REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-UKHPR1000-0021
Revision:	0
Date sent:	23/09/19
Acknowledgement required by:	14/10/19
Agreement of Resolution Plan Required by:	31/10/19
CM9 Ref:	2019/238787
Related RQ / RO No. and CM9 Ref: (if any):	RQ-UKHPR1000-0084 (2018/145259) RQ-UKHPR1000-0171 (2018/402843) RO-UKHPR1000-0004.A4 (2018/255957)
Observation title:	Demonstration of the adequacy of Examination, Maintenance, Inspection and Testing (EMIT) of structures, systems and components important to safety
Lead technical topic: 9. Fault Studies	**Related technical topic(s):** 2. Civil Engineering 3. Control & Instrumentation 6. Cross Cutting 7. Electrical Engineering 14. Mechanical Engineering 15. Probabilistic Safety Analysis 16. Radiological Protection 20. Structural Integrity

Regulatory Observation

Background

Examination, Maintenance, Inspection and Testing (EMIT) of Structures, Systems and Components (SSC) important to safety needs to be adequately considered by the Requesting Party (RP) as part of the Generic Design Assessment (GDA) process. This is required to demonstrate:

- the adequacy of the generic UK HPR1000 design, in particular regarding the relationship between equipment redundancy and EMIT;
- that UK legal requirements regarding EMIT are likely to be met;
- that EMIT has been informed by and appropriately considered within the safety analysis and engineering; and
- the operating rules identified within the safety case consider EMIT.

EMIT identified during the GDA of UK HPR1000 will be a key input for the future licensee to define their arrangements to ensure the on-going safe operation of the facility. During GDA, ONR therefore requires confidence that the EMIT requirements identified or assumed in the safety case are consistent with the design and engineering of the SSCs, and vice versa.

The submissions received to date do not provide sufficient confidence in this regard and the scope, breadth and depth of information is currently inconsistent between technical topics. Often the information received is at the level of general principles, is ambiguous, and is unclear as to what is proposed to be completed during GDA. Importantly, it is unclear how the RP intends to identify the permitted combinations of equipment unavailability for each permitted operating state. Additionally, the safety case links between the EMIT requirements and the safety analysis need to be demonstrated.

The purpose of this RO is therefore to establish:

- the overall strategy and approach to EMIT proposed by the RP;
- the EMIT requirements and assumptions proposed for the generic UK HPR1000 design; and
- whether the design and safety case is consistent with UK legal requirements and regulatory expectations.

Relevant Legislation, Standards and Guidance

A number of regulations place legal obligations on duty holders relating to EMIT. It is important the generic UK HPR1000 design is demonstrated to be compatible with these UK specific requirements. These regulations include, but are not limited to Refs [1] to [6].

ONR's Safety Assessment Principles (SAPs) [7] contain numerous principles of relevance to EMIT. The EMT (Maintenance, inspection and testing) principles define ONR's regulatory expectations to consider EMIT within the safety case. These principles outline the complete lifecycle from identifying requirements through to the assessment of the continued reliability following an event. In particular, EMT.1, 2, 5, 6 and 7 and supporting paragraphs describe the principles that are most applicable during GDA. These SAPs are;

- ***EMT.1*** *– Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case.*

- ***EMT.2*** *– Structures, systems and components should receive regular and systematic examination, inspection, maintenance and testing as defined in the safety case.*

- ***EMT.5*** *– commissioning and in-service inspection and test procedures should be adopted that ensure initial and continuing quality and reliability.*

- ***EMT.6*** *– provision should be made for testing, maintaining, monitoring and inspecting structures systems and components (including portable equipment) in service or at intervals throughout their life, commensurate with the reliability required of each item.*

- ***EMT.7*** *– In-service functional testing of structures, systems and components should prove the complete system and the safety function of each functional group.*

Furthermore, SAP ESS.2 and ESS.23 from the ESS (safety systems) series of principles explain ONR expectations regarding how EMIT may influence the claims made in the safety case and vice versa. These are:

- ***ESS.2*** *– The extent of safety systems provision, their function, levels of protection necessary to achieve defence in depth and reliability requirements should be specified.*

  399. The design basis (Principles FA.4 (paragraph 626 ff.) and FA.9 (paragraph 641 ff.)) and probabilistic safety (Principle FA.14 (paragraph 660 ff.)) analyses (or other suitable analyses) should determine the safety system provisions, functions and required reliabilities.

- ***ESS.23*** *– In determining the safety systems to be provided, allowance should be made for the potential unavailability of equipment.*

  419. The safety case should identify the permitted combinations of equipment unavailability for each permitted operating state (operating rules), applying design basis analysis (see paragraph 631) and probabilistic safety analysis (see paragraph 653). Reasons for equipment unavailability considered in the safety case should include:

  (a) the need for testing and maintenance;
  (b) …

ONR also expects that the EMIT requirements defined in the safety case are represented appropriately within the safety analysis. Of relevance is SAP FA.2:

- ***FA.6*** *– For each initiating fault within the design basis, the relevant design basis fault sequences should be identified.*

  631. Each design basis fault sequence should include as appropriate:

…
(c) the worst normally permitted configuration of equipment outages for maintenance, test or repair; and
(d) …

ONR also expects that the EMIT requirements defined in the safety case are represented appropriately and consistently within the probabilistic safety analysis (PSA). Of relevance is SAPs FA.13 and FA.14:

- ***FA.13*** *– The PSA model should provide an adequate representation of the facility and/or site.*

  653. The PSA should account for contributions to the risk including, but not necessarily restricted to:

  …
  (d) unavailabilities due to testing and maintenance;
  (e) …

- ***FA.14*** *– PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities.*

  661. Appropriate use of PSA should be made in activities such as:

  …
  (f) informing arrangements for examination, maintenance inspection and testing (eg the frequencies of these activities).
  (g) plant configuration control (including maintenance planning), which for power reactors is normally through the use of risk monitors;
  (h)…

The SAPs are further supported by the associated Technical Assessment Guides (TAG), in particular NS-TAST-GD-009 - Examination, Inspection, Maintenance and Testing of Items Important to Safety [8]. Para. 5.1.1 and 5.1.2 of [8] provide a useful summary of the fundamental expectations.

Regulatory Expectations

To date, ONR does not understand the overall strategy for the identification and justification of the EMIT requirements for the generic UK HPR1000 design, nor the process by which they will be derived and applied consistently throughout the safety case.

Relevant UK legal requirements (from UK regulations) do not appear to have been considered to date in defining any EMIT.

ONR is not confident that the consideration of EMIT is consistent with other aspects of the safety case and associated engineering. PCSR chapter 31 [9] provides a general overview of EMIT. It describes some general principles that are proposed to be applied. However it is unclear what scope of information will be provided as part of GDA, and what the intention is for further developing this information (either during or post-GDA).

Chapter 6 of the System Design Manuals (SDM) (for example [10]) presents the System Operation and Maintenance. These describe, amongst other things, the EMIT requirements for the SSCs. These documents provide important safety case information and the basis for EMIT requirements and management. However, it is stated that "*Detailed information will be supplemented during the site phase*".

In addition, across the technical topics, it is not always clear how the requirements and assumptions which form the basis for the safety analysis are consistent with any engineering requirements, and conversely, how any EMIT requirements that affect the availability of equipment are suitably reflected in the safety analysis. This is particularly true for those SSCs providing the diverse means of delivering Category A safety functions. ONR's expectation is that the worst configuration is considered within the design basis analysis (SAP FA.6). Therefore ONR expect where online EMIT affecting the availability of a SSC providing a safety function is anticipated, this is reflected in the demonstration of fault tolerance and may need to be included in operating rules.

Fundamentally therefore, in response to this RO, ONR is seeking to gain:

- Clarity of the scope of information relating to EMIT that will be submitted during GDA and what will be considered as part of site specific activities (noting that ONR accepts that detailed EMIT procedures and methodologies, for example, are for the site specific stage);

- A demonstration that the EMIT identified in the safety case is consistent with relevant UK legal requirements;

- A demonstration that EMIT proposed for the generic UK HPR1000 design:

  - can be delivered within the operating rules defined by the safety case;
  - is compatible with the necessary engineering requirements, including redundancy, reliability and availability;
  - is consistent with the safety analysis; and
  - is consistent with achieving the reliability claims made on the SSCs.

- Information on how any identified EMIT will be documented, and justified as part of the safety case. This includes how these may be captured as part of the response to RO-UKHPR1000-0004 Action 4 [11].

References

[1] *The Management of Health and Safety at Work Regulations 1999*.
[2] *The Lifting Operations and Lifting Equipment Regulations 1998*.
[3] *The Provisions and Use of Work Equipment Regulations 1998*.
[4] *The Pressure Systems Safety Regulations 2000*.
[5] *Electricity at Work Regulations 1989*.
[6] *The Ionising Radiation Regulations 2017*.
[7] *Safety Assessment Principles for Nuclear Facilities*, 2014 Edition, Revision 0, Office for Nuclear Regulation, 2014. www.onr.org.uk/saps/saps2014.pdf
[8] *Nuclear Safety Technical Assessment Guide, Examination, Inspection, Maintenance and Testing of Items Important to Safety*, NS-TAST-GD-009 Revision 4, Office for Nuclear Regulation, 2018. www.onr.org.uk/operational/tech_asst_guides/index.htm
[9] *Pre-Construction Safety Report, Chapter 31, Operational Management*, HPR/GDA/PCSR/0031, Revision 000, General Nuclear System Ltd, November 2018. www.ukhpr1000.co.uk/documents-library/pre-construction-safety-report/
[10] *RCV – Chemical and Volume Control System Design Manual, Chapter 6 System Operation and Maintenance*, GHX17RCV006DNHX45GN, Rev. B, CGN, August 2018.
[11] *Regulatory Observation - Development of a Suitable and Sufficient Safety Case*, RO-UKHPR1000-0004, Revision 0, Office for Nuclear Regulation, 3 September 2018. www.onr.org.uk/new-reactors/uk-hpr1000/ro-res-plan.htm

Regulatory Observation Actions

RO-UKHPR1000-0021.A1 – Examination, Maintenance, Inspection and Testing (EMIT) Strategy

In response to this Regulatory Observation Action, GNS should:

- Provide a strategy which explains how EMIT will be derived, justified and included within the safety case for the generic UK HPR1000 design. This should adequately describe the scope of the EMIT aspects of the safety case to be produced during GDA, and what is proposed to be carried over to site specific stages. The information provided should enable ONR to judge whether a suitable and sufficient safety case will be produced that is likely to meet UK legal requirements and regulatory expectations.

- ONR considers that the response to this Action should include information on:

  - How UK specific legal requirements related to EMIT will be identified and addressed within the generic safety case.
  - The intended operating profile assumed for the design and how this relates to EMIT, including refuelling outages and maintenance windows, as appropriate.
  - An explanation and justifcation of the underpinning rationale (philosophy) for EMIT of SSCs important to safety in the UK HPR1000 design and how this is consistent with the safety analysis.

- How EMIT requirements for SSCs important to safety will be derived during GDA, taking into account relevant factors such as good practice or likely (key) supplier or manufacturer requirements.
- How codes and standards will inform the development of EMIT requirements.
- How the safety case will demonstrate that the regulatory expectations of the SAPs will be met, in particular those SAPs detailed above.
- How any EMIT will be captured as part of the generic safety case produced during GDA, and how these could be further developed by a future licensee as part of site specific stages.
- How operating rules will be informed by EMIT requirements.

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

RO-UKHPR1000-0021.A2 – Demonstration that the UK HPR1000 design and safety case is compatible with the EMIT Strategy

In response to this Regulatory Observation Action, GNS should:

- Provide sufficent information to demonstrate that the UK HPR1000 generic safety case is consistent with the EMIT strategy produced in response to Action 1. The response should provide a proportionate response for key aspects. ONR considers that the response to this Action should include a demonstration that:

    - Redundancy, availability and reliability requirements will be derived from and reflected in the safety analysis. This should include both probabilistic and deterministic analysis and take account of relevent regulatory expectations.
    - Identified EMIT is consistent with engineering requirements for the SSCs, and vice versa.
    - Appropriate codes and standards are used to inform the EMIT.
    - The PSA has included explicit consideration of EMIT, and how the component reliability information has been informed by EMIT.
    - EMIT has influenced the design or layout of SSCs important to safety, where necessary.
    - Identified operating rules take account of EMIT.

- Provide a suitable and sufficient forward work plan to fully implement the relevent aspects of the EMIT strategy (produced in response to Action 1) into the generic safety case during GDA. This may also need to capture any topic specfic aspects, as necessary.

- Provide evidence that EMIT, including that identified to be taken forward by a future licensee as part of site specific stages, is appropriately captured as part of the generic safety case.

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:	