General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0057	Rev.：0	Page：1 / 9
		GDA-REC-GNSL-008090	

REGULATORY OBSERVATION Resolution Plan	
RO Unique No.:	RO-UKHPR1000-0057
RO Title:	Independent Confidence Building Measures for complex control and instrumentation systems
Technical Area(s)	Control & Instrumentation
Revision:	0
Overall RO Closure Date (Planned):	2021-04-22
Linked RQ(s)	-
Linked RO(s)	-
Related Technical Area(s)	-
Other Related Documentation	Refer to Appendix A

Scope of Work

Background

An important element of the GDA process is the justification of Computer-Based Systems Important to Safety (CBSIS). There is a particular focus on the use of software and programmable elements in such systems and this is captured in the ONR's Safety Assessment Principles (SAPs) and Technical Assessment Guidelines (TAGs), particularly SAP ESS.27 and TAG 046.

The UK HPR1000 approach for justification of CBSIS follows the two-legged approach; comprising Production Excellence (PE) and Independent Confidence Building Measures (ICBMs). The PE leg is required to demonstrate high quality system production, which is largely achieved by the system supplier adopting appropriate practices for the development of the system. The ICBM leg is required to provide an additional level of assurance in the system's fitness for purpose through the application of independently conducted Techniques and Measures (T&Ms) dissimilar from those applied in production.

The selection and application of T&Ms for the ICBM leg is a specialist area which has been extensively researched and reported on by the Control and Instrumentation Nuclear Industry Forum (CINIF). The information produced and held by CINIF is considered by ONR to be relevant good practice for the selection and application of ICBMs in complex C&I systems. The RP has been unable to gain access to CINIF information and are instead developing an approach to the identification and substantiation of suitable ICBMs with the support of a UK contractor.

Initial engagements with ONR on this subject have so far not identified any significant gaps. However, ONR remains concerned that the identification and substantiation of suitable ICBMs sufficient to meet the UK regulatory expectations may not be achieved within GDA.

Scope of work

The GDA scope of work in the area of ICBMs can be divided into two key areas:

- Strategies for the ICBMs for centralised I&C systems,
- Feasibility studies for certain techniques.

The RP has already engaged a UK consultant to assist in the development of the ICBM strategy for the centralised I&C systems and the feasibility studies into certain techniques for ICBMs.

The RP is developing Revision B of the following documents to inform the ICBM strategy for each centralised I&C system:

- Strategy for Conducting ICBMs Activities for RPS [PS],
- Strategy for Conducting ICBMs Activities for SAS,
- Strategy for Conducting ICBMs Activities for KDA [SA I&C],
- Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS].

The initial Revision A of these documents [1], [2], [3] and [4] were submitted in the period up to April 2020. The next revision of these documents will, for each centralised I&C system:

- Present the generic strategy for ICBMs,
- Provide an overview of the PE, with a view to informing the selection of appropriately diverse/dissimilar techniques in the ICBM leg,
- A discussion of the ICBMs selected and how they are appropriate for the system under consideration,
- Identify any plans for feasibility studies as necessary.

The feasibility studies for certain techniques are selected and justified within the relevant ICBM strategy documents. In accordance with this, the RP is developing desktop feasibility studies into the following ICBM techniques:

- Statistical Testing,
- Static Analysis,
- Compiler Validation (using Source Code Comparison).

To address this RO, the following documents will be updated or developed:

- Strategy for Conducting ICBMs Activities for RPS [PS]
- Strategy for Conducting ICBMs Activities for SAS
- Strategy for Conducting ICBMs Activities for KDA [SA I&C]
- Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS]
- Feasibility Study Report for Statistical Testing of Protection System
- Feasibility Study Report for Static Analysis of Protection System
- Feasibility Study Report for Source Code Comparison of Protection System

Deliverable Description

RO-UKHPR1000-0057.A1 – Suitability of the ICBM approach to achieve UK relevant good practice

The RO action states that:

In response to this Regulatory Observation Action, GNSL should, for each C&I system requiring ICBMs, present the strategy for conducting ICBMs. The strategy should address the following as a minimum:

1. *Detail the options and factors considered in identifying those ICBM techniques that are most suitable to the systems, according to UK relevant good practice, and justify why other techniques have been rejected.*
2. *Demonstrate that the chosen techniques are suitably diverse from those techniques applied during PE.*
3. *Justify the suitability of the approach to ICBM, including:*
    a. *Demonstration that the chosen techniques are the most suitable and effective for the technologies that comprise each system;*
    b. *Demonstration that the approach meets UK regulatory expectations in the selection and application of ICBMs; and*
    c. *Demonstration that the approach represents an ALARP position – for example that the application of further ICBMs will not further reduce risk, so far as is reasonably practicable, and why.*

Resolution Plan

The RP is developing Revision B of the following documents to inform the ICBM strategy for each centralised I&C system and address the above points within the RO action:

- Strategy for Conducting ICBMs Activities for RPS [PS],
- Strategy for Conducting ICBMs Activities for SAS,
- Strategy for Conducting ICBMs Activities for KDA [SA I&C],
- Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS].

The strategy documents will present the general approach to the ICBM leg applicable for all CBSIS. The approach is graded based on the safety classification of the system. The ICBM leg is split into the independent PE review activities and additional ICBM assessment activities. It identifies those ICBM techniques that are most suitable to the systems with the rigour proportionate with the safety class of the system (*part of point 1 of A1*). The generic approach is derived using reference to relevant standards (*point 3b of A1*).

Each strategy document provides a summary of the relevant aspects of the System Development Process. The system development process lies within the PE leg and is covered in detail within the relevant “demonstration of PE” documents. However, the aim is to summarise the specific T&Ms used within the development process such that the techniques chosen for the ICBM leg are suitably diverse from those techniques applied during PE (*point 2 of A1*).

Each strategy then builds on the generic strategy to develop a system specific approach. Each of the T&Ms are discussed in turn in a qualitative discussion of the application of the technique and the relative benefits and disbenefits (*point 1 of A1*). The discussion of the identified T&Ms covers the following considerations, as necessary:

- Diversity from the T&Ms in the PE leg (*point 2 of A1*);
- The technology of the system (i.e. microprocessor vs HPD) (*point 3a of A1*);
- The safety class of the system and the safety functions assigned to it (*point 3b of A1*);
- Overall rigour of the combination of T&Ms proposed for the system ICBM leg (*point 3c of A1*).

Each strategy will then identify any necessary feasibility studies identified. Finally, each strategy will provide a high-level summary and conclusion as to the suitability of the proposals (*point 3c of A1*).

The RP will update the ICBM strategy documents to address the expectations set out in this RO action. Revision B of these documents will be provided as follows:

- Strategy for Conducting ICBMs Activities for RPS [PS], Revision B [5],
- Strategy for Conducting ICBMs Activities for SAS, Revision B [6].
- Strategy for Conducting ICBMs Activities for KDA [SA I&C], Revision B [7],
- Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS], Revision B [8].

ONR’s assessment of these Revision B documents is ongoing and it is likely for a further revision to be required to incorporate regulatory comments. Revision C of these strategy documents will be provided as necessary to address any regulatory comments or updates arising and are intended to be submitted by 22nd January 2021 (if required).

RO-UKHPR1000-0057.A2 – Demonstration of feasibility

The RO action states that:

In response to this Regulatory Observation Action, GNSL should, for those ICBMs that it considers ‘new or novel’:

- *Detail the methodology that will be applied for each technique;*
- *Undertake case studies that demonstrate how the techniques will be implemented in future project phases.*

Resolution Plan

The RP has identified the need for some limited feasibility studies within the GDA to demonstrate the feasibility of new and/or novel techniques. This will provide the necessary confidence that the identified ICBM techniques will be able to be performed within the future NSL phase. The full justification for the selection of the techniques for feasibility studies will be set out within the relevant ICBM strategies documents. The ICBM strategy documents will detail the scope and activities for the feasibility studies identified.

Each feasibility study will focus on the general method to be applied for each technique and select appropriate case studies for consideration within the study. The following desktop feasibility studies are currently proposed, further details on each study are provided below:

- Feasibility study of Static Analysis (up to compliance analysis / formal proof),
- Feasibility study of Source Code Comparison,
- Feasibility study of Statistical Testing.

a) Static Analysis

The Strategy for Conducting ICBMs Activities for RPS [PS], Revision B [5], identifies that a feasibility study for static analysis should be performed. The feasibility study will focus on the more rigorous static analysis techniques appropriate for an F-SC1 system, such as compliance analysis which supports a formal proof that a procedure behaves in accordance with its specification. The study scope will involve a desktop review of the key risks relating to implementing static analysis of the RPS [PS] through engagement with the system manufacturer. The risk-based approach will be supported by a checklist to effectively manage information, share limited example information and to ensure key issues are adequately covered. The feasibility study will consider the following potential issues:

- Compatibility of tools, approach and process to implement Static Analysis in the NSL phase,
- Review of software functional specification documentation to confirm that there is sufficient detail of the software functionality to develop proof conditions for compliance analysis in the NSL phase,
- Consideration of scheduling issues and estimation of effort to implement a full assessment in the NSL phase.

It is not possible to perform trial analysis within the GDA phase due to restrictions on the source code and restrictions on international travel. The feasibility study will provide a plan for any further feasibility activities related to this technique which are to be performed within the NSL phase.

b) Source Code Comparison

The Strategy for Conducting ICBMs Activities for RPS [PS], Revision B [5], identifies that a feasibility study for source code comparison should be performed. Source code comparison provides confidence in the compilation of a specific executable by disassembling it and comparing its behaviour to the source code implementation. The study scope will involve a desktop review of the key risks relating to implementing source code comparison of the RPS [PS] through engagement with the system manufacturer. The risk-based approach will be supported by a checklist to effectively manage information, share limited example information and to ensure key issues are adequately covered. The feasibility study will consider the following potential issues:

- Compatibility of tools (such as possible disassembler tools), approach and process to implement Source Code Comparison in the NSL phase,
- Review of the software implementation process to establish how tools for Source Code Comparison can be used (e.g. compilers used, optimisation options, etc.),
- Consideration of scheduling issues and estimation of effort to implement a full assessment in the NSL phase.

It is not possible to perform trial analysis within the GDA phase due to restrictions on the source code and restrictions on international travel. The feasibility study will contain a plan for any further feasibility activities related to this technique which are to be performed within the NSL phase.

c) Statistical Testing

The Strategy for Conducting ICBMs Activities for RPS [PS], Revision B [5], identifies that a feasibility study for statistical testing should be performed. Statistical testing (referred to as probabilistic testing within IEC 61508-3 [9]) is a method of dynamically testing a system in order to demonstrate a specified reliability claim. The feasibility study will set out the methodology to perform statistical testing, identify the key challenges associated with statistical testing and describe how these can be addressed, including the following:

- Recommended tools, approach and process for applying statistical testing,
- Scope of the equipment under test,
- How oracle and test harness may be designed,
- How operational profiles are derived and generated,
- How independence between tests could be achieved,
- Estimation of effort to complete statistical testing.

The study will provide sufficient confidence that statistical testing is feasible within the NSL phase.

Impact on the GDA Submissions

The submissions that are impacted by this resolution plan include:

- CGN, Strategy for Conducting ICBMs Activities for RPS [PS], GHX06100015DIYK03GN, Revision A, November 2019.
- CGN, Strategy for Conducting ICBMs Activities for SAS, GHX06100001DIYK03GN, Revision A, April 2020.
- CGN, Strategy for Conducting ICBMs Activities for KDA [SA I&C], GHX06100020DIYK03GN, Revision A, April 2020.
- CGN, Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS], GHX06100021DIYK03GN, Revision A, April 2020.

Timetable and Milestone Programme Leading to the Deliverables

No.	Document No.	Document Title	Rev.	Submission Time
1	GHX06100015DIYK03GN	Strategy for Conducting ICBMs Activities for RPS [PS]	B	2020-08-30
2	GHX06100001DIYK03GN	Strategy for Conducting ICBMs Activities for SAS	B	2020-08-30
3	GHX06100020DIYK03GN	Strategy for Conducting ICBMs Activities for KDA [SA I&C]	B	2020-09-30
4	GHX06100021DIYK03GN	Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS]	B	2020-09-30
5	GHX06100010DIYK03GN	Feasibility Study Report for Static Analysis of Protection System	A	2020-11-30
6	GHX06100011DIYK03GN	Feasibility Study Report for Source Code Comparison of Protection System	A	2020-11-30
7	GHX06100012DIYK03GN	Feasibility Study Report for Statistical Testing of Protection System	A	2020-11-30

8	GHX06100015DIYK03GN	Strategy for Conducting ICBMs Activities for RPS [PS]	C	2021-01-22 (if required)
9	GHX06100001DIYK03GN	Strategy for Conducting ICBMs Activities for SAS	C	2021-01-22 (if required)
10	GHX06100020DIYK03GN	Strategy for Conducting ICBMs Activities for KDA [SA I&C]	C	2021-01-22 (if required)
11	GHX06100021DIYK03GN	Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS]	C	2021-01-22 (if required)

The Gantt Chart is provided in APPENDIX A.

Reference

[1] CGN, Strategy for Conducting ICBMs Activities for RPS [PS], GHX06100015DIYK03GN, Revision A, November 2019.

[2] CGN, Strategy for Conducting ICBMs Activities for SAS, GHX06100001DIYK03GN, Revision A, April 2020.

[3] CGN, Strategy for Conducting ICBMs Activities for KDA [SA I&C], GHX06100020DIYK03GN, Revision A, April 2020.

[4] CGN, Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS], GHX06100021DIYK03GN, Revision A, April 2020.

[5] CGN, Strategy for Conducting ICBMs Activities for RPS [PS], GHX06100015DIYK03GN, Revision B, August 2020.

[6] CGN, Strategy for Conducting ICBMs Activities for SAS, GHX06100001DIYK03GN, Revision B, August 2020.

[7] CGN, Strategy for Conducting ICBMs Activities for KDA [SA I&C], GHX06100020DIYK03GN, Revision B, September 2020.

[8] CGN, Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS], GHX06100021DIYK03GN, Revision B, September 2020.

[9] IEC, Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 3: Software requirements, IEC 61508-3, Revision 2, 2010.

PREVIOUS REVISIONS RECORD

Rev.	Author	Scope/Reason of Revision	Date	Page

APPENDIX A RO-UKHPR1000-0057 Gantt Chart

Tasks	**Steps**	**2020**					**2021**			
		Aug	**Sep**	**Oct**	**Nov**	**Dec**	**Jan**	**Feb**	**Mar**	**Apr**
RO Action 1										
Deliverable: Strategy for Conducting ICBMs Activities for RPS [PS], Revision B	Development	🟩								
	Submission	▲								
Deliverable: Strategy for Conducting ICBMs Activities for SAS, Revision B	Development	🟩								
	Submission	▲								
Deliverable: Strategy for Conducting ICBMs Activities for KDA [SA I&C], Revision B	Development	🟩	🟩							
	Submission		▲							
Deliverable: Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS], Revision B	Development	🟩	🟩							
	Submission		▲							
Deliverable: Strategy for Conducting ICBMs Activities for RPS [PS], Revision C (if required)	Development			🟩	🟩	🟩	🟩			
	Submission						▲			
Deliverable: Strategy for Conducting ICBMs Activities for SAS, Revision C (if required)	Development			🟩	🟩	🟩	🟩			
	Submission						▲			
Deliverable: Strategy for Conducting ICBMs Activities for KDA [SA I&C], Revision C (if required)	Development				🟩	🟩	🟩			
	Submission						▲			
Deliverable: Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS], Revision C (if required)	Development				🟩	🟩	🟩			
	Submission						▲			

Tasks	Steps	2020					2021			
		Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr
RO Action 2										
Deliverable: Feasibility Study Report for Statistical Testing of Protection System, Revision A	Development	🟩	🟩	🟩	🟩					
	Submission				▲					
Deliverable: Feasibility Study Report for Static Analysis of Protection System, Revision A	Development	🟩	🟩	🟩	🟩					
	Submission				▲					
Deliverable: Feasibility Study Report for Source Code Comparison of Protection System, Revision A	Development	🟩	🟩	🟩	🟩					
	Submission				▲					
Regulator Assessment			🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Target RO Closure Date										▲