Office for Nuclear Regulation

New Reactor Division – Generic Design Assessment

Step 2 Assessment of the Electrical Engineering of the UK HPR1000 Reactor

Assessment Report ONR-GDA-UKHPR1000-AR-18-002
Revision 0
October 2018

Published 10/18

For published documents, the electronic copy on the ONR website remains the most current publicly available version and copying or printing renders this document uncontrolled.

EXECUTIVE SUMMARY

This report presents the results of my Electrical Engineering assessment of the UK HPR1000 reactor design fundamentals 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 electrical engineering aspects within the UK HPR1000 Preliminary Safety Report (PSR), and a number of supporting references and supplementary documents submitted by the RP, focusing on design concepts and claims for nuclear safety.

The standards I have used to judge the adequacy of the RP's submissions in the area of electrical engineering have been ONR's Safety Assessment Principles (SAPs) and Technical Assessment Guides (TAGs). I have based my judgement of the claims primarily against the following SAPs: EDR, ELO, ECS, ESR and EKP. In assessing adequacy, I have been guided by the following TAGs: NS-TAST-GD-003, NS-TAST-GD-019 and NS-TAST-GD-094. I have also considered if the electrical system architecture is consistent with the International Atomic Energy Agency Specific Safety Guide SSG-34.

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

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

- The electrical systems are designed so that the safety of the power plant is assured through the continuity of electrical power supplies, regardless of the initiating event or fault.
- The electrical systems provide power to ensure that, in the event of a loss of offsite power, the reactor can be shut down and the facilities safely cooled.
- Redundant Class 1 electrical systems are provided, which are to be physically separated and independent.

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

- The RP has presented high level claims that set out the principles by which the electrical system should be designed; and
- The architecture of the electrical systems, with redundant divisions fed by multiple offsite and onsite power sources, should provide the basis of a design which should be capable of being demonstrated to meet international standards and ONR's expectations for redundancy and defence-in-depth.

During my GDA Step 2 assessment of the UK HPR1000 aspects of the safety case related to Electrical Engineering, I have identified the following areas that require follow-up during Step 3:

- The categorisation and classification of the electrical equipment to ensure the assigned Class is consistent with the safety function(s) that the equipment it supports;
- Requirements for diversity of the electrical equipment address any issues identified in the common cause failure (CCF) analysis of the architecture and equipment;

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

LIST OF ABBREVIATIONS

AC	Alternating Current
ALARP	As Low As Reasonably Practicable
BAT	Best Available Techniques
BMS	Business Management System
BS	British Standard
C&I	Control and Instrumentation
CCF	Common Cause Failure
CGN	China General Nuclear Power Corporation
DAC	Design Acceptance Confirmation
DC	Direct Current
DG	Diesel Generator
EA	Environment Agency
EDF	Électricité de France
EDG	Emergency Diesel Generator
EN	European Norm
FCG3	Fangchenggang Nuclear Power Plant Unit 3
GNI	General Nuclear International
GNS	Generic Nuclear System Ltd
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
LOOP	Loss of Offsite Power
MSQA	Management of Safety and Quality Assurance
NPP	Nuclear Power Plant
ONR	Office for Nuclear Regulation
OPEX	Operational Experience
PCSR	Pre-construction Safety Report
PSA	Probabilistic Safety Analysis
PSR	Preliminary Safety Report (includes security and environment)

RGP	Relevant Good Practice
RP	UK HPR1000 GDA Requesting Party
RQ	Regulatory Query
SAP	Safety Assessment Principle
SBO	Station Blackout
TAG	Technical Assessment Guide
TLACP	Total Loss of AC Power
TSC	Technical Support Contractor
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' (RP).

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, in accordance with the regulatory regime of Great Britain, of the reactor design fundamentals, including ONR's assessment 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 permitting the construction of a power station based on the design after completion of the overall GDA process.

4. My assessment has followed my GDA Step 2 Assessment Plan for Electrical Engineering (Ref. 1) prepared in October 2017 and shared with GNS to maximise openness and transparency.

5. This report presents the results of my Electrical Engineering assessment of the UK HPR1000 as presented in the UK HPR1000 Preliminary Safety Report (PSR) (Ref. 2) and its supporting documentation (Refs. 3-5).

2 ASSESSMENT STRATEGY

6. This section presents my strategy for the GDA Step 2 assessment of the Electrical Engineering aspects of the UK HPR1000. It also includes the scope of the assessment and the standards and criteria I have applied.

2.1 Scope of the Step 2 Electrical Engineering Assessment

7. The objective of my GDA Step 2 assessment was to assess relevant design concepts and claims made by the RP related to the Electrical Engineering. In particular, my assessment has focussed on the following:

- Electrical system architecture
- Categorisation of safety functions and classification of electrical systems
- Demonstration of ALARP as applied by the RP to the design of electrical systems

8. During GDA Step 2 I have also evaluated whether the safety claims related to Electrical Engineering are supported by a body of technical documentation sufficient to allow me to proceed with GDA work beyond Step 2.

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

- Reviewed the RPs GDA scope in relation to Electrical Engineering
- Discussed with the RP their intentions regarding submissions for Step 3

2.2 Standards and Criteria

10. 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. 6).

11. In addition, the Safety Assessment Principles (SAPs) (Ref. 7) 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 (Ref. 7) are aligned with the International Atomic Energy Agency (IAEA) standards and guidance.

12. 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.

13. The relevant SAPs, IAEA standards and WENRA reference levels are embodied and expanded on in the Technical Assessment Guides (TAGs) on Essential Services. This guide provides the principal means for assessing the Electrical Engineering aspects in practice.

2.2.1 Safety Assessment Principles

14. The key SAPs (Ref. 7) applied within my assessment are SAPs EDR.2, EDR.3, EDR.4, ELO.1, EKP.3, EKP.5, EES.8 and ESR.7 (see Table 1 for full details of all SAPs considered).

2.2.2 Technical Assessment Guides

15. The following Technical Assessment Guides have been used as part of this assessment (Ref. 8):

- NS-TAST-GD-003 – Safety Systems
- NS-TAST-GD-019 – Essential Services
- NS-TAST-GD-094 – Categorisation of Safety Functions and Classification of Structures and Components

2.2.3 National and International Standards and Guidance

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

- Relevant IAEA standards (Ref. 9)
  - SSR-2/1 Rev.1 – Specific Safety Requirements ~ Safety of Nuclear Power Plants: Design
  - SSG-30: Safety Classification of Structures, Systems and Components in Nuclear Power Plants
  - SSG-34: Design of Electrical Power Systems for Nuclear Power Plants
- WENRA references (Ref. 10)
  - Reactor Safety Reference Levels (January 2008)
  - Safety Objectives for New Power Reactors (December 2009)
  - Statement on Safety Objectives for New Nuclear Power Plants (November 2010)
  - Statement on Safety Objectives for New Nuclear Power Plants (March 2013)
  - Safety of New NPP Designs (March 2013)
- Other national standards (Ref. 11 and 12)
  - BS EN 61226:2010 - Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions
  - BS IEC 62855:2016 - Nuclear power plants - Electrical power systems - Analysis

2.3 Use of Technical Support Contractors

17. During Step 2, I have not engaged Technical Support Contractors (TSCs) to support my assessment of the Electrical Engineering for the UK HPR1000.

2.4 Integration with Other Assessment Topics

18. Early in GDA, I recognised the importance of working closely with other inspectors (including Environment Agency's inspectors) as part of the Electrical Engineering assessment process. Similarly, other inspectors sought input from my assessment of the Electrical Engineering 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 Electrical Engineering and other

technical areas, with the understanding that this position will evolve throughout the UK HPR1000 GDA.

19. The key interactions I have identified are:

- The fault schedule will identify those systems that will deliver the safety functions during normal operations and fault conditions. This will inform the architecture and load allocation aspects of the Electrical Engineering assessment. Interactions with the RP on the development of the fault schedule have commenced during GDA Step 2 and are being led by a Fault Studies Inspector.
- The Probabilistic Safety Analysis (PSA) provides input to the architecture aspects of the Electrical Engineering assessment. This interaction has commenced during GDA Step 2 and is being led by a PSA Inspector.
- Due to the requirement for the electrical system to provide power to the various Control and Instrumentation (C&I) systems and the use of C&I systems to support the operation of the electrical systems, there is close interaction between my assessment and that of the C&I Inspector. This interaction commenced during GDA Step 2.
- Ensuring that the design reduces risks so far is reasonably practicable and appropriately categorises safety functions are topics which span many technical disciplines. To ensure the RPs approach is consistent across all disciplines, interactions on this are being led by a GDA Project Technical Inspector. There is close interactions between my assessment and theirs and this interaction has commenced in GDA Step 2.

20. In addition to the above, during GDA Step 2 there have been interactions between other technical assessment areas and myself, including mechanical engineering, management for safety and quality assurance (MSQA), internal hazards, external hazards and human factors. Although these interactions have been of an informal nature, they are essential to ensure ONR maintains a consistent assessment approach and the RP's approach to safety is also consistent. Such informal interactions are expected to continue through Steps 3 and 4.

3 REQUESTING PARTY'S SAFETY CASE

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

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

22. The aspects covered by the UK HPR1000 preliminary safety case in the area of Electrical Engineering can be broadly grouped under four headings which can be summarised as follows:

- Alternating Current (AC) power system architecture: The AC power system is designed so that the safety of the reactor facilities can be assured by ensuring continuity of electrical power supplies, regardless of transient disturbances and faults during operation.
- Direct Current (DC) power system architecture: The DC power system is designed so that the safety of the reactor facilities can be assured by ensuring continuity of electrical power supplies, regardless of transient disturbances and faults during operation.
- Lighting and communications: The lighting system is designed to give necessary illumination during plant operation, maintenance, test conditions and emergency conditions. The communication systems are designed to communicate within the plant and to external organisations during normal operations and emergency conditions.
- Categorisation of safety functions and classification of systems, structures and components: The categorisation and classification of the electrical system is designed to be consistent with the requirements and configuration of the plant systems, structures and components to which the electrical power is applied.

3.2 Basis of Assessment: RP's Documentation

23. The RP's documentation that has formed the basis for my GDA Step 2 assessment of the safety claims related to the Electrical Engineering aspects of the UK HPR1000 is:

- UK HPR1000 PSR Chapter 9 on Electric Power (Ref. 2): This document describes the intended electrical system architecture of the UK HPR1000, including the offsite power system connections, on-site AC and DC power distribution systems. It also describes the roles of the standby AC power sources, alternate AC power sources and battery systems in support of facility safety systems.
- UK HPR1000 PSR Chapter 4 on General Safety and Design Principles (Ref. 2): This document describes a summary of the overarching design process that the RP will follow to ensure a consistent and robust design.
- Unified Technical Regulation for Electrical Design (Ref. 3): This document sets out the basic technical requirements for the design of the electrical system and equipment of the HPR1000 nuclear power plant at Fangchanggang Nuclear Power Plant Unit 3 (FCG3).
- Nuclear Island Cable Routing Guidelines (Ref. 4): This document sets out the basic cabling principles adopted by CGN for the HPR1000 at FCG3, including the separation design principles between different trains and voltage levels.
- Methodology of Safety Categorisation and Classification (Ref. 5): This document aims to identify the categorisation and classification principles, why

the principles are suitable for the UK context and to provide a high level overview of the application of the categorisation and classification.

- Scope for UK HPR1000 GDA Report (Ref. 13): This document describes the proposed technical scope for the UK HPR1000 GDA project, including generic site layout, buildings, plant systems, components and level of detail and analysis that it is intended to provide in future steps.
- Responses to Regulatory Queries (Ref. 14)

4 ONR ASSESSMENT

24. This assessment has been carried out in accordance with HOW2 guide NS-PER-GD-014, “Purpose and Scope of Permissioning” (Ref. 6).

25. My Step 2 assessment has involved regular engagement with the RP’s Electrical Engineering specialists. This has included one Technical Exchange Workshop in China and seven progress meetings held in the UK.

26. 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. 15), these lead to Regulatory Queries (RQs) being issued. At the time of writing my assessment report, during Step 2, I have raised fourteen RQs (Ref. 14) to facilitate my assessment.

27. In addition, I have considered a response from the RP to RQ-UKHPR1000-0095 (Ref. 14) that was raised by an ONR Fault Studies Inspector concerning the approach to analysing common cause failures.

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

4.1 AC Power System Architecture

4.1.1 Assessment

29. I have assessed the UK HPR1000 AC power system architecture based on the information provided in the PSR (Ref. 2), responses to the RQs (Ref. 14) and supported by discussions with the RP during the workshop and progress meetings.

30. My main focus at this stage of the assessment has been:

- connection of off-site power supplies;
- on-site power sources;
- divisional segregation of the AC systems;
- application of categorisation and classification principles to the electrical systems;
- resilience to common cause failure; and
- effects of operating modes on the system.

31. I have used SAPs EKP.3 (Defence in depth), EKP.5 (Safety measures), EDR.2 (Redundancy, diversity and segregation), EDR.3 (Common cause failure), EDR.4 (Single failure criterion) and ESS.8 (Automatic initiation) as the basis of my assessment. The Safety Systems and Essential Services TAGs (Ref. 8) along with the IAEA Safety Standard SSG-34 (Ref. 9) have been used to support my judgements.

32. The high level claims made by the RP are that the electrical power systems shall be designed to assure that no design basis events cause a loss of electric power to engineered safety functions or to equipment that could result in a reactor transient capable of causing significant damage to the fuel cladding or reactor pressure boundary. It is also stated that the safety equipment is required to meet the single failure criterion and that the redundancy level of the emergency distribution system shall match the required redundancy level of the safety equipment.

33. Whilst the claims presented in the Chapter 9 of the PSR (Ref. 2) for Electrical Engineering are at a high level at this stage, I consider this is sufficient. As the depth of my assessment increases in subsequent GDA steps, I would expect more specific claims and arguments to be presented, each ultimately supported by evidence demonstrating compliance with the argument. In my discussions, the RP has recognised this and advised it intends to develop a specific claims, arguments and evidence structure for the PCSR.

34. I consider that the AC power system architecture of the UK HPR1000 is consistent with that identified in IAEA Specific Safety Guide SSG-34 (Ref. 9) reflecting two offsite grid connections supplying the main electrical switchboards, each to be as independent as practicable. The safety power supply system consists of three independent electrical trains, each backed up by an Emergency Diesel Generator (EDG), which is consistent with the three loop architecture of the main Nuclear Steam Supply System. Whilst I consider that such an approach will meet the single failure criterion, it does preclude undertaking maintenance at power; something recognised by the RP. I will consider in GDA Step 3 how the RP proposes to ensure that constraining maintenance to refuelling outages does not increase the risk maintenance induced CCF.

35. The RP states that during normal operation no interconnections exist for maintenance at power. I consider this a positive action which ensures the systems maintain independence. During later stages I shall review any approach to their intended use during maintenance periods to seek assurance they are only used when the risks of a resulting multi-train failure are reduced so far as is reasonably practicable.

36. I was concerned about the diversity of the EDG and Station Blackout (SBO) DG systems, which are both based on 10kV systems. Whilst the RP has identified that the two diesel generator systems were diverse being of different manufacturers, different capacities and sited in different locations, it had not undertaken a full CCF analysis for the complete architecture. However, in its own gap analysis for UK HPR1000, the RP has identified that it needs to complete a CCF analysis considering both individual component and system architecture, including design, operation and maintenance aspects across the whole electrical system. I will review the outcome of this analysis during Step 3, including how any application of equipment diversity is used to address any shortfalls.

37. During my assessment, I was concerned that the analysis by the RP may not have adequately considered the effect of electrical system disturbances on the ability of the safety power supply system to assure supplies. In response to an RQ, the RP confirmed such analyses have been undertaken for FCG3. Whilst they consider these to be aligned with the expectations of BS IEC 62855:2016 (Ref. 12), it confirmed in Reference 13 that it intends to either show these studies are aligned or has undertaken additional modelling in alignment with the guidance of this standard. I will review the outcome of these studies during Step 4.

4.1.2 Strengths

38. I have identified the following areas of strength in the AC Power System:

- The AC power system architecture follows the guidance given in the IAEA Specific Safety Standard SSG-34 (Ref. 9). The nuclear power plant is connected to the offsite power system through two connections, which are to be as independent as practicable.
- During power operation, the three Class 1 divisions operate independently.
- A Class 1 EDG is fitted to each of the three Class 1 divisions; any one of which it is claimed can support the necessary safety functions in the event of a loss of offsite power and main generator.

- SBO DGs are installed on two divisions to provide power to the necessary safety functions following the loss of offsite power, the main generator and all EDGs.

4.1.3 Items that Require Follow-up

39. During my GDA Step 2 assessment of AC Power System Architecture I have identified the following potential shortfalls that I will follow-up during Step 3:

- I expect the RP to ensure the electrical systems are resilient to common cause failures (CCF). In particular, I am concerned that the common voltage level of the EDG supplied system and the SBO DG supplied system increases susceptibility to CCF. The RP recognises this and has identified work to undertake a CCF analysis of the complete electrical distribution system. I intend to carry out an assessment of this work during Step 3 and, where complete diversity is not achieved, I will seek design modifications, so far is reasonably practicable, to ensure the independence of levels of defence in depth is not compromised.

4.1.4 Conclusions

40. Based on the outcome of my Step 2 assessment of the AC power system architecture, I have concluded that the fundamental architecture is robust and consistent with ONR SAPs EKP.3, EKP.5, EDR.2, EDR.3, EDR.4, ESS.8 and IAEA Safety Guide SSG-34 (Ref. 9).

41. Given the common voltage level, I have concerns that the RP may not be able to demonstrate that the equipment associated with the EDG and SBO DG systems is diverse. I have discussed this issue with the RP and they have recognised the need to demonstrate this, not only for the EDG and SBO DG switchboards but the complete electrical distribution system, and are seeking to present their findings and preliminary options at the start of Step 3.

42. During Step 3, I will carry out further assessment of the AC power system architecture.

4.2 DC Power System Architecture

4.2.1 Assessment

43. I have assessed the UK HPR1000 DC power system architecture based on the information provided in the PSR (Ref. 2), responses to the RQs (Ref. 14) and supported by discussions with the RP during the workshop and progress meetings.

44. My main focus at this stage of the assessment has been:

- battery autonomy times;
- divisional segregation of the DC systems;
- resilience to Loss of Offsite Power (LOOP) and SBO situations;
- ability to support Reactor Protection System;
- application of categorisation and classification principles to the electrical systems;
- resilience to common cause failure; and
- effect of operating modes on the system.

45. I have used SAPs EKP.3 (Defence in depth), EKP.5 (Safety measures), EDR.2 (Redundancy, diversity and segregation), EDR.3 (Common cause failure), EDR.4 (Single failure criterion) and ESS.8 (Automatic initiation) as the basis of my assessment. The Safety Systems and Essential Services TAGs (Ref. 8) along with the

IAEA Specific Safety Guide SSG-34 (Ref. 9) have been used to support my judgements.

46. The high level claims made by the RP on the DC power system architecture are naturally consistent with those for the AC power system architecture. It is stated that the specific purpose of the main battery system is to continuously provide power for two hours in a design basis accident and SBO situation to the required I&C systems, electrical distribution system control and valve actuators. In addition, it is stated that severe accident batteries are provided to supply power to support an extended SBO situation and ensure the integrity of containment and prevent radioactive release exceeding safety objectives. As with my assessment of the AC power system architecture, I expect the RP will have to further develop its claims, arguments and evidence structure during subsequent GDA steps.

47. I consider that the DC power system architecture of the UK HPR1000 is consistent with the architectural design principles of the IAEA Specific Safety Guide SSG-34 (Ref. 9) with three independent electrical trains, each with an associated two hour battery.

48. I identified that the RP proposes to introduce a fourth 2-hour battery backed DC power system to support the fourth channel of a C&I-based reactor protection system. I consider this is a reasonable approach which ensures that the expected level of independence is maintained between the four channels. Noting that this battery has a very specific function, I will assess whether the sizing of this system is appropriate for the loads that it needs to support and the duration that it needs to support them.

49. The RP states that the design has two severe accident batteries aligned with the SBO DGs. I consider this reasonable, although I was concerned that the autonomy time of these batteries is limited to 12 hours. I do not consider this is consistent with international good practice following the Fukushima accident or previous GDAs. I, however, noted that the RP in its own gap analysis has identified the need to review this duration, and will review the outcome of this analysis alongside the functions required of the system with a Severe Accident inspector during Step 3.

50. Noting that the RP intends to complete a component and system architecture CCF analysis, I will review the outcome of this analysis to ensure that it includes the DC systems, including uninterruptible power supplies (UPSs) and batteries.

4.2.2 Strengths

51. I have identified the following areas of strength in the DC Power System:

- The DC power system architecture provides three independent divisions;
- The RP proposes to introduce a fourth independent DC supply to support a four channel reactor protection system; and
- The autonomy time of the main DC batteries are consistent with international practice.

4.2.3 Items that Require Follow-up

52. During my GDA Step 2 assessment of DC power system architecture I have identified the following potential shortfalls that I will follow-up during Step 3:

- As with the AC power system, I expect the RP to demonstrate that the effects of CCF have been adequately considered and where appropriate, I will seek design modifications to ensure that sufficient resilience to CCF has been built into the design. As part of the work outlined in Section 4.1, above, the RP has recognised the need to undertake a common cause failure analysis of the full

electrical distribution system and I will undertake further assessment during Step 3.

4.2.4 Conclusions

53. Based on the outcome of my Step 2 assessment of the DC Power System Architecture, I have concluded that the fundamental architecture is robust and consistent with ONR SAPs EKP.3, EKP.5, EDR.2, EDR.3, EDR.4, ESS.8, and IAEA Specific Safety Guide SSG-34 (Ref. 9).

54. During Step 3, I will carry out further assessment of the DC power system architecture.

4.3 Lighting and Communications

4.3.1 Assessment

55. I assessed the lighting and communications based on the description in the PSR together with the supporting documentation.

56. The principal consideration at this time was to ensure that the RP recognised the importance of these systems to support operator action during normal operation and accident conditions,

57. Whilst Chapter 9 of the PSR (Ref. 2) did not include reference to these systems, the Scope for UK HPR1000 GDA Project (Ref. 13) has confirmed that both of these systems are considered within scope.

58. The Unified Technical Regulations (Ref. 3) sets out principles for the design of lighting systems. This states that, in accordance with IAEA Safety Requirement SSR-2/1 (Ref. 9), the lighting system should provide adequate lighting for all operating areas of the plant under normal and accident conditions, in addition to supporting emergency evacuation. Reference 3 states that whilst the normal lighting system is powered by the offsite supplied AC power system, those systems for emergency lighting are diesel generator backed, whilst safety or evacuation lighting is battery backed. I consider this approach should meet the expectations of ONR SAP ELO.1 and will review in Step 3 that the design provides the necessary lighting for operator action, both in the main control room and at any plant equipment.

59. I raised RQ-UKHPR1000-0131 (Ref. 14) to establish the principles for the design of the communication systems. The response (Ref. 14) to this stated that the high level aim is to provide suitable and diverse means of communication within the nuclear power plant for use during all modes of normal operation and after all postulated initiating events and in accident conditions. It states that communication provision includes a normal and secondary telephone system, public address system and alarm systems. I consider that at a high level this meets the expectations of ONR SAP ESR.7. During Step 3, I will work with an ONR C&I inspector to assess the resilience of these systems to accident conditions and ensure that their reliability is consistent with any claims made on operator action, and that their power supply is consistent with this duty.

4.3.2 Strengths

60. From an initial assessment of Unified Technical Regulations (Ref. 3) and the response to the RQ (Ref. 14), I have identified the following areas of strength:

- The plant lighting is divided into normal and emergency systems; the latter including standby, safety and emergency escape lighting;
- The emergency lighting systems are backed by the emergency electrical distribution systems;

- The escape lighting systems are locally battery backed; and
- The communication systems claim to provide a defence in depth approach to support the response to accident scenarios

4.3.3 Items that Require Follow-up

61. During Step 3, I intend to follow-up on the following potential shortcomings:

- I will expect the RP to demonstrate how the lighting systems respond to the progressive loss of electrical systems to ensure that operator response identified in the Safety Analysis is not adversely compromised by a Loss of Offsite Power (LOOP), SBO or Total Loss of AC Power (TLACP) scenario; and
- Demonstrate that the design of the communication systems provides the claimed levels of defence in depth.

4.3.4 Conclusions

62. Based on the outcome of my Step 2 assessment of the lighting and communication systems, I have concluded that the fundamental architecture appears to be robust.

63. During Step 3, I will carry out further assessment to ensure that the design meets the expectations of the systems. I will liaise with other ONR GDA Inspectors to ensure these systems provide appropriate capability in the various design basis and design extension conditions.

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

4.4.1 Assessment

64. I have assessed the approach to Categorisation and Classification for UK HPR1000 (Ref. 7) in the context of Electrical Engineering. Since electrical systems do not typically directly provide safety functions, but rather provide electrical power to equipment that does, I consider that any Categorisation and Classification process should reflect this.

65. I have used SAPs ECS.1 (Safety categorisation), ECS.2 (Safety classification of structures, systems and components) as the basis of my assessment. The Categorisation and Classification TAG (Ref. 8) has been used to support my judgements together with BS IEC 61226:2010 (Ref. 11).

66. The RP has identified that its initial classification of electrical equipment is based on that adopted for FCG3. I also note that the RP intends to undertake a re-assessment of the classification of the electrical equipment following the issue of its methodology (Ref. 5). I have considered if the classification of the AC and DC Power Systems are consistent with the roles that the systems will perform in response to a LOOP, SBO or TLACP scenario.

67. In general, I am content that the approach identified in Reference 5 recognises the expectation of the Categorisation and Classification TAG, in that support systems should reflect the classification of the systems that they support. I am content that the approach recognises the application of BS IEC 61226:2010 (Ref. 11) to the process for C&I equipment. I am also satisfied that their approach to the isolation between equipment of two different classifications through the use of a higher classification isolation device is consistent with the expectations of SAP ECS.2.

68. I note that based on the FCG3 classification process, the SBO DG and severe accident batteries are Class 3. Whilst I would have anticipated that these would be

Class 2, I recognise that the RP has committed to undertaking a review of the electrical equipment classification in line with its GDA specific methodology (Ref. 5). I will assess how that review considers the classification of these systems, and if necessary engage further with the RP.

69. My assessment has informed the ONR cross-cutting assessment of Categorisation and Classification (Ref. 16), led by a Fault Studies inspector.

4.4.2 Strengths

70. From an initial assessment of the Chapter 4 of the PSR (Ref. 2) and the Categorisation and Classification methodology (Refs. 2 and 5), I have identified the following areas of strength in the approach:

- The methodology recognises that the Categorisation and Classification of support systems should align with that of the systems they support;
- The methodology for safety categorisation and classification of the electrical distribution system is generally consistent with UK practice; and
- Where loads are connected to higher classification switchboards, the classification of the isolation devices is consistent with that of the switchboard.

4.4.3 Items that Require Follow-up

71. During Step 3, I expect the RP to demonstrate that the Categorisation and Classification of the electrical equipment for the UK HPR1000 is in line with relevant SAPs (Ref.7), taking due cognisance of the expectations of BS EN 61226:2010 (Ref. 11) for the classification of C&I systems and appropriately classifies electrical systems to align with the classification of main and diverse lines of protection that they support.

4.4.4 Conclusions

72. Based on the outcome of my Step 2 assessment, I have concluded that the fundamental methodology developed for Categorisation and Classification of the electrical equipment appears to be reasonable.

73. During Step 3, I will carry out further assessment to ensure that the classification of the electrical equipment is consistent with the functions that they support.

4.5 ALARP Considerations

74. Given that design substantiation is still in the early stages of GDA, the RP has not yet completed any CCF or diversity analysis and therefore presented any options to improve their design and demonstrated their application of ALARP in my area. I will follow this up in Step 3. This work has informed the project summary report (Ref. 17).

4.6 Out of Scope Items

75. This assessment has focussed on the proposed electrical architecture. Since the purpose of Step 2 is focussed on the presentation and assessment of key claims to enable the identification of any fundamental safety shortfall, there is little information provided in the PSR or its supporting documents on specific electrical equipment design or qualification requirements resulting from fault analysis. These aspects will be considered during later Steps of my GDA assessment.

4.7 Comparison with Standards, Guidance and Relevant Good Practice

76. In Section 2.2, above, I have listed the standards and criteria I have used during my GDA Step 2 assessment of the UK HPR1000 Electrical Engineering, to judge the

adequacy of the preliminary safety case. In this regard, my overall conclusions can be summarised as follows:

- ONR SAPs: I have reviewed the design of the electrical systems against the the following SAPS: EDR.2; EDR.3; EDR.4; ELO.1; EKP.3; EKP.5; and EES.8. I am satisfied that at this stage of the GDA there are no fundamental discrepancies between the design and the SAPs, and where gaps do exist the RP has identified these and have a plan to analyse and address these.
- ONR TAGs: I have reviewed the design of the electrical systems against the TAGs identified in Section 2.2.2. I am content that the design proposed in Step 2 is generally compliant with these TAGs.
- IAEA Safety Standard SSR-2/1 and SSG-34 (Ref. 9): I have reviewed the design of the electrical system against SSG-34 and the electrical system aspects of SSR-2/1 and am generally content that the architecture appears aligned with these standards.

77. I have also considered ONR SAP ECS.3 (Codes and Standards) as the basis of my assessment. The expectation of the SAP is that the codes and standards used should be commensurate with the safety classification of the respective systems, structure and component. The RP has stated in Chapter 9 of the PSR (Ref. 2) that FCG3 is based on Chinese code and standards, which are generally derived from international IEC or American IEEE standards. I consider that this approach supports a principle for achieving high reliability, although the precise nature of any differences between the original are not clear nor the consequences.

78. The RP states in PSR Chapter 9 that it intends to adopt IEC codes and standards as a basis, using other standards where no suitable IEC equivalent exists, providing further justification to support its adequacy. I consider this consistent with the high level expectations of the SAP. As further information is provided in subsequent GDA Steps to justify how the design of the electrical systems and equipment of the UK HPR1000 conforms to relevant IEC codes and standards, I will review how this reflected in the evidence to the safety case and ensure that it is applying appropriate high integrity standards in its application of this approach.

4.8 Interactions with Other Regulators

79. There have been no interactions with other regulators during my Step 2 assessment.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

80. 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. I consider that the PSR together with its supporting references presents the high level claims in the area of Electrical Engineering that underpin the safety of the UK HPR1000.

81. During Step 2 of GDA I have targeted my assessment at the content of the PSR and its references that are of most relevance to the area of Electrical Engineering; against the expectations of ONR's SAPs and TAGs and other guidance which ONR regards as relevant good practice. From my Step 2 assessment of the UK HPR1000, I conclude the following:

- There is the potential for shortfalls in the resilience of the design to common cause failure, which the RP is currently assessing, and I will assess during Step 3.
- Based on my discussions with the RP, I am satisfied with the proposed GDA scope of the UK HPR1000 and the initial intentions for submissions for Steps 3 and 4.

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

5.2 Recommendations

83. 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 Electrical Engineering Assessment Plan for the UK HPR1000.

6 REFERENCES

1. *Generic Design Assessment of GNS UK HPR1000 Reactor - Step 2 Assessment Plan for Electrical Engineering*, ONR-GDA-UKHPR1000-AP-17-002 Revision 0, ONR, October 2017. TRIM Ref. 2017/352679

2. UK HPR1000 GDA Preliminary Safety Report

   Chapter 4 – General Safety and Design Principles, HPR-GDA-PSR-0004 Revision 000, GNS, October 2017. TRIM Ref. 2017/401351

   Chapter 9 – Electric Power, HPR-GDA-PSR-0009 Revision 000, GNS, October 2017. TRIM Ref. 2017/401359

3. *Unified Technical Regulation for Electrical Design*, GH-0-00500-001-DEDQ-03-GN Rev. B, CGN, March 2018. TRIM Ref. 2018/121142

4. *NI Cable Routing Guidelines*, NE15BW-X-DQ-0000-000138 Rev. A, CGN, January 2018. TRIM Ref. 2018/108061

5. *Methodology of Safety Categorisation and Classification*, GH-X-00100-062-DOZJ-03-GN Rev. B, CGN, June 2018. TRIM Ref. 2018/199731

6. *Purpose and Scope of Permissioning*, NS-PER-GD-014 Revision 6, ONR, July 2014. http://www.onr.org.uk/operational/assessment/index.htm

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

8. Technical Assessment Guides
   http://www.onr.org.uk/operational/tech_asst_guides/index.htm

   Safety Systems, NS-TAST-GD-003 Revision 8, ONR, March 2018

   Essential Services, NS-TAST-GD-019 Revision 3, ONR, July 2016

   Categorisation of Safety Functions and Classification of Structures, Systems and Components, NS-TAST-GD-094 Revision 0, ONR, November 2015

9. IAEA Standards and Guidance www.iaea.org

   Specific Safety Requirements ~ Safety of Nuclear Power Plants: Design, SSR-2/1 (Rev.1), February 2016
   Specific Safety Guide ~ Safety Classification of Structures, Systems and Components in Nuclear Power Plants, SSG-30, IAEA, May 2014
   Specific Safety Guide ~ Design of Electrical Power Systems for Nuclear Power Plants, SSG-34, IAEA, March 2016

10. Western European Nuclear Regulators' Association www.wenra.org

    Reactor Safety Reference Levels, WENRA, January 2008
    Safety Objectives for New Power Reactors, WENRA, December 2009
    Statement on Safety Objectives for New Nuclear Power Plants, WENRA, November 2010
    Statement on Safety Objectives for New Nuclear Power Plants, WENRA, March 2013
    Safety of New NPP Designs, WENRA, March 2013

11. *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*, BS EN 61226:2010, British Standards Institution

12. *Nuclear power plants – Electrical power systems – Analysis*, BS IEC 62855:2016, British Standards Institution

13. *Scope for UK HPR1000 GDA Project*, HPR/GDA/REPO/0007 Rev. 000, GNS, May 2018. TRIM Ref. 2018/179809

14. *GNS UK HPR1000 - Schedule of Regulatory Queries raised during Step 2*, ONR. TRIM Ref. 2018/315144

15. *New nuclear reactors: Generic Design Assessment - Guidance to Requesting Parties*, ONR-GDA-GD-001 Revision 3, ONR, September 2016 http://www.onr.org.uk/new-reactors/guidance-assessment.htm

16. *Step 2 Assessment of the Fault Studies of UK HPR1000 Reactor*, ONR-GDA-UKHPR1000-AR-18-010 Rev. 0, ONR. TRIM Ref. 2018/237156

17. *Summary of the Step 2 Assessment of the UK HPR1000 Reactor*, ONR-GDA-UKHPR1000-AR-18-007 Rev. 0, ONR. TRIM Ref. 2018/238474

Table 1

Relevant Safety Assessment Principles Considered During the Assessment

SAP No and Title	Description	Interpretation	Comment
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.	The submissions of the RP recognise that the architecture and claims on the electrical systems should provide appropriate levels of defence in depth to the safety of the power plant.
EKP.5	**Engineering Principles: Key Principles - Safety Measures**	Safety measures should be identified to deliver the required safety function(s).	The approach taken to identification of fault sequences forms the basis to identify the safety functions, which then align with the required support systems.
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.	The submissions of the RP recognise the requirement for equipment to be designed and qualified for the operating conditions, including accident conditions, that it may be required to operate in.
ERL.3	**Engineering principles: reliability claims – Engineered Safety Measures**	Where reliable and rapid protective action is required, automatically initiated, engineered safety measures should be provided.	The submissions of the RP recognise that where rapid response to an event is required, the electrical systems should provide an automatic, or uninterrupted response.
EMT.1	**Engineering principles: 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.	The submissions of the RP recognise that equipment design and the operating arrangements need to recognise the need to undertake inspection and maintenance.
EMT.3	**Engineering principles: 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.	The submissions of the RP recognise that equipment should be type tested under the conditions it will be required to operate under and that such tests should be in accordance with relevant international standards.

SAP No and Title	Description	Interpretation	Comment
EMT.7	**Engineering principles: 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.	The submissions of the RP recognise that equipment should be periodically tested, and that where practicable, this should be at a system level.
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.	The submissions of the RP recognise that the electrical systems should be designed to achieve at least the required reliability.
EDR.3	**Engineering principles: design for reliability - Common cause failure**	Common cause failure (CCF) should be addressed explicitly where a structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability.	The submissions of the RP recognise that the design should be tolerant to common cause failure.
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.	The submissions of the RP recognise that the design of systems to support a Category A function should meet the single failure criterion.
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.	The submissions of the RP recognise that the categorisation of functions should be based on a hierarchical structure based on the role it plays in ensuring nuclear safety.
ECS.2	**Engineering principles: safety classification and standards - Safety classification of structures, systems and components**	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.	The submissions of the RP recognise that the classification of systems, structures and components should be linked to the categorisation scheme and that the classification of support systems should align with that of the systems they support.
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.	The submissions of the RP recognise that the codes and standards applied to electrical engineering equipment should reflect its reliability requirements and be commensurate with its safety classification reflecting, where available, nuclear specific codes and standards.

SAP No and Title	Description	Interpretation	Comment
ESS.2	**Engineering principles: safety systems - Safety system specification**	The extent of safety system provisions, their functions, levels of protection necessary to achieve defence in depth and reliability requirements should be specified.	The submissions of the RP recognise that the design of an electrical system needs to be commensurate with the requirements of the safety functions it supports.
ESS.8	**Engineering principles: safety systems - Automatic initiation**	For all fast acting faults (typically less than 30 minutes) safety systems should be initiated automatically and no human intervention should then be necessary to deliver the safety function(s).	The submissions of the RP recognise that where safety systems require timely action then the electrical systems that support those need similar response capabilities.
ESS.16	**Engineering principles: safety systems - No dependence on external sources of energy**	Where practicable, following a safety system action, maintaining a stable, safe state should not depend on an external source of energy.	The submissions of the RP recognise that electrical systems should not be dependent on an external source of energy for a sustained period.
ESS.23	**Engineering principles: safety Systems - Allowance for unavailability of equipment**	In determining the safety systems to be provided, allowance should be made for the potential unavailability of equipment.	The submissions of the RP recognise that the design of the electrical systems needs to recognise the potential unavailability due to maintenance or testing in determining its permitted operating states.
ESR.7	**Engineering principles: control and instrumentation of safety-related systems - Communications systems**	Adequate communications systems should be provided to enable information and instructions to be transmitted between locations on and, where necessary, off the site. The systems should provide robust means of communication during normal operations, fault conditions and severe accidents.	The submissions of the RP recognise that a robust communication is necessary to ensure communication between operators and for emergency evacuation.
EES.3	**Engineering principles: essential services - Capacity, duration, availability, resilience and reliability**	Each source should have the capacity, duration, availability, resilience and reliability to meet the maximum demands of its dependent systems.	The submissions of the RP recognise that each electrical power source needs to be sufficient for a sufficient time to allow the facility to be brought to a safe, stable state.
EES.7	**Engineering principles: essential services - Protection devices**	The protection devices provided for essential service components or systems should be consistent with the safe operation of the facility and limited to those justified as necessary in the safety case.	The submissions of the RP recognise that it may be appropriate to vary the protective arrangements of electrical systems during certain events.
EES.9	**Engineering principles: essential services -**	Essential services should be designed so that the simultaneous loss of both normal and	The submissions of the RP recognise that the loss of normal and backup electrical supplies should not

SAP No and Title	Description	Interpretation	Comment
	Simultaneous loss of service	back-up services will not lead to unacceptable consequences.	result in unacceptable consequences.
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.	The submissions of the RP recognise that lighting systems are required to facilitate operator action during normal operations and accident conditions and to facilitate emergency egress.