REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-UKHPR1000-0025
Revision:	0
Date sent:	10/12/19
Acknowledgement required by:	02/01/20
Agreement of Resolution Plan Required by:	13/01/20
TRIM Ref:	2019/324427
Related RQ / RO No. and TRIM Ref: (if any)**:**	
Observation title:	Vital Area Identification and Categorisation
Lead technical topic: 18. Security	**Related technical topic(s):** 2. Civil Engineering 6. Cross Cutting 8. External Hazards 9. Fault Studies 12. Internal Hazards 16. Radiological Protection 19. Severe Accident Analysis 20. Structural Integrity

Regulatory Observation

Background

Vital Area Identification (VAI) is part of the overall process that a dutyholder should apply to understand the potential vulnerability of plant areas to sabotage. A Vital Area (VA) is defined as '*an area containing nuclear material and/or other radioactive material (including radioactive sources) or equipment, systems, structures or devices the sabotage or failure of which, alone or in combination, through malevolent acts as defined in the extant NIMCA* [Nuclear Industries Malicious Capabilities Planning Assumptions] *document, could directly or indirectly result in Unacceptable Radiological Consequences (URCs), thereby endangering public health and safety by exposure to radiation*' [1]. To ensure that VAs are provided with a proportionate level of protection, each should be categorised as a Vital Area or a High Consequence Vital Area in accordance with the table in Annex B of the SyAPs [2].

During GDA, ONR expects the Requesting Party (RP) to undertake suitable and sufficient Vital Area Identification (VAI) work, including categorisation of the identified VAs. This should take account of the potential to give rise to an Unacceptable Radiological Consequence (URC) from direct application of the UK Design Basis Threats (DBT) [3] or where the threats could be used in combination over a number of systems to either give rise to a URC or increase the size of a URC. This is an important part of demonstrating that the generic UK HPR1000 design is robust to potential sabotage against the UK DBT [3].

The RP submitted the latest version of their VAI study [4] in September 2019. ONR subsequently provided feedback on this document at a technical meeting in October 2019 [5], which highlighted a number of shortfalls in meeting regulatory expectations, in particular regarding the categorisation of the identified VAs and the scope of VAI that had been completed to date. These shortfalls form the basis for this Regulatory Observation (RO).

The purpose of this RO is therefore to establish:

- the improvements necessary in the RP's application of its Vital Area Categorisation and Classification methodology [based on the original submission at 6]; and

- the regulatory expectations regarding the work necessary to be completed during GDA to deliver a suitable and sufficient VAI study for the generic UK HPR1000 design, and demonstrate compliance with relevant SyAPs [7].

Relevant Legislation, Standards and Guidance

Further details of the regulatory expectations regarding identification and categorisation of VAs are provided in the SyAPs [7]. Fundamental Security Principle (FSyP) 6 – Physical Protection Systems (PPS), and associated paragraphs, provides the overall expectation within the scope of GDA:

Fundamental Security Principle	Physical Protection Systems	FSyP 6
Dutyholders must implement and maintain a proportional physical protection system that integrates technical and procedural controls to form layers of security that build defence-in-depth and are graded according to the potential consequence of a successful attack.		

147. *Physical Protection Systems (PPS) integrate people, procedures and equipment for the protection of assets against theft, sabotage or other malicious activity. The design of a physical protection system requires a methodical approach in which the designer weighs the objectives of the system (i.e. protection of identified targets) and then evaluates the performance of the proposed design to determine how well it meets the objectives.*

148. *Accordingly, these SyDPs are ordered in such a way that starts with a process of target identification for theft and sabotage, followed by a graded model of system design incorporating a security outcome and posture for the system and an assessment of effectiveness through vulnerability analysis.*

Security Delivery Principle (SyDP) 6.2 – Categorisation for Sabotage, provides further expectations regarding categorisation against sabotage.

FSyP 6 - Physical Protection Systems	Categorisation for Sabotage	SyDP 6.2
Dutyholders should undertake a characterisation of their site and facilities in order to determine the categorisation for sabotage.		

152. Dutyholders should categorise their site and facilities for sabotage by undertaking a process of vital area identification (refer to the sabotage categorisation table at Annex B). This is essential to determine the required outcome for the protective security system and allow the graded approach to be applied. Vital areas may be identified where there is no NM/ORM present, for example on generating power stations where systems are essential to maintain control, containment or cooling.

Further details can be found in the associated Technical Assessment Guide (TAG) [1]. This provides specific expectations regarding the adequacy of a VAI study.

Regulatory Expectations

In responding to this RO, ONR expects the RP to:

- Further develop their arrangements for Vital Area Identification (VAI) [4] throughout the remainder of Step 3 and into Step 4 of GDA, on timescales commensurate with delivering suitable and sufficient VAI and categorisation work for the generic UK HPR1000 design. These arrangements, when implemented, must be able to accurately identify the Systems, Structures and Components (SSCs) and areas within and around the generic UK HPR1000 design which are potential VAs.

- Provide suitably categorised VAs, in accordance with regulatory expectations. The RP's Vital Area Categorisation and Classification methodology [1] was submitted with the Annex G Phase 5: Identification of Vital Areas [4]. The methodology stated that "*In accordance with the requirements of SyAPs all VAs are categorised based on the potential radiological consequence*". This categorisation has not yet been presented to ONR for assessment, but this is required.

- As part of the VAI and Categorisation, provide the basis upon which the radiological consequences have been determined and the assumptions which have been applied as a result of the limits of the information available at this stage of the GDA.

Within the Assessment Plan for Step 3, it was ONR's understanding that the RP would issue a VAI and Categorisation for Operating State A (reactor at power) in order to demonstrate their process and allow this to be assessed by ONR. However, the RP did not deliver this in detail and instead presented a document which identifies potential VAs and gives their location by room. Consequently, ONR now expects the RP to present the VAI and Categorisation for Operating State A as soon as practicable. This should be done in time to allow the assessment of and feedback on the Operating State A submission, prior to the RP completing the work on the remaining reactor operating states.

Overall, during Step 4 of GDA the RP should demonstrate the implementation of their arrangements and present a VAI and Categorisation commensurate with the information available at that stage of the GDA. High level guidance as to ONR's expectations of what the RP's arrangements should demonstrate in the VAI and Categorisation are provided below and further guidance can be found in [1 and 2]:

- The RP should assume that all threats described in the NIMCA [3] will be deployed in any conceivable combination.

- The interdependency between SSCs in delivery of safety functional requirements should be considered. This is to include but not limited to redundancy, diversity, segregation, common cause failure, single failure criterion. Further detail can be found in [8].

- A loss of off-site power (LOOP) should be assumed as this cannot be protected by the RP.

- All plant operating states should be considered including both active and passive systems required to maintain plant safety. The intent for this RO is that ONR will assess the submission for Plant Operating State A such that any feedback can be incorporated into the RP's assessments of the other plant states.

- The VA Categorisation should allow for the identification of the PPS outcomes given in the SyAPs document [6] that need to be met (not the PPS design itself in this work).

- The VAI and Categorisation should present a linkage between the identified VAs, the relevant malicious capabilities (in the UK DBT [2]) and the radiological consequences that could result, thus informing the selection of appropriate PPS.

- The assumptions, conclusions and recommendations in any VAI study should be explained and justified. The arguments developed in any study should be supported with factual evidence, and the necessary understanding of the behaviour of associated systems or processes should be established.

- Any analytical methods, such as Deterministic Safety Analysis (DSA), used by the RP to substantiate safety arrangements in a VAI study should be shown to be 'fit for purpose' with adequate verification.

- The RP should ensure a holistic VAI study is developed with clear links between any engineering/technical substantiation or analysis. It should also define where VA protection depends on external facilities and services, and clearly substantiate any associated assumptions that are made.

The output of the RP's VAI and Categorisation for sabotage is to be used as the starting point for the design of PPS measures. PPS design is out of scope of this RO, and ONR expects that no claims and arguments made against perceived or planned PPS will be made within the VAI and categorisation for sabotage submissions.

References

[1] *Nuclear Security Technical Assessment Guide, Target Identification for Sabotage*, CNS-TAST-GD-6.2 Revision 0, Office for Nuclear Regulation, 2017. www.onr.org.uk/operational/tech_asst_guides/index.htm
[2] [Official Sensitive] Annex B of SyAPs – by request to ONR only.
[3] Nuclear Industries Malicious Capabilities Planning Assumptions.
[4] *Annex G Phase 5: Identification of Vital Areas*, GNS-REC-EDF-SEC-000006, Revision 001, General Nuclear System Ltd, September 2019. CM9: 2019/281924.
[5] *Contact Record - UK HPR1000 Generic Design Assessment – Level 4 Security Meeting*, 25 October 2019, ONR-NR-CR-19-298 Revision 0. CM9: 2019/311919
[6] *UK HPR1000 Vital Area Categorisation and Classification Methodology,* HPR-GDA-REPO-0131, Revision 001, General Nuclear System Ltd, September 2019. CM9: 2019/281912.
[7] *Security Assessment Principles for the Civil Nuclear Industry*, 2017 Edition Version 0, Office for Nuclear Regulation, 2017. www.onr.org.uk/syaps/security-assessment-principles-2017.pdf
[8] *Safety Assessment Principles for Nuclear Facilities*, 2014 Edition, Revision 0, Office for Nuclear Regulation, 2014. www.onr.org.uk/saps/saps2014.pdf

Regulatory Observation Actions

RO-UKHPR1000-0025.A1 – Vital Area Identification and Categorisation for Operating State A

In response to this Regulatory Observation Action, GNS should:

- Provide a revised VAI and Categorisation methodology.
- Develop and apply suitable arrangements to deliver a VAI and Categorisation submission for Operating State A, in line with the maturity of the generic UK HPR1000 design.
- ONR considers that the response to this Action should:
    - Identify each vital area and accurately categorise them for sabotage, in line with the regulatory expectations described in this RO.
    - Be subject to an appropriate internal peer review by the RP and be subject to an assurance and governance process prior to being issued.

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

RO-UKHPR1000-0025.A2 – Completion of Vital Area Identification and Categoriastion for all plant operating states

In response to this Regulatory Observation Action, GNS should:

- Provide the VAI and Categorisation for all the remaining reactor Operating States (B to F), based upon the arrangements developed in response to Action 1. The output is to be a submission which, for each of those operating states, identifies the vital areas and accurately categorises them for sabotage in line with the regulatory expectations given in this RO.

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:	