 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0059	Rev.: 0	Page: 1 / 14
			GDA-REC-GNSL-008599

REGULATORY OBSERVATION Resolution Plan

RO Unique No.:	RO-UKHPR1000-0059
RO Title:	Evidence of Production Excellence for the FirmSys Platform
Technical Area(s)	Control & Instrumentation
Revision:	Rev 0
Overall RO Closure Date (Planned):	2021-07-30
Linked RQ(s)	RQs (930/ 959/ 960/ 1000/ 1096/ 1116/ 1117/ 1169/ 1170/ 1268/ 1269/ 1360/ 1399)
Linked RO(s)	
Related Technical Area(s)	3. Control & Instrumentation
Other Related Documentation	


Scope of Work

Background

In the UK nuclear industry, there is a particular focus on the use of Computer Based Systems Important to Safety (CBSIS), whose safety demonstration is expected to use a two-legged approach, i.e. Production Excellence (PE) and Independence Confidence Building Measures (ICBMs), with reference to the Safety Assessment Principle (SAP) ESS.27, Reference [1], and NS-TAST-GD-046, Reference [2]. The PE leg is required to demonstrate high quality system production, which is largely achieved by the supplier by adopting appropriate practices for the development of the system.

To satisfy the requirements of Generic Design Assessment (GDA) Step 4, and to remain consistent with previous GDAs, ONR sought to sample detailed evidence regarding the processes used in the design and development of the FirmSys platform to confirm that PE can be demonstrated, as this forms the basis for both the Class 1 Protection System (RPS [PS]) and Class 2 Safety Automation System (SAS).

ONR identified 10 shortfalls from the PE evidence available. Moreover, ONR pointed out that there may be

	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0059	Rev.: 0	Page: 2 / 14
		GDA-REC-GNSL-008599	

other shortfalls in the PE demonstration associated with other aspects of the FirmSys platform.

ONR's expectations for this demonstration of adequacy of the PE evidence for the FirmSys platform are described in NS-TAST-GD-046, Reference [2] and the SAP ESS.27, Reference [1]. The FirmSys platform is the basis of the implementation of the F-SC1 classified RPS [PS] system and relevant good practice, including international nuclear standards, will be applied to demonstrate PE.

ONR expects that gaps in the PE evidence are adequately identified, and suitable compensating measures are proposed in order to provide the necessary confidence that risks are being adequately managed.

Scope of Work

The resolution plan (RP) will perform the following activities to address this RO:

- Assessment of the PE for the FirmSys platform, including the identification of the potential gaps;
- Identification and justification of appropriate compensating measures to address these gaps;
- Development of a strategy for undertaking the compensating measures.

To address this RO, the following document will be developed:

- The *Assessment Report of Production Excellence for FirmSys Platform*, Reference [3], will be produced to describe the assessment process, identified gaps, and compensating measures with the strategy and relevant justifications.


Deliverable Description

RO-UKHPR1000-0059.A1 – Identification of shortfalls in production excellence

The RO action states that:

In response to this RO Action, the RP should present evidence to address the following, as a minimum:

- Review the FirmSys documentation, as appropriate, to identify and recognise the significance of shortfalls in production excellence, including, but not limited to, those shortfalls identified in the background section of this RO. Of particular significance are the following:
 - Comparison of existing practices with the requirements for platform development arising from relevant international standards and guidance for production excellence and UK regulatory expectations;
 - Identification of potential sources of requirements, including those arising from potential internal

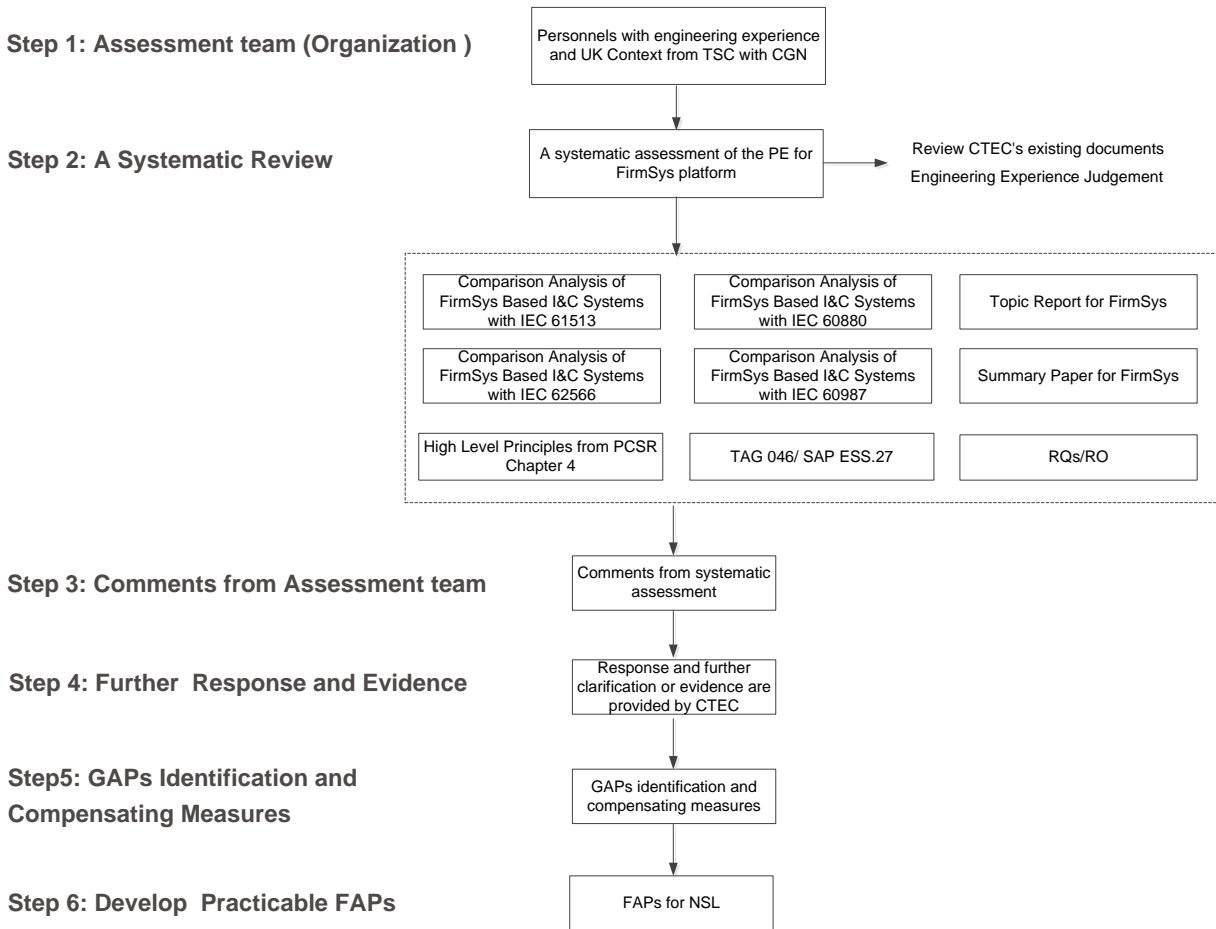
	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0059	Rev.: 0	Page: 3 / 14
			GDA-REC-GNSL-008599

faults that could lead to an unsafe condition;


- Assessment of the adequacy of existing design principles;
- Management of requirements including relevant processes to control iterative design, implementation and integration;
- Application of suitable techniques and measures for adequate verification for each lifecycle stage.

Resolution Plan

The identification of shortfalls in the PE will be implemented by establishing an assessment team made up of CGN, CTEC, GNSL and third-party personnel with engineering experience and understanding of the UK regulatory context (Technical Support Contractor (TSC)) to review the PE evidence. F-1 describes the methodology of PE Assessment for FirmSys platform.



Methodology of PE Assessment for the FirmSys Platform

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0059	Rev.: 0	Page: 4 / 14
		GDA-REC-GNSL-008599	

The methodology is further described as follows:

Step 1 – Assessment team


Establish an assessment team including representatives of CGN, CTEC, GNSL and TSC. The assessment team will be responsible for reviewing the PE, answers and documents provided by CTEC and for identifying the gaps and drawing up the compensating measures.

Step 2 – A systematic review

A systematic evaluation of the PE for the FirmSys platform will be performed by the assessment team in order to provide a judgement on whether relevant good practice is followed, review the shortfalls identified by ONR and determine any additional shortfalls. The starting point of this review will be to consider CTEC's compliance analysis reports against IEC standards, and any clauses from the standards omitted in these reports will be justified. These reports reflect the manufacturer's considerations of how compliance with relevant international standards is achieved. The assessment team will challenge the answers given by CTEC and will provide further assessment and scrutiny of these responses in the "question-answer" format. This will subsequently lead on to areas of deeper assessment of other evidence documents.

CTEC will make an evidence pack available to the assessment team as a baseline, the documents involved are (but not limited to) as follows:

- Topic Report of FirmSys Platform, Reference [4];
- FirmSys Platform Compliance Analysis with IEC61513, Reference [5];
- FirmSys Platform Compliance Analysis with IEC60987, Reference [6];
- FirmSys Platform Compliance Analysis with IEC60880, Reference [7];
- FirmSys Platform Compliance Analysis with IEC62566, Reference [8];
- Demonstration of Production Excellence for FirmSys Platform, Reference [9];
- Product Excellence Summary Paper for CPLD-Based Watchdog Circuit of FirmSys, Reference [10];
- Product Excellence Summary Paper for the HNU DP-RAM Circuit of FirmSys, Reference [11];
- Product Excellence Summary Paper for Software Self-diagnostics Function of FirmSys, Reference [12];
- RQs (930/959/960/1000/1096/1116/1117/1169/1170/1268/1269/1360/1399), Reference [13] ~ Reference [26], related with FirmSys platform PE;
- S.P1893.42.7 Notes for L4 Workshop, Reference [26];

 <p>REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0059</p>	Rev.: 0	Page: 5 / 14
	GDA-REC-GNSL-008599	


- Pre-Construction Safety Report Chapter 4 General Safety and Design Principles, Reference [27];
- NS-TAST-GD-046, Reference [2];
- Procedures and development documents by CTEC.

The assessment team is free to ask further questions in any area and are not restricted by the previous compliance analysis responses.

Specifically, in Step 2 (as well as Steps 3, 4 & 5), ONR’s findings in this RO will be analyzed and managed by following the approach in Table T-1.

T-1 The Approach Corresponding to ONR’s Findings

ONR’s Findings in this RO	Approach
Comparison of existing practices with the requirements for platform development arising from relevant international standards and guidance for production excellence and UK regulatory expectations	Existing practices will be reviewed during steps 2-4 of the methodology. The review will be based on IEC nuclear standards, as described above, as well as UK regulatory expectations provided in the SAPs, Reference [28] and NS-TAST-GD-046, Reference [2].
Identification of potential sources of requirements, including those arising from potential internal faults that could lead to an unsafe condition	The standards considered in step 2 include consideration of potential sources of requirements, including, for example, results of reliability analysis, human factors assessments, and performance requirements. The systematic review (step 2) and the following steps will consider any potential sources of requirements that might have been overlooked and will identify compensation measures, as required (step 5).
Assessment of the adequacy of existing design principles	IEC 61513 requires that systems are designed using a structured approach that takes into account overarching design principles, including, for example,

 <p>REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0059</p>	Rev.: 0	Page: 6 / 14
	GDA-REC-GNSL-008599	


	the need to meet requirements such as the single failure criterion. Adequacy of design principles will be one aspect of the review that will be taken from step 2 to step 5.
Management of requirements including relevant processes to control iterative design, implementation and integration	The management of requirements is considered in IEC 61513 and associated clauses in IEC 60987, IEC 60880 and IEC 62566. During the detailed assessment of CTEC's development processes and approaches, answers and evidence provided will be reviewed to ensure that specific shortcomings related to requirements management processes are identified. This includes consideration of traceability of requirements throughout the lifecycle to ensure adequate management during iterative design, implementation and integration. Strategies to address these will be developed in step 5.
Application of suitable techniques and measures for adequate verification for each lifecycle stage	All standards considered in step 2 include guidance on techniques and measures for verification for the lifecycle phases. CTEC's approach to verification will be reviewed in steps 2-4 and shortfalls identified will be the subject of compensating measures developed in step 5.

Step 3 - Comments from the Assessment Team

The assessment team will raise comments and clarification questions about the compliance documentation provided by CTEC identified during step 2.

Step 4 –Further Response and Evidence

The assessment team will collaborate to explore the comments and identify areas for further consideration. A series of evidence workshops are expected to be held in which CTEC will be able to provide additional information and evidence documentation as necessary. All additional evidence shared will be recorded in the assessment report. The assessment report will also document where it has not been possible to share further information at this GDA stage. The aim of these evidence workshops is to discuss the comments and areas

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN	Rev.: 0	Page: 7 / 14
	RO-UKHPR1000-0059	GDA-REC-GNSL-008599	

for further consideration from step 3, and to identify shortfalls and their associated root causes. It is noted that steps 2, 3 and 4 are iterative and will be fully documented in the assessment report.

Step 5– Gaps identification and compensating measures

A summary of all gaps/shortfalls identified will be produced. These will include the issues identified from step 4 as well as those already identified by the ONR within this RO. The identification of compensating measures is covered within Action 2 of this resolution plan.

Step 6–Develop Practicable FAPs

This is detailed in Action 3 of this resolution plan.

The assessment findings and responses from steps 2, 3 and 4, as well as the identified gaps in step 5 will be analysed and documented in the first version of *Assessment Report of Production Excellence for FirmSys Platform*, , Reference [3].

RO-UKHPR1000-0059.A2 – Identification and justification of compensating measures to address production excellence shortfalls

The RO action states that:


In response to this RO action, the RP should as a minimum identify and justify suitable and sufficient compensating measures to address the identified production excellence shortfalls.

Resolution Plan

For the identified shortfalls within Action 1, including the shortfalls already identified by ONR, the assessment team will identify and justify appropriate compensating measures with consideration of the ALARP principle to give confidence of correct behaviour of the platform. According to the procedure management of commitments for *UK HPR1000 Generic Design Assessment (GDA) Project*, Reference [29], the forward actions to be implemented in the Nuclear Site Licensing (NSL) phase will be collected in the commitment capture log list and documented in the post-GDA commitment lists, during GDA. Furthermore, these lists will be transmitted to the future licensee.

The RP will choose compensation measures according to the following principles:

- Complete and comprehensive. The assessment team will consider how the compensating measures address the shortfall and its associated root causes. It may be necessary to implement several compensating measures to fully address one shortfall. A justification will be provided to explain how each shortfall is fully addressed by the proposed compensating measures;

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0059	Rev.: 0	Page: 8 / 14
		GDA-REC-GNSL-008599	

- Direct and simple. The compensating measures should not include redundant activities but should directly address gaps with as few activities as possible;
- Feasible. The compensating measures should be feasible and achievable in post-GDA.

Depending on the type of gaps identified, compensating measures include (but are not limited to) the following :

- Elaborating further details, clarifying descriptions and provision of additional justification;
- Clarification of requirements sources, the content of requirements or the traceability between requirements, specification items and testing;
- Documentation improvement including updates or producing additional documentation;
- Optioneering tasks;
- Design changes;
- Additional verification activities including testing;
- Development process improvement.

The compensating measures will be described in the final version of *Assessment Report of Production Excellence for FirmSys Platform*, Reference [3].

RO-UKHPR1000-0059.A3 – Develop a strategy for undertaking the compensating measures and demonstrating this is practicable


The RO action states that:

In response to this RO action, the RP should address the following, as a minimum:

- Show how the activities will be effective and are adequate, considering:
 - Detailed description of the scope of work to be undertaken;
 - Identification of the necessary competence management arrangements;
 - Indicative project plan and schedule for implementation of compensating activities.

Resolution Plan

In the GDA phase, the gaps and corresponding compensating measures will be identified and a strategy for

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0059	Rev.: 0	Page: 9 / 14
		GDA-REC-GNSL-008599	

undertaking the compensating measures will be developed. All the compensating measures will be done in the NSL phase.

The following information will be described in detail in the strategy:

- Safety. Describe the impact of compensation measures on safety;
- Scope. Describe which compensating measures will be implemented and how they will be implemented;
- Competency requirements. Identify the competency requirements for each activity;
- Human resource needs. Describe the human resources needed to implement the compensating measures;
- Plan and schedule. Describe the plan and schedule, determine the priority of implementation, identify dependencies including the sequencing both between different compensating measures activities and wider design activities, and establish milestones to demonstrate that the approach is feasible within the project schedule.

The strategy for undertaking the compensating measures will be documented in the final version of *Assessment Report of Production Excellence for FirmSys Platform*, Reference [3].

Summary


The main document for the closure of this RO is the *Assessment Report of Production Excellence for FirmSys Platform*, Reference [3]. The report will capture the outcomes of each of the RO actions and include the following:

- Methodology

Set out the systematic review methodology, describe the assessment team and its corresponding responsibilities, and describe the activities and output of each step in detail.
- Assessment and Gap Identification (relating to RO Action 1)

Document the implementation of RO Action 1 which includes the comments identified from the review performed by the assessment team, the clarifications and further responses of the RP and the consolidated list of shortfalls.
- Compensating Measures (relating to RO Action 2)

Record the identified compensating measures, describe in detail what should be done in the measures,

 <p>REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0059</p>	Rev.: 0	Page: 10 / 14
	GDA-REC-GNSL-008599	

and demonstrate why the measures can address the gaps. For some shortfalls, if there is no reasonably practicable compensating measure, a supporting justification will be required.

- Strategy (relating to RO Action 3)

Describe the strategy for undertaking the compensating measures, which includes the detailed scope of work, competency requirements, human resource requirements, the indicative plan and schedule.

Where necessary, forward actions to update safety case documentation for consistency will be recorded in the *Assessment Report of Production Excellence for FirmSys Platform*, Reference [3].

Impact on the GDA Submissions

The submissions that are impacted by this resolution plan include:

- CTEC, Assessment report of Production Excellence for FirmSys Platform, Revision A, 2021.
- CTEC, Assessment report of Production Excellence for FirmSys Platform, Revision B, 2021.


Timetable and Milestone Programme Leading to the Deliverables

No.	Document No.	Document Title	Rev.	Submission Time
1	TBD	<i>Assessment Report of Production Excellence for FirmSys Platform</i>	A	2021-3-15
1	TBD	<i>Assessment Report of Production Excellence for FirmSys Platform</i>	B	2021-4-30


The Gantt Chart is provided in APPENDIX A.

References


- [1] ONR, Safety Assessment Principle for Nuclear Facilities, ESS.27, Revision 1, 2020.
- [2] ONR, Computer based safety systems, NS-TAST-GD-046, Revision 6, 2020.
- [3] CGN, Assessment Report of Production Excellence for FirmSys Platform, Revision A&B, 2021.

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0059	Rev.: 0	Page: 11 / 14
		GDA-REC-GNSL-008599	


- [4] CTEC, Topic Report of FirmSys Platform, GHX56100001GSNS44TR, Revision B, 2020.
- [5] IEC, Instrumentation and control important to safety – General requirements for systems, IEC61513, 2011.
- [6] IEC, Instrumentation and control important to safety – Hardware design requirements for computer-based systems, IEC60987, 2007.
- [7] IEC, Instrumentation and Control Important to Safety - Software Aspects for Computer-based Systems Performing Category A Functions, IEC60880, 2006.
- [8] IEC, Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A functions IEC62566, 2012.
- [9] CTEC, Demonstration of Production Excellence for FirmSys Platform, GHX56100036GSNS44TR, Revision A, 2020.
- [10] CTEC, Product Excellence Summary Paper for CPLD-Based Watchdog Circuit of FirmSys, GHX56100163GSNS44TR, Revision A, 2020.
- [11] CTEC, Product Excellence Summary Paper for the HNU DP-RAM Circuit of FirmSys, GHX56100164GSNS44TR, Revision A, 2020.
- [12] CTEC, Product Excellence Summary Paper for Software Self-diagnostics Function of FirmSys, GHX56100155GSNS44TR, Revision A, 2020.
- [13] ONR, RQ-UKHPR1000-0930 - Control & Instrumentation - Evidence Supporting FirmSys Production Excellence Demonstration, CM9 2020/205639, 2020.
- [14] ONR, RQ-UKHPR1000-0959 - Control & Instrumentation - FirmSys Components and Classification Baseline Definition, CM9 2020/213491, 2020.
- [15] ONR, RQ-UKHPR1000-0960 - Control & Instrumentation - FirmSys Programmable Hardware Device Development and Standards, CM9 2020/213523, 2020.
- [16] ONR, RQ-UKHPR1000-1000 - Control & Instrumentation - FirmSys Software and IEC 60880 Compliance, CM9 2020/237115, 2020.
- [17] ONR, RQ-UKHPR1000-1096 - Control & Instrumentation - Clarification of the Software V&V Plan (FirmSys), CM9 2020/269817, 2020.
- [18] ONR, RQ-UKHPR1000-1116 - Control & Instrumentation - FirmSys Hardware and IEC 60987 Compliance, CM9 2020/274935, 2020.

	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0059	Rev.: 0	Page: 12 / 14
		GDA-REC-GNSL-008599	

- [19] ONR, RQ-UKHPR1000-1117 - Control & Instrumentation - FirmSys Software Processes and Procedures, CM9 2020/274949, 2020.
- [20] ONR, RQ-UKHPR1000-1169 - C&I -Suitability Analysis Report of the Selected Platform Applicability to the RPS [PS] & SAS System Requirements – Clarifications, CM9 2020/293649, 2020.
- [21] ONR, RQ-UKHPR1000-1170 - C&I - Demonstration of Production Excellence of FirmSys Platform - Clarifications, CM9 2020/293657, 2020.
- [22] ONR, RQ-UKHPR1000-1268 - C&I - FirmSys Tools - Production Excellence Demonstration, CM9 2020/308822.
- [23] ONR, RQ-UKHPR1000-1269 - C&I - FirmSys Programmable Devices and Standards Compliance, CM9 2020/3091320, 2020.
- [24] ONR, RQ-UKHPR1000-1360 - C&I - Comparison Analysis for FirmSys based Systems with 60987, CM9 2020/318226, 2020.
- [25] ONR, RQ-UKHPR1000-1360 - C&I - CPLD-Based Watchdog, CM9 2020/322839, 2020.
- [26] CGN, S.P1893.42.7 Notes for L4 Workshop - FirmSys Demonstration of PE for self-diagnostics, 2020.
- [27] CGN, Pre-Construction Safety Report Chapter 4 General Safety and Design Principles, GHX00620004KPGB02GN, Revision G, 2019.
- [28] ONR, Safety Assessment Principles, Revision 0, November 2014.
- [29] CGN, Management of Commitments for UK HPR1000 Generic Design Assessment (GDA) Project, GH-40M-020, Revision C, 2020.

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0059	Rev.: 0	Page: 13 / 14
		GDA-REC-GNSL-008599	

PREVIOUS REVISIONS RECORD				
Rev.	Author	Scope/Reason of Revision	Date	Page

 <p>General Nuclear System</p>	<p>REGULATORY OBSERVATION RESOLUTION PLAN</p> <p>NOT PROTECTIVELY MARKED</p>	Rev.: 0	Page: 14 / 14
		GDA-REC-GNSL-008599	

APPENDIX A Gantt Chart

Tasks	Steps	2021									
		Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	
RO Action 1											
Deliverable: <i>Assessment Report of Production Excellence for FirmSys Platform, Revision A</i>	Development										
	Submission			▲							
RO Action 2 and RO Action 3											
Deliverable: <i>Assessment Report of Production Excellence for FirmSys Platform, Revision B</i>	Development										
	Submission				▲						
Regulator Assessment											
Target RO Closure Date										▲	