alternative approaches. The first step is to define the scope of the tasks to assess each of the Independent Confidence Building Measures and prepare the programmes needed to complete them.

Tasks 1 to 3 and 5 will perform the assessments and produce the justifications, proposals and programmes. Task 4 is the feasibility study for the compiler validation Independent Confidence Building Measure and is a prerequisite for task 5.

Task 6 is the final justification and reporting task that will provide the formal input to enable issue GI-UKEPR-CI-02 to be resolved.

The output of these tasks will provide a thorough independent justification of the Protection System.

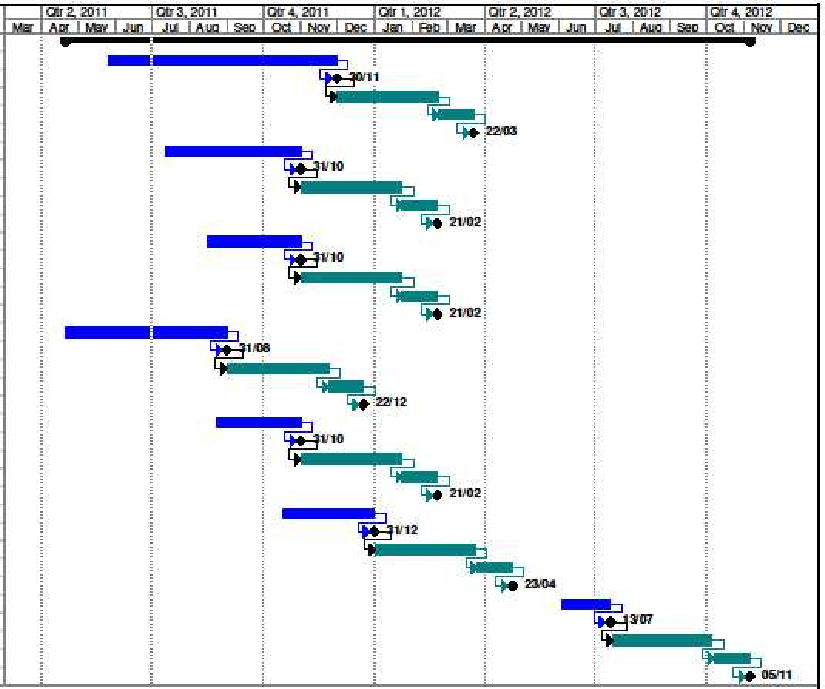
Task 7 is the necessary final task to update Chapter 7 of the PCSR to reflect the proposals made. The main changes will be in Sub-chapter 7.7 and the overview Sub-chapters and Class 1 systems Sub-chapter will be reviewed to determine if any of the resolutions impact them.

At each significant stage during the process, following internal reviews, proposals will be presented to the ONR to confirm that they are also satisfactory from the licensor’s viewpoint.

6.0 TIMETABLE AND MILESTONE PROGRAMME LEADING TO THE DELIVERABLES

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

ID		Task Name
36		**CI02**
37		Programme of statistical testing activities
38		Programme of statistical testing activities - Issue to ONR
39		Programme of statistical testing activities - ONR review
40		Programme of statistical testing activities - Converge with ONR
41		Programme of statistical testing activities - Final issue
42		Research task proposal - Platform simulation approach for ST of PS
43		Research task proposal - Platform simulation approach for ST of PS - Issue to ONR
44		Research task proposal - Platform simulation approach for ST of PS - ONR review
45		Research task proposal - Platform simulation approach for ST of PS - Converge with ONR
46		Research task proposal - Platform simulation approach for ST of PS - Final issue
47		Static Analysis - scope of PS software MALPAS analysis work and outline programme
48		Static Analysis - scope of PS software MALPAS analysis work and outline programme - Issue to ONR
49		Static Analysis - scope of PS software MALPAS analysis work and outline programme - ONR review
50		Static Analysis - scope of PS software MALPAS analysis work and outline programme - Converge with ONR
51		Static Analysis - scope of PS software MALPAS analysis work and outline programme - Final issue
52		Compiler Validation – Feasibility study and technical proposal
53		Compiler Validation – Feasibility study and technical proposal - Issue to ONR
54		Compiler Validation – Feasibility study and technical proposal - ONR review
55		Compiler Validation – Feasibility study and technical proposal - Converge with ONR
56		Compiler Validation – Feasibility study and technical proposal - Final issue
57		Compiler Validation - Scope and programme of work to address 'compiler validation'
58		Compiler Validation - Scope and programme of work to address 'compiler validation' - Issue to ONR
59		Compiler Validation - Scope and programme of work to address 'compiler validation' - ONR review
60		Compiler Validation - Scope and programme of work to address 'compiler validation' - Converge with ONR
61		Compiler Validation - Scope and programme of work to address 'compiler validation' - Final issue
62		Protection System – Summary and justification of proposed ICBMs
63		Protection System – Summary and justification of proposed ICBMs - Issue to ONR
64		Protection System – Summary and justification of proposed ICBMs - ONR review
65		Protection System – Summary and justification of proposed ICBMs - Converge with ONR
66		Protection System – Summary and justification of proposed ICBMs - Final issue
67		PCSR Chapter 7.7 Update for agreed PS ICBM
68		PCSR Chapter 7.7 Update for agreed PS ICBM - Issue to ONR
69		PCSR Chapter 7.7 Update for agreed PS ICBM - ONR review
70		PCSR Chapter 7.7 Update for agreed PS ICBM - Converge with ONR
71		PCSR Chapter 7.7 Update for agreed PS ICBM - Final issue



Task	▬	Progress	▬	Summary	▬	External Tasks	▬	Deadline	⇩
Split	┈	Milestone	◆	Project Summary	▬	External Milestone	◆		