REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-UKHPR1000-0052
Revision:	0
Date sent:	03/11/20
Acknowledgement required by:	24/11/20
Agreement of Resolution Plan Required by:	30/12/20
CM9 Ref:	2020/305756
Related RQ / RO No. and CM9 Ref: (if any)**:**	2020/290197
Observation title:	Design and Safety Case for Class 1 and 2 Human Machine Interfaces Employed in the Main Control Room and Remote Shutdown Station
Lead technical topic: 3. Control & Instrumentation	**Related technical topic(s):** 11. Human Factors

Regulatory Observation

Background

The Requesting Party (RP) has submitted a number of documents to describe the Human-Machine Interface (HMI) safety case for the UKHPR1000 Main Control Room (MCR) and Remote Shutdown Station (RSS) for the purposes of Generic Design Assessment (GDA) Step 4 as detailed in ONR guidance [4]. ONR has assessed these submissions and sought further information through Regulatory Queries (RQs). Furthermore this topic has been discussed at Level 4 meetings between the RP and ONR. This Regulatory Observation (RO) is specifically concerned with the Class 1 and Class 2 HMI deployed in the MCR and RSS. A brief summary of these interactions is provided below as the background to this RO:

- Received submissions relevant to Class 1 and Class 2 HMI:
  - The 'Pre-Construction Safety Report Chapter 8' [1] describes the HMI architecture of the MCR and gives a brief description of the types of HMI systems employed in the MCR and RSS.
  - The 'Strategy for the use of HMIs' [2] describes the layout of the MCR and RSS with regard to HMI, and explains which plant states each HMI is required to monitor and/or control. The document further describes some of the visual aspects of the HMI screens.
  - 'Overall Scheme for Control Room System' [5] provides details on the layout of the workstations in both MCR and RSS.

From the assessment carried out to date it is not clear where the safety functional and performance requirements of the HMI design scheme are defined, how they have been derived and how they are addressed. Furthermore the assessment has highlighted the use of touchscreen technology for Class 1 HMI.

ONR has raised a number of Regulatory Queries (RQs) to seek further information:

- RQ-UKHPR1000-0231 'Use of touchscreen displays for class 1 system' [6]:
  - ONR queried the use of Class 1 touchscreen HMIs and requested a description of the justification used for these devices. In response, the RP provided a brief overview of features associated with the device; this was not considered to be sufficient to address ONR's concerns with respect to the use of touchscreen technology in a Class 1 system.
- RQ-UKHPR1000-0354 'Further queries on the justification of touch screen displays for class 1 system' [7]:
  - ONR requested further information regarding the Production Excellence (PE) and Independent Confidence Building Measures (ICBMs) that would be performed on the PS-

SCID200s. The response claims that the PE [12] and ICBM [13] documentation that is to be produced for the FirmSys platform will cover this. However, ONR's assessment of these submissions has not identified any argumentation or evidence to justify the use of the PS-SCID200s in a safety Class 1 system, or where this information could be found.
    - Further claims are made in the RQ response on the suitability of the touchscreen technology, detailing size constraints in the MCR, however no argumentation or evidence is provided to demonstrate the adequacy of the PS-SCID200s for their proposed role.
- RQ-UKHPR1000-0817 'Further queries on the justification of touch screen displays for class 1 system' [8]:
    - ONR requested further information on the PS-SCID200s, referring the RP to publicly available information from previous GDAs on how this issue was addressed. The RP acknowledged the challenge in providing a safety justification for Class 1 touchscreens for the UK HPR1000 and committed to performing optioneering on the use of alternative technology.
    - ONR also requested information on where the requirements for the Class 1 HMIs were derived and how these requirements were used to design the HMI. The RP's response made no reference to the safety functional requirements. ONR also requested information on differing class system connecting to each other. The RP referred to the response to RQ-UKHPR1000-0812.
- RQ-UKHPR1000-0812 'UK HPR1000 Interconnection between I&C systems' [3]
    - ONR requested further information on the interconnection of systems of different classes. The response to this RQ gave a description of every connection with a rationale for why the connection was necessary. However, it did not provide a justification of adequacy for cases involving communication flow from systems of lower class to systems of higher class. Of specific relevance to this RO is the interconnection between the Class 3 plant computer information and control system (KIC [PCICS]) and the Class 2 SAS for the purposes of enabling control on the SAS-SCIDs.
- Level 4 meeting on 15 July 2020 [9]:
    - ONR discussed the FirmSys ICBM strategy with the RP. During the discussion the presence of third-party software in the Class 1 and Class 2 HMI was discussed.
- Level 4 meeting on 5 August 2020 [11]:
    - The results of the HMI optioneering discussed in RQ-0817 was presented by the RP. The RP presented a proposed modification to the design reference which would replace the touchscreen technology on the PS-SCID200, SAS-SCID200, and SAS-SCID300.
    - ONR had a number of concerns regarding the content of the presentation, notably that the rationale for the revised HMI technology selection had not been demonstrated.

Following these interactions, ONR has a number of concerns regarding the adequacy of the PS and SAS, Class 1 and Class 2 HMI design and safety case. These are summarised as:

- There is a lack of a suitable and sufficient safety case for the Class 1 and Class 2 HMI design.
- There is a lack of specific PE demonstration and ICBM strategy for the Class 1 and Class 2 HMI.
- There is a lack of design documentation for the HMI, specifically with regard to functional and performance requirements.
- The presence of touchscreen technology in the current design reference has not been justified.
- It is unclear to what extent the analysis of C&I spurious actuation has considered spurious actuation due to HMI, and what the sensitivity of the safety systems is to HMI mal-operation.
- It is unclear how Human Factors have been considered in the design of the HMI.
- The presence of third-party software in the Class 1 and Class 2 HMI is unclear.
- The rationale behind the selection of HMI technology has not been demonstrated.
- It is unclear if flexibility has been incorporated into the design for future expansion and modification.
- It is unclear how the communication flow from lower class to higher class HMI will be justified.

This Regulatory Observation (RO) has therefore been raised to:

- Explain ONR's regulatory expectations for the use of HMI devices for Class 1 and Class 2 systems.
- Ensure that the safety functional and performance requirements of the Class 1 and Class 2 HMI technologies are clearly defined.
- Ensure that the technologies chosen to meet the safety functional and performance requirements are appropriate.
- Ensure that a suitable and sufficient safety case is presented during GDA.

Relevant Legislation, Standards and Guidance

The following ONR Safety Assessment Principles (SAPs) [15] and Technical Assessment Guides (TAGs) [16] are of particular relevance to this RO:

ECS.2 – Safety classification of structures, systems and components
Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance to safety.

A key paragraph of ECS.2 for this RO is paragraph 167:
Appropriately designed interfaces should be provided between (or within) structures, systems and components of different classes to ensure that any failure in a lower class item will not propagate to an item of a higher class. Equipment providing the function to prevent the propagation of failures should be assigned to the higher class.

EDR.1 – Failure to safety
Due account should be taken of the need for structures, systems and components to be designed to be inherently safe, or to fail in a safe manner, and potential failure modes should be identified, using a formal analysis where appropriate.

EDR.2 – Redundancy, Diversity, and Segregation
Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components.

EDR.3 – Common cause failure
Common cause failure should be addressed explicitly where a structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability.

EDR.4 - Single failure criterion.
During any normally permissible state of plant availability, no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.

ESS.17 – Faults originating from safety systems
Potential faults originating from within safety systems (e.g. due to spurious or mal-operation) should be identified and protection against them provided.

ESS.20 – Avoidance of connections to other systems
Connections between any part of a safety system and a system external to the facility (other than to safety system support and monitoring features) should be avoided.

ESS.21 – Reliability
The design of safety systems should avoid complexity, apply a failsafe approach and incorporate means of revealing internal faults at the time of their occurrence.

ESS.22 – Avoidance of spurious actuation
Spurious actuation of safety systems should be avoided by means such as the provision of multiple independent divisions within the design architecture and majority voting.

ESS.25 - Taking safety systems out of service
The vetoing or the taking out of service of any safety system function should be avoided.

ESS.27 – Computer-based Safety Systems
Where the system reliability is significantly dependent upon the performance of computer software, compliance with appropriate standards and practices throughout the software development lifecycle should be established in order to provide assurance of the final design.

ESR.1 – Provision in control rooms and other locations
Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate secondary control or monitoring locations.

ESR.2 – Performance requirements
The reliability, accuracy, stability, response time, range and, where appropriate, the readability of instrumentation, should be adequate for it to deliver its safety functions.

EHF.1 – Integration with design, assessment and management
A systematic approach to integrating human factors within the design, assessment and management of systems and processes should be applied throughout the facility's lifecycle.

EHF.7 – User interfaces
Suitable and sufficient user interfaces should be provided at appropriate locations to provide effective monitoring and control of the facility in normal operations, faults and accident conditions.

ONR technical assessment guide NS-TAST-GD-046 provides details on ONR expectations for the justification of complex software systems in safety roles.

ONR technical assessment guide NS-TAST-GD-051 provides details on ONR expectations for the scope and content of nuclear safety cases.

In addition the following international standards are of particular relevance:

IEC 61513 Nuclear power plants. Instrumentation and control important to safety. General requirements for systems. Specific clauses: 5.4.2.3, 5.4.2.4, 5.4.3, 5.4.4.2, and 5.5.2 are of particular relevance to this RO.

IEC 60987 Nuclear power plants. Instrumentation and control important to safety. Hardware design requirements for computer-based systems. Specific clauses: 5.2.1, 5.2.3, 6.2.1, 6.3.1, and 6.9.1 are of particular relevance to this RO.

IEC 60880 Nuclear power plants. Instrumentation and control important to safety. Software aspects for computer-based systems performing category A functions. Specific clauses: 6.1.2, 6.1.3, 6.1.6, 6.4.1, and 6.4.2 are of particular relevance to this RO.

IEC 62138 Nuclear power plants. Instrumentation and control important to safety. Software aspects for computer-based systems performing category B or C functions. Specific clauses: 6.2.1.2, 6.3, 6.3.2.1.1, and 6.3.2.2.4 are of particular relevance to this RO.

Regulatory Expectations

A key expectation in the UK is that nuclear facilities should be designed such that the HMIs are considered as an integral part of the system(s) with which they interface, and that they should be designed in accordance with the classification of the overall system. Any hazards that the HMI can introduce to the system should be defined in the safety case and mitigated through appropriate safety measures and robust engineering design. A suitable and sufficient safety case should be presented such that the key design features relating to the safety of the HMI and the safety impact of the HMI is communicable to stakeholders of the UK HPR1000 project.

ONR expects the RP to produce a safety case justifying the Class 1 and Class 2 HMI design scheme for the MCR and the RSS, with safety claims, arguments, and evidence associated with each technology utilised. This

safety case is expected to substantiate the design which should include why the technologies employed by the HMI were chosen and how this impacts the safety of the systems with which they interface. ONR expects that the safety case will give due consideration to the PE demonstration and selection of suitable ICBMs to demonstrate the fitness for purpose of the HMI design as it is developed.

ONR expects that the design and justification of HMI equipment will meet UK relevant good practice (RGP), as defined in the legislation, standards and guidance identified above.

A justification should be provided that risks from the Class 1 and Class 2 HMI design for the MCR and RSS have been reduced 'As Low As Reasonably Practicable' (ALARP) [10].

Where RGP is not met; ONR expects that the RP will conduct an optioneering study, as part of the ALARP justification, as presented for the three touchscreen SCIDs systems in the Level 4 on 5 August 2020 [11]. This process should also generate a programme of work for when the optioneering results will be incorporated into a modification of the reference design. ONR expects as a minimum a suitable concept design to be developed within GDA. The information provided should be sufficient to give ONR confidence in the feasibility of the proposed design.

ONR expects that the RP will select technologies that offer the optimised solution between the C&I and Human Factors safety case requirements. This should also take into account the necessary flexibility and spare capacity in the system design to make alterations during the licensing phase and beyond. This should also take into account any expected interfaces to other C&I systems, such as the Emergency Control Room.

ONR expects the RP to consider any modifications in the context of the overall design of the MCR and RSS HMI. Specific consideration should be given to the Human Performance aspects of including multiple interface types within the MCR (i.e. touchscreen, mouse and keyboard, dials and buttons, etc.) versus the benefits of maintaining a small plant footprint (as explained by the RP in [7] to be a key reason touchscreen technology was specified).

The RP should identify and justify where in the HMI design of the Class 1 and Class 2 systems third party software is used, and how the integrity of this software will be demonstrated given the PE and ICBM requirements set out in the FirmSys platform PE [12] and/or ICBM [13] documents. Third party software is software that has been developed by another organisation or organisations, and for which little to 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.

ONR expects that the RP will have recognised all areas in which the HMI can spuriously actuate (such as by taking safety systems out of service by inhibiting safety functions during plant operation phases). ONR expects that the RP will address spurious actuation by design, not by arguing likelihood. The work undertaken by the RP in Step 3 to address the effects of spurious actuation on safety systems should be used to inform an analysis of the sensitivity of the Class 1 and Class 2 systems to spurious HMI actuation.

ONR expects that the RP provide a suitable and sufficient justification for the interconnection from the KIC [PCICS] to the SAS-SCIDs, in particular demonstration that failure of the lower class system cannot affect the safety function of the higher class system. ONR expects that the higher class system can operate independently of the lower class system.

References

[1] HPR/GDA/PCSR/0008 - Pre Construction Safety Report Chapter 8 Instrumentation and Control, Rev 001, 10 January 2020, CM9 Ref. 2020/13661
[2] GHX06100012DIKX03GN - Strategy for the use of HMIs, Rev A, 26 June 2019, CM9 Ref. 2019/183990
[3] RQ-UKHPR1000-0812 'UK HPR1000 Interconnection Between I&C Systems' CM9 Ref. 2020/151975
[4] ONR-GDA-GD-001 – 'New Nuclear Reactors: Generic Design Assessment - Guidance to Requesting Parties for the UK HPR1000, Rev 4, October 2019
[5] GHX06001009DIKX03GN – Overall Scheme for Control Room System, Rev E, 30 May 2019, CM9 Ref. 2019/156200
[6] RQ–UKHPR1000-0231 'Use of touchscreen displays for class 1 system'
[7] RQ-UKHPR1000-0354 'Further queries on the justification of touch screen displays for class 1'
[8] RQ-UKHPR1000-0817 'Further queries on the justification of touch screen displays for class 1'

[9] ONR-NR-CR-292, Level 4, Control & Instrumentation Independent Confidence Building Measures (ICBMs) Strategy, 15 July 2020, CM9 Ref. 2020/218852
[10] NS-TAST-GD-005 – 'Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), Rev 10, December 2019, CM9 Ref. 2019/315236
[11] ONR-NR-CR-392, Level 4 Meeting, Control and Instrumentation Smart Devices Qualification Strategy, 05 August 2020, CM9 Ref. 2020/250441
[12] FirmSys PE document GHX56100036GSNS44TR – Demonstration of Production Excellence for FirmSys Platform, Rev B, 26 May 2020, CM9 Ref. 2020/159500
[13] GHX06100015DIYK03GN – Strategy for Conducting ICBMs Activities for RPS [PS], Rev A, 29 November 2019, CM9 Ref. 2019/354885
[14] GHX06002024DIYK03GN – Optioneering Analysis Report for CIM Improvement, Rev A, 05 August 2020, CM9 Ref. 2020/235629
[15] ONR Safety Assessment Principles – 2014 edition, Rev 1, January 2020, CM9 Ref. 2019/367414
[16] ONR TAGs NS-TAST-GD-46 (Rev 6) 'Computer Based Safety Systems' & NS-TAST-GD-51 (rev 6) 'The purpose, scope, and content of nuclear safety cases'

Regulatory Observation Actions

RO-UKHPR1000-0052.A1 – HMI Requirements for Class 1 and Class 2 HMI in the MCR and RSS

In response to this Regulatory Observation Action, GNSL should provide documentation that defines:

- the safety functional and performance requirements for both C&I and Human Factors aspects of the Class 1 and Class 2 HMI;
- how these safety requirements are implemented in the design; and
- how these safety requirements will be validated.

RO-UKHPR1000-0052.A2 – Class 1 and Class 2 Computer-Based HMI Technology Optioneering

In response to this Regulatory Observation Action, GNSL should:

- Present a suitable and sufficient optioneering study for the Class 1 and Class 2 touchscreen systems (PS-SCID and SAS-SCID). The information presented should include, but not be limited to:
    - options considered;
    - criteria applied;
    - analysis of options;
    - selection of a preferred option; and
    - a program of work for incorporating any modification to the current design.

  ONR expects that the optioneering will consider the impact of any modification to the HMI on the overall justification of the MCR design. Specific consideration should be given to the Human Performance aspects of including multiple interface types within the MCR versus the benefits of maintaining a small plant footprint.

  ONR also expects that the optioneering and technology selection will consider human factors requirements, and how these will be balanced with C&I requirements to achieve the optimal design.

  The CIM optioneering paper provided to ONR recently provides an example of what is expected [14].

RO-UKHPR1000-0052.A3 – Suitable and sufficient Safety Case for Class 1 and Class 2 HMI in the MCR and RSS

In response to this Regulatory Observation Action, GNSL should provide a suitable and sufficient safety case justifying the selected design for the Class 1 and Class 2 HMI in the MCR and RSS. The safety case should address the following in particular:

- Justification of how the technologies will meet the HMI safety functional and performance requirements identified in the resolution of RO-UKHPR1000-0052.A1, and how interfaces to other C&I systems will be demonstrated to be adequately safe.

- Identification of the presence of any third-party software in the Class 1 and Class 2 HMI, justification for the use of this software and a description of how the required integrity will be demonstrated. Specific consideration should be given to the demonstration of PE and the selection of suitable ICBM to demonstrate the fitness for purpose of the HMI

- Explanation of the extent to which the analysis of spurious actuation of C&I systems has considered the potential for spurious actuation to be initiated by HMI faults or mal-operation.

- Justification for the interconnection of the Class 3 KIC to the Class 2 SAS HMI, including how fault propagation from a lower class to a higher class system will be prevented and how the delivery of the SAS safety functions will not be compromised by a failure of the KIC.

- Justification that the Class 1 and Class 2 HMI design in the MCR and RSS reduces risk ALARP.

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