REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-UKHPR1000-0016
Revision:	0
Date sent:	20/09/19
Acknowledgement required by:	11/10/19
Agreement of Resolution Plan Required by:	31/10/19
TRIM Ref:	2019/209165
Related RQ / RO No. and TRIM Ref: (if any)**:**	
Observation title:	Demonstration of compliance with relevant good practice for control and instrumentation
Lead technical topic: 3. Control & Instrumentation	**Related technical topic(s):** 7. Electrical Engineering 9. Fault Studies

Regulatory Observation

Background

The requirement for duty holders to demonstrate that risks have been reduced as low as reasonably practicable (ALARP) is fundamental to UK health and safety legislation and applies to the design, construction and operation of nuclear power plants. It is therefore an essential objective of generic design assessment (GDA) for the requesting party's (RP's) nuclear safety submissions during generic design assessment to demonstrate that risks have been reduced ALARP.

A key element of ALARP is the demonstration of the application of established relevant good practice (RGP). ONR considers RGP as those standards for controlling risk which have been judged and recognised by us as satisfying the law, when applied to a particular relevant case in an appropriate manner.

Sources of RGP include:

- Guidance within Approved Codes of Practice; for example, the Provision and Use of Work Equipment Regulations 1998;
- Office for Nuclear Regulation (ONR) guidance including ONR's Safety Assessment Principles, Technical Assessment Guides and Technical Inspection Guides;
- Standards produced by standards making organisations, for example British Standards Institution (BSI), International Electrotechnical Commission (IEC), International Atomic Energy Agency (IAEA) and Western European Nuclear Regulators' Association (WENRA);
- Guidance agreed by a body representing an industrial / occupational sector; and
- Well defined and established standard practice adopted by an industrial / operational sector.

In the control and instrumentation (C&I) discipline, ONR has assessed several of the requesting RP's safety case submissions and has found that while in many cases sources of RGP are identified, the level of substantiation of how the normative and informative requirements set out in the RGP has been considered and addressed within the C&I design is inadequate. The following issues in particular have been encountered:

- Compliance statements provide very high level analysis against clauses and principles but do not provide visibility of the claims, arguments and evidence that demonstrate how the design of the UK HPR1000 C&I architecture and systems is adequate. For example, the *'SAPs Conformance*

Assessment of I&C Systems Design' [3] only provides high level, generic statements against each principle but does not describe how the C&I design addresses the expectations and claims made, nor does it provide links to the evidence to demonstrate compliance in each case.

- Some standards that ONR would consider as RGP in a particular application appear not to have been considered. For example, the *Component Interface Module (CIM) Requirement Specification* [1] does not identify IEC 62566 as an applicable standard for the use of programmable logic devices.

- Compliance statements against some standards only consider a narrow selection of clauses, with no justification provided as to those clauses that have been excluded from assessment. For example, the *'Comparison of the overall UK HPR1000 C&I architecture with IEC 61513'* [2] addresses only clauses 5.4.1 – 5.4.4 of the standard.

- Where claims are made that draw on the Reference Plant design (Fanhchenggang Unit 3 (FCG3)), the arguments and evidence provided do not discuss relevant information from the FCG3 design, or how this relates to the UK HPR1000 safety case. (Note: This point is relates to the RP's response to RQ-UKHPR1000-0238 [5] and the subsequent letter from ONR to GNS on 28 June 2019 *'Concerns Regarding Development of the Generic UK HPR1000 Safety Case'* [6].)

Note: the above is a list of examples identified during ONR's assessment to date. It should not be considered an exhaustive list.

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

- Explain ONR's regulatory expectations for the identification of and demonstration of compliance with RGP;
- Ensure the RP adequately identifies all RGP they consider applicable to the UK HPR1000 C&I design, and that a suitable and sufficient justification of compliance with that RGP is provided in the UK HPR1000 safety case;
- Ensure that all relevant evidence, including information from the FCG3 design is appropriately identified and provided in the UK HPR1000 safety case; and
- Obtain confidence that shortfalls against C&I RGP are identified and suitably addressed in the UK HPR1000 generic design, thereby supporting a robust ALARP case.

Relevant Legislation, Standards and Guidance

There are a number of safety assessment principles (SAPs) [6] that are relevant to this RO:

SC.1 – Safety case production process
The process for producing safety cases should be designed and operated commensurate with the hazard, using concepts applied to high reliability engineered systems,

ECS.3 – Codes and standards
Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate codes and standards.

ECS.4 – Absence of established codes and standards
Where there are no appropriate established codes or standards, an approach derived from existing codes or standards for similar equipment, in applications with similar safety significance, should be adopted.

ECS.5 – Use of experience, tests or analysis
In the absence of applicable or relevant codes and standards, the results of experience, tests, analysis, or a combination thereof, should be applied to demonstrate that the structure, system or component will perform its safety function(s) to a level commensurate with its classification.

ONR technical assessment guide NS-TAST-GD-005 [7] provides ONR expectations for the demonstration of ALARP. Of particular relevance to this RO are the following paragraphs:

"1.3 The requirement for risks to be ALARP is fundamental and applies to all activities within the scope of the Health and Safety at Work (etc) Act 1974 [HSWA]. It is important that inspectors in whatever role are aware of the need to ensure that licensees meet this requirement where it applies. In simple terms it is a requirement to

take all measures to reduce risk where doing so is reasonable. In most cases this is not done through an explicit comparison of costs and benefits, but rather by applying established relevant good practice and standards. The development of relevant good practice and standards includes ALARP considerations so in many cases meeting them is sufficient. In other cases, either where standards and relevant good practice are less evident or not fully applicable, the onus is on the licensee to implement measures to the point where the costs of any additional measures (in terms of money, time or trouble – the sacrifice) would be grossly disproportionate to the further risk reduction that would be achieved (the safety benefit)"

"4.4 The criteria for determining whether an explicit ALARP demonstration is required in relation to the Engineering SAPs, which represent ONR's views of relevant good practice, are not set out in numerical terms. Instead, if the relevant SAP is evidently well satisfied, then the facility should be considered to be meeting the equivalent of the TOR broadly acceptable criterion on that particular point and therefore there is unlikely to be a need for further assessment against ALARP. Conversely, any non-conformance with relevant good practice should be explicitly highlighted and then justified as reducing risks to ALARP within the safety case"

"6.8 In many cases licensees will claim that the implementation of a particular relevant good practice or standards is sufficient to demonstrate ALARP. In assessing such claims inspectors should apply SAPs ECS.3 to ECS.5 and EQU1 (paras 169 to 177) and in particular may consider:

- *the good practice or standard should be relevant to the specific application, plant, facility or industry in question.*
- *the good practice or standard should be up-to-date, taking account of the current state-of-the-art: any practice or standard more than a few years old, or not subject to active ongoing monitoring and review or not written by acknowledged experts may be suspect.*
- *the good practice or standard should not be in the form of a minimum requirement.*
- *where a good practice or standard allows for more than one option, these should be tested to determine those which are reasonably practicable.*
- *the good practice or standard should include explicitly all relevant factors, particularly relating to assumptions on the standards of contingent systems or inputs/outputs. Standards and good practice may relate to single Systems, Structures and Components and further consideration may need to be given to possible interactions.*
- *there should be no doubt about the applicability of the good practice or standard to the case in point."*

Regulatory Expectations

ONR's regulatory expectation is that the safety case for the UK HPR1000 generic design should adequately identify and address C&I RGP in the UK context, providing a clear 'line of sight' from the safety case claims to the detailed arguments and evidence. It should clearly identify where gaps or shortfalls against RGP exist and articulate how these impact the generic design. Any gaps should be adequately progressed to provide a robust demonstration that the UK HPR1000 C&I design reduces relevant risks to ALARP. Where claims are made that rely on evidence from the reference plant design, this should be clearly articulated in the arguments with links to the specific evidence provided. The relevant evidence should be provided to ONR in a way that provides a clear link to the claims and arguments and demonstrates how these are met.

To achieve this, as part of the resolution of this RO, the RP will need to undertake and document the following activities:

- Identify the sources of C&I RGP in the UK context, and justify its applicability to the UK HPR1000 C&I design.

- Undertake a comprehensive comparison of the UK HPR1000 C&I design against the identified RGP and provide detailed justifications in the safety case of how the RGP is adequately addressed.

- Identify gaps against RGP for the UK HPR1000 generic design. The significance of any identified gaps should be articulated and an explanation of how these will be addressed during GDA should be provided. Plans and timescales for the application of the RP's ALARP methodologies should also be included in order to demonstrate the UK HPR1000 C&I design reduces risks to ALARP.

- Identify and provide any relevant information from the reference plant design (in the context of C&I) on which the claims in the generic UK HPR1000 safety case depend, including the following:
    - Its purpose and position in the safety case, including key links to other safety case documentation.

- o Detailed justification (i.e. arguments) the relevance of this information (i.e. evidence) and how it demonstrates that the safety case claims are addressed.

The Regulatory Observation Actions (ROAs) given below are therefore structured in such a way as to enable the above information to be provided in a logical and step-wise manner, to facilitate ONR's assessment as GDA progresses.

References

[1] Component Interface Module (CIM) Requirement Specification, GHX06002027DIYK03GN, Revision A
[2] Comparison of the overall UK HPR1000 C&I architecture with IEC 61513, GHX00630001DIYK03GN, Revision A.
[3] SAPs Conformance Assessment of I&C Systems Design, GHX00630003DIYK03N, Revision A
[4] Independence Analysis of I&C Systems, GHX06002020DIYK03GN, Revision A
[5] Defence in Depth and Diversity Analysis Report, GHX06002014DIYK03GN, Revision A
[6] Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Revision 0
[7] ONR technical assessment guide NS-TAST-GD-005 Guidance on the Demonstration of ALARP, Revision 9

Regulatory Observation Actions

RO-UKHPR1000-0016.A1 – Identification of relevant good practice

In response to this Regulatory Observation Action, GNS should:

- Identify all sources of RPG considered applicable to the UK HPR1000 C&I design and justify its applicability.

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

RO-UKHPR1000-0016.A2 – Identification of relevant reference design information

In response to this Regulatory Observation Action, GNS should:

- Identify all relevant evidence, including any information from the FCG3 C&I design, on which the claims made in the UK HPR1000 safety case depend, inluding its role in the safety case, the claims it supports and key links to other safety case documentation.
- Provide a clear trail from the safety case claims, through detailed arguments to the evidence that demonstrates that the claims are addressed.

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

RO-UKHPR1000-0016.A3 – Demonstration of compliance with relevant good practice

In response to this Regulatory Observation Action, GNS should:

- Undertake a complete and consistent comparison of the UK HPR1000 C&I design against the identified RGP, including both the normative and informative requirements of RGP.
- Provide detailed justification of compliance with the RGP.
- Identify any gaps or non-compliances against RGP, articulate their significance and provide an explanation of how they will be addressed in GDA.
- Provide a robust demonstration of how the UK HPR1000 C&I design reduces risks ALARP. Where the RP intends to justify a gap or non-compliance with RGP on ALARP grounds, this should demonstrate the options that were considered, why the selected option(s) achieve the optimum safety benefit, why other options were deselected and why measures to further reduce risks are not reasonably practicable.

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:	