Office for Nuclear Regulation

New Reactor Division – Generic Design Assessment

GDA Step 2 Assessment of Mechanical Engineering for the UK HPR1000 Reactor

Assessment Report ONR-GDA-UKHPR1000-AR-18-014
Revision 0
October 2018

EXECUTIVE SUMMARY

This report presents the results of my Mechanical Engineering assessment of the UK HPR1000. The assessment is part of the Office for Nuclear Regulation (ONR) Step 2 Generic Design Assessment (GDA).

The GDA of the Requesting Party (RP) safety submission increases in detail as the project progresses. Step 2 of the GDA is an overview of the acceptability, in accordance with the regulatory regime of Great Britain, of the design fundamentals. It includes ONR's review of important 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 Step 2, I assessed the Mechanical Engineering aspects within the UK HPR1000 Preliminary Safety Report (PSR). A number of supporting references and supplementary document submissions, focusing on design concepts and claims, support the PSR.

I considered the adequacy of the RP's submissions, in the area of Mechanical Engineering, primarily against ONR's Safety Assessment Principles (SAPs) and ONR's Technical Assessments Guides. I have also made use other relevant standards and guidance.

My Step 2 assessment work involved regular engagement with the RP. This included technical exchange workshops, planning meetings and meetings with the plant designers.

The UK HPR1000 PSR is primarily based on the reference design, Fangchenggang Nuclear Power Plant Unit 3. This is currently under construction in China. Important Mechanical Engineering aspects of the RP's UK HPR1000 preliminary safety case, as presented in the PSR and its supporting documents, provide:

- An outline of the Mechanical Engineering reactor equipment and supporting structures, based on the reference design.
- The Mechanical Engineering codes and standards applied in the design.
- Work to understand UK Relevant Good Practice (RGP) relative to Mechanical Engineering.
- An initial safety categorisation / classification methodology.
- An approach to undertaking As Low As Reasonably Practicable (ALARP) judgements.
- A preliminary GDA Mechanical Engineering scope.
- A Mechanical Engineering safety case strategy to progress to Step 3.

My Step 2 assessment, of the UK HPR1000 Mechanical Engineering aspects of the safety case, has identified the following areas of good practice:

- Development of a sample list of Mechanical Engineering SSC's for later GDA.
- Identification of main design characteristics differences between the reference design and the generic UK site envelope.
- Willingness to develop the generic safety case to align with UK expectation.
- Development of a technical risk register to manage gaps against UK relevant good practice.
- Review of previous GDA's, SAPs, TAGs and ONR's Mechanical Engineering assessment strategy.

My Step 2 assessment, of the UK HPR1000 Mechanical Engineering aspects of the safety case, has identified the following areas requiring follow up:

- Mechanical Engineering GDA scope.

- Generic safety case architecture.
- Alignment of the design with the generic site envelope.
- Proposals to link, through an engineering schedule, the safety analysis and the engineering structures, systems and components.
- Management of gaps in RGP between reference plant (Fangchenggang Nuclear Power Plant Unit 3) and UK HPR1000 (including application of ALARP principles).
- Approach to design development (i.e. continuous improvement).
- Approach to design assurance.
- Approach to asset management (i.e. safeguarding safety of assets through life).
- Codes, standards and regulations.
- Approach to insulating the primary circuit components.
- Design of the heating, ventilation and air conditioning systems.
- Approach to undertaking nuclear lifts.
- Application of the safety categorisation / classification methodology.

My Step 2 assessment has not identified any fundamental safety shortfalls 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
DAC	Design Acceptance Confirmation
EA	Environment Agency
EIMT	Examination, Inspection, Maintenance and Testing
EMT	Examination, Maintenance and Testing
EDF	Électricité de France
FCG 3	Fangchenggang Nuclear Power Plant Unit 3
GDA	Generic Design Assessment
GNI	General Nuclear International
GNS	Generic Nuclear System Ltd
HSE	Health and Safety Executive
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
MSQA	Management of Safety and Quality Assurance
ONR	Office for Nuclear Regulation
P&ID	Process and Instrumentation Diagram
PCSR	Pre-construction Safety Report
PSR	Preliminary Safety Report (includes security and environment)
RGP	Relevant Good Practice
RCC-M	“Règles de Conception et de Construction des Matériels Mècaniques des Ilots Nucléaires PWR”, or in English, “Design and Construction Rules for the Mechanical Components of PWR Nuclear Islands”,
RI	Regulatory Issue
RO	Regulatory Observation
RP	Requesting Party
RQ	Regulatory Query
SAP(s)	Safety Assessment Principle(s)

SFAIRP	So far as is reasonably practicable
SSC	Structure, System and Component
SSOE	Safety, security or environmental
TAG	Technical Assessment Guide(s)
TBC	To Be Confirmed
TSC	Technical Support Contractor
UK	United Kingdom
WENRA	Western European Nuclear Regulators' Association
WGWD	Working Group on Waste and Decommissioning

TABLE OF CONTENTS

Tables

1 INTRODUCTION

1. The Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA) process calls for a stepwise assessment of the Requesting Party (RP) safety submission. The GDA increases in detail as the project increases. 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. For practical purposes, GNS is referred to as the 'UK HPR1000 GDA Requesting Party' (RP).

2. During Step 1 of the GDA, which is the preparatory part of the design assessment process, the RP established its project management and technical teams. The RP also made arrangements for the GDA of the UK HPR1000 reactor and 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 the GDA is an overview of the acceptability, in accordance with the regulatory regime of Great Britain, of the design fundamentals. It included ONR's assessment of important nuclear safety and nuclear security claims (or assertions). The aim 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 my Step 2 assessment plan for Mechanical Engineering (Ref 1). This plan was prepared in October 2017 and shared with the RP to maximise openness and transparency.

5. This report presents the results of my Mechanical Engineering Step 2 GDA (termed Step 2 assessment within the body of the report) of the UK HPR1000 reactor (termed UK HPR1000 within the body of this report). This is presented in the UK HPR1000 Preliminary Safety Report (PSR) (Ref. 2) and the supporting documentation (Refs 3 to 9).

2 ASSESSMENT STRATEGY

6. This section presents my strategy (Ref. 10) for the Step 2 assessment, of the Mechanical Engineering aspects, of the UK HPR1000. It also includes the scope of the assessment and the standards and criteria I have considered.

2.1 Scope of the Step 2 Mechanical Engineering Assessment

7. The objective of my Step 2 assessment was to assess mechanically engineering related design concepts and safety case claims made by the RP. In particular, my assessment has focussed on considering the following:

- Reviewing the RP’s safety submission’s to confirm whether the Mechanical Engineering claims underpinning the safety of the UK HPR1000, are suitable and sufficient for the Step 2 GDA.
- Familiarising myself with the UK HPR1000 design to provide a basis for planning, more detailed assessment, during Steps 3 and 4 of the GDA.
- Seeking further clarification on the design by raising Regulatory Queries (RQ).
- Engaging with the RP via planning teleconferences, face-to-face technical meetings and workshops.
- Undertaking a high level review of relevant chapters of the UK HPR1000 Pre Construction Safety Report (PCSR) (Ref. 12).

8. During my Step 2 assessment, I have evaluated whether the Mechanical Engineering safety case claims are supported by a body of technical documentation sufficient to support proceeding with GDA beyond Step 2.

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

- Identifying likely topic areas for future Mechanical Engineering assessment where Technical Support Contactors (TSCs) can provide assistance.
- Assuring myself that the RP's future Step 3 Mechanical Engineering submissions will align with my expectations.
- Obtaining an understanding of the RP phased Step 3 submission timeline for Mechanical Engineering.
- Developing a Mechanical Engineering assessment plan for Step 3.

10. For Mechanical Engineering the term “safety claim” is interpreted as being; the ability of a SSC to deliver its safety function during normal operation (including for shutdown), fault sequences and accidents with adequate consideration to the following characteristics:

- Inherent safety – hazard avoidance, in preference to hazard control.
- Fault tolerance – sensitivity to potential faults to be minimised.
- Defence in depth – provision of adequate levels of protection.
- Safety function – structured fault analysis undertaken for both normal operation (including shutdown), and fault sequences.

11. During my Step 2 assessment, I have provided the RP with advice and guidance against the above expectations, i.e. the Mechanical Engineering SSC's related safety case expectations.

2.2 Standards and Criteria

12. The purpose of ONR's Step 2 assessment is to reach an independent and informed judgment on the adequacy of a preliminary nuclear safety and security cases for the reactor technology being assessed. My 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. 13).

13. In addition, the Safety Assessment Principles (SAPs) (Ref. 11) constitute the regulatory principles against which duty holders' and RP's safety cases are judged. Consequently, the SAPs have been used for the Step 2 assessment of the UK HPR1000. The SAPs 2014 Edition aligns with the International Atomic Energy Agency (IAEA) standards and guidance (Ref. 18).

14. Furthermore, ONR is a member of the Western European Nuclear Regulators Association (WENRA). WENRA has developed reference levels (Ref. 19), which represent good practices for existing nuclear power plants, and safety objectives for new reactors.

15. The relevant SAPs, IAEA standards and WENRA reference levels are embodied and expanded on in the Technical Assessment Guides (TAGs) relevant to Mechanical Engineering. These guides provide the principal means for assessing the Mechanical Engineering aspects in practice

16. Mechanical engineering is generally assessed at a component level. This covers a diverse and large number of items of Mechanical Engineering equipment. This equipment interfaces with numerous plant process systems and disciplines. As a consequence, a wide range of SAPs and TAGs (Ref. 11 and 17) can be applicable to undertaking an effective assessment. Accordingly, the Mechanical Engineering approach to carrying out an effective assessment is to select the most appropriate SAPs and TAGs specific to the aspect to be assessed.

2.2.1 Safety Assessment Principles

17. The important SAPs (Ref. 11) applied within my assessment are detailed within Table 1. Individual SAPs are also detailed within the assessment text of this document against the relevant section.

18. The SAPs are used to make regulatory judgements. They provide the fundamental guidance in scoping an assessment topic and in undertaking an effective assessment. This approach ensures the assessment provides a targeted, consistent and transparent consideration on the adequacy of the UK HPR1000 design proposal.

2.2.2 Technical Assessment Guides

19. The following Technical Assessment Guides have been used as part of this assessment (Ref. 17):

Document ID	Title
NS-TAST-GD-003	Safety Systems

NS-TAST-GD-004	Fundamental principles
NS-TAST-GD-005	Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)
NS-TAST-GD-009	Examination, Inspection, Maintenance and Testing of Items Important to Safety
NS-TAST-GD-019	Essential Services
NS-TAST-GD-022	Ventilation
NS-TAST-GD-035	The Limits and Conditions for Nuclear Plant Safety
NS-TAST-GD-036	Diversity, redundancy, segregation and layout of Mechanical plant
NS-TAST-GD-051	The purpose, scope and content of nuclear safety cases
NS-TAST-GD-056	Nuclear Lifting Operations
NS-TAST-GD-057	Design Safety Assurance
NS-TAST-GD-081	Safety aspects specific to storage of spent nuclear fuel
NS-TAST-GD-094	Categorisation of Safety Functions and Classification of Structures and Components
NS-TAST-GD-098	Asset Management

20. Individual TAGs are detailed within the assessment text of this document against the relevant section

2.3 National and International Standards and Guidance

21. The following national and international standards and guidance have been used as part of this assessment.

- Health and Safety Executive (HSE) (Ref. 20)
  - Short Guide to Health and Safety Regulations

    http://www.hse.gov.uk/pubns/hsc13.pdf

    Health and Safety Executives Approved Codes of Practice

    http://www.hse.gov.uk/pubns/books/index-legal-ref.htm
- International Atomic Energy Agency (IAEA) (Ref. 18)

- IAEA – Safety Standards: Safety of Nuclear Power Plants: Design, Specific Safety Requirement; SSR-2/1; IAEA 2016

  http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1534_web.pdf

- IAEA – Safety Standards: Fundamental Safety Principles; SF-1; IAEA 2006

  http://www-pub.iaea.org/MTCD/publications/PDF/Pub1273_web.pdf

- IAEA - Safety Standards: Operating Experience Feedback for Nuclear Installations, Specific Safety Guide; No. SSG-50; IAEA 2018

  https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1805_web.pdf

- IAEA - Safety Standards: Ageing Management for Nuclear Power Plants, Safety Guide; NS-G-2.12; IAEA 2009

  http://www-pub.iaea.org/MTCD/publications/PDF/Pub1373_web.pdf

- IAEA - Safety Standards: Design of Fuel Handling and Storage Facilities for Nuclear Power Plants Safety Guide; NS-G-1.4; IAEA 2003

  http://www-pub.iaea.org/MTCD/publications/PDF/Pub1156_web.pdf

- IAEA - Safety Standards: Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants Safety Guide; NS-G-2.6; IAEA 2002

  http://www-pub.iaea.org/MTCD/publications/PDF/Pub1136_scr.pdf

- Western European Nuclear Regulators Association (WENRA) (Ref.19)

  - Reactor Safety Levels for Existing Reactors (September 2014)

    http://www.wenra.org/media/filer_public/2014/09/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf

  - Working Group on Waste and Decommissioning (WGWD); Waste and Spent Fuel Storage Safety Reference Levels (February 2011);

    http://www.wenra.org/media/filer_public/2012/11/05/wgwd_v2-1waste-and-spent-fuel-storage-safety-reference-levels.pdf

  - Waste and Spent Fuel Storage Safety Reference Levels (February 2011);

    http://www.wenra.org/media/filer_public/2012/08/30/wgwd_v1-2waste-and-spent-fuel-storage-safety-reference-levels.pdf

2.4 Use of Technical Support Contractors

22. During my Step 2 assessment, I have not engaged Technical Support Contractors (TSCs) to support the Mechanical Engineering assessment of the UK HPR1000. However, as part of Step 2, I have considered and identified a number of potential topic areas for technical review as part of my Step 3 assessment. A prerequisite to undertaking these technical reviews will be the adequacy of the RP’s Step 3 submission, in terms of sufficiency of documents and associated timescales.

2.5 Integration with Other Assessment Topics

23. Early in GDA, I recognised the importance of working closely with other ONR and external inspectors (including Environment Agency's inspectors) as part of the Mechanical Engineering assessment process. Similarly, other inspectors sought input from my assessment of the Mechanical Engineering aspects of the UK HPR1000. I consider these interactions are important to the success of the project to prevent or mitigate any gaps, duplications or inconsistencies in ONR's assessment. From the start of the project, I have identified potential interactions between Mechanical Engineering and other technical areas, with the understanding that this position will evolve throughout the UK HPR1000 GDA.

24. The important interactions where Mechanical Engineering assessment will, where required, provide input are:

- External hazards relating to the generic site envelope.
- Internal hazards related to screening assessment of Mechanical Engineering equipment.
- Nuclear liabilities relating to spent fuel export, interim storage facilities and decommissioning.
- Chemistry aspects of material selection regarding Mechanical Engineering SSC's.
- Probabilistic Safety Analysis (PSA) relating to Mechanical Engineering reliabilities.
- Fault studies considerations of Mechanical Engineering equipment.
- Security aspects relating to the Mechanical Engineering equipment.
- Conventional health & safety assessment of the Construction (Design and Management) CDM Regulations 2015.
- Management of Safety and Quality Assurance (MSQA) assessment relating to the RP's design arrangements for Mechanical Engineering equipment.
- Radiological protection aspects associated with the asset management of mechanical equipment.
- Human factors aspects associated with operation of mechanical equipment.

25. Each of the above topics will be led by ONR's respective topic lead inspector.

26. I have also provided Mechanical Engineering input into the following cross-cutting topics:

- PCSR safety case development.
- Categorisation of safety functions and classification of structures, systems and components (SSCs).
- ALARP methodologies.
- GDA scope.

27. These interactions are expected to continue throughout the GDA. These interactions are considered important to ensure consistency across the various technical assessment areas. The interactions listed above are not exhaustive, as they will continue to develop as GDA progresses.

3 REQUESTING PARTY SAFETY CASE

28. During Step 2 of the GDA, the RP submitted a PSR and other supporting references. These submissions constitute a preliminary safety case for the UK HPR1000. This section presents a summary of the RP's preliminary safety case in the area of Mechanical Engineering. It also identifies the documents submitted by the RP. These submissions formed the basis of my Mechanical Engineering assessment of the UK HPR1000 during GDA Step 2.

3.1 Summary of the RP's Safety Case in the Area of Mechanical Engineering

29. The PSR (Ref. 2) did not contain a specific Mechanical Engineering chapter. Instead, the RP has incorporated Mechanical Engineering aspects across a selection of the UK HPR1000 PSR chapters.

30. In my opinion, the following four headings summarise the important Mechanical Engineering related safety claims contained in the UK HPR1000 preliminary safety case. The headings are derived from Chapter 1 of PSR (Ref. 2) and the safety categorisation / classification methodology report (Ref. 7)

- Design characteristics - the design characteristics of the UK HPR1000 reflect a generic UK site that bounds suitable locations.

- Design development - the UK HPR1000 design will be developed in an evolutionary manner, using robust design process, building on relevant good international practice, to achieve a strong safety and environmental performance.

- ALARP principles - the design, and intended construction and operation, of the UK HPR1000 will be developed to reduce, so far as is reasonably practicable (SFAIRP), the impact on the workers, the public, and the environment.

- Categorisation of safety functions and classification of structures, systems and components – the categorisation and classification principles for the UK HPR1000 are suitable for the UK context.

3.2 Basis of Assessment: RP's Documentation

31. The RP's documentation that form the basis for my Step 2 Mechanical Engineering assessment of the safety case claims of the UK HPR1000 are:

- UK HPR1000 GDA Project Preliminary Safety Report HPR/GDA/PSR/001 Chapters 1 to 27 (Ref. 2) – See comments above concerning the absence of a specific Mechanical Engineering chapter.

  The PSR is supported by the following lower tier documents:

- GDA for UK HPR1000 - Design Manual for Valve Selection (Ref. 3)

- GDA for UK HPR1000 – Applicable Codes and Standards on Context of Mechanical Engineering (Ref. 4)

- GDA for UK HPR1000 – Safety Case Strategy of Mechanical Engineering (Ref. 5)

- GDA Project Scope for UK HPR1000 GDA Project (Ref. 6)

- GDA for UK HPR1000 – Methodology of Safety categorisation / classification (Ref. 7)
- GDA Project – ALARP and BAT Principles and Requirements for UK HPR1000 GDA (Ref. 8)
- GDA for UK HPR1000 – ALARP Methodology (Ref. 9)

32. In addition, during April 2018, the RP submitted to ONR for information an advance copy of the UK HPR1000 Pre-Construction Safety Report (PCSR) (Ref. 12). Similar to the PSR, the PCSR did not contain a specific Mechanical Engineering chapter. Having early visibility of the scope and content of the PCSR has informed the planning and preparation of my GDA Step 3 assessment work.

4 ONR ASSESSMENT

33. This assessment has been carried out in accordance with HOW2 guide [NS-PER-GD-014, “Purpose and Scope of Permissioning” (Ref. 13)].

34. My Step 2 assessment has involved regular engagement with the RP’s Mechanical Engineering specialists, i.e. five technical exchange workshops (two in China and three in the UK) and frequent planning meetings.

35. These Mechanical Engineering engagements included visits to:

- Fangchenggang Nuclear Power Plant Unit 3, where I observed the construction site including the nuclear island.
- Fangchenggang Nuclear Power Plant Unit 1 and Unit 2 site, where I walked around the plant and observed reactor operations from the main control room.

36. My Step 2 assessment has identified some gaps in documentation formally submitted to ONR. Consistent with ONR’s Guidance to Requesting Parties (Ref. 14), these gaps have led to Regulatory Queries (RQs) being issued.

37. My Step 2 assessment has raised the following eight RQs (Ref. 15):

- RQ-UKHPR1000-0001 – Gaps in relevant good practice
- RQ-UKHPR1000-0005 – Process & instrumentation diagram notation
- RQ-UKHPR1000-0010 – Mechanical structures, systems and components candidate list
- RQ-UKHPR1000-0025 – Mechanical engineering research and development (continuous improvement)
- RQ-UKHPR1000-0066 – Design manual for valve selection
- RQ-UKHPR1000-0075 – Asset management arrangements
- RQ-UKHPR1000-0077 – Mechanical codes and standards
- RQ-UKHPR1000-0101 – (Follow up to RQ-UKHPR1000-0025) - Mechanical engineering research and development (continuous improvement)

38. In addition, the RP produces and manages a Mechanical Engineering meeting action tracker (Ref, 22). This action tracker contains Mechanical Engineering GDA actions relevant to the UK HPR1000 design. Examples of Mechanical Engineering RP actions, resulting from L4 mechanical technical meetings, include the following:

- Explaining the link between the safety analysis and the engineering. The RP considers this link can be delivered through the production of an engineering schedule submission.
- Explaining the arrangements for nuclear lifting operations. The RP considers the lifting arrangements can be justified through a lifting schedule submission.
- Discussing the mechanical safety case strategy for the UK HPR1000 PCSR.
- Discussing the contents of the system design manuals. The manuals convey the design basis for the UK HPR1000 Mechanical Engineering components.

- Discussing aspects of the UK HPR1000 design. Examples considered included fuel route lifting arrangements; reactor main coolant pump; heating, ventilation and air conditioning (HVAC) systems; and the control rod drive mechanism (CRDM).

39. My Step 2 assessment has not raised any Regulatory Observations (RO's). Nevertheless, some aspects of RO-UKHPR1000-002 - Demonstration that the UK HPR1000 Suitably Aligns with the Generic Site Envelope (Ref. 0) that was raised by ONR's external hazards inspector are relevant to my Mechanical Engineering aspects of the UK HPR1000.

40. The principal aims of ONR's Step 2 assessment are to:

- Identify fundamental safety shortfalls preventing the issue of a design acceptance certificate.
- Identify the important safety case claims, confirming they are complete and reasonable.
- Identify the availability of supporting arguments and evidence for assessment during Step 3 and 4 of the GDA.

41. Mechanical Engineering SSCs typically deliver the principal safety functions of:

- reactivity control
- heat transfer and removal
- confinement of radioactive substances

42. My assessment has also targeted the RP's design philosophies, through consideration of its design process arrangement. I expect the RP's design process approach should be able to provide the necessary assurance and confidence to demonstrate a SSC('s):

- Design has been adequately optioneered, taking account of operational experience and Relevant Good Practice (RGP).
- Is suitable for the purpose for which it is to be used.
- Risks have been reduced SFAIRP, a requirement of UK legislation (Health & Safety at Work etc. Act 1974.
- Have adequate asset management arrangements in place.

43. My Step 2 assessment has targeted the following RP's safety case claims:

- Claims against the UK HPR1000 design characteristics (against a 60 year claimed design life).
- Claims against the UK HPR1000 design development and ALARP principles.
- Claims against its safety categorisation / classification methodology for the UK HPR1000.

44. I have also considered the RP's Mechanical Engineering safety case strategy (Ref. 5). The strategy focuses on the required Step 3 Mechanical Engineering work, which is

based on the current Step 2 status. The RP acknowledges that the safety case strategy may require updating as GDA develops.

45. Details of my Step 2 Mechanical Engineering assessment of the UK HPR1000 preliminary safety case, including conclusions, are identified in the following sub sections. Areas of good practice, and items requiring later GDA follow up, are also identified.

46. ONR's summary of the Step 2 assessment of the UK HPR1000 report (Ref. 21) presents ONR's consolidated position. It provides ONR's overall regulatory judgement on the adequacy of the RP's work, during Step 2, on the following cross cutting topics:

- Safety case development approach for the UK HPR1000.
- Categorisation of safety functions and classification of structures, systems and components for the UK HPR1000.
- ALARP methodology for the UK HPR1000.

4.1 UK HPR1000 Mechanical Engineering PCSR Safety Case Strategy

4.1.1 Assessment - PCSR Safety Case Strategy

47. At Step 2, ONR's guidance to RPs (Ref 14) expects:

- Details of the safety case development process, including peer review arrangements, and how this gives assurance that nuclear risks are identified and managed.

48. The RP has produced a Mechanical Engineering safety case strategy (Ref. 5). In summary, the strategy details the:

- GDA objectives relative to ONR's guidance to RPs (Ref. 14).
- Mechanical engineering structures, systems and components (SSC's) contained within the scope of the GDA.
- Safety case route map for Mechanical Engineering, which provides an overview of the safety case claims and argument structure for the UK HPR1000 PCSR (SAP SC.1 – Safety Case Production Process).
- Gaps that the RP has identified between its reference design FCG.3 and the UK HPR1000.
- RP's proposals of a sample list of Mechanical Engineering SSC's for later GDA.
- RP's description of Mechanical Engineering documentation hierarchy for the generic safety case.
- The RP's Mechanical Engineering GDA document submission plan.

49. At Step 2, based on my assessment, I consider the RP's Mechanical Engineering safety case strategy (Ref. 5):

- Adequately sets out the GDA objectives relative to Mechanical Engineering.

- Proposes a preliminary GDA scope. I consider the scope requires further developed. I expect the GDA scope should cover all Mechanical Engineering SSC's, delivering nuclear safety functions.

- Proposes a reasonable high level safety case claims and arguments structure, for Mechanical Engineering SSC's.

- Provides a good early indication of the Mechanical Engineering gaps, against UK expectations, it has identified (see Paragraph 4.3).

- Provides a useful sample list of Mechanical Engineering UK HPR1000 SSC's. This list will inform my assessment during later GDA steps.

- Details a UK HPR1000 generic safety case structure, which appears reasonable for Step 2. However, I expect the adequacy of the safety case architecture, detailing the claims, arguments and evidence approach, to be the subject of an ONR project intervention as GDA progresses. [TAG NS-TAST-GD-051 – The Scope, Purpose and Content of Nuclear Safety Cases (Ref. 17)].

- Proposes a provisional Mechanical Engineering document submission plan that will need to be further developed and formally agreed.

4.1.2 Areas of Good Practice - PCSR Safety Case Strategy

I have identified the following area of good practice:

- Developing a sample list of Mechanical Engineering SSC's for later GDA.

4.1.3 Follow Up Items - PCSR Safety Case Strategy

50. During my Step 2 assessment of the RP's PCSR safety case strategy (Ref. 5), I have identified the following specific shortfalls. I will follow these up during later GDA steps:

- The full scope of UK HGPR1000 Mechanical Engineering SSC's will need to be developed and agreed by ONR. I expect the RP to develop the GDA Mechanical Engineering scope to include all Mechanical Engineering SSC's that support the UK HPR1000 nuclear safety case.

- Adequacy of the UK HPR1000 generic safety case architecture relevant to Mechanical Engineering SSC's. I expect the RP to develop its safety case approach to an adequate standard. [TAG NS-TAST-GD-051 – The Scope, Purpose and Content of Nuclear Safety Cases (Ref. 17) and SAP SC series (Ref. 11)].

4.1.4 Conclusion - PCSR Safety Case Strategy Assessment

51. Based on my Step 2 assessment of the RP's strategy (Ref. 5), I have concluded that further intervention will be required to confirm the UK HPR1000 GDA Mechanical Engineering scope and safety case architecture aligns with my expectations.

52. I consider the PCSR safety case strategy (Ref. 5) delivers a reasonable starting point for Step 2.

4.2 UK HPR1000 Design Characteristics

4.2.1 Assessment – Design Characteristics

53. Chapter 1 of PSR (Ref. 2) claims that the design characteristics of the UK HPR1000 reflect a generic UK site that bounds suitable locations (for a 60-year design life).

54. At Step 2, ONR's Guidance to RPs (Ref 14) expects the specification of the site characteristics to be used as the basis for the safety analysis (the generic site envelope).

<u>UK HPR1000 Site Characteristics</u>

55. The RP has identified several important differences between the reference design (FCG 3) and the generic site envelope for the UK HPR1000, e.g. deviations in FCG 3 air and water temperatures and earthquake data, when compared with the UK generic site. These shortfalls, amongst others, are being managed via an external hazard regulatory observation, RO-UKHPR1000-0002 (Ref. 0). In summary, the RO requires the RP to demonstrate that the UK HPR1000 design is suitably aligned with the generic site envelope.

56. The RP has indicated that the following UK HPR1000 Mechanical Engineering systems may be impacted by the difference in site characteristic:

- Heating, ventilation, and air-conditioning (HVAC) systems. [TAG NS-TAST-GD-022 – Ventilation (Ref. 17)].
- A number of reactor cooling systems. [TAG NS-NST-GD-003 – Safety Systems (Ref. 17)].
- Seismic design of a number of Mechanical Engineering components, i.e. pumps, valves etc. (SAP EHA.9 – Earthquakes).

57. Justification that the UK HPR1000 Mechanical Engineering design suitably aligns with the generic site envelope will require enhanced regulatory attention as GDA develops. I will be working closely with ONR's external hazards inspector, to ensure aspects of RO-UKHPR1000-0002 (Ref, 0) directly affecting my Mechanical Engineering assessment are adequately resolved.

<u>Linkage of UK HPR1000 Safety Analysis to Mechanical Engineering SSC's</u>

58. An important aspect of any safety submission is the ability for it to link the safety analysis with the engineering that provides it (SAPs FA.4 – Fault Tolerance). I identified that the PSR information, providing this link was limited. To address this shortfall, the RP has committed to producing an engineering schedule as a UK HPR1000 generic PCSR supporting document. The aim of the engineering schedule will be to link the safety analysis with the engineering SSC's.

59. I consider judging the overall adequacy of the engineering schedule to be a multi-disciplined matter. I intend to work closely with other relevant disciplines to review its adequacy, relative to Mechanical Engineering, as GDA develops. A constraint is that the UK HPR1000 safety analysis needs to reach a suitable level maturity, to enable a meaningful engineering schedule to be developed.

60. I expect the RP to use its engineering judgement (of the UK HPR1000 systems safety categorisations / classifications) to develop the engineering schedule; thus allowing a timely staged engineering schedule submission.

4.2.2 Areas of Good Practice - Design Characteristics

61. I have identified the following areas of good practice:

- The RP identification of the main differences in design characteristics between its reference design (FCG.3) and the generic UK site envelope.

- The RP's willingness to develop the UK HPR1000 generic safety case to align with UK expectations.

4.2.3 Follow Up Items - Design Characteristics

62. During my Step 2 assessment of the RP's design characteristics claims, I have identified the following specific shortfalls. I will follow these up during later GDA steps:

- Full alignment of the Mechanical Engineering UK HPR1000 design with the requirements of the generic site envelope.

- The RP's proposals to link, through an engineering schedule, the safety analysis to the engineering SSC's.

4.2.4 Conclusion - Design Characteristics Assessment

63. Based on my Step 2 assessment of the RP's design characteristics claims, I have concluded that further intervention will be required to confirm the Mechanical Engineering UK HPR1000 design suitably aligns with the generic site envelope.

64. Additionally, the RP should demonstrate (through its engineering schedule) the link between the safety analysis and the engineering SSC's.

65. I consider the claims against design characteristics present a reasonable starting point for Step 2.

4.3 UK HPR1000 Design Development and ALARP Claims

4.3.1 Assessment - Design Development and ALARP

66. Design Development - Chapter 1 of the PSR (Ref. 2) claims that the UK HPR1000 design will be developed in an evolutionary manner, using robust design process, building on relevant good international practice, to achieve a strong safety and environmental performance.

67. ALARP – The UK HPR1000 ALARP and BAT Principles and Requirements (Ref. 8) and the ALARP Methodology (Ref. 9) present the RP's arrangements for ALARP. My consideration of these ALARP arrangements, which for Step 2 appears reasonable, has been limited to undertaking a high level review. Chapter 1 of the PSR (Ref. 2) claims the design, and intended construction and operation, of the UK HPR1000 will be developed to reduce, so far as is reasonably practicable (i.e. reduce risks ALARP), the impact on the workers, the public, and the environment.

68. A Step 2, ONR's guidance to RPs (Ref 14) expects:

- Identification and explanation of any deviations from modern, international good practices.

- Identification of outstanding information that remains to be developed and its significance.

- Explicit reference to standards and design codes used, justification of their applicability, and that they present relevant good practice, and are broad demonstration that they have been met (or exceptions justified).

- A description of the process being adopted by the RP to demonstrate compliance with the legal duty in Great Britain to ensure that the risks to human health arising from the operation of a power station based on the proposed design are reduced 'So Far As Is Reasonably Practicable' (SFAIRP). For ONR's assessment purposes, the terms ALARP (As Low As Reasonably Practicable) and SFAIRP are interchangeable and require the same tests to be applied.

Gaps in UK HPR1000 Relevant Good Practice

69. An important aspect any ALARP demonstration is presenting how relevant good practice (RGP) has been identified and the extent to which it has been implemented. This is the one of basic requirement for demonstrating the legal requirements of reducing risks SFAIRP has been met (or in the context of GDA, likely to be). [TAG NS-TAST-GD-005 Guidance on the Demonstration of ALARP (Ref. 17)].

70. I raised RQ-UKHPR1000-0001 - Identified gaps in RGP (Ref. 15). The aim of the query was to identify and explain the gaps in RGP between the reference design and UK HPR1000.

71. In its response to RQ-UKHPR1000-0001 (Ref. 15), the RP identified the following Mechanical Engineering areas of potential shortfalls (when comparing the FCG 3 reference design against UK HPR1000 expectations):

- Codes and standards when considered against SAP ECS.3 – Codes and Standards.

- Categorisation of safety functions and classification of structures, systems and components when considered against SAPs ECS.1 – Safety Categorisation and ECS.2 – Safety Classification of SSC's.

- Maintenance, inspection and testing when considered against SAPs EMT Series – Maintenance Inspection and Testing.

- Diversity and redundancy when considered against SAPs EDR.2 – Redundancy, Diversity and Segregation, EDR.3 – Common Cause Failure & TAG NS-TAST-GD-036 - Diversity, Redundancy, Segregation and Layout of Mechanical Plant (Ref. 17).

- Nuclear lifting equipment when considered against TAG NS-TAST-GD-056 – Nuclear Lifting Operations (Ref. 17).

- Primary circuit insulation approach when considered against SAPs EDR.1 – Failure to Safety and TAG NS-TAST-GD-004 – Fundamental Principles (Ref. 17).

- Approach to controlling modifications when considered against satisfying SAPs SC.7 – Safety Case Maintenance.

72. The RP has stated that the shortfalls are included within the RP's technical risk register. The RP has indicated that mitigation strategies are being developed for each of the shortfalls. I will expect emerging risks to be added to the register as GDA progresses

73. The RP has agreed to present the results of the gap analysis against mechanically related UK RGP (Ref. 5) at the start of Step 3. I consider this an important aspect of demonstrating the Mechanical Engineering design satisfies the ALARP / SFAIRP principles. The results of this UK HPR1000 gap analysis, together with the implementation of its UK HPR1000 ALARP arrangements (Ref. 8 and Ref. 9), will require regulatory scrutiny as the GDA develops. [TAG NS-TAST-GD-005 Guidance on the Demonstration of ALARP (Ref. 17)].

UK HPR1000 Continuous Improvement

74. The principle of continuous improvement is central to achieving sustained high standards of nuclear safety. The legal requirements for risk reduction SFAIRP underpin this principle. [TAG NS-TAST-GD-005 Guidance on the Demonstration of ALARP (Ref. 17)].

75. I raised RQ-UKHPR1000-0025 & 0101 – Design, Mechanical Engineering Research (Continuous Improvement) (Ref. 15). The aim of the queries were to seek evidence of the RP's approach to developing the UK HPR1000 to address continuous improvement expectations set out within ONR's SAPs (Ref. 11).

76. The RP response identified a series of system and component research topics (together with their technical objective, which involved consideration of operational lessons learned) leading to improvements in the FCG.3 HPR1000 reference design. At this stage, I consider this supports the RP's high-level claim that the UK HPR1000 has been developed in an evolutionary manner. Nevertheless, I will required further clarity of the RP's application of continuous improvement (relevant to the ALARP principles) as GDA develops. [TAG NS-TAST-GD-005 – Guidance on the Demonstration of ALARP (Ref. 17)].

UK HPR1000 Design Process

77. There are duties on designers to take due recognition of health and safety in the design process. [TAG NS-TAST-GD-057 – Design Assurance (Ref. 17)].

78. I raised RQ-UKHPR1000-0066 – Design Process, Design Manual Valve Selection (Ref. 15) against the RP's Design Manual for Valve Selection submission (Ref. 3). The aim of the query was to consider, at a high level, the adequacy of RP's design arrangements to support the UK HPR1000 valves role in supporting the following key fundamental safety functions. (SAPs ERC.1- Design and Operation of Reactors).

- control of reactivity (including re-criticality following an event)
- removal of heat from the core
- confinement of radioactive material

79. In response to the RQ (Ref. 15), the RP highlighted:

- The different design arrangements it has in place for special (usually assigned with the highest safety classification) and general valves.
- The three staged valve design process (concept, basic and detailed). This considered, amongst a number of other topics, safety function and operational requirements.
- Its safety classification methodology (SAPs ECS.2 – Safety Classification of SSC's).

- Its specification arrangement (including quality control) (SAPs EKP.3 – Defence in Depth).

80. At this stage, the RP's response provides high-level support to the claim that the UK HPR1000 will be developed using adequate design processes. Nevertheless, I expect to see further clarity as to the adequacy of the RP's design assurance arrangements as GDA develops. [TAG NS-TAST-GD-057 – Design Assurance (Ref. 17)]. I consider the RP's approach of managing changes to the design reference point (and resultant safety case and / or engineering changes) as important. Consequently, I will be working closely with the management of safety and quality assurance (MSQA) inspector to ensure the RP's design change approach is adequate.

UK HPR1000 Asset Management Approach

81. Asset Management is the through life approach to manage risks that may challenge an identified assets capability to support or deliver a safety, security or environmental (SSoE) function. This corresponds to ONR EMT and EAD series of SAPs (Ref. 11) and ONR's TAGs (Ref. 17).

82. I raised RQ-UKHPR1000-0075 – Design Process, Asset Management Arrangements (Ref. 15). The aim of the query was to consider, at a high level, the adequacy of RP's design approach to safeguard the through life asset management of UK HPR1000 Mechanical Engineering assets. [TAG NS-TAST-GD-009 - EIMT of Items Important to Safety and TAG NS-TAST-GD-098 – Asset Management (Ref. 17)].

83. The RP's response (Ref. 15) identified the design requirements for asset management for the UK HPR1000. This included equipment identification, process design, equipment design, equipment qualification, state monitoring, EIMT, commissioning, operation and decommissioning. Additionally, its response summarised where asset management would be considered in the UK HPR1000 PCSR, as GDA progresses.

84. At this stage, I consider the RP has demonstrated a reasonable understanding of the requirement to safeguard UK HPR1000 Mechanical Engineering assets through life (NS-TAST-GD-098 – Asset Management). Nevertheless, I intend to consider the RP's design approach for asset management. [SAPs EMT Series – Maintenance, Inspection and Testing, EAD Series – Ageing and Degradation and ELO.1 – Layout (Ref. 17)], as GDA develops.

UK HPR1000 Mechanical Engineering Codes, Standards and Regulations

85. UK HPR1000 Mechanical Engineering equipment important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate codes and standards (SAPs ECS.3 – Codes and Standards).

86. The RP's Mechanical Engineering codes and standards report (Ref. 4) details the UK HPR1000 mechanical codes and standards. The report is not fully complete, for the UK context, and requires further development. One area for further development is reference to satisfying UK regulations, which is currently missing.

87. Design and construction rules for the Mechanical Engineering components of PWR nuclear islands (RCC-M) is listed as an UK HPR1000 code and standard report (Ref. 4). I raised RQ-UKHPR1000-0077 – Design Process, Mechanical Engineering Codes and Standards (Ref. 15) querying the RP's approach to using RCC-M for the UK HPR1000.

88. The RP's response listed UK HPR1000 Mechanical Engineering equipment that will be designed in accordance with RCC-M. It also listed other mechanically related codes

and standard (where either RCC-M requires supplementing or where it is not deemed applicable). ONR has previously accepted the use of the RCC-M code (for pressure retaining components). However, I consider that some of the UK HPR1000 codes and standards listed (for example, non –pressure related Mechanical Engineering equipment such as lifting equipment, HVAC systems, diesel generators etc.) require further justification to satisfy my expectations. (SAPs ECS.3 – Codes and Standards).

89. The RP has agreed to develop its Mechanical Engineering codes and standards submission (Ref. 4) as GDA develops. For Step 2, whilst still under development, I consider the RP's initial consideration of codes and standards for the UK HPR1000 to be reasonable. I intend to seek further demonstration of the adequacy of UK HPR1000 specific Mechanical Engineering related codes, standards and regulations. (SAPs ECS.3 – Codes and Standards and HSE Guidance (Ref. 20). This will require regulatory scrutiny as GDA develops.

<u>List of UK HPR1000 Mechanical Engineering Structures, Systems and Components for future GDA</u>

90. It is essential that Mechanical Engineering equipment important to safety is clearly identified (SAPs ECS.3 – Codes and standards, EMT.7 – Functional Testing, EAD.1 – Safe Working Life, EAD.5 - Obsolescence).

91. I raised RQ-UKHPR1000-0010 – Mechanical Structures, Systems and Components (SSC's) Candidate List (Ref. 15). The aim of the query was to influence the RP to develop a list of Mechanical Engineering SSC's with information necessary to assist my future assessment. This list was developed from the FCG 3 reference plant and represents a sample of HPR1000 SSC's important to nuclear safety. A similar approach has been used for previous GDA's

92. I requested the RP's proposed a sample list of mechanical SSC's considered the following screening criteria. The screening criteria was based on UK RGP [See SAP references (Ref. 11)]:

- The type of Mechanical Engineering SSC.
- The Mechanical Engineering SSC's safety function (SAPs EKP.4 – Safety Function).
- The Mechanical Engineering SSC's safety category, in both normal and fault conditions (SAPs ECS.1 – Safety Categorisation).
- The Mechanical Engineering SSC's safety classification (SAPs ECS.2 – Safety Classification of SSC's).
- Whether the Mechanical Engineering SSC is novel (SAPs Paragraph 27).
- Whether the Mechanical Engineering SSC acts as 'safety system' or 'safety related system' (SAPs Paragraph 181).
- Whether the Mechanical Engineering SSC fulfils a redundant, diverse or independent means of delivering its safety function within the design (SAPs Paragraph 162).
- The Mechanical Engineering SSC's physical location within a system and / or building. (SAPs ELO.1 – Access).

93. In response to RQ-UKHPR1000-0010, the RP produced a Mechanical Engineering safety case strategy (Ref. 5). This strategy outlines a sample list of important

Mechanical Engineering SSC's, initial based on FCG.3 reference design. I intend to use the list to inform my future Mechanical Engineering assessment. This list does not confine my UK HPR1000 GDA scope should I identify other areas of Mechanical Engineering requiring assessment.

4.3.2 Areas of Good Practice – Design Development and ALARP

94. I have identified the following areas of good practice:

- The RP's development of a technical risk register to manage gaps against UK expectations (Ref. 15).
- The RP's review of previous GDA's, SAPs (Ref. 11), TAG's (Ref. 17) and ONR's Mechanical Engineering Assessment Strategy (Ref. 10) to identify gaps in RGP.

4.3.3 Follow Up Items – Design Development and ALARP

95. My Step 2 assessment of the design development and ALARP claims has identified the following Mechanical Engineering areas for follow during later GDA steps:

- The RP's management of any gaps in RGP between the reference design and UK HPR1000. I expect the RP to demonstrate, through the implementation of its ALARP arrangements (Ref. 8 and Ref. 9) that it is taking reasonably practicable measures to address any gaps in RGP. [TAG NS-TAST-GD-005 - ALARP Guidance (Ref. 17)].
- The RP's design development approach for the UK HPR1000, i.e. continuous improvement, which is applicable to the application of ALARP. I expect the RP to demonstrate that any design changes are / have been subject to an adequate ALARP assessment. [TAG NS-TAST-GD-005 - ALARP Guidance (Ref. 17)].
- Adequacy of the RP's design assurance approach for Mechanical Engineering related SSC's. I expect the RP to demonstrate that any changes to the UK HPR1000 design follow a comprehensive design assurance process. [TAG NS-TAST-GD-057 - Design Assurance (Ref. 17)].
- The RP's approach to safeguard the safety of the UK HPR1000 Mechanical Engineering assets through life. I expect the RP to demonstrate it has an adequate asset management approach in place. [TAG NS-TAST-GD-009 - EIMT of Items important to Safety, TAG NS-TAST-GD-098 - Asset Management. SAPs EMT – Maintenance, Inspection and Testing and EAD Series – Ageing and Degradation (Ref. 17)].
- Adequacy of the UK HPR1000 Mechanical Engineering related codes, standards and regulations. I expect the RP to explicitly state and justify the codes, standards and regulations it proposes for UK HPR1000 Mechanical Engineering related plant. SAPs ECS.3 – Codes and Standards. I will expect specific attention be given to non-reactor plant components. i.e. those Mechanical Engineering components not forming part of the reactor pressure boundary.
- Adequacy of the UK HPR1000 insulation approach for the mechanically engineering related primary circuit components. I expect the RP to justification, through an ALARP submission, why the insulation approach for the UK HPR1000 plant components is suitable and sufficient. (SAPs EDR.1 – Failure to Safety).

- Adequacy of the design of the UK HPR 1000 heating, ventilation, and air-conditioning (HVAC) systems (SAP ECV.10). I intend to involve a Technical Support Contractor, during later GDA steps, to consider this area. [TAG NS-TAST-GD-022 – Ventilation (Ref. 17)].

- Adequacy of the UK HPR1000 approach to undertake nuclear lifts i.e. any lift with the potential to create a radiological hazard. I expect the RP to justify why its approach to lifting reduces risks ALARP. [TAG NS-TAST-GD-056 Nuclear Lifting Operations (Ref. 17)].

4.3.4 Conclusion – Design Development and ALARP Principles Assessment

96. Based on my Step 2 assessment of the RP's design development and ALARP claims, I have concluded that further intervention will be required to ensure a number of design development and ALARP areas for follow up achieve a satisfactory outcome.

97. I consider the claims against design development and ALARP present a reasonable starting point for Step 2.

4.4 UK HPR1000 Categorisation of Safety Functions and Classification of Structures, Systems and Components

4.4.1 Assessment - Categorisation of Safety Functions and Classification of Structures, Systems and Components Methodology

98. The PSR safety case claims the categorisation and classification principles are suitable for the UK context.

99. At Step 2, ONR Guidance to RPs (Ref 14) expects:

- Safety function categorisation and the safety classification of SSC's – with a demonstration of how this is reflected in the design.

<u>UK HPR1000 Safety categorisation / classification Methodology</u>

100. The RP's extant safety categorisation / classification approach, within its PSR submission (Ref. 2), was based on its reference plant (FCG.3). The RP issued (in the later phase of Step 2) its revised safety categorisation / classification methodology (Ref. 7) for the UK HPR1000. Consequently, my consideration of the methodology has been limited to a high level review.

101. ONR summary of its consolidated position (Ref. 21) details the regulatory position on the RP's safety categorisation / classification methodology (Ref. 7). From a Mechanical Engineering perspective, I would expect the methodology to adequately cover:

- SSC reliabilities (SAPs ERL.1).

- The degree of design substantiation require to satisfy any given safety classification [TAG NS-TAST-GD-094 - Categorisation of Safety Functions and Classification of Structures and Components (Ref. 17)}

102. In response RQ-UKHPR1000-001 (Ref. 15), regarding gaps against RGP, the RP identified shortfalls in the safety classification of its UK HPR1000 nuclear lifting equipment (e.g. polar crane) [TAG NS-TAST-GD-094 - Categorisation of Safety Functions and Classification of Structures and Components (Ref. 17)]; when considered against the guidance given in TAG NS-TAST –GD-056 - Nuclear Lifting

Operations (Ref. 17)]. These shortfall concern the extant use of a non-classification safety rating for nuclear lifting equipment for its reference plant (FCG.3).

103. I have identified that the RP's safety categorisation / classification methodology (Ref. 7) has been expanded to include consideration of non-reactor type faults. I judge this an improvement to the methodology. I consider that application of the revised methodology is likely to impact the safety classification assigned to the UK HPR1000 Mechanical Engineering SSC's

104. I consider the safety categorisation / classification methodology, and its application relative to all of the UK HPR1000 Mechanical Engineering SSC's, will require regulatory attention as GDA develops. I also intend to consider the adequacy of the RP's design substantiation approach (including reliability claims) for the UK HPR1000 Mechanical Engineering SSC's.

4.4.2 Areas of Good Practice – Categorisation of Safety Functions and Classification of Structures, Systems and Components

105. I have not identified any areas of good practice.

4.4.3 Follow Up Item – Categorisation of Safety Functions and Classification of Structures, Systems and Components

106. My Step 2 assessment of the RP's safety categorisation / classification methodology claims, has identified the following Mechanical Engineering areas for follow up during later GDA steps:

- Adequacy and application of the RP's revised safety categorisation / classification methodology, relative to Mechanical Engineering SSC's, requires further demonstration. I will consider the methodology against SAPs ECS.1 – Safety Categorisation and ECS.2 – Safety Classification of SSC's and TAG NS-TAST-GD-094 - Categorisation of Safety Functions and Classification of Structures and Components (Ref. 17).

4.4.4 Conclusion – Categorisation of Safety functions and Classification of Structures, Systems and Components

107. Based on my high level Step 2 assessment of the RP's safety categorisation / classification methodology claims, I have concluded that further intervention will be required to confirm that the methodology, and its application (relevant to Mechanical Engineering SSC's) aligns with my expectations.

108. I consider the current claims against categorisation of safety functions and classification of structures, systems and components present a reasonable starting point for Step 2.

4.5 Out of Scope Items

109. There are no out of scoped items.

110. My Step 2 Mechanical Engineering assessment plan (Ref. 1) did not predict the absence of a specific PSR Mechanical Engineering chapter. Consequently, my Mechanical Engineering assessment of the safety case claims was limited to at a high level, i.e. not at a detailed Mechanical Engineering component level. This approach ensured that the Mechanical Engineering resource was targeted and proportionately focused.

111. The approach above does not invalidate the conclusions from my Step 2 assessment. During my GDA Step 3 assessment, I will follow-up the above as appropriate. I will capture this within my GDA Step 3 assessment plan.

4.6 Comparison with Standards, Guidance and Relevant Good Practice

112. In Section 2.2, above, I have listed the standards and criteria I have used during my Step 2 Mechanical Engineering GDA of the UK UKHPR1000 reactor, to judge the adequacy of the preliminary safety case. Based on these judgements, my overall conclusions can be summarised as follows:

- ONR Safety Assessment Principles: For Step 2, Table 1 details the level of compliance against the SAPs. This table identifies Mechanical Engineering areas to follow up during later GDA steps.
- ONR Technical Assessment Guides: This report identifies several Mechanical Engineering areas of interest that will require follow up during later GDA steps. These include consideration of the UK HPR1000:
  - a. Reactor cooling safety systems. [TAG NS-TAST-GD-003 (Ref. 17)].
  - b. Primary circuit insulation approach. [TAG NS-TAST-GD-004 (Ref. 17)].
  - c. ALARP justifications. [TAG NS-TAST-GD-005 (Ref. 17)].
  - d. Asset management arrangements. [TAG NS-TAST-GD-009 &098 (Ref. 17)].
  - e. Heating, ventilation, and air conditioning systems design. [TAG NS-TAST-GD-022 (Ref. 17)].
  - f. Diversity, redundancy, segregation and layout arrangements. [TAG NS-TAST-GD-036 (Ref. 17)].
  - g. Nuclear lifting arrangements. [TAG NS-TAST-GD-056 (Ref. 17)]
  - h. Design assurance arrangements. [TAG NS-TAST-GD-057 (Ref. 17)].
  - i. Safety categorisation / classification arrangements. [TAG NS-TAST-GD-094 (Ref. 17)].
- Other international standards, IAEA (Ref. 18) and WENRA (Ref 19), have been reflected through the consideration of ONR's SAPs and TAGs.

4.7 Interactions with Other Regulators

113. As part of my Step 2 assessment, I have worked with the Environment Agency under the ONR memorandum of understanding arrangement as an integral part of the assessment process. However, at this stage I have not identified any specific areas of Mechanical Engineering interest where formal detailed discussions have been considered necessary.

114. In accordance with its strategy, ONR work with overseas regulators, both bilateral and multinational. At this stage of my assessment, I have not identified any specific areas of Mechanical Engineering where detailed discussions have been considered necessary.

115. As part of my Step 3 assessment process, I shall continue to consider Mechanical Engineering specific topic areas that would benefit from undertaking detailed discussions with other regulators.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

116. During Step 2 of the GDA, the RP submitted a PSR and other supporting references. These documents outline a preliminary safety case for the UK HPR1000. This preliminary safety case present high-level safety case claims, in the area of Mechanical Engineering, which underpin the safety of the UK HPR1000. My assessment has been undertaken against the Relevant Good Practice expectations of ONR's SAPs (Ref. 11) and TAGs (Ref. 17) and other guidance (Ref. 18 to 20).

117. In conclusion:

- I have identified the following areas of good practice:
  - The RP's development of a list of sample Mechanical Engineering SSC's for later GDA.
  - The RP's identification of the main differences in design characteristics between its reference design (FCG.3) and the generic UK site envelope.
  - The RP's willingness to develop the UK HPR1000 generic safety case to align with UK expectation.
  - The RP's development of a technical risk register to manage gaps against UK RGP.
  - The RP's review of previous GDA's, SAPs, TAGs & ONR's Mechanical Engineering assessment strategy.
- I have identified the following Mechanical Engineering areas requiring follow up:
  - The full scope of UK HPR1000 Mechanical Engineering SSC's will need to be developed and agreed by ONR.
  - Adequacy of the UK HPR1000 generic safety case architecture relevant to Mechanical Engineering.
  - Full alignment of the Mechanical Engineering UK HPR1000 design with the generic site envelope.
  - The RP's proposals to link, through an engineering schedule, the safety analysis and the engineering SSC's.
  - The RP's management of gaps between the reference design and UK HPR1000 (including ALARP application).
  - The RP's design development approach for the UK HPR1000 (relevant to continuous improvement and ALARP application)
  - The RP's design assurance approach for Mechanical Engineering SSC's.
  - The RP's approach to safeguard the safety of the UK HPR1000 Mechanical Engineering assets through life (i.e. asset management).
  - Adequacy of the UK HPR1000 Mechanical Engineering codes, standards and regulations.

- Adequacy of the UK HPR1000 insulation approach for the Mechanical Engineering related primary circuit components.
- Adequacy of the UK HPR1000 heating, ventilation, and air conditioning systems design.
- Adequacy of the UK HPR1000 approach to undertake nuclear lifts.
- Adequacy and application of the RP's UK HPR1000 safety categorisation / classification methodology.

- My Step 2 assessment of the UK HPR1000 has supported my understanding of the technology to an appropriate level at this stage. My familiarisation will increase as GDA develops.
- I expect the level of Mechanical Engineering related claims, arguments and evidence to increase during later GDA steps

118. My Step 2 assessment has not identified any fundamental safety shortfalls that might prevent the issue of a Design Acceptance Confirmation (DAC) for the UK HPR1000 design.

5.2 Recommendations

119. My recommendations are as follows:

- Recommendation 1: ONR should consider the findings of my assessment in deciding whether to proceed to Step 3 GDA for the UK HPR1000.
- Recommendation 2: All the items identified in Step 2, as Mechanical Engineering areas requiring follow up, should be included in ONR's GDA Step 3 Mechanical Engineering Assessment Plan for the UK HPR1000.

6 REFERENCES

1. ONR Step 2 Assessment Plan for Mechanical Engineering, October 2017, TRIM 2017/351574.

2. UK HPR1000 GDA Project Preliminary Safety Report HPR/GDA/PSR/001 Chapters 1 to 27, GNS, October 2017, TRIM 2018/14773.

3. Generic Design Assessment (GDA) for UK HPR1000 - Design Manual for Valve Selection, GNS, February 2018, TRIM 2018/41435.

4. Generic Design Assessment (GDA) for UK HPR1000 – Applicable Codes and Standards on Context of Mechanical Engineering, GNS, March 2018, TRIM 2018/110002.

5. Generic Design Assessment (GDA) for UK HPR1000 – Safety Case Strategy of Mechanical Engineering, GNS, May 2018, TRIM 2018/159750.

6. GDA Project Scope for UK HPR1000 GDA Project, GNS, May 2018, TRIM 2018/179809

7. Generic Design Assessment (GDA) for UK HPR1000 – Methodology of Safety categorisation and classification, GNS, June 2018, TRIM 2018/199731

8. GDA Project – ALARP and BAT Principles and Requirements for UK HPR1000 GDA, GNS, May 2018, TRIM 2018/181393

9. Generic Design Assessment (GDA) for UK HPR1000 – ALARP Methodology, GNS, May 2018, TRIM 2018/181415

10. UK HPR1000 Mechanical Engineering Assessment Strategy, GNS, November 2017, TRIM 2017/419457

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

12. Generic Design Assessment (GDA) for UK HPR1000 - Pre-Construction Safety Report, GNS, April 2018, TRIM 2018/127683

13. 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

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

15. ONR UK HPR1000 - Regulatory Query (RQ) Tracking Sheet - Reference for Step 2 Assessment Reports, TRIM 2018/315144:

    RQ-UKHPR1000-0001 – Gaps in Relevant Good Practice (Mechanical Engineering), TRIM 2017/452664

    RQ-UKHPR1000-0005 – Process and Instrumentation Diagram (P&ID) Notation, TRIM 2017/454596

    RQ-UKHPR1000-0010 – Mechanical Structures, Systems and Components Candidate List, TRIM 2018/14542

    RQ-UKHPR1000-0025 – Design, Mechanical Engineering Research (Continuous Improvement), TRIM 2018/31023

RQ-UKHPR1000-0066 – Design Process, Design Manual Valve Selection, TRIM 2018/103337

RQ-UKHPR1000-0075 – Design Process, Asset Management Arrangements, TRIM 2018/165773

RQ-UKHPR1000-0077 – Design Process, Mechanical Codes and Standards, TRIM 2018/155312

RQ-UKHPR1000-0101 – Follow up to RQ-UKHPR1000-0025 – Design Process, Mechanical Engineering Research (Continuous Improvement), TRIM 2018/199458

RO-UKHPR1000-0002 – Demonstration that the UK HPR1000 Design is Suitably Aligned with the Generic Site Envelope, TRIM 2018/43924.

16. ONR UK HPR1000 - Regulatory Observation (RO) Tracking Sheet - Reference for Step 2 Assessment Reports, TRIM 2018/315147:

    RO-UKHPR1000-0002 Demonstration that the UK HPR1000 Suitably Aligns with the Generic Site Envelope, TRIM 2018/43924

17. ONR Technical Assessment Guides

    http://www.onr.org.uk/operational/tech_asst_guides/index.htm

18. IAEA guidance

    http://www-ns.iaea.org/standards/

19. Western European Nuclear Regulators' Association

    http://www.wenra.org/publications/

20. Health and Safety Executive Guidance

    http://www.hse.gov.uk/pubns/hsc13.pdf

    http://www.hse.gov.uk/pubns/books/index-legal-ref.htm

21. ONR Summary of the Step 2 Assessment for the UK HPR1000, TRIM 2018/238474

22. UK HPR1000 Mechanical Action Tracker, CGN, TRIM 2018/234428

Table 1

Relevant Safety Assessment Principles Considered During the Assessment

SAP No and Title	Description	Interpretation	Comment*
SAPs ECS Series Engineering Principles: Safety Classification and Standards			
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.	Addressed in Sections 4.3 and 4.4 of this report. The RP has revised its safety categorisation / classification methodology to reflect UK expectations. Implementation and development of these safety categorisation / classification arrangements, relevant to Mechanical Engineering, will be the focus of regulatory scrutiny in later GDA steps. Hence, this SAP is partly demonstrated.
ECS.2 Engineering principles: safety classification and standards	Safety classification	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.	See ECS.1 Hence, this SAP is partly demonstrated.
ECS.3 Engineering principles: safety classification and standards	Codes and standards	Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate codes and standards.	Addressed in Sections 4.3 and 4.4 of this report. Whilst the RP has undertaken some work to identify specific UK HPR1000 Mechanical Engineering codes and standards further work is required Consideration of the Mechanical Engineering codes and standards will be the focus of regulatory scrutiny in later GDA steps. Hence, the SAP is partly demonstrated
SAPs SC Series The Regulatory Assessment of Safety Cases: Safety Cases			

SC.1 The regulatory assessment of safety cases	Safety case production process	The process for producing safety cases should be designed and operated commensurate with the hazard, using concepts applied to high reliability engineered systems.	Addressed in Sections 4.1 and 4.3 of this report The RP has developed a high level UK HPR1000 PCSR safety case strategy. Consideration of the scope and extent of Mechanical Engineering PCSR submissions (and its architecture) will be the focus of regulatory scrutiny in later GDA steps Hence, this SAP is partly demonstrated
SC.7 The regulatory assessment of safety cases	Safety case maintenance	A safety case should be actively maintained throughout each of the lifecycle stages, and reviewed regularly.	Addressed in Section 4.3 of this report The need for a modification procedure, for the UK HPR1000 design and its safety case, has been recognised. The development of the modification procedure, relevant to Mechanical Engineering, will be the focus of regulatory scrutiny in later GDA steps Hence, this SAP is not demonstrated.
SAPs EMT Series Engineering Principles: Maintenance, Inspection and Testing			
EMT.1 Maintenance inspection and testing	Identification of requirements	Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case.	Addressed in Section 4.3 of this report The need to ensure that the UK HPR1000 system design satisfies UK RGP (with respect to EMT) has been recognised (high level only). Consideration of the UK HPR1000 EMT arrangements, relative to Mechanical Engineering, will be the focus of regulatory scrutiny in later GDA steps Hence, this SAP is not demonstrated

EMT.2 Maintenance inspection and testing	Frequency	Structures, systems and components should receive regular and systematic examination, inspection, maintenance and testing as defined in the safety case.	See EMT.1 Hence, this SAP is not demonstrated
EMT.3 Maintenance inspection and testing	Type Testing	Structures, systems and components should be type tested before they are installed to conditions equal to, at least, the most onerous for which they are designed.	See EMT.1 Hence, this SAP is not demonstrated
EMT.4 Maintenance inspection and testing	Validation of equipment qualification	The continuing validity of equipment qualification of structures, systems and components should not be unacceptably degraded by any modification or by the carrying out of any maintenance, inspection or testing activity.	See EMT.1 Hence, this SAP is not demonstrated
EMT.5 Maintenance inspection and testing	Procedures	Commissioning and in-service inspection and test procedures should be adopted that ensure initial and continuing quality and reliability	See EMT.1 Hence, this SAP is not demonstrated
EMT.6 Maintenance inspection and testing	Reliability Claims	Provision should be made for testing, maintaining, monitoring and inspecting structures, systems and components (including portable equipment) in service or at intervals throughout their life, commensurate with the reliability required of each item.	See EMT.1 Hence, this SAP is not demonstrated
EMT.7 Maintenance inspection and testing	Functional Testing	In-service functional testing of structures, systems and components should prove the complete system and the safety function of each functional group.	See EMT.1 Hence, this SAP is not demonstrated
EMT.8 Maintenance inspection and testing	Continuing reliability following events	Structures, systems and components should be inspected and / or re-validated after any event that might have challenged their continuing reliability.	See EMT.1 Hence, this SAP is not demonstrated
SAPs ERC Series Engineering Principles Reactor Core			
ERC.1 Reactor core	Design and operation of reactors	The design and operation of the reactor should ensure the fundamental safety functions are delivered with an appropriate degree of confidence for permitted operating modes of the reactor.	Addressed in Section 4.3 of this report. The RP has outlined how its design arrangements to enable the Mechanical Engineering design of valves

			to satisfy their safety function and operational requirements. Further justification of the adequacy of the RP's design assurance approach is required. Hence, this SAP is partly demonstrated.
SAPs EDR Series Engineering Principles: Design for Reliability			
EDR.1 Design for reliability	Failure to safety	Due account should be taken of the need for structures, systems and components to be designed to be inherently safe, or to fail in a safe manner, and potential failure modes should be identified, using a formal analysis where appropriate.	Addressed in Section 4.3 of this report. Further ALARP justification, as to why the insulation approach for the UK HPR1000 plant components is appropriate, is required. Consideration of the RP's primary circuit component insulation approach, will be the focus of regulatory scrutiny in later GDA steps Hence, this SAP is not demonstrated
EDR.2 Design for reliability	Redundancy, diversity and segregation	Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components.	Addressed in Section 4.3 of this report The RP recognises that the diversity and redundancy / common cause failure of some systems may need to be modified during GDA. Adequacy of compliance against these SAPs will be informed as the fault schedule develops. Consideration of diversity and redundancy / common cause failure, relative to Mechanical Engineering, will be the focus of regulatory scrutiny in later GDA steps Hence, this SAP is not demonstrated.
EDR.3 Design for Reliability	Common cause failure (CCF) should be addressed explicitly where a structure, system or	Common cause failure (CCF) should be addressed explicitly where a structure, system or component	See EDR.2 Hence, this SAP is not demonstrated.

	component employs redundant or diverse components, measurements or actions to provide high reliability.	employs redundant or diverse components, measurements or actions to provide high reliability.	
SAPs EAD Series Engineering Principles: Ageing and Degradation			
EAD.1 Engineering principles: ageing and degradation	Safe working life	The safe working life of structures, systems and components that are important to safety should be evaluated and defined at the design stage.	Addressed in Section 4.3 of this report The RP has recognised the need to produce an engineering schedule that links the requirements of the safety case (i.e. Mechanical Engineering substantiation) with the engineering that provides it. The development of this engineering schedule will be the focus of regulatory scrutiny in later GDA steps Hence, this SAP is not demonstrated.
EAD.5 Engineering principles: ageing and degradation	Obsolescence	A process for reviewing the obsolescence of structures, systems and components important to safety should be in place.	See EAD.1 Hence, this SAP is not demonstrated.
SAPs EKP Series Engineering Principles: Key Principles			
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.	Addressed in Sections 4.3 of this report. The RP has partially demonstrated that the UK HPR1000 will be developed using adequate design processes. The adequacy of the UK HPR1000 design process will be the focus of regulatory scrutiny in later GDA steps. Hence, this SAP is partly demonstrated.
EKP.4	Safety Function	The safety function(s) to be delivered within the facility should be identified by a structured analysis.	Addressed in Sections 4.2 and 4.3 of this report.

			The RP has recognised the need to produce an engineering schedule that will need to identify the safety functions associated with the Mechanical Engineering equipment The development of this engineering schedule will be the focus of regulatory scrutiny in later GDA steps. Hence, this SAP is not demonstrated
SAPs ELO Series Engineering Series: Equipment Layout			
ELO.1 Engineering principles: layout	Access	The design and layout should facilitate access for necessary activities and minimise adverse interactions while not compromising security aspects.	Addressed in Section 4.2 of this report. The RP has demonstrated a reasonable understanding of asset management requirements for Mechanical Engineering SSC's, which includes the need to facilitate access and egress. Consideration of adequacy of layout provisions will be the focus of regulatory scrutiny in later GDA steps. Hence, this SAP is not demonstrated.
SAPS FA.4 Series Fault Analysis: Fault Tolerance			
FA.4 Fault analysis: general	Fault Tolerance	DBA should be carried out to provide a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safety measures.	Addressed in Section 4.2 of this report. The RP has recognised the need to produce an engineering schedule that links the requirements of the safety case (i.e. DBA to demonstrate fault tolerance) with the engineering that provides it. The development of this engineering schedule will be the focus of regulatory scrutiny in later GDA steps. Hence, this SAP is not demonstrated

SAPs ECV Series Engineering Principles: Containment and Ventilation			
ECV.10 Engineering principles: containment and ventilation: ventilation design	Ventilation system safety functions	The safety functions of the ventilation system should be clearly identified and the safety philosophy for the system in normal, fault and accident conditions should be defined.	Addressed in Sections 4.2 and 4.3 of this report. The RP has identified that the UK HPR1000 HVAC design may be impact by differences in site characteristics. A technical support contract will be placed to consider the adequacy of the UK HPR1000 HVAC design later GDA steps. Hence, the SAP is not demonstrated.
SAPs EHA Series Engineering principles: external and internal hazards			
EHA.9 Engineering principles: external and internal hazards	Earthquakes	The seismology and geology of the area around the site and the geology and hydrogeology of the site should be evaluated to derive a design basis earthquake (DBE).	Addressed in Section 4.2 of this report. The RP has identified differences in site characteristics between the reference plant and the UK HPR1000 site. The output of the RP's review of impacted mechanical SSC's will be the focus of regulatory scrutiny in later GDA steps. Hence, this SAP is not demonstrated

*Note – comments against SAP compliance are provided against a sample of UK HPR1000 Mechanical Engineering aspect considered.