REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-UKHPR1000-0059
Revision:	0
Date sent:	08/02/21
Acknowledgement required by:	01/03/21
Agreement of Resolution Plan Required by:	19/02/21
CM9 Ref:	2020/322494
Related RQ / RO No. and CM9 Ref: (if any):	
Observation title:	Evidence of Production Excellence for the FirmSys platform
Lead technical topic: 3. Control & Instrumentation	**Related technical topic(s):**

Regulatory Observation

Background

The subject of this regulatory observation (RO) is the demonstration of the adequacy of production excellence (PE) activities for the FirmSys platform during the UK HPR1000 generic design assessment (GDA).

To satisfy the requirements of 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 production excellence can be demonstrated, as this forms the basis for both the Class 1 reactor protection system (RPS) and Class 2 safety automation system (SAS).

ONR selected software self-diagnostics, also commonly referred to as self-supervision, as an initial sample topic for which adequate PE of the FirmSys platform components should be demonstrated.

Information relating to the PE of self-diagnostics was presented by the RP to ONR during a workshop held over 3 days [1]. However, this was not effective at enabling ONR to view the evidence necessary to progress the assessment.

After discussions on how adequate evidence could be presented to ONR, the RP produced and submitted a PE summary paper [2] containing relevant parts of processes & procedures, requirements & design information, and assurance documents. ONR assessed this PE summary paper, producing a number of queries [3] that were communicated to the RP and subsequently discussed during a two-day workshop [4]. During this workshop ONR identified shortfalls in the PE evidence available to support the claims made on the FirmSys platform.

ONR selected a second sample on information relating to the PE of the complex programmable logic device watchdog circuit for FirmSys. The RP produced a summary paper for this sample [5] and ONR assessed this.

ONRs findings from this assessment [6] aligned with the findings from the first sample, confirming these shortfalls are more widespread than the areas covered by the first sample.

During this process ONR raised further RQ's, e.g. [7, 8, 9, 10, 11, 12, 13, 14, 15, 16] relating to the FirmSys PE demonstration, but many of ONRs concerns were not adequately addressed by the responses to these. The intent of this RO is to resolve these concerns at a higher level.

ONR was able to gather enough information to be able to be identify shortfalls in the PE evidence available. Specifically, ONR noted that:

1. It is not clearly stated what safety design principles have been used to determine the functionality and properties of the FirmSys platform, and how these have been captured and demonstrated to have been fulfilled.
2. The evidence presented in respect of self-diagnosis suggests that the requirements are 'standard' checks that are identified at a high level in standards such as IEC 60880. ONRs expectation is that the requirements for self-diagnosis would be based on the identification of potential faults within the platform, arising from the actual hardware and the architectural arrangement deployed.
3. From the evidence sampled ONR has concluded that developers and testers require a detailed understanding of the design of FirmSys in order to be able to confirm that the design is correct. ONR could not identify an effective mechanism to ensure that all personnel involved with the project can hold a common understanding of design objectives and how these are satisfied.
4. There is limited evidence of refinement of high-level requirements into specific requirements for the system design as requirements flow through the document hierarchy. For example, system requirements, system design, software requirements, software design, were generally a repetition of, or paraphrasing of, the parent requirement. This makes it difficult to confirm that the requirements have been satisfied by the design.
5. There is a lack of atomicity of requirements (individually numbered requirements include a number of specific requirements). Where parent requirements trace to a number of child requirements, it is not always clear which part of the parent the child relates to, and how all the child requirements collectively satisfy the parent requirement.
6. It is not possible to determine how the detailed design is derived from the system requirements, for example pseudo code exactly matches the software. This calls into question how verification activities can confirm that the software behaves as intended.
7. Review criteria such as redundancy, correctness, consistency, completeness, etc. were described, but no evidence of these being applied has been provided. Therefore, ONR could not determine how these criteria have been used to measure the adequacy of the design. In addition, it is not clear to ONR on what basis these criteria have been selected, and their suitability in identifying potential errors or design faults.
8. Some requirements are vague and cannot be considered to be complete and unambiguous. It was also noted that some of the corresponding test cases included more details than the requirement under test, leading to a concern of how the independent tester determined the test cases, and whether this is adequate to confirm the requirement.
9. The review criteria for each phase of the lifecycle are stated in high level terms, and review conclusions generally state that the criteria have been satisfied, with a lack of substantiation evidence.
10. There were similarities in the review criteria used at each stage of development. On the basis that documents produced at each stage serve different purposes, ONR's expectation is that there would be criteria specific to the purpose of each document.

These are the shortfalls that ONR has identified based on the evidence sampled to date. There may be other shortfalls in the PE demonstration associated with other aspects of the platform.

Relevant Legislation, Standards and Guidance

1. 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:
2. NS-TAST-GD-046 (Rev 6) – Computer based safety systems, ONR Technical Assessment Guides, http://www.onr.org.uk/operational/tech_asst_guides/index.htm
3. IEC 60880 Nuclear power plants — Instrumentation and control systems important to safety — Software aspects for computer-based systems performing category A functions

4. IEC 61513 Nuclear power plants — Instrumentation and control important to safety — General requirements for systems
5. IEC 60987 Nuclear power plants — Instrumentation and control important to safety — Hardware design requirements for computer-based systems
6. IEC 61508 Functional safety of electrical electronic programmable electronic safety-related systems

ONR's expectations

ONR's expectations for this demonstration of adequacy of the PE evidence for FirmSys platform are described in NS-TAST-GD-046 Revision 6 "Computer Based Safety Systems", and the safety assessment principle ESS.27. Because the FirmSys platform is the basis of the F-SC1 RPS, the international standards IEC 60880, IEC 61513, IEC 60987, and IEC 61508 apply.

ESS.27 states in respect of production excellence:

"422. The rigour of the standards and practices applied should be commensurate with the level of reliability required. The standards and practices should demonstrate 'production excellence' and, through the application of 'confidence-building' measures, provide proportionate confidence in the final design.

423. Production excellence' is a demonstration of excellence in all aspects of production from the initial specification through to the finally commissioned system. It should include the following elements:

a) thorough application of technical design practice consistent with current accepted standards for the development of software for computer-based safety systems;
b) implementation of a modern standards quality management system; and
c) application of a comprehensive testing programme formulated to check every system function, including:
   (i) prior to installation on site, the verification of all phases of the system production process and the validation of the integrated system against its specification by persons not involved in the specification and design activities;
   (ii) following installation on site, a demonstration that the safety system, in conjunction with the plant, performs in accordance with its specification. This demonstration should be devised by persons not involved in the system's specification, design or manufacture; and
   (iii) a programme of dynamic testing, applied to the complete system to demonstrate that the system is functioning as intended.

425. When demonstrating 'production excellence' and applying 'confidence-building' measures for computer-based safety systems:

- verification is the process of ensuring that a phase in the system lifecycle meets the requirements imposed on it by the previous phase; and
- validation is the process of testing and evaluation of the integrated computer system (hardware and software) to ensure compliance with functional, performance and interface requirements.

427. If weaknesses are identified in the production process, compensating measures should be applied to address these. The choice of compensating measures and their effectiveness should be justified in the safety case."

In the experience of ONR it common for gaps in the PE demonstration to be identified. ONR's expectation is that these gaps are recognised and compensating measures are identified, in order to provide the necessary confidence that risks are being adequately managed.

References

1. ONR-NR-CR-20-258 - UK HPR1000 - I&C Inspection - Teleconference to Review Evidence Associated with Production Excellence Case for FirmSys Platform - Level 4 - 29 June - 01 July 2020, CM9 2020/221259
2. Product Excellence Summary Paper for Software Self-diagnostics Function of FirmSys, GHX56100155GSNS44TR, Rev. A, CM9 2020/254193

3. S.P1893.42.7 Notes for L4 Workshop - FirmSys Demonstration of PE for self-diagnostics, 20, 21 October 2020", CM9 2020/305651
4. ONR-NR-CR-20-645 - UK HPR1000 - Level 4 Workshop to Discuss ONR's Queries on the FirmSys Production Evidence Information Supplied in the PE Summary Paper and Other Documents - 20-21 October 2020, CM9 2020/308557
5. PROTECT PROPRIETARY - UK HPR1000 - GHX56100163GSNS44TR - Product Excellence Summary Paper for the CPLD-based Watchdog Circuit of FirmSys - Rev A - 30 November 2020, CM9 2020/316469
6. S.P1893.45.4 Review of PE Summary Papers, CM9 2020/319660
7. RQ-UKHPR1000-0930 - Control & Instrumentation - Evidence Supporting FirmSys Production Excellence Demonstration - 08 July 2020, CM9 2020/205639
8. RQ-UKHPR1000-0959 - Control & Instrumentation - Firmsys Components and Classification Baseline Definition - 15 July 2020, CM9 2020/213491
9. RQ-UKHPR1000-0960 - Control & Instrumentation - Firmsys Programmable Hardware Device Development and Standards - 15 July 2020, CM9 2020/213523
10. RQ-UKHPR1000-1000 - Control & Instrumentation - Firmsys Software and IEC 60880 Compliance - 06 August 2020, CM9 2020/237115
11. RQ-UKHPR1000-1096 - Control & Instrumentation - Clarification of the Software V&V Plan (FirmSys) - 11 September 2020, CM9 2020/269817
12. RQ-UKHPR1000-1116 - Control & Instrumentation - FirmSys Hardware and IEC 60987 Compliance - 16 September 2020, CM9 2020/274935
13. RQ-UKHPR1000-1117 - Control & Instrumentation - FirmSys Software Processes and Procedures - 16 September 2020, CM9 2020/274949
14. RQ-UKHPR1000-1170 - C&I - Demonstration of Production Excellence of FirmSys Platform - Clarifications - 05 October 2020, CM9 2020/293657
15. RQ-UKHPR1000-1269 - C&I - FirmSys Programmable Devices and Standards Compliance - 13 November 2020, CM9 2020/309132
16. RQ-UKHPR1000-1360 - C&I - Comparison Analysis for FirmSys based Systems with 60987 - 07 December 2020, CM9 2020/318226

Regulatory Observation Actions

In addressing the actions listed below, please take into account the information provided in the background section of this RO.

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

In response to this Regulatory Observation 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 points 1 to 10 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 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.

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

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

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

In response to this Regulatory Observation 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 required by '*to be determined by General Nuclear System Resolution Plan*'

REQUESTING PARTY TO COMPLETE

Actual Acknowledgement date:	
RP stated Resolution Plan agreement date:	