**New Reactor Division – Generic Design Assessment**

# Step 2 Assessment of the Internal Hazards for the UK HPR1000 Reactor

Assessment Report ONR-GDA-UKHPR1000-AR-18-003
Revision 0
October 2018

Published 10/18

## EXECUTIVE SUMMARY

This report presents the results of my Internal Hazards assessment of the UK HPR1000 undertaken as part of Step 2 of the Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA).

The GDA process calls for a step-wise assessment of the Requesting Party's (RP) safety submission with the assessments increasing in detail as the project progresses. Step 2 of GDA is an overview of the acceptability, in accordance with the regulatory regime of Great Britain, of the design fundamentals, including ONR's review of key nuclear safety and nuclear security claims (or assertions). The aim is to identify any fundamental safety or security shortfalls that could prevent ONR from permitting the construction of a power station based on the design.

During GDA Step 2 my work has focused on the assessment of the Internal Hazards aspects within the UK HPR1000 Preliminary Safety Report (PSR), and a number of supplementary documents submitted by the RP, focusing on design concepts, claims and consequences analysis methodologies.

The standards I have used to judge the adequacy of the RP's submissions in the area of Internal Hazards have been primarily ONR's Safety Assessment Principles (SAPs), in particular the Engineering Principles SAPs, and ONR's Technical Assessment Guide NS-TAST-GD-014. I have also made use of other relevant standards and guidance from the International Atomic Energy Agency (IAEA) and the Western European Nuclear Regulators' Association (WENRA).

My GDA Step 2 assessment work has involved regular engagement with the RP in the form of technical exchange workshops and progress meetings, including meetings with the plant designers.

The UK HPR1000 PSR is primarily based on the Reference Design, Fangchenggang Unit 3 (FCG3), which is currently under construction in China. Key aspects of the UK HPR1000 preliminary safety case related to Internal Hazards, as presented in the PSR, its supporting references and the supplementary documents submitted by the RP, can be summarised as follows:

- A design basis event internal hazard will be limited to one division by robust hazard barriers segregating redundant divisions of structures, systems and components (SSCs), such that it will not prevent the delivery of the fundamental safety functions of:
  - Control of reactivity;
  - Removal of heat from the reactor and from fuel store; and
  - Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.
- In areas where segregation by hazard barriers is not feasible, spatial separation between the different divisions of structures, systems and components, or local protection will be incorporated to ensure delivery of the fundamental safety functions.

During my GDA Step 2 assessment of the UK HPR1000 aspects of the safety case related to Internal Hazards, I have identified the following areas of strength:

- The RP has adopted a reasonable approach in their Internal Hazards methodologies, which comprises of: identification of internal hazards sources, identification of safety related SSCs, quantification of loads (hazard specific), identification of unmitigated

consequences, identification of safety measures, assessment of safety measures, and production of a hazard schedule.

- The RP has undertaken an appropriate literature review to support its internal hazards identification study and has commenced its combined hazards identification work to identify credible hazard combinations.
- The RP responded positively to my regulatory expectations on the analysis methodologies for high energy pipes failures. Firstly, the RP accepted the need for postulating gross failure in the analysis methodology and, secondly, it identified all the pipes that have been excluded from analysis of the FCG3 design under the Leak Before Break criteria and containment penetration rupture exclusion rules, and made a commitment to consider them in GDA.
- During my interactions with the RP, the RP presented examples of the consequences analysis undertaken for FCG3 for some internal hazards, and demonstrated reasonable understanding of what is expected in GDA.

During my GDA Step 2 assessment of the UK HPR1000 aspects of the safety case related to Internal Hazards I have identified the following areas that require follow-up during GDA:

- Development of suitable and sufficient claims for all Internal Hazards including EMI, toxic and corrosive material and gases, vehicular impact and combined hazards.
- Development of the hazard barriers claims further to include all penetrations on hazard barriers including doors, access hatches, ventilation ducts and others.
- Demonstration that the UK HPR1000 plant layout is optimised against all Internal Hazards for all building and plant states and reflecting the competing needs from other technical disciplines as appropriate.
- Identification of all exception to segregation areas for all buildings and plant states, and development of suitable Internal Hazards consequence analysis for those areas. Demonstration that segregation of redundant SSCs is provided wherever it is reasonably practicable to do so.
- Demonstration that the revised identification and screening process of internal and external hazards captures the technical gaps that I identified in my assessment.
- Demonstration that the combined hazards identification, screening and analysis methodology captures my regulatory expectations in the derivation of credible combined hazards, and that the derived combined hazards are relevant to the UK HPR1000 design.
- Demonstration that the revised general requirements of protection design against internal and external hazards captures the technical gaps that I identified in my assessment.
- A complete demonstration that all Internal Hazards analysis methodologies are in line with ONR’s expectations and have adequately addressed all of the technical gaps I identified in Step 2.
- The application of the methodology of safety categorisation and classification to all engineering measures delivering the safety claims identified during Step 3 and 4 of GDA.
- Demonstration that the risk from Internal Hazards is reduced to As Low As Reasonably Practicable (ALARP).

During my GDA Step 2 assessment, I have not identified any fundamental safety shortfalls in the area of Internal Hazards that might prevent the issue of a Design Acceptance Confirmation (DAC) for the UK HPR1000 design.

## LIST OF ABBREVIATIONS

| | |
|---|---|
| ALARP | As Low As Reasonably Practicable |
| BMS | Business Management System |
| CGN | China General Nuclear Power Corporation |
| CRDM | Control Rod Drive Mechanism |
| DAC | Design Acceptance Confirmation |
| EA | Environment Agency |
| EDF | Électricité de France |
| EMI | Electromagnetic Interference |
| FCG3 | Fangchenggang Nuclear Power Plant Unit 3 |
| GNI | General Nuclear International |
| GNS | Generic Nuclear System Ltd |
| GDA | Generic Design Assessment |
| HEAF | High Energy Arching Faults |
| IAEA | International Atomic Energy Agency |
| IEEE | Institute of Electrical and Electronics Engineers |
| LBB | Leak Before Break |
| MCR | Main Control Room |
| MOFIS-Z | Systematic Modelling Solution to Fire Safety Design of Nuclear Power Plants |
| NPP | Nuclear Power Plant |
| ONR | Office for Nuclear Regulation |
| PCSR | Pre-construction Safety Report |
| PSR | Preliminary Safety Report (includes security and environment) |
| RO | Regulatory Observation |
| RP | Requesting Party |
| RQ | Regulatory Query |
| SAP(s) | Safety Assessment Principle(s) |
| SSC | Structures, systems and components |
| TAG | Technical Assessment Guide(s) |

| | |
|---|---|
| TSC | Technical Support Contractor |
| UK | United Kingdom |
| WENRA | Western European Nuclear Regulators' Association |

## TABLE OF CONTENTS



### Tables

# 1 INTRODUCTION

1. The Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA) process calls for a step-wise assessment of the Requesting Party's (RP) safety submission with the assessments increasing in detail as the project progresses. General Nuclear System Ltd (GNS) has been established to act on behalf of the three joint requesting parties (China General Nuclear Power Corporation (CGN), Électricité de France (EDF) and General Nuclear International (GNI)) to implement the GDA of the UK HPR1000 reactor. For practical purposes GNS is referred to as the 'UK HPR1000 GDA Requesting Party'.

2. During Step 1 of GDA, which is the preparatory part of the design assessment process, the RP established its project management and technical teams and made arrangements for the GDA of the UK HPR1000 reactor. Also, during Step 1 the RP prepared submissions to be assessed by ONR and the Environment Agency (EA) during Step 2.

3. Step 2 commenced in November 2017. Step 2 of GDA is an overview of the acceptability of the design fundamentals, including the key nuclear safety and nuclear security claims (or assertions) against the regulatory expectations in Great Britain. The aim of Step 2 is to identify any fundamental safety or security shortfalls that could prevent ONR permitting the construction of a power station based on the design.

4. My assessment has followed the GDA Step 2 Assessment Plan for Internal Hazards (Ref. 1), which I prepared in October 2017 and shared with the RP to maximise openness and transparency.

5. This report presents the results of my GDA Step 2 Internal Hazards assessment of the UK HPR1000 safety case as presented in the UK HPR1000 Preliminary Safety Report (PSR) (Ref. 2) and its supporting documentation (Refs 3 – 12 and 23).

# 2 ASSESSMENT STRATEGY

6. This section presents my strategy for the GDA Step 2 assessment of the Internal Hazards aspects of the UK HPR1000 (Ref. 1). It also includes the scope of the assessment and the standards and criteria I have applied.

## 2.1 Scope of the Step 2 Internal Hazards Assessment

7. The objective of my GDA Step 2 assessment was to assess relevant design concepts and claims made by the RP related to Internal Hazards, identification, screening and general requirements of protection design against Internal Hazards, and finally Internal Hazards analysis methodologies and the proposed methodology on categorisation and classification. In particular, my assessment focussed on the following:

- Familiarisation with the UK HPR1000 design;
- Reviewing RP's safety submissions to confirm whether the safety claims related to Internal Hazards are reasonable and complete in light of my current understanding of reactor technology;
- Completeness of the Internal Hazards identification study;
- The adequacy of the general design protection requirements;
- The suitability and sufficiency of the proposed analysis methodologies;
- The suitability and application of the proposed methodology of safety categorisation and classification; and
- Raising Regulatory Queries (RQs) as defined in the Guidance to Requesting Parties (Ref. 21).

8. During GDA Step 2, I have also evaluated whether the safety claims related to Internal Hazards are supported by a body of technical documentation sufficient to allow me to proceed with GDA assessment beyond Step 2. The technical documentation provided by the RP during Step 2, which were reflected in my assessment, included:

- The Identification and Screening Process of Internal and External Hazards, (Ref. 3);
- The General Requirements of Protection Design against Internal and External Hazards (Ref. 4);
- Fangchenggang Nuclear Power Plant Unit 3 (FCG3) drawings for fire zoning and flooding zoning (Ref. 5);
- Internal Hazards analysis methodologies (Refs. 6 – 11);
- Hazards Schedule Methodology (Ref. 12)
- Methodology of Safety Categorisation and Classification (Ref. 23).

9. My assessment of these references is documented in section 4.

10. Finally, during Step 2 I have undertaken the following preparatory work for my Step 3 assessment:

- Preliminary review of Chapter 19 (Internal Hazards) of the Pre-construction Safety Report (PCSR) (Ref. 13);
- Engaged with the RP to develop its PCSR document structure, including the "route-map" of various supporting documents, and submissions schedule. This will allow me to develop a Step 3 Assessment Plan; and
- Preliminary planning of Step 3 assessment activities and commenced interfaces with other disciplines for Step 3.

### 2.2 Standards and Criteria

11. For ONR, the primary goal of the GDA Step 2 assessment is to reach an independent and informed judgment on the adequacy of a preliminary nuclear safety and security case for the reactor technology being assessed. Assessment was undertaken in accordance with the requirements of the Office for Nuclear Regulation (ONR) How2 Business Management System (BMS) guide NS-PER-GD-014 (Ref. 14) and with the Guidance on Mechanics of Assessment within the ONR (Ref.15).

12. In addition, the Safety Assessment Principles (SAPs) (Ref. 16) constitute the regulatory principles against which duty holders' and RP's safety cases are judged. Consequently the SAPs are the basis for ONR's nuclear safety assessment and have therefore been used for the GDA Step 2 assessment of the UK HPR1000. The SAPs 2014 Edition are aligned with the International Atomic Energy Agency (IAEA) standards and guidance.

13. Furthermore, ONR is a member of the Western European Nuclear Regulators' Association (WENRA). WENRA has developed Reference Levels, which represent good practices for existing nuclear power plants, and Safety Objectives for new reactors.

14. The relevant SAPs (Ref. 16), IAEA standards (Ref. 18) and WENRA reference levels (Ref. 19) are embodied and expanded on in the Technical Assessment Guides (TAGs) on Internal Hazards (NS-TAST-GD-014, Ref. 17). This guide provides the principal means for assessing the Internal Hazards aspects in practice.

#### 2.2.1 Safety Assessment Principles

15. The key SAPs (Ref. 16) applied within my assessment are shown below (see also Table 1 for further details):

- Safety Cases: SC.4;
- Key Principles: EKP.3, EKP.5;
- Safety Classification and Standards: ECS.1 and ECS.2
- Equipment Qualification: EQU.1;
- Design for Reliability: EDR.2 and EDR.4;
- Layout: ELO.4;
- External and Internal Hazards: EHA.1, EHA.5, EHA.6, EHA.7, EHA.10, , EHA.14, EHA.15, EHA.16, and EHA.19;
- Safety Systems: ESS.18;
- Fault Analysis: FA.8; and
- Assurance of Validity of Data and Models: AV.2, AV.3, AV.4 and AV.6.

#### 2.2.2 Technical Assessment Guides

16. The following Technical Assessment Guide has been used as part of this assessment:

- NS-TAST-GD-014 Revision 4 (Ref. 17).

#### 2.2.3 National and International Standards and Guidance

17. The following national and international standards and guidance have been considered as part of this assessment:

- Relevant IAEA standards (Ref. 18):

- Specific Safety Requirements No. SSR-2/1. Safety of Nuclear Power Plants: Design. International Atomic Energy Agency (IAEA), 2016.

- Safety Guide No. NS-G-1.7. Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants. International Atomic Energy Agency (IAEA), 2004.
- Safety Guide No. NS-G-1.11. Protection against Internal Hazards other than Fire and Explosions in the Design of Nuclear Power Plants. International Atomic Energy Agency (IAEA), 2004.
- Specific Safety Guide No SSG-30. Safety Classification of Structures, Systems and Components in Nuclear Power Plants. International Atomic Energy Agency (IAEA), 2014.

- Relevant WENRA references (Ref. 19):

- WENRA Reactor Safety Levels for Existing Reactors (September 2014);
- Statement on Safety Objectives for New Nuclear Power Plants (November 2013); and
- Safety of New Nuclear Power Plant (NPP) Designs (March 2013).

## 2.3 Use of Technical Support Contractors

18. During Step 2 I have not engaged Technical Support Contractors (TSCs) to support the assessment for the UK HPR1000.

## 2.4 Integration with Other Assessment Topics

19. Early in GDA, I recognised the importance of working closely with other assessors (including Environment Agency's assessors) as part of the Internal Hazards assessment process. Similarly, other assessors sought input from my assessment of the Internal Hazards for the UK HPR1000. I consider these interactions are key to the success of the project in order to prevent or mitigate any gaps, duplications or inconsistencies in ONR's assessment. From the start of the project, I have endeavoured to identify potential interactions between the Internal Hazards and other technical areas, with the understanding that this position will evolve throughout the UK HPR1000 GDA.

20. The key interactions I have identified are:

- Internal Hazards provide input to design aspects and substantiation of the civil structures by Civil Engineering. This formal interaction has commenced during GDA Step 2. The assessment of internal hazard loads to civil barriers work is being led by the Internal Hazards inspector. Substantiation of the civil barriers will be led by Internal Hazards in coordination with Civil Engineering.
- External Hazards provide input to the identification of combined hazards, which can involve combinations of both internal and external hazards. This formal interaction has commenced during GDA Step 2. The assessment of consequential Internal Hazards will be led by Internal Hazards in coordination with the External Hazards inspector.
- Mechanical Engineering provides input to design aspects of lifting equipment and lifting schedules, which are used in the Internal Hazards consequences analysis of dropped loads. This formal interaction has commenced during GDA Step 2. The dropped load consequence analysis is being led by the Internal Hazards inspector.
- Control and Instrumentation provides input to the claims aspect of the Internal Hazards assessment for example in the appropriate engineering of protective systems such as detection systems for hydrogen atmospheres. In addition, control and instrumentation equipment can be impaired by Internal Hazards compromising the ability to deliver the safety functions unless they are located and specified consistently with the Internal Hazards consequences analysis.

This formal interaction has not commenced during GDA Step 2 work. This work will be led by Internal Hazards in coordination with the Control and Instrumentation inspector.

- Structural Integrity provides input to the analyses and claims aspects of the Internal Hazards assessment. The Internal Hazards analysis will aid in the assessment of the categorisation and classification of Structural Integrity Structures, Systems and Components (SSCs). In addition, an Internal Hazard could affect Structural Integrity related SSCs. This formal interaction has commenced during GDA Step 2 work. This work will be led by Internal Hazards in coordination with the Structural Integrity inspector.
- Fault Studies provides input to the analyses and claims aspects of the Internal Hazards assessment. This formal interaction has not commenced during GDA Step 2 work. This work will be led by Internal Hazards in coordination with the Fault Studies inspector.
- The Internal Hazards analysis provides input to the analyses and claims aspects of the Probabilistic Safety Assessment. This formal interaction has not commenced during GDA Step 2 work. This work will be led by Internal Hazards inspector.
- Human Factors provide input to the analyses and claims aspects of the Internal Hazards assessment. This formal interaction has not commenced during GDA Step 2 work. This work will be led by Internal Hazards in coordination with the Human Factors inspector.

# 3 REQUESTING PARTY'S SAFETY CASE

21. During Step 2 of GDA the RP submitted a Preliminary Safety Case (PSR) and other supporting references, which outline the preliminary nuclear safety case for the UK HPR1000. This section presents a summary of the RP's PSR in the area of Internal Hazards. It also identifies the documents submitted by the RP which have formed the basis of my Internal Hazards assessment of the UK HPR1000 during GDA Step 2.

## 3.1 Summary of the RP's Preliminary Safety Case in the Area of Internal Hazards

22. The aspects covered by the UK HPR1000 PSR and supporting submissions in the area of Internal Hazards can be broadly grouped under four headings which can be summarised as follows:

- Internal Hazards safety case as described in PSR;
- Identification, screening and general requirements of protection design against Internal Hazards;
- Internal Hazards analysis methodologies; and
- Safety categorisation and classification methodology.

### 3.1.1 Internal Hazards Preliminary Safety Report

23. As part of its Step 2 submission the RP has issued a PSR for Internal Hazards, which was based on FCG3 (Ref. 2). The PSR discussed the identification process of Internal Hazards, defined the safety philosophy for Internal Hazards, outlined the assessment methodology and presented safety measures for protection against Internal Hazards.

24. The PSR identified the following Internal Hazards:

- Internal fire;
- Internal flooding/ spray;
- High energy pipe failures;
- Dropped load;
- Internal missiles; and
- Internal explosions.

25. The PSR identified that the Internal Hazards of toxic and corrosive material release, vehicular impact and electromagnetic interference (EMI) will also require consideration during GDA.

26. The PSR also outlined a methodology for identification of combined hazards.

27. The safety philosophy of the UK HPR1000 is based on three segregated divisions of SSCs delivering the fundamental safety functions. A design basis event internal hazard will be limited to one division by robust hazard barriers segregating redundant divisions of SSCs, and therefore will not prevent the delivery of the fundamental safety functions of:

- Control of reactivity;
- Removal of heat from the reactor and from fuel store; and
- Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

28. The PSR stated that where items of different divisions are located in the same hazard influence zone (where segregation of SSCs by robust hazard barriers is not feasible i.e. exceptions to segregation) these will be identified for assessment post Step 2 of GDA.

29. The proposed Internal Hazards assessment methodology included the following steps:

- Identification of Internal Hazards sources;
- Identification of safety related SSCs;
- Quantification of loads (hazard specific);
- Identification of unmitigated consequences;
- Identification of safety measures;
- Assessment of safety measures; and
- Production of a hazard schedule.

30. The PSR presented, at high level, the defence in depth measures that have been applied to the FCG3 design for each internal hazard listed above.

31. The PSR claimed that the hazard barriers are designed to accommodate the loads from all individual Internal Hazards including credible combinations of Internal Hazards.

32. No explicit claims were presented in the areas where segregation is not provided.

### 3.1.2 Identification, Screening and General Requirements of Protection Design Against Internal Hazards

33. In support of the PSR, the RP submitted the Identification and Screening Process of Internal and External Hazards (Ref. 3), and the General Requirements of Protection Design against Internal and External Hazards for the UK HPR1000 design (Ref. 4).

34. In Reference 3 the RP confirmed the list of Internal Hazards that will be considered in GDA. In addition, the RP identified the following additional Internal Hazards: EMI, toxic and corrosive materials and gases and vehicular transport.

35. In Reference 4 the RP presented high level safety requirements for the protection design basis against Internal Hazards.

### 3.1.3 Internal Hazards Analysis Methodologies

36. The RP submitted the following Internal Hazards methodologies:

- Fire Analysis Methodology Report (Ref. 6);
- Internal Explosion Safety Evaluation Methodology Report (Ref. 7);
- Internal Flooding Analysis Methodology Report (Ref. 8);
- High Energy Pipe Failures Safety Evaluation Methodology Report (Ref. 9);
- Internal Missiles Safety Evaluation Methodology Report (Ref. 10);
- Dropped Loads Safety Evaluation Methodology Report (Ref. 11); and
- Internal and External Hazards Schedule Methodology Report (Ref. 12).

### 3.1.4 Methodology of Safety Categorisation and Classification

37. The RP submitted a methodology for the Safety Categorisation and Classification (Ref. 23). Within this methodology the RP is proposing a scheme based upon IAEA SSG-30 (Ref. 18).

## 3.2 Basis of Assessment: RP's Documentation

38. The RP's documentation that has formed the basis for my GDA Step 2 assessment of the safety claims and supporting information related to the Internal Hazards aspects of the UK HPR1000 is presented in References 2 to 12 and 23.

39. My Step 2 assessment has been limited to the extent of the issued submissions given in the references above. A number of responses to my RQs relevant to Internal

Hazards analysis methodologies will be submitted after the completion of this assessment report. These will be fully considered in Step 3.

40. I also acknowledge that a number of submissions are at an early stage of development, and these will be the subject of controlled updates as the RP develops its UK HPR1000 safety case and to take account my regulatory expectations in this area.

41. In addition, during April 2018 the RP submitted to ONR, for information, an early version/ draft of the UK HPR1000 PCSR. Chapter 19 addresses Internal Hazards (Ref.13). Having early visibility of the scope and content of this chapter has been useful in the planning and preparation for my GDA Step 3 assessment work.

# 4 ONR ASSESSMENT

42. This assessment has been carried out in accordance with HOW2 guide NS-PER-GD-014, "Purpose and Scope of Permissioning" (Ref. 14).

43. My Step 2 assessment work has involved regular engagement with the RP's Internal Hazards specialists, i.e. two Technical Exchange Workshops (one in China and one in the UK) and four progress meetings have been held.

44. During my GDA Step 2 assessment, I have identified some gaps in the documentation formally submitted to ONR. Consistent with ONR's Guidance to Requesting Parties (Ref. 21), these normally lead to RQs being issued. At the time of writing this Step 2 assessment report, I had raised 19 RQs to understand the significance of the gaps identified (Ref. 20).

45. Similarly, and again consistent with ONR's Guidance to Requesting Parties (Ref. 21), more significant shortfalls against regulatory expectations in the generic safety case are captured by issuing Regulatory Observations (ROs). At the time of writing my assessment report, during Step 2, I had not raised any ROs.

46. Details of my GDA Step 2 assessment of the UK HPR1000 preliminary safety case and supporting references in the area of Internal Hazards, including the conclusions I have reached, are presented in the following sub-sections of the report. This includes the areas of strength that I have identified, as well as the items that require follow-up during subsequent Steps of the GDA of UK HPR1000.

## 4.1 Assessment of UK HPR1000 Internal Hazards Preliminary Safety Report

### 4.1.1 Assessment

47. The Internal Hazards PSR Chapter 19 presented, at high level, the fundamental safety functions, the Internal Hazards philosophy and safety measures of the FCG3 design. I subjected the PSR Chapter 19 to assessment focusing on the following areas:

- Internal Hazards design philosophy;
- Claims made; and
- Methodologies and scope of analysis.

48. The primary aim of the RQs was to seek the necessary clarifications and gain confidence that the UK HPR1000 design will be robust against Internal Hazards. I raised the following RQs (Ref. 20):

- RQ-UKHPR1000-0002 - on internal fire codes and standards and terminology used. The RP in its response confirmed that the code ETC-F 2010 will be used in the design of fire protection for the UK HPR1000, which includes both approaches: "fire containment" and "fire influence".
- RQ-UKHPR1000-0003 - on GDA scope of Internal Hazards. The RP confirmed that design basis and beyond design basis analysis (e.g. to address cliff edge effects) will be undertaken during GDA. The RP also confirmed that the Internal Hazards analysis will include all six modes of operations (plant states) including reactor power operation, shutdown, refuelling and defueling.
- RQ-UKHPR1000-0004 - on how hazards are limited to one division. The RP confirmed that hazard barriers segregate redundant SSCs delivering the fundamental safety functions. In areas where segregation is not provided, the RP will demonstrate that sufficient separation by distance between different trains or some local protection will be incorporated.

- RQ-UKHPR1000-0020 - on combined consequential hazards analysis. The RP outlined its methodology on combined hazards and deferred its full response to the combined hazards methodology report to be submitted later in Step 2.
- RQ-UKHPR1000-0021 - on internal explosions design philosophy and analysis methodology. The RP deferred its full response to the internal explosion safety evaluation methodology report (see section 4.3).
- RQ-UKHPR1000-0022 - on the consequence analysis approach for internal missile hazards. The RP outlined the assumptions, criteria and guidance used in the identification and analysis of internal missiles (see also section 4.3).
- RQ-UKHPR1000-0023 - on the consequence analysis approach for dropped and collapsed load hazards. The RP outlined its approach to consequences analysis and presented three examples of dropped loads consequences analysis from the FCG3 plant. This included identification of lifting device, identification of SSCs affected, functional analysis and identification of protective measures (additional to FCG3 design).
- RQ-UKHPR1000-0026 - on “fire influence” approach claims and areas used. The RP explained the approach where the “fire influence” approach has been used and provided a list of areas from the FCG3 design. No explicit claims were presented.

49. The Internal Hazards philosophy and key claim made in the PSR is that an Internal Hazards design basis event will be limited to one division by robust hazard barriers, segregating the three redundant divisions of SSCs, delivering the fundamental safety functions. This will ensure that an internal hazard will not prevent the delivery of the fundamental safety functions. The RP indicated that divisional segregation exists between the three Safeguard Buildings and the Fuel Building. I consider the design philosophy on segregation by hazard barriers to be in line with SAP EDR.2 and ESS.18 (Ref. 16), IAEA guidance (Ref.18) and WENRA (Ref. 19). The provisions of passive safety measures such as hazard barriers that do not rely on control systems, active safety systems or human intervention is also on the top of the hierarchy of safety measures given in SAP EKP.5.

50. In order to provide further confidence on the hazard barriers, the RP submitted the following FCG3 fire zoning and flooding zoning drawings (Ref. 5):

- Safeguard Building Fire Zoning Drawing;
- Safeguard Building Flooding Zoning Drawing;
- Reactor Building Fire Zoning;
- Reactor Building Flooding Zoning Drawing;
- Fuel Building Fire Zoning Drawing;
- Fuel Building Flooding Zoning Drawing; and
- General Layout.

51. The location of key SSCs delivering fundamental safety functions (which inform the hazard barriers location and segregation approach) was not submitted with the drawings above and therefore definitive conclusions on their suitability cannot be drawn at this early stage in GDA. However, the drawings provide clear evidence of segregation by barriers between the three Safeguard Buildings and within the Fuel Building for the FCG3 design, and specific to Internal Hazards for fire and flood.

52. The hazard barriers location and segregation approach of redundant SSCs, for all Internal Hazards will be further assessed during Step 3 once the Internal Hazards consequences analysis and further detail design information is made available. This will include all penetrations on hazard barriers. My expectation in this area is that penetrations should be minimised, where practicable, and their location should be optimised against Internal Hazards and taking into consideration other competing demands from other technical disciplines such as security and conventional fire. During Step 2, the RP indicated that there are some single doors on hazard barriers

segregating redundant SSCs delivering the fundamental safety functions. The number and use of single doors on the hazard barriers will be followed-up in Step 3 focusing on evidence to satisfy the single failure criterion in line with SAP EDR.4.

53. Within the Reactor Building a number of barriers (partial barriers) are also incorporated in the FCG3 design. The RP indicated that no safety claims on these barriers will be made. However, these barriers may play a role in safely managing Internal Hazards. This is an area that I will follow-up during my Step 3 assessment.

54. The PSR recognised that within the UK HPR1000 design, a number of areas exist where segregation of SSCs by robust hazard barriers is not feasible (i.e. exceptions to segregation). Examples include the Reactor Building and the Main Control Room (MCR). The RP indicated that these areas will be identified and assessed post GDA Step 2.

55. No explicit claims have been presented for the areas where segregation of SSCs by robust hazard barriers is not feasible, but the response to RQ-UKHPR1000-0004 (Ref. 20) (as well as in References 2 and 4), indicates that spatial separation between the different divisions, or local protection will be incorporated, to ensure delivery of the fundamental safety functions. The RP also proposed to undertake functional analysis to confirm that adequate SSCs will remain available. Whilst during Step 2 no explicit claims have been presented in areas where exceptions to segregation exist, I am confident that the RP on completion of the consequences analysis would be able to identify explicit claims and safety measures for all exceptions to segregation areas and applicable Internal Hazards.

56. I sought to obtain some confidence on the credibility of the implicit claim made on spatial separation by subjecting the Reactor Building fire zoning and flooding zoning drawings (Ref. 5) into a high level assessment. However, due to the lack of a narrative of the potential initiating events, lack of consequences analysis and lack of knowledge of the location of SSCs, my assessment was inconclusive on the adequacy of spatial separation in the Reactor Building or on the viability of this implicit claim.

57. To test the validity of the implicit claim on spatial separation further, I sampled one area within the Safeguard Building "B", where both the "B" and "C" divisions are routed through Safeguard Building "B". Jointly with the external hazards inspector I raised RQ-UKHPR1000-0126 (Ref. 20). The consequential effects of an internal hazard in this area such as high energy pipe failure, including multiple high energy pipe failures (domino effect), has the potential to compromise two divisions of SSCs of the feed and steam systems. The degree of adequate spatial separation against the combined consequential events of pipe whip, jet impact, flooding and pressurisation will be challenging to quantify. Whilst spatial separation may play a role against Internal Hazards, depending on the type and severity of the Internal Hazards, segregation should be provided where is reasonably practicable to do so. Where that is not the case, multi-leg arguments should be developed and this may involve a number of additional measures in line with SAP EKP.5.

58. In RQ-UKHPR1000-0126 (Ref. 20), I sought to obtain clarity on the plant layout in relation to feed and steam systems in Safeguard Building "B", whether the layout was optimised against Internal Hazards, whether consequential analysis had been undertaken and whether robust safety measures would be in place. In response to RQ-UKHPR1000-0126, the RP explained the layout of the various systems in Safeguard Building "B". The RP confirmed that the reason behind the routing of the main steam system and main feedwater flow control system divisions "B" and "C", which are high energy pipes, through Safeguard Building "B" was to avoid routing them around the MCR in Safeguard Building "C". The atmospheric steam dump system divisions "B" and "C", are also routed through Safeguard Building "B". The response to RQ-UKHPR1000-0126 did not provide any evidence of consequence analysis or the

adequacy of safety measures in place from the Internal Hazards perspective. However, I am confident that the RP will be able to identify appropriate safety measures in GDA once the consequences analysis is complete in this area. RQ-UKHPR1000-0126 will be followed-up during Step 3.

59. Where segregation of redundant SSCs is not provided, there is potential for novel or complex design features, which may be challenging to substantiate. This will be an area that I will focus my assessment during Step 3 to satisfy myself that SAPs EDR.2, ESS.18 and ELO.4 (on the minimisation of the effects of incidents) have been appropriately considered in the design of UK HPR1000. As a result of my Step 2 assessment, I have identified the following areas that the RP needs to make progress with during Step 3 of GDA:

- A systematic identification of all areas where segregation between different safety divisions is not provided i.e. exceptions to segregation;
- A systematic identification of Internal Hazards and SSCs affected, and determination of the overall importance to safety of each exception to segregation SSCs;
- Identification of alternative systems that can support the functions of SSCs when lost due to an internal hazard. Priority should be given to the identification of alternative systems segregated by barriers.
- Studies to define whether it would be reasonably practicable to segregate SSCs by passive safety barriers in those locations; and
- Identification of further defence in depth / risk reduction measures that may be reasonably practicable.

60. Furthermore, the claims presented at Step 2, may not be suitable or sufficient for the Internal Hazards of EMI, toxic and corrosive material and gases, and vehicular impact as the RP proposed to capture them in the PCSR post Step 2 (Ref. 20 response to RQ-UKHPR1000-0116). The claims in these areas will be followed-up during Step 3 of GDA. I am confident that the RP will be able to develop appropriate claims in GDA once the consequences analysis is complete.

61. Overall, the claims and safety measures presented at Step 2 are incomplete, are in some areas not suitable (e.g. where there is no segregation by barriers) or sufficient and therefore do not satisfy SAPs EKP.3 and EKP.5. However, I am confident that the RP on completion of the consequences analysis will be able to present all claims for all buildings in the UK HPR1000 design. This conclusion is further supported by the RP's recognition that depending on the consequences analysis and the functional analysis further measures may be identified, see also section 4.3 below. This was also reflected in the draft PCSR (Ref. 13).

During Step 2, I also undertook a preliminary review of the draft PCSR and provided some feedback on my expectations to guide the RP in the development of the PCSR (Ref. 25).

### 4.1.2 Strengths

62. During my GDA Step 2 assessment of the UK HPR1000 Internal Hazards PSR I have identified the following areas of strength:

- The RP has adopted a reasonable approach for the Internal Hazards analysis which comprises of: identification of Internal Hazards sources, identification of safety related SSCs, quantification of loads (hazard specific), identification of unmitigated consequences, identification of safety measures, assessment of safety measures, and production of a hazard schedule.

- The RP has recognised the challenges presented by combined hazards and associated consequences analysis, and has outlined a methodology in the PSR.
- The RP presented evidence, based on FCG3 design, on segregations by barriers.

### 4.1.3 Items that Require Follow-up

63. The information presented in PSR was pertinent to FCG3. During my GDA Step 2 assessment of the PSR, I have identified the following specific shortfalls that I will follow-up during Step 3 of GDA:

- Development of suitable and sufficient claims for all Internal Hazards including EMI, toxic and corrosive material and gases, vehicular impact and combined hazards. The claims should cover all relevant buildings, plant states, and areas where exceptions to segregation of SSCs by hazards barrier exists.
- Development of hazard barriers claims further to include all penetrations on hazard barriers including doors, access hatches, ventilation ducts and others.
- Demonstration that the UK HPR1000 plant layout is optimised against all Internal Hazards for all building and plant states and reflecting the competing needs from other technical disciplines as appropriate.
- Identification of all exception to segregation areas for all buildings and plant states, and development of suitable Internal Hazards consequences analysis for those areas. Demonstration that segregation of redundant SSCs is provided wherever it is reasonably practicable to do so.

### 4.1.4 Conclusions

64. Based on the outcome of my Step 2 assessment of PSR Chapter 19, for this stage in GDA, overall, I am satisfied with the RP’s proposed approach to Internal Hazards and with the claim made on the hazard barriers.

65. There are implicit claims in areas where segregation of SSCs by robust hazard barriers is not feasible. However, based on my experience on light water reactors with similar design features, I am confident that the RP will be able to present robust claims in all areas once the consequence analyses is complete later in GDA.

## 4.2 Identification, Screening and General Requirements of Protection Design Against Internal and External Hazards

### 4.2.1 Assessment

66. In support of the PSR the RP submitted the following two documents:

- The Identification and Screening Process of Internal and External Hazards (Ref. 3); and
- The General Requirements of Protection Design against Internal and External Hazards (Ref. 4).

67. I subjected the above documents to a sample assessment, from an Internal Hazards perspective, focusing on the following aspects:

- Adequacy and completeness of the Internal Hazards identification and screening study; and
- The suitability and sufficiency of the design features protecting against Internal Hazards.

**Assessment of the Identification and Screening Process of Internal and External Hazards**

68. The RP's Identification and Screening Process of Internal and External Hazards takes cognisance of ONR guidance, international guidance and previous GDAs (Ref. 3). Firstly it confirmed the list of Internal Hazards listed in the PSR (see section 4.1 above), and secondly it identifies three additional Internal Hazards; EMI, toxic and corrosive materials and gases, and vehicular transport.

69. The RP proposes to capture the EMI assessment within the electrical and control and instrumentation technical disciplines, whereas the consequences from toxic and corrosive materials and gases on SSCs, are currently dismissed, on the basis that they are very slow to materialise. The RP also proposes to undertake some bounding analysis for the vehicular impact hazard in Step 3 of GDA. The proposed treatment of EMI and toxic and corrosive materials and gases was identified as a gap to be further assessed during Step 3 of GDA.

70. Whilst the literature review undertaken is a reasonable process and satisfies to some degree the Internal Hazards identification aspect as stipulated in SAP EHA.1, my assessment identified a number of gaps in line with SAPs EHA.14, and EHA.19. These gaps were detailed in RQ-UKHPR1000-0116 and can be summarised as follows (Ref. 20):

- The identification study did not explicitly capture a number of potential Internal Hazards either sources or consequences in the final list of Internal Hazards e.g. High Energy Arching Faults (HEAF), oil mist, spray effects, turbine disintegration, collapsed structures, steam release, release of pressure from vessels and tanks and moderate energy pipes.
- Some hazards were screened out (e.g. collapse of structures and falling objects) or bounded by other Internal Hazards (e.g. tanks, pumps and valve failures bounded by high energy pipe failures, internal missiles and internal flooding), without the requisite justification.
- Appropriate claims from an internal hazard perspective were not presented for a number of Internal Hazards including EMI, toxic and corrosive materials and gases, and vehicular impact hazards.

71. Some of the gaps I have identified could potentially impact on the development of numerous hazard analysis methodologies and the delivery of consequences analysis during Step 3, and on the completion of claims for all Internal Hazards during Steps 3 and 4 of GDA.

72. My assessment of the analysis methodologies presented in section 4.3 revealed that some sources and consequences of Internal Hazards that were not explicitly listed in Reference 3 have been captured in the analysis methodologies. Although this gives me confidence that the methodologies should reflect all applicable Internal Hazards, it also revealed a lack of consistency between the submissions and therefore the generic safety case may not currently be in line with SAP SC.4.

73. The RP in its response to RQ-UKHPR1000-0116 (Ref. 20) provided some useful clarification and made the following commitments:

- To update Reference 3 to capture the gaps identified in RQ-UKHPR1000-116;
- The PCSR Chapter 19 will address claims and arguments for EMI, toxic and corrosive materials and gases, and vehicular transport. During Step 2 the RP prioritised its work on the development of methodologies and proposed no specific methodology reports for these three Internal Hazards. This is a gap which needs addressing early in Step 3. I will follow-up this shortfall during my Step 3 assessment to ensure that appropriate methodologies are in place for all

Internal Hazards to enable the RP to undertake meaningful consequences analysis in Step 3 and beyond.

74. During my Step 3 assessment, I will follow-up the response to RQ-UKHPR1000-116, the revised Reference 3 and PCSR Chapter 19 relevant to identification and screening of internal hazard.

75. The Identification and Screening Process of Internal and External Hazards (Ref. 3) also identifies three categorises of combined hazards: consequential hazards, correlated hazards and independent hazards. It presents a number of combinations of Internal Hazards and combinations of external and Internal Hazards. Whilst no justification for the selection of generic combined hazards was presented in reference 3, I consider that the list identified so far represents good progress for this stage of GDA, and is in line with SAP EHA.1. My expectations on combined hazards were communicated in RQ-UKHPR1000-0020 (Ref. 20).

76. The RP has committed to submit an analysis methodology on combined hazards at a later date in Step 2. As GDA progresses, I will assess this methodology to ensure the queries I raised in RQ-UKHP1000-0020 have been adequately addressed. In addition, I will be looking to see whether the RP's identification study captures credible and, where relevant, more onerous than individual Internal Hazards challenges for consequences assessment reflecting the UK HPR1000 design.

**Assessment of General Requirements of Protection Design Against Internal and External Hazards**

77. The General Requirements of Protection Design against Internal and External Hazards (Ref. 4) considered the Internal Hazards identified and carried forward in Reference 3 namely: internal fire, internal flooding, internal explosion, internal missile, dropped load and high energy pipe failure. It presented high level principles of hazard protection design and requirements of protection design against all identified Internal Hazards.

78. Whilst I am content with the general principles described in this document, the internal hazard specific design requirements are either incomplete (especially in areas where exceptions to segregation exist), or do not reflect specific design aspects of the UK HPR1000. At this stage in GDA, I therefore consider the expectations laid out in SAPs EKP.3 and EKP.5 have not been met. Furthermore, at this stage in GDA, the safety measures are insufficient to demonstrate relevant risks from Internal Hazards have been reduced to As Low As Reasonably Practicable (ALARP). All of the gaps I identified during my assessment of Reference 4 were captured in RQ-UKHPR1000-0114 (Ref. 20). In summary, they are:

- The RP has not yet considered all relevant Internal Hazards sources and consequences including combined hazards.
- The engineering measures delivering the claims for UK HPR1000 design are not explicit for all Internal Hazards and all areas, including exceptions to segregation.
- At this stage, defence in depth measures to prevent, protect or mitigate the effects of all relevant Internal Hazards, specific to the design requirements of UK HPR1000, have not been presented.
- A robust justification demonstrating how sufficient separation is established for all applicable Internal Hazards within the Reactor Building, and in areas where exception to segregation exist, need to be provided (see also section 4.1.1 above relevant to the claims made, demonstration of segregation of redundant SSCs where reasonably practicable and overall adherence to SAP EKP.5 on hierarchy of safety measures).

79. The RP in its response to RQ-UKHPR1000-0114 (Ref. 20) provided some clarification and made the following commitments:

- To update Reference 4 to capture the gaps identified in RQ-UKHPR1000-0114;
- PCSR Chapter 19 will present claims and specific safety measures according to hazard evaluation results for all areas; and
- To update their Internal Hazards analysis methodologies.

**80.** During my Step 3 assessment I will follow-up the RP's commitments made in response to RQ-UKHPR1000-0114 (Ref. 20).

81. Although the gaps identified by my assessment are significant, I consider they are largely symptomatic of being in the earlier, less detailed stages, of the GDA process. As GDA progresses and the UK HPR1000 generic design and safety case evolve, Reference 4 will be updated by the RP when the Internal Hazards consequence analysis is complete, capturing all claims for all buildings specific to UK HPR1000 design. It isn't proportionate to expect this work to have been completed at this stage of GDA. However, based on my interactions with the RP and the assessment I have performed to date, I am confident they will be able to develop this document further during Steps 3 and 4 of GDA. I have not identified any insurmountable gaps that could not be resolved during those later stages.

### 4.2.2 Strengths

82. During my GDA Step 2 assessment of the identification and screening process, and the general requirements of protection design against internal and external hazards I have identified the following areas of strength:

- The RP's identification of Internal Hazards study is based on a literature review which captures relevant sources of relevant good practice, including international guidance and lessons learnt from previous GDAs.
- The RP has commenced its work on combined hazards.
- The RP is committed to update the identification and screening process of internal and external hazards and the general requirements of protection design against internal and external hazards, and reflect relevant aspects in PCSR Chapter 19, as GDA progresses.

### 4.2.3 Items that Require Follow-up

83. During my GDA Step 2 assessment of the identification and screening process, and the general requirements of protection design against internal and external hazards, I have identified the following specific shortfalls, which I will follow-up during my Step 3 assessment:

- Demonstration that the revised identification and screening process of internal and external hazards will capture the technical gaps that I identified in my assessment.
- Demonstration that the combined hazards identification, screening and analysis methodology captures my regulatory expectations in the derivation of credible combined hazards, and that the derived combined hazards are relevant to the UK HPR1000 design.
- Demonstration that the revised general requirements of protection design against internal and external hazards captures the technical gaps that I identified in my assessment.

### 4.2.4 Conclusions

84. Based on the outcome of my Step 2 assessment of the Identification and Screening Process of Internal and External Hazards, and the General Requirements of Protection Design Against Internal and External Hazards I conclude the following:

- Whilst my assessment has identified a number of gaps in the identification and screening process of internal and external hazards, I am satisfied, from the Internal Hazards perspective, that the RP has made a commitment to revise this document to address all technical gaps and fully reflect all Internal Hazards within PCSR Chapter 19. The RP has already captured a number of sources or consequence of Internal Hazards within the methodologies submitted. I am also satisfied with the progress made in the identification of credible combined hazards.
- I consider that the RP has made a reasonable start in developing the Internal Hazards safety case and defence in depth arguments as reflected in the general requirements of protection design against internal and external hazards. The information in this document needs to be developed further, during GDA, and reflected in the Internal Hazards safety case and detailed design. I am satisfied, from the Internal Hazards perspective, that the RP has made a commitment to revise this document to address all technical gaps and capture all claims and safety measures within PCSR Chapter 19.

## 4.3 Internal Hazards Methodologies

### 4.3.1 Assessment

85. The RP submitted the following Internal Hazards methodologies:

- Fire Analysis Methodology Report (Ref. 6);
- Internal Explosions Safety Evaluation Methodology Report (Ref. 7);
- Internal Flooding Analysis Methodology Report (Ref. 8);
- High Energy Pipe Failures Safety Evaluation Methodology Report (Ref. 9);
- Internal Missiles Safety Evaluation Methodology Report (Ref. 10);
- Dropped Load Safety Evaluation Methodology Report (Ref. 11); and
- Internal and External Hazards Schedule Methodology Report (Ref. 12).

86. The RP proposed that the methodologies on EMI, toxic and corrosive materials and gases, and vehicular transport to be captured within the PCSR Chapter 19 (Ref. 20). The methodology for combined hazard will be submitted later in Step 2.

87. I have subjected all Internal Hazards methodologies to a detailed assessment and I have raised a number of RQs, which are summarised below.

### Fire Analysis Methodology Report

88. The Fire Analysis Methodology Report (Ref. 6) presents the RP's fire zoning design methodology, high level criteria and assumptions for the determination of fire zoning, criteria for fire evaluation methodology and the approach to fire area verification. This is largely based on the ETC-F 2010 design code. The fire area verification is based on the determination of room fire curve using the MOFIS-Z code (Systematic Modelling Solution to Fire Safety Design of Nuclear Power Plants) followed by a comparison with a performance-based code (ISO 834). The MOFIS-Z code is a "two zone fire model" developed by the RP and used in China and in particular in FCG3. A fire common mode analysis (including criteria and assumptions) relevant to areas where there is no segregation was also presented.

89. For this stage of GDA, whilst I am broadly content with the RP's proposed approach to the overall quantification of the fire resistance of barriers, my assessment identified a number of both technical gaps and items that I will need to follow-up during the next stages of my assessment in GDA Steps 3 and 4. These were captured in my RQ-UKHPR1000-0125 (Ref. 20), and can be summarised as follows:

- The analysis methodology is based on ETC-F 2010. The latest version of this design code is RCC-F 2017. The RP should undertake a gap analysis to identify any changes that may affect the fire analysis to be undertaken for the UK HPR1000 design during GDA.
- The criteria used in the determination of the various fire zones need to be adequately justified and their conservatism of the assumptions clearly explained. .
- Appropriate validation and verification of the MOFIS-Z code, used in the fire analysis, should be presented including its limitations, in line with SAPs AV.2, AV.3 and AV.4.
- The extent of the fire analysis for each type of zone is ambiguous. My expectation is that a systematic room-by-room fire analysis (including full compartment fires) should be undertaken which should include quantification of fire loads (based on total burnout), sensitivity analysis, identification of safety measures and substantiation of safety measures in line with SAPs EHA.1, EHA.5, EHA.6, EHA.7, EHA.14 and EHA.16, EKP.3, EKP.5 and AV.6.
- The methodology for substantiation of the fire barriers including penetrations should be presented.
- The fire common mode analysis should be based on a systematic identification of all common mode areas. All assumptions should be justified.
- The role of the fixed fire extinguishing system and smoke control service should be clarified in line with SAP EHA.16.

90. At the time of writing this report, the RP is developing a response to RQ-UKHPR1000-0125. During Step 3 I will follow-up the response to RQ-UKHPR1000-0125 and any new updates to the fire analysis methodology to ensure that the fire consequences analysis, to be submitted in Step 3, is appropriate and in line with my expectations.

### Internal Explosions Safety Evaluation Methodology Report

91. The Internal Explosion Safety Evaluation Methodology Report focuses on explosions inside the buildings important to safety, due to: explosive gas production, oil mist, HEAF and high pressure tank or pipe fracture (Ref. 7). For each type of explosion scenario it presents potential sources, a screening analysis and explosion consequences analysis. It also presents some consideration of explosion sources outside buildings important to safety.

92. I am content that the methodology considers different types of explosion scenarios, including flammable gases, oil mist, HEAF and release of energy from pressurised

vessels. However, a number of scenarios were not explicitly identified in the identification and screening process of internal and external hazards, see section 4.1 above (Ref. 3). This discrepancy appears to highlight a consistency issue between with the various early submissions, which is not in line with SAPs SC.4.

93. My assessment identified a number of both technical gaps and items that I will need to follow-up during the next stages of my assessment in GDA Steps 3 and 4. These were captured in RQ-UKHPR1000-0124 (Ref. 20), and can be summarised as follows):

- ONR expects the consequences analysis should be based on a room-by-room systematic identification of all explosions scenarios and sources.
- The consequences analysis should be based on worst case unmitigated scenario(s) which should include adequate sensitivity studies, in line with SAP AV.6.
- Justification of all screening criteria, assumptions and analysis used in the methodology, and for all type of scenarios and buildings important to safety, should be presented in line with SAPs EHA.5, EHA.6, EHA.7, EHA.14 and EHA.16.
- Justification of the suitability of the various modelling techniques proposed to be used for the various explosion scenarios, in line with SAPs AV.2, AV.3 and AV.4.
- Appropriate validation and verification of the MOFIS-H code used in the explosion analysis should be presented including, its limitations, to satisfy SAPs AV.2, AV.3 and AV.4.
- The analysis presented on oil mist and HEAF is not in line with relevant good practice. For example the methodology on oil mist needs to take into account the system properties and conditions including oil mist ignitability, droplet size and distribution. The methodology on HEAF needs to reflect the current and developing knowledge of the phenomena as described in international literature and guidance such as the Institute of Electrical and Electronics Engineers IEEE 1584-2002 – Guide for performing Arc Flash Hazards calculations, and international research.
- The role of gas detection systems in the evaluation of explosion concentration should be clarified.
- The methodology for substantiating the barriers against explosion loads, including penetrations, should be presented.

94. At the time of writing this report, the RP is developing a response to RQ-UKHPR1000-0124. During Step 3 I will consider the response to RQ-UKHPR1000-0124 and any new updates to the explosions analysis methodology to ensure that the explosions consequences analysis, to be submitted in Step 3, is appropriate and in line with my expectations.

**Internal Flooding Analysis Methodology Report**

95. The scope of the Internal Flooding Analysis Methodology Report aims to capture the methodologies for submergence, spray and steam release (condensation effects only) (Ref. 8). It identifies different types of flooding zones, principles and presented a safety evaluation methodology which includes identification of internal flooding zones, calculates of release volume, durations and spread paths. The methodology also briefly considers: the identification of target equipment, functional analysis, protection measures, barrier substantiation and a strategy for cliff edge effects.

96. I am content that the methodology identified different scenarios such as submergence, spray and steam release with the latter only capturing the condensation aspect of a steam release contribution to flooding. The RP proposed to capture the pressurisation aspect of the steam release within the high energy pipe failure safety methodology. However, my assessment identified a number of both technical gaps and items that I

will need to follow-up during the next stages of my assessment in GDA Steps 3 and 4. These were captured in RQ-UKHPR1000-0127 (Ref. 20), and can be summarised as follows:

- The internal flooding analysis methodology should include the detailed methodology for spray and steam release (condensation effects).
- The boundaries of flooding zones are based on a number of internal flooding zone principles. Justification of all zone principles has not been presented and no specific zone principles for the “forbidden internal flooding zones” put forward.
- ONR’s expectation is that the flooding consequences analysis should be based on a systematic identification (room-by- room) of all sources, including very large inventories and scenarios where isolation will be difficult to achieve. Clarity is required on how the worst case scenario will be selected and the hydrostatic loads calculated, reflecting on the selection of leakage paths, spread of flooding, extent of flooding zones and level of challenge to SSCs. All assumptions should be presented, justified and sensitivity analysis should be undertaken in line with SAPs EHA.1, EHA.5, EHA.6, EHA.7, EHA.14, EHA.15, EHA.16 and AV.6.
- Justification of the formula presented, in term of reflecting relevant good practice, and clarification of the level of conservatism applied in the analysis should be presented.
- Clarity on implicit claims on detection, isolation means including when human action is required.
- Clarity on how equipment will be identified and qualified against the effects of internal flooding to satisfy SAP EQU.1 is required.
- The methodology on barrier substantiation was not comprehensive to allow me to undertake a meaningful assessment.

97. At the time of writing this report, the RP is considering its response to RQ-UKHPR1000-0127. During Step 3, I will consider the response to RQ-UKHPR1000-0127and any new updates to the internal flooding analysis methodology to ensure that the internal flooding consequences analysis, to be submitted in Step 3, is appropriate and in line with my expectations.

**High Energy Pipe Failure Safety Evaluation Methodology Report**

98. This methodology focuses on the criteria for identification of high energy pipe failures location, based on the RCC-M code, identification of influence scope of pipe whip and jet impingement, a preliminary analysis, additional analysis (quantitative), barrier substantiation, protection measures and consideration of cliff edge effects (Ref. 9).

99. Early in Step 2 of GDA the structural integrity inspector raised RQ-UKHPR1000-0007 (Ref. 20) on underlying assumptions in structural integrity classification. In response, the RP acknowledged the potential for a gap between meeting UK expectations for the UK HPR1000 and the HPR1000 FCG3 design with respect to the application of the Leak Before Break (LBB) concept. In the UK the emphasis is placed on a robust demonstration of defence in depth and so LBB concepts are not expected to feature as primary arguments in safety cases. The LBB concepts are welcome as affording defence in depth provision in the design of nuclear plant. In the UK the expectations is that the consequences of postulated gross failure on the delivery of safety functions are assessed. RQ-UKHPR1000-0102 (Ref. 20) sought clarity on the extent to which LBB concept has been applied for the FCG Reference Plant. In response to RQ-UKHPR1000-0102, the RP explained that the LBB principle has been applied to: the main coolant loop lines, surge lines and part of the main steam lines (from the nozzle of the steam generators outlet to penetration in containment).

100. In addition to the above RQ, I raised RQ-UKHPR1000-0115 to gain an understanding of

all areas currently excluded from consequences analysis other than those listed under the LBB criteria stated above. The RP in its response to RQ-UKHPR1000-0115 (Ref. 20) explained that the main steam lines, steam generator blowdown lines in the Safeguard Buildings, and the primary coolant lines and surge lines in the Reactor Building were precluded from analysis, for FCG3. This is either because of the application of LBB criteria, or because they are high energy pipes within containment penetration rupture exclusion area rules. The RP confirmed that high energy pipe failures consequences (based on gross failure) will be carried out for UK HPR1000 for all pipes including those excluded under the containment penetration rupture exclusion area rules, and those under the LBB concept, that were applied in FCG3 design.

101. During my interactions with the RP I also articulated my regulatory expectations on systems that may have been previously excluded from consequences analysis under a low utilisation criteria (2%). I urged the RP to include all those in the analysis, if that was the case. The high energy pipe failures safety evaluation methodology did not make any explicit statements on exclusion of pipe lines due to low utilisation criteria. Therefore, my assumption is that all high energy lines under the low utilisation criteria will be also included in the gross failure consequences analysis.

102. ONR's assessment of the RP's responses to RQ-UKHPR1000-0102 and RQ-UKHPR1000-0115 from the structural integrity point of view is captured in Reference 27.

103. From an Internal Hazards perspective, I am satisfied that the RP's proposed approach to gross failure consequences analysis of the high energy pipe failures, if applied correctly, should meet UK expectations. However, my assessment identified a number of both technical gaps and items that I will need to follow-up during the next stages of my assessment in GDA Steps 3 and 4. These were captured in RQ-UKHPR1000-0137 (Ref. 20), and can be summarised as follows:

- The steam release methodology (specific to pressurisation rather than contribution to flooding) including: identification of sources, release paths, consequences analysis, safety measures and substantiation of the safety measures, should be presented in line with SAPs EHA.1, EHA.5, EHA.6, EHA.7, and EHA.14.
- Justification, in terms of relevant good practice, is required to underpin the adequacy of using standards and guidance such as: NUREG 0800 (2007), ANSI/ANS 58.2 (1988), and the RCC-M (2007) code, in high energy pipe failures for the UK HPR1000.
- Justification of the assumptions and criteria used in the selection of intermediate failure locations to derive bounding scenarios to satisfy SAP EHA.7.
- Justification of all assumptions used in the consequences analysis including those relevant to domino effect (pipe-to-pipe interactions), in line with SAP EHA.7.
- Justification of the selection of influence scope of pipe whip and spray.
- The selection of scenarios for further analysis was based on insufficient justification.
- The proposed "additional analysis" was not comprehensive to allow me to undertake a meaningful assessment.
- The methodology on barrier substantiation was not comprehensive enough to allow me to undertake a meaningful assessment.

104. At the time of writing this report, the RP is considering its response to RQ-UKHPR1000-0137 (Ref. 20). During Step 3, I will consider the response to RQ-UKHPR1000-0137 and any new updates to this methodology to ensure that the high energy pipe failure consequences analysis, to be submitted in Step 3, is appropriate and in line with my expectations.

### Internal Missiles Safety Evaluation Methodology Report

105. The Internal Missiles Safety Evaluation Methodology Report focuses on internal missiles from high energy fluid systems (Ref. 10). Missiles from rotating equipment were dismissed based on robust equipment procurement specification. The methodology presented some screening criteria for each of the sources considered, a preliminary consequences evaluation, calculation of internal missile parameters from valves, vessels and the Control Rod Drive Mechanism (CRDM). No specific detailed methodology for turbine disintegration nor for barrier substantiation, is presented.

106. I am content that the methodology identified different scenarios such as missiles generated from rotating equipment and high energy components failure. However, my assessment identified a number of both technical gaps and items that I will need to follow-up during the next stages of my assessment in GDA Steps 3 and 4. These were captured in RQ-UKHPR1000-0138 (Ref. 20), and can be summarised as follows:

- A consequence analysis methodology for rotating equipment failure should be presented. Equipment specification may play a role and this should be used as a defence in depth argument where appropriate.
- All assumption used in the screening of internal missiles sources should be presented, including those for rotating equipment, and justified as to why they are appropriate, in line with SAPs EHA.7 and EHA.19.
- The purpose, scope and comprehensiveness of the preliminary analyses are not clear. ONR’s expectation is that a systematic room-by-room identification of all potential missile sources and characterisation of consequences analysis should be presented including evaluation of the internal missiles impact on barriers in line with SAPs EHA.1, EHA.5, EHA.6, EHA.7 and EHA.14.
- It is not clear how the screening approach will be used in the areas where exceptions to segregation exist in line with SAP EHA.19.
- The scope of trajectory of missiles assessment should be clarified.
- The proposed calculation of the characteristics of missiles from valves, vessels and the CRDM including on the assumptions used, conservatism applied, limitation and whether they reflect relevant good practice should be clarified.
- The detailed methodology on turbine disintegration should be presented.
- The methodology on barrier substantiation was not comprehensive enough to allow me to undertake a meaningful assessment.

107. At the time of writing this report, the RP is considering its response to RQ-UKHPR1000-0138 (Ref. 20). During Step 3, I will consider the response to RQ-UKHPR1000-0138 and any new updates to this methodology to ensure that the internal missile consequences analysis, to be submitted in Step 3, is appropriate and in line with my expectations.

### Dropped Load Safety Evaluation Methodology Report

108. The Dropped Load Safety Evaluation Methodology Report focuses on dropped loads from lifting devices and includes: identification of sources, identification of target, consequences analysis in terms of loss of a function, identification of additional protection measures and the RP’s analysis strategy for cliff edge effects (Ref. 11).

109. During my Step 2 assessment of dropped loads, I initially raised RQ-UKHPR1000-0023 (Ref. 20) (see section 4.1 above). In response, the RP provided three examples of dropped load consequences analysis and proactively identified potential modifications in areas where the dropped loads consequences analysis were judged to be unacceptable. During a technical exchange workshop in Shenzhen – China in May 2018, the RP also explained their approach to spent fuel cask export dropped load scenario, which is one of the areas where I will focus my assessment during Step 3 (Ref. 22). The examples presented gave me confidence that the RP has

a good level of understanding of the dropped load consequences analysis required in GDA.

110. I am overall content with the proposed methodology. However, my assessment of Reference 11 identified a number of both technical gaps and items that I will need to follow-up during the next stages of my assessment in GDA Steps 3 and 4. These were captured in RQ-UKHPR1000-0143 (Ref. 20), and can be summarised as follows:

- The arguments and evidence to exclude non-seismically classified collapsed structures should be presented in line with SAP EHA.19.
- The methodology for analysis of falling structures and lifting devices should be presented. This should include a systematic identification of all non-seismically classified structures (including temporary structures) and lifting equipment, and consequences assessment, which should include consequential events such as explosions and flooding in line with SAPs EHA.1, EHA.5, EHA.6 and EHA.14.
- The justification to dismiss seismically classified lifting devices should be presented in line with SAP EHA.19.
- A “transfer path” and a “lifting schedule” should be developed to aid the dropped load consequences analysis.
- The criteria for applying “load tip” and “swing load” to dropped loads should be presented.
- The methodology and computational models for calculating the impact on structures should be presented in line with SAPs AV.2, AV.3 and AV.4.
- The scope of analysis in areas where exception to segregation exists should be presented.
- The methodology on barrier substantiation is required.

111. At the time of writing this report, the RP is considering its response to RQ-UKHPR1000-0143 (Ref. 20). During Step 3, I will consider the response to RQ-UKHPR1000-0143 and any new updates to this methodology to ensure that the dropped loads consequences analysis, to be submitted in Step 3, is appropriate and in line with my expectations.

**Internal and External Hazards Schedule Methodology Report**

112. An Internal and External Hazards Schedule Methodology Report has been presented which largely follows the format of the fault schedule that is currently being developed for UK HPR1000 (Ref. 12).

113. From an Internal Hazards perspective, I am content with the format of the hazard schedule presented as it broadly satisfies SAP FA.8. I also recognise that the hazard schedule will further evolve during Steps 3 and 4 of GDA.

**Summary of my Assessment of the Internal Hazards Methodologies**

114. Overall, my assessment has identified a number of either technical gaps, or important items that I will follow-up during Step 3 of GDA, for all of the RP’s Internal Hazards methodologies submitted in Step 2. For the technical gaps, if some are not addressed adequately, they could affect the scope and quality of the consequence analysis in each internal hazard area and including the barriers substantiation. ONR expects to be completed during Step 3 of GDA. This could also in turn affect other technical disciplines such as structural integrity (i.e. safety categorisation and classification of SSCs) and civil engineering (on the design of civil structures to withstand Internal Hazards).

115. I will therefore prioritise the review of all relevant RQ responses as they are received from the RP.

It is also important to note that during my Step 2 interactions with the RP, they have openly acknowledged some of the key differences between the Chinese and UK regulatory contexts with respect to expectations in the Internal Hazards discipline. In addition, during my technical exchange workshop in Shenzhen – China in May 2018, the RP demonstrated a reasonable understanding of the consequences analysis and barriers substantiation for a number of Internal Hazards. This provides me with some confidence about their understanding of the approach to, breadth and depth of consequences analysis expected in the UK regulatory context (Ref. 22).

### 4.3.2 Strengths

116. During my GDA Step 2 assessment of the UK HPR1000 Internal Hazards analysis methodologies, I have identified the following areas of strength:

- The RP has commenced its work on Internal Hazards analysis methodologies and demonstrated an awareness of relevant international guidance, standards and UK regulatory expectations.
- The RP responded positively on ONR’s regulatory expectations on high energy pipes failure and incorporated gross failure into the analysis methodology of all high energy pipe failures to be applied for the UK HPR1000 design. The RP has also clearly identified all high energy pipes which, for the HPR1000 FCG3 Reference Plant, were excluded from analysis under the LBB criteria and containment penetration rupture exclusion rules.
- During my interactions with the RP, they have presented preliminary examples, in some areas, of the consequences analysis undertaken and demonstrated a good understanding of what is expected in GDA.

### 4.3.3 Items that Require Follow-up

117. During my GDA Step 2 assessment of the Internal Hazards analysis methodologies I have identified the following specific shortfalls:

- A complete demonstration that all Internal Hazards analysis methodologies are in line with ONR’s expectations and have adequately addressed all of the technical gaps I identified in Step 2, is required.

### 4.3.4 Conclusions

118. During Step 2 the RP has commenced the development of the Internal Hazards analysis methodologies for six Internal Hazards. My assessment of the methodologies submitted identified a number of either technical gaps or important items for follow-up during Step 3 of GDA, for each internal hazard analysis methodology. This may potentially affect the scope and contents of the Internal Hazards consequences analysis and the claims and arguments to be submitted during Step 3.

119. Notwithstanding the above, during Step 2 I obtained some confidence that the RP with sufficient resources should be able to develop the methodologies further to address all technical gaps that I identified.

120. My assessment of Internal Hazards methodologies will continue during Step 3.

### 4.4 Categorisation of Safety Functions and Classification of Structures, Systems and Components

#### 4.4.1 Assessment

121. The RP has submitted a Methodology for the Safety Categorisation and Classification of SSCs (Ref. 23). This methodology is based on the guidance given in IAEA Safety Guide SSG-30 (Ref. 18).

122. ONR's overall assessment of the RP's proposed methodology for the safety categorisation and classification of SSCs is reported in the summary of the Step 2 Assessment of the UK HPR1000 Reactor (Ref. 24).

123. In Step 2, I undertook a high level assessment of the Methodology of Safety Categorisation and Classification and concluded that the proposed methodology aims to meet SAPs ECS.1 and ECS.2. I also focused on the application of the proposed methodology to the explicit claim made on hazard barriers in the Internal Hazards area during Step 2. Whilst a complete list of the categorisation and classification of the UK HPR1000 civil structures is not available in Step 2, according to the methodology on categorisation and classification of SSC's, the hazard barriers should be Category 1 and Class 1. This is in line with my expectations.

124. The correct application of the categorisation and classification of SSC's claimed in Internal Hazards area would depend on the consequences analysis and the assumptions made for each internal hazard. My assessment of the Internal Hazards methodologies is given in section 4.3 above.

#### 4.4.2 Strengths

125. The methodology is based on IAEA Safety Guide SSG-30 (Ref. 18).

#### 4.4.3 Items that Require Follow-up

126. The application of the Methodology of Safety Categorisation and Classification will be a focus of my assessment during Step 3 and 4 of GDA.

#### 4.4.4 Conclusions

127. Based on a high level assessment of the Methodology of Safety Categorisation and Classification, I have concluded that the RP's methodology should provide an adequate basis for the classification of SSCs during GDA Step 3 and 4.

### 4.5 Out of Scope Items

128. There are no items left outside the scope of my GDA Step 2 assessment of the UK HPR1000 Internal Hazards. My assessment covered all topics identified in my assessment plan (Ref. 1).

129. The RP has also submitted a report on ALARP methodology (Ref. 26). I have not assessed this reference from an Internal Hazards perspective. However, ONR's assessment of this methodology is captured in the summary of the Step 2 Assessment of the UK HPR1000 Reactor (Ref. 24).

### 4.6 Comparison with Standards, Guidance and Relevant Good Practice

130. In Section 2.2, above, I have listed the standards and criteria I have used during my GDA Step 2 assessment of the UK UKHPR1000 Internal Hazards case, to judge the adequacy of the preliminary safety case. In this regard, my overall conclusions can be summarised as follows:

- SAPs: I have reviewed the PSR and supporting documents taking into account the relevant SAPs. I have concluded that the submission partially satisfies the expectations set out in each SAP. Considering the breadth and depth of the assessment required at Step 2, a number of SAPs have not been considered as yet. I expect, however, that as these documents will be further developed during Step 3, ONR's relevant SAPs to be fully satisfied.
- TAGs: I have concluded that the submission only partly satisfies the expectations set out in ONR's TAG. This has been reflected within my assessment. I have made a number of recommendations that the RP should address during Step 3 of the GDA.

### 4.7 Interactions with Other Regulators

131. During Step 2, I did not undertake any interactions with other regulators.

# 5 CONCLUSIONS AND RECOMMENDATIONS

## 5.1 Conclusions

132. During Step 2 of GDA the RP submitted a PSR and other supporting references, which outline a preliminary nuclear safety case for the UK HPR1000. These documents have been formally assessed by ONR. The PSR together with its supporting references present partially the claims in the area of Internal Hazards that underpin the safety of the UK HPR1000.

133. During Step 2 of GDA I have targeted my assessment at the content of the PSR and its supporting submissions that are of most relevance to the area of Internal Hazards; against the expectations of ONR's relevant SAPs and TAGs and other guidance which ONR regards as Relevant Good Practice. From the UK HPR1000 assessment done so far, I conclude the following:

- The RP has adopted a reasonable approach for the Internal Hazards analysis methodology which comprises: identification of Internal Hazards sources, identification of safety related SSCs, quantification of loads (hazard specific), identification of unmitigated consequences, identification of safety measures, assessment of safety measures, and production of a hazard schedule.
- The RP has undertaken an appropriate literature review to support its Internal Hazards identification study and has commenced its combined hazards identification work to identify credible hazard combinations.
- The claim on hazard barriers against Internal Hazards and credible combined hazards is appropriate in all buildings where segregation of SSCs delivering the fundamental safety functions by hazard barriers exists. The claims in areas where exceptions to segregation exist need development on completion of the consequences analysis. Overall, at Step 2, the degree of development of the safety case and supporting evidence is necessarily insufficiently advanced to fully demonstrate that the risks from Internal Hazards have been reduced to ALARP. I am confident, however, that the RP, on completion of the consequences analysis, later in GDA, will be able to articulate reasonable claims in the PCSR and underpin them with sufficient arguments and robust evidence. I am also confident that the RP on completion of the consequences analysis will be able to demonstrate that the risks from Internal Hazards have been reduced to ALARP.
- The RP has commenced its work on six Internal Hazards analysis methodologies. These will need further development during Step 3 to address a number of technical gaps that I have identified. During Step 2 I obtained some confidence that the RP with sufficient resources should be able to develop the methodologies further to address all technical gaps identified.
- Currently, I would regard my understanding of UK HPR1000 technology as sufficient to undertake a meaningful Step 2 assessment, but relatively high-level. As GDA progresses I will increase my familiarity with the UK HPR1000 design layout and claims, especially in areas where exceptions to segregation exist.
- I have identified a number of shortfalls during my assessment, which are captured in Section 4 of this report. I will follow up these matters during Step 3 of GDA.

134. Overall, during my GDA Step 2 assessment, I have not identified any fundamental safety shortfalls in the area of Internal Hazards that might prevent the issue of a Design Acceptance Confirmation (DAC) for the UK HPR1000 design.

## 5.2 Recommendations

135. My recommendations are as follows:

- Recommendation 1: ONR should consider the findings of my assessment in deciding whether to proceed to Step 3 of GDA for the UK HPR1000.
- Recommendation 2: All the items identified in Step 2 as important to be followed-up should be included in ONR's GDA Step 3 Internal Hazards assessment plan for the UK HPR1000.

# 6 REFERENCES

1. Generic Design Assessment of GNS's UK HPR1000, Step 2 Assessment Plan for Internal Hazards, ONR-GDA-UKHPR1000-AP-17-003 Revision 0, November 2017; TRIM Ref. 2017/352533.

2. GNS, UK HPR1000 GDA Project, Preliminary Safety Report Chapters 1-27, HPR/GDA/PSR/0001 Revision 0, October 2017, TRIM Ref. 2018/14773.

3. The Identification and Screening Process of Internal and External Hazards, GHX00100037DOZJ03GN Rev C, March 2018, TRIM 2018/99013.

4. The General Requirements of Protection Design against Internal and External Hazards, GHX00100028DOZJ03GN, Rev. C, March 2018, TRIM 2018/98992.

5. Translation Version of Fangchenggang Nuclear Power Plant Unit 3 Drawings:

   - Safeguard Building Fire Zoning Drawing, BS340300002DOZJ03DD, Rev D, December 2017, TRIM 2018/40949.
   - Reactor Building Fire Zoning Drawing, BS340300001DOZJ03DD, Rev. D, December 2017, TRIM 2018/40958.
   - Fuel Building Fire Zoning Drawing, BS340300003DOZJ03DD, Rev. C, December 2017, TRIM 2018/40833.
   - Safeguard Building Flooding Zoning Drawing, BS340400002DOZJ03DD, Rev. C, December 2017, TRIM 2018/40905.
   - Reactor Building Flooding Zoning Drawing, BS340400001DOZJ03DD, Rev. C, December 2017, TRIM 2018/40926.
   - Fuel Building Flooding Zoning Drawing, BS340400003DOZJ03DD , Rev. C, December 2017, TRIM 2018/40859.
   - General Layout, BSY01B00001DCZT42DD, Rev. F, November 2017, TRIM 2018/40885.

6. Fire Analysis Methodology Report, GHX00100022DOZJ03GN, Rev. B, March 2018, TRIM 2018/145855.

7. Internal Explosion Safety Evaluation Methodology Report, GHX00100033DOZJ03GN, Rev. C, May 2018, TRIM 2018/181311.

8. Internal Flooding Analysis Methodology Report, GHX84200002DOZJ03GN , Rev. C, May 2018, TRIM 2018/181352.

9. High Energy Pipe Failures Safety Evaluation Methodology Report, GHX00100040DOZJ03GN, Rev. D, May 2018,TRIM 2018/181344.

10. Internal Missiles Safety Evaluation Methodology Report, GHX00100041DOZJ03GN, Rev. C, June 2018, TRIM 2018/207313.

11. Dropped Loads Safety Evaluation Methodology Report, GHX00100035DOZJ03GN, Rev. D, June 2018, TRIM 2018/2017322.

12. Internal and External Hazards Schedule Methodology Report, GHX00100044DOZJ03GN, Rev. C, April 2018, TRIM 2018/151809.

13. Pre-Construction Safety Report, Chapter 19 Internal Hazards (Draft for Information), GHX00620019KPGB02GN Rev. B, April 2018, TRIM 2018/122074.

14. ONR HOW2 Guide NS-PER-GD-014 Revision 4 - Purpose and Scope of Permissioning. July 2014, http://www.onr.org.uk/operational/assessment/index.htm

15. Guidance on Mechanics of Assessment within the Office for Nuclear Regulation (ONR) – TRIM 2013/204124.

16. Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0. November 2014. http://www.onr.org.uk/saps/saps2014.pdf

17. Technical Assessment Guide - Internal Hazards NS-TAST-GD-014 Revision 4. ONR. September 2016. http://www.onr.org.uk/operational/tech_asst_guides/index.htm

18. IAEA Safety Guides:

- Specific Safety Requirements No. SSR-2/1. Safety of Nuclear Power Plants: Design. International Atomic Energy Agency (IAEA), 2016.
- Safety Guide No. NS-G-1.7. Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants. International Atomic Energy Agency (IAEA), 2004.
- Safety Guide No. NS-G-1.11. Protection against Internal Hazards other than Fire and Explosions in the Design of Nuclear Power Plants. International Atomic Energy Agency (IAEA), 2004.
- Specific Safety Guide No SSG-30. Safety Classification of Structures, Systems and Components in Nuclear Power Plants. International Atomic Energy Agency (IAEA), 2014

http://www.iaea.org.

19. Western European Nuclear Regulators' Association:

- WENRA Reactor Safety Levels for Existing Reactors, September 2014.
- Statement on Safety Objectives for New Nuclear Power Plants, November 2010.
- Safety of New NPP Designs, March 2013.

http://www.wenra.org/

20. UK HPR1000 - Regulatory Query (RQ) Tracking Sheet - Reference for Step 2 Assessment Reports, 2 November 2017, TRIM 2018/315144.

21. ONR, New Nuclear Reactors: Generic Design Assessment Guidance to Requesting Parties, ONR-GDA-GD-001 Rev. 3, September 2016.

22. Contact Record, ONR-NR-CR-18-115 - UK HPR1000 GDA Step 2 Internal Hazards Workshop Shenzhen 9th – 12th May 2018, TRIM 2018/165488.

23. Methodology of Safety Categorisation and Classification, GHX00100062DOZJ03GN Rev. B, June 2018, TRIM 2018/199731.

24. GDA Step 2 Summary of the Step 2 Assessment of the UK HPR1000 Reactor, ONR-NR-PAR-18-007, TRIM 2018/238474.

25. ONR Review of Draft UK HPR1000 PCSR Chapter 19, April 2018, TRIM 2018/122074.

26. ALARP Methodology, GH X 00100 051 DOZJ 03 GN, Rev. B, May 2018, TRIM 2018/181415.

27. GDA Step 2 Assessment for Structural Integrity of the UK HPR1000 Reactor, ONR-GDA-UKHPR1000-AR-18-018, Rev. 0, September 2018, TRIM 2018/251179.

## Table 1

Relevant Safety Assessment Principles Considered During the Assessment

| SAP No and Title | Description | Interpretation | Comment |
|---|---|---|---|
| **SC.4 The regulatory assessment of safety cases:** Safety case characteristics. | A safety case should be accurate, objective and demonstrably complete for its intended purpose. | This principle establishes the need that the Internal Hazards safety case should be accurate, coherent and consistent between the various submissions. | Addressed in Section 4 of this Report. Submitted PSR and supporting references are not fully aligned. Hence, this SAP is not yet demonstrated. |
| **EKP.3 Engineering principles: key principles.** Defence in depth. | Nuclear facilities should be designed and operated so that defence in depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression. | This principle establishes the need that the Internal Hazards safety case should identify independent safety measures (inherent features, equipment and procedures) against internal hazards. | Addressed in Section 4 of this report. PSR and the general requirements of protection design against internal and external hazards provided, at high level, some defence in depth discussion. This will be addressed in future GDA submissions specific to UK HPR1000. Hence, this SAP is not yet demonstrated. |
| **EKP.5 Engineering principles: key principles.** Safety measures. | Safety measures should be identified to deliver the required safety function(s). | This principle establishes the need that the Internal Hazards safety case should identify safety measures against all internal hazards. This principle also sets expectations on hierarchy of safety measures. Passive safety measures, such as hazard barriers sit on the top of the list, where these are categorised as not relying on control systems, active safety systems or human intervention. | Addressed in Section 4 of this report. Submitted PSR and the general requirements of protection design against internal and external hazards provided limited information. This will be addressed in future GDA submissions. Hence, this SAP is not yet demonstrated. |
| **ECS.1 Engineering principles: safety classification and standards.** Safety categorisation. | The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be identified and then categorised based on their significance with regard to safety. | This principle sets the expectation that Internal Hazards should be considered in the categorisation of the fundamental safety functions and that the categorisation should be linked to Internal Hazards analysis. | Addressed in Section 4. The methodology of safety categorisation and classification provides a scheme which is broadly in line with ECS.1. The application of the scheme is not possible to assess during Step 2. This will be addressed in future GDA submissions. Hence, this SAP is not fully demonstrated. |
| **ECS.2 Engineering principles: safety classification and standards.** Safety classification of structures, systems and | 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. | This principle sets the expectation that the Internal Hazards deterministic analysis should identify all SSCs that deliver the fundamental safety functions and classify them on the basis of their significance to safety. | Addressed in Section 4. The methodology of safety categorisation and classification provides a scheme which is broadly in line with ECS.2. The application of the scheme is not possible to fully assess during Step 2. This will be addressed in future GDA submissions. Hence, this SAP is not fully demonstrated. |

| | | | |
|---|---|---|---|
| components. | | | |
| **EQU.1 Engineering principles: equipment qualification**. Qualification procedures. | Qualification procedures should be applied to confirm that structures, systems and components will perform their allocated safety function(s) in all normal operational, fault and accident conditions identified in the safety case and for the duration of their operational lives. | This principle sets the expectation that qualification procedures should be developed based on the requirements identified in the Internal Hazards analysis and applied to all those SSCs identified in the Internal Hazards safety case. | Addressed in Section 4 of this report. The internal flooding methodology refers to equipment qualification. Equipment required to withstand the effects of flooding (submergence and spray) should be identified and qualification procedures should be developed. This will be addressed in future GDA submissions. Hence, this SAP is not yet demonstrated. |
| **EDR.2 Engineering principles: design for reliability**. Redundancy, diversity and segregation. | Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components. | This principle sets the expectation that redundancy, diversity and segregation should be incorporated in the design of SSCs delivering the fundamental safety functions, against Internal Hazards. The Internal Hazards consequences analysis should consider the availability of redundant SSCs to deliver the fundamental safety functions. | Addressed in Section 4 of this report. The PSR claimed that the hazard barriers segregate redundant key SSCs delivering the fundamental safety functions. This was supported by the general requirements of protection design against internal and external hazard and by the drawings for the FCG3 plant. However, segregation by barriers is not always feasible in all buildings. The RP is committed to identify all areas where exceptions to segregation exist and to undertake a consequences analysis. This will be addressed in future GDA submissions. Hence, this SAP is not fully demonstrated. |
| **EDR.4 Engineering principles: design for reliability**. 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 | This principle sets the general expectation that single failure criterion should be considered in the Internal Hazards analysis. | Addressed in Section 4 of this report. EDR.4 is relevant to the use of single doors on hazard barriers segregating SSCs delivering the fundamental safety functions. This will be addressed in future GDA submissions. Hence, this SAP not yet demonstrated. |
| **ELO.4 Engineering principles: layout**. Minimisation of the effects of Incidents. | The design and layout of the site, its facilities (including enclosed plant), support facilities and services should be such that the effects of faults and accidents are minimised | This principle sets the expectation that the effects of Internal Hazards on SSCs should be minimised by optimising the design and layout of the site and buildings against Internal Hazards. | Addressed in Section 4 of this report. The PSR claimed that the hazard barriers segregate redundant key SSCs delivering the fundamental safety functions. This was supported by the general requirements of protection design against internal and external hazard and by the drawings for the FCG3 plant. However, segregation by barriers is not always feasible in all buildings. Furthermore, there is a need to demonstrate that the design is optimised against Internal Hazards. The RP is committed to identify all areas where exceptions to segregation exist and to undertake a consequences analysis. This will be addressed in future GDA |

| | | | |
|---|---|---|---|
| | | | submissions. Hence, this SAP is not fully demonstrated. |
| **EHA.1 Engineering principles: external and internal hazards**. Identification and characterisation. | An effective process should be applied to identify and characterise all External and Internal Hazards that could affect the safety of the facility | This principle establishes the need for a thorough and systematic identification study to identify potential Internal Hazards sources including credible combination of Internal and External hazards. | Addressed in Section 4 of this report. Whilst the RP undertook a literature review to identify all applicable Internal Hazards, the identification study did not explicitly capture all sources or consequences. In addition a number of Internal Hazards were screened out or bounded by other hazards without the requisite justification. The RP is committed to update and re-submit the identification and screening process of internal and external hazards. Hence, this SAP is not fully demonstrated. |
| **EHA.5 Engineering principles: external and internal hazards**. Design basis event operating states. | Analysis of design basis events should assume the event occurs simultaneously with the facility's most adverse permitted operating state. | This principle sets the expectation that the Internal Hazard consequences analysis should be based on the worst case unmitigated scenario. The consequences analysis should identify the potential impact on SSCs delivering the fundamental safety functions and determine the need for segregation and redundancy of SSCs by barrier. Credible hazard combinations and common cause failures should be also considered. | The RP indicated that the Internal Hazards consequence analysis will cover all plant states. This will be addressed by future GDA submissions. Hence, this SAP not yet demonstrated. |
| **EHA.6 Engineering principles: external and internal hazards**. Analysis. | The effects of Internal and External Hazards that could affect the safety of the facility should be analysed. The analysis should take into account hazard combinations, simultaneous effects, common cause failures, defence in depth and consequential effects. | See EHA.5 above. | Internal Hazards consequences analysis will be covered by future GDA submissions. Hence, this SAP not yet demonstrated. |
| **EHA.7 Engineering principles: external and internal hazards**. 'Cliff-edge' effects. | A small change in design basis fault or event assumptions should not lead to a disproportionate increase in radiological consequences. | This principle sets the expectation that sensitivity analysis should be undertaken for all Internal Hazards including credible combined hazards to identify potential 'cliff edge' effect and determine the adequacy of the safety measures identified (e.g. hazard barriers). | A number of Internal Hazards methodologies included a section on cliff edge effects. This will be covered by future submissions. Hence, this SAP not yet demonstrated. |
| **EHA.10 Engineering principles: external and internal hazards**. Electromagnetic interference. | The facility design should include preventative and/or protective measures against the effects of electromagnetic interference. | This principle sets the expectation that the Internal Hazards analysis should identify all electromagnetic interference sources, assess the consequences and identify all safety measures against this fault. | Addressed in Section 4 of this report. The RP proposed to capture this internal hazard within the PCSR. Hence, this SAP not yet demonstrated. |
| **EHA.14 Engineering principles: external** | Sources that could give rise to fire, explosion, missiles, toxic gas | This principle sets the expectation that all sources of Internal Hazards, including credible combined hazards | Addressed in Section 4 of this report. Whilst the RP undertook a literature review to identify all applicable |

| | | | |
|---|---|---|---|
| **and internal hazards**. Fire, explosion, missiles, toxic gases etc – sources of harm. | release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, quantified and analysed within the safety case. | should be identified and quantified in the Internal Hazards safety case. | Internal Hazards, the identification study did not explicitly capture all sources or consequences. In addition a number of Internal Hazards were screened out or bounded by other hazards without the requisite justification. The RP is committed to update and re-submit the identification and screening process of internal and external hazards. Internal Hazards consequence analysis will be covered by future GDA submissions. Hence, this SAP is not fully demonstrated. |
| **EHA.15 Engineering principles: external and internal hazards**. Hazards due to water. | The design of the facility should prevent water from adversely affecting structures, systems and components. | This principle set the expectation that all internal flood sources should be identified and the effects on SSCs should be quantified. | The RP identified internal flooding hazard as applicable to UK HPR1000 and submitted an internal flooding analysis methodology report. Consequences analysis and design aspects of the UK HPR1000 will be covered by future GDA submissions.  Hence, this SAP not yet demonstrated. |
| **EHA.16 Engineering principles: external and internal hazards**. Fire detection and fighting. | Fire detection and fire-fighting systems of a capacity and capability commensurate with the worst-case design basis scenarios should be provided. | This principle set the expectation that a fire analysis should be undertaken. The effects of a fire on SSCs delivering the fundamental safety functions should be quantified including quantification of the fire resistance of the barriers. Consideration should be given to segregation of SSCs by barriers and the role, capacity and capability of the fire fighting systems. | There is a need to undertake a fire analysis to determine the need for segregation of plant and equipment and to determine the capacity and capability of the detection and fire fighting systems. During Step 2 no explicit claims on fire detection and fire fighting made. This will be covered by future submissions. Hence, this SAP not yet demonstrated. |
| **EHA.19 Engineering principles: external and internal hazards**. Screening. | Hazards whose associated faults make no significant contribution to overall risks from the facility should be excluded from the fault analysis. | This principle sets the expectation that robust screening criteria should be developed and applied in the Internal Hazards analysis including combined hazards. Appropriate justification should be provided for all those Internal Hazards initiating events or sources screened out. | Addressed in Section 4 of this report.  The identification and screening of Internal and External Hazards screened out a number of Internal Hazards or bounded by other hazards without the requisite justification. The identification of combined hazards also commenced but not completed. The RP is committed to update the identification and screening process of Internal and External Hazards and will also issue a combined hazards analysis methodology. Hence, this SAP not fully demonstrated. |
| **FA.8 Fault analysis: design basis analysis**. Linking of initiating faults, fault sequences and safety measures. | Design Basis Analysis should provide a clear and auditable linking of initiating faults, fault sequences and safety measures. | This principle sets the expectation that a design basis analysis should be undertaken for all Internal Hazards initiating events. An Internal Hazard schedule should be developed providing the link between the Internal Hazards initiating event, consequences analysis and identification of safety measures. | The RP submitted a methodology on Internal and External Hazards schedule, which on completion of the consequences analysis will link the initiating faults sequences and safety measures. This will be covered by future submissions. Hence, this SAP not yet demonstrated. |
| **AV.2 Fault analysis:** | Calculation methods used for the | This principle sets the expectation that all calculation | Addressed in Section 4 of this report. The RP proposed to |

| | | | |
|---|---|---|---|
| **assurance of validity of data and models**. Calculation methods. | analyses should adequately represent the physical and chemical processes taking place. | methods and computer models used in the Internal Hazards consequences analysis should be validated by comparison with actual experiments and should reflect the physical and chemical processes taking place. | use a number of models in the calculation of the Internal Hazards consequences analysis and substantiation of barriers. Validation of the proposed models is required. This will be covered by future submissions. Hence, this SAP not yet demonstrated. |
| **AV.3 Fault analysis: assurance of validity of data and models**. Use of data | The data used in the analysis of aspects of plant performance with safety significance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means. | This principle sets the expectation that all data and assumptions used in the Internal Hazards consequences analysis should be valid and conservative. Where uncertainty exists sensitivity analysis should be undertaken to establish suitable safety margins. | Addressed in Section 4 of this report. The RP proposed to use a number of models in the calculation of the consequences analysis in Internal Hazards and substantiation of barriers. Validation of the proposed models is required. This will be covered by future submissions. Hence, this SAP not yet demonstrated. |
| **AV.4 Fault analysis: assurance of validity of data and models**. Computer models. | Computer models and datasets used in support of the safety analysis should be developed, maintained and applied in accordance with quality management procedures. | This principle sets the expectation that appropriate quality management procedures should be in place for the development and use of computer models in the Internal Hazards analysis and to provide confidence that the calculations are undertaken without errors. | Addressed in Section 4 of this report. The RP proposed to use a number of models in the calculation of the consequences analysis in Internal Hazards and substantiation of barriers. This SAP will be demonstrated later in GDA. Hence, this SAP not yet demonstrated. |
| **AV.6 Fault analysis: assurance of validity of data and models**. Sensitivity studies. | Studies should be carried out to determine the sensitivity of the analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation. | This principle sets the expectation that sensitivity studies should be undertaken in all Internal Hazards consequences analysis to establish the worst case scenario, the design requirements of the safety measures, such as hazard barriers, and to determine the margins of safety. | Addressed in Section 4 of this report. The RP proposed to use a number of models in the calculation of the consequences analysis in Internal Hazards and substantiation of barriers. Sensitivities studies required to determine the sensitivity of the analysis to the data and assumptions used in the analysis to demonstrate adequate margins of safety. This will be covered by future submissions. Hence, this SAP not yet demonstrated. |