REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-UKHPR1000-0057
Revision:	0
Date sent:	03/12/20
Acknowledgement required by:	24/12/20
Agreement of Resolution Plan Required by:	25/01/21
CM9 Ref:	2020/315704
Related RQ / RO No. and CM9 Ref: (if any)**:**	2020/290199
Observation title:	Independent Confidence Building Measures for complex control and instrumentation systems
Lead technical topic: 3. Control & Instrumentation	**Related technical topic(s):**

Regulatory Observation

Background

The subject of this regulatory observation (RO) is the selection and demonstration of the adequacy of independent confidence building measures (ICBMs) for complex[1] control and instrumentation (C&I) systems during the UK HPR1000 generic design assessment (GDA).

During GDA Step 4 the requesting party (RP) submitted the pre-construction safety report (PCSR) for instrumentation and control, chapter 8, [1] that provides an overview of the proposed approach to the justification of computer based systems important to safety for the UK HPR1000 in section 8.14.2. This states that the justification of these systems will be based on a two-legged approach involving a demonstration of production excellence (PE) and ICBMs.

The PCSR chapter 8 states that the ICBM activities will be described in the basis of safety case (BSC) documents BSC of Protection System [2], Revision B, BSC of Safety Automation System [3], and BSC of Plant

[1] In the context of C&I systems the term complex is taken to mean that it is not practical to confirm their behaviour by testing alone due to the very large number of potential internal states that they possess. C&I systems containing a microprocessor or complex logic circuit such as a field programmable gate array (FPGA) are considered to be complex.

Standard Automation System [4]. The PCSR states that ICBMs will not be performed during GDA, but that feasibility studies will. This refers to forward action plans FAP-08-04 and FAP-08-11 in chapter 8.19.

The FAP-08-04 task states:

"*The methodology for ICBM of computer based systems important to safety described in PCSR Sub-chapter 8.14.2 will be provided, including:*

a) Graded approach and activities on ICBM demonstration of computer based systems important to safety;

b) Technology which may be applied in the activities;

c) Scope of activities to be performed.", with a completion date of December 2019

This indicates that in respect of action a) the following documents will be issued :

- BSC of Protection System, GHX06002002DIYK03GN;
- BSC of Safety Automation System, GHX06002003DIYK03GN;
- BSC of Severe Accident I&C System, GHX06002005DIYK03GN;
- BSC of Plant Standard Automation System GHX06002004DIYK03GN;
- BSC of Plant Computer Information and Control System, GHX06120010DIKX03GN.

FAP-08-11 task states:

"*Perform the feasibility studies for new or novel techniques for ICBM activities*", with a completion date of November 2020.

The BSC of Protection System, GHX06002002DIYK03GN has been subsequently updated and was submitted to ONR on 29th June 2020 [2]. The other BSC's referenced in FAP-08-04 have yet to be updated and submitted to ONR in Step 4.

ONR's review of BSC of Protection System [2] has revealed:

- Sub-claim C1.1.1.1 in this document relating to the measures necessary to substantiate the reliability of the RPS to 1E-04 pfd is supported by argument A4 "*Production Excellence (PE) and Independent Confidence Building Measures (ICBMs) activities are undertaken with a level of rigour suitable for an F-SC1 system"*
- In respect of ICBMs, argument A4 states "*…ICBM activities for the RPS [PS] are considered for both platform and plant-specific engineering, which are broadly divided into two sets:*
    a) *Independent production excellence review: consists of independent checking of the supplier's design, the production process and the comprehensive test program;*
    b) *Independent product assessment: consists of independent assessments of the final software using checking or analysis techniques*

  The selected techniques for the ICBMs will be diverse from those used in the development process and compensatory measures. The rigours of the PE review and product assessment will be commensurate with the safety significance and the F-SC1 class of the RPS [PS]. (refer to evidence "E1-c" for details)"

- *Evidence E1-c* cites the document Strategy for Conducting ICBMs Activities for RPS [PS] [5].

In respect of ICBMs the document Strategy for Conducting ICBMs Activities for RPS [PS] [5] analyses techniques and measures recommended by IEC 61508 [6] for a system of equivalent reliability (SIL4), and selects techniques and measures that have not been applied in the PE activities as ICBMs.

ONR notes that the full ICBM strategy for all C&I systems will only become visible to ONR as the BSCs for the C&I systems and any supporting references and relevant documents are submitted later in GDA step 4.

The selection and application of ICBMs is a specialist area which has been extensively researched and reported on by the control and instrumentation nuclear industry forum (CINIF), a consortium of UK licensees that investigates and shares information, across the industry. 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.

At the start of the UK HPR1000 GDA it was anticipated that the RP would be able to join the CINIF consortium and gain access to the information available to members, including historical reports relating to the selection and application of ICBMs. As GDA step 4 has progressed it has become apparent that this is unlikely to be possible within GDA, and that the RP will have to find alternative approach to the identification and substantiation of suitable ICBMs. As a consequence on 15 July 2020 ONR met with the RP, to discuss this challenge and ascertain the RP's proposed approach to the selection and application of ICBMs to C&I safety and safety-related systems containing microprocessors and complex logic devices[2]. The ONR report on this meeting is at reference [7].

The RP, with the support of a UK technical support contractor, indicated that a number of strategy and feasibility study documents in relation to the feasibility of applying new or novel ICBMs to UK HPR1000 C&I systems would be submitted to ONR during GDA Step 4, namely:

- ICBM strategy document for PSAS & KIC [PCICS] (REV.B)
- ICBM strategy document for KDA [SA I&C] (REV.B)
- Feasibility study of Statistical Testing for RPS [PS]
- Feasibility study of Static Analysis for RPS [PS]
- Feasibility study of Compiler Validation for RPS [PS]

Further relevant points for this RO include:

- UK regulatory expectation is not that ICBM activities will be performed during GDA, but that suitable ICBMs will be identified and demonstrated to be appropriate during GDA.
- ONR accepts that feasibility studies will not include Field Programmable Gate Arrays (FPGAs) and Complex Programmable Logic Devices (CPLDs) during GDA however, ICBM strategies should be produced that will define appropriate techniques for these devices during GDA, with a commitment to perform feasibility studies during the licensing phase.
- The hazards arising from incorrect FPGA or CPLD configuration should be identified during GDA, so that during the licensing phase strategies to manage these can be developed and demonstrated to adequately control risks.

[2] Complex configurable logic devices such as FPGAs and CPLDs may be used to perform functions of similar complexity to a microprocessor, and due to this complexity are required to be substantiated to the same extent.

- Whilst the RP does not consider third party software[3] will be present in the RPS and SAS Class 1 platform (FirmSys) there will be a need to confirm this during GDA. Also there may be some third party software in Class 2 and Class 3 systems. Where third party software is identified there will be a need to confirm this will not interfere with the ability of the system to deliver safety functions.
- UK RGP is that a 99% confidence level will be selected for statistical testing, any lower confidence level would need to be justified.
- It is common for divisions of the RPS to be performing different functions and therefore have different software. It will be necessary to demonstrate that statistical testing will remain valid for all divisions.

This meeting gave ONR some confidence that the RP may be able to use this approach to offset the inability to gain access to CINIF material on ICBMs. However, ONR remains concerned that the identification and substantiation of suitable ICBMs sufficient to meet the UK regulatory expectations will not be achieved within GDA. For this reason the actions described within this RO have been identified as necessary to ensure that the RP is able to demonstrate a coherent ICBM strategy for all relevant C&I systems.

Relevant Legislation, Standards and Guidance

ESS.27 – Computer-based Safety Systems, ONR Safety Assessment Principles (SAP's), 2014 edition, Revision 1 (January 2020), http://www.onr.org.uk/saps/saps2014.pdf:

NS-TAST-GD-046 (Rev 5) – Computer based safety systems,

ONR Technical Assessment Guides, http://www.onr.org.uk/operational/tech_asst_guides/index.htm

IEC 61508 Functional safety of electrical electronic programmable electronic safety-related systems — Part 3 Software requirements

IEC 61513 Nuclear power plants — Instrumentation and control important to safety — General requirements for systems

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

IEC 62138 Nuclear power plants — Instrumentation and control important for safety — Software aspects for computer-based systems performing category B or C functions

Regulatory Expectations

[3] Third party software is software that has been developed by another organisation or organisations, and for which little of no design or testing information in the context of use is available. This includes operating system software, software incorporated from libraries, software to implement communications interfaces, etc. A fault in this software has the potential to introduce a fault into a C&I system.

It is a UK legal requirement that nuclear site licensees can demonstrate that structures, systems, and components on nuclear licensed sites are able to reduce risk, so far as is reasonably practicable (SFAIRP)[4]. Where control and instrumentation (C&I) systems contribute to this it should be demonstrated that these do likewise. Thus it should be demonstrated that C&I systems contain the functional and non-functional capability to manage risk, working with other technology measures, and are able to achieve the reliability claimed for them, during all foreseeable conditions of operation and maintenance.

UK regulatory expectations are that UK relevant good practice systems in respect of C&I systems is applied, according to the classification of the system. Where a C&I system contains complex logic or software[5] a claim of adequacy should be based on the selection and application of adequate PE and ICBMs.

These expectations are set out in SAP ESS.27, and the technical assessment guide (TAG) for ONR inspectors, NS-TAST-GD-046 (Rev 5) – Computer based safety systems. In summary, PE is demonstrated by showing that relevant standards and guidance have been followed in the design and development of the system (or that an equivalent standard has been achieved), and that any gaps are filled by appropriately selected compensating measures (CM's). ICBMs provide confidence that the processes and methods used in PE have actually produced a system with the appropriate attributes, including adequate reliability.

SAP ESS.27 describes the UK regulatory expectations for the selection and application of ICBMs:

"*Independent 'confidence-building' should provide an independent and thorough*

assessment of the safety system's fitness for purpose. This should include the following elements:

- *a) complete, and preferably diverse, checking of the finally validated production software by a team that is independent of the system's suppliers, including:*
  - *(i) independent product checking that provides a searching analysis of the final system;*
  - *(ii) independent checking of the design and production processes, including the activities undertaken to confirm the realisation of the design intent; and*
- *b) independent assessment of the comprehensive testing programme covering the full scope of the test activities."*

When TAG 46 and SAP ESS.27 refer to "computer based safety systems", this is interpreted to mean safety and safety-related C&I systems containing a microprocessor or complex logic.

It is important that ICBMs are independent, in that they do not replicate the activities performed during PE but identify techniques and measures that, in conjunction with PE activities, provide confidence the finished system will achieve the required integrity.

A justification should be provided that risks have been reduced 'As Low As Reasonably Practicable' (ALARP). A key aspect of ALARP justification is optioneering, where all relevant options for the engineering solution are considered followed by a consideration of cost, time and trouble to determine which options provide the best

[4] The term SFAIRP is considered to be equivalent to the term ALARP (as low as reasonably practicable).

[5] Software that used to perform control or protection functions is always considered to be complex in that it is not possible to completely analyse or test it due to the large number of combinations of input and internal states necessary to perform the specified functionality.

risk reduction, and which can be demonstrated to be ALARP. It is expected that the most suitable and effective techniques will be considered, including modern technologies, to maximise the efficacy of ICBMs, and to reduce or eliminate gaps.

During GDA ONR expects the RP will identify the selected ICBMs and justify their suitability for the UK HPR1000 C&I systems identified in the "Background" section of this RO, documenting this in the form of a safety case. This safety case is expected to show how the proposed ICBMs are feasible and will work together with PE to substantiate the design, and to identify any remaining gaps. It is not expected that the full range of ICBMs will be applied to the C&I systems during GDA but that, where necessary, the feasibility of applying the selected techniques will be demonstrated, providing confidence these can be successfully applied post-GDA.

References

[1] UK HPR1000 - HPR GDA PCSR 0008 - PCSR - Chapter 8 - Control and Instrumentation - Rev 001 - 10 January 2020, CM9 Ref. 2020/13661

[2] CGN, BSC of Protection System, GHX06002002DIYK03GN, Revision C, 29 June 2020, CM9 2020/196626.

[3] CGN, BSC of Safety Automation System, GHX06002003DIYK03GN, Revision A, 2019.

[4] CGN, BSC of Plant Standard Automation System, GHX06002004DIYK03GN, Revision A, 2019,

[5] Strategy for Conducting ICBMs Activities for RPS [PS], GHX06100015DIYK03GN, Revision A, 2019.

[6] IEC 61508 Functional safety of electrical electronic programmable electronic safety-related systems, 2010.

[7] ONR-NR-CR-20-292 - UK HPR1000 - Level 4 Control & Instrumentation Independent Confidence Building Measures (ICBMs) Strategy - 15 July 2020 - Revision 1, CM9 Ref, 2020/218852

Regulatory Observation Actions

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

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

- Detail the options and factors considered in identifying those ICBM techniques that are most applicable to the systems, according to UK relevant good practice, and justify why other techniques have been rejected.
- Demonstrate that the chosen techniques are suitably diverse from those techniques applied during PE.
- Justify the suitability of the approach to ICBM, including:

- Demonstration that the chosen techniques are the most suitable and effective for the technologies that comprise each system;
- Demonstration that the approach meets UK regulatory expectations in the selection and application of ICBMs; and
- 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.

RO-UKHPR1000-0057.A2 – Demonstration of feasibility

In response to this Regulatory Observation Action, The Requesting Party should, for those ICBMs that it considers 'new or novel':

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

Resolution required by: '*to be determined by General Nuclear System Resolution Plan*'

REQUESTING PARTY TO COMPLETE	
Actual Acknowledgement date:	
RP stated Resolution Plan agreement date:	