Office for Nuclear Regulation

New Reactor Division – Generic Design Assessment

Step 2 Assessment of the Fault Studies of UK HPR1000 Reactor

Assessment Report ONR-GDA-UKHPR1000-AR-18-010
Revision 0
October 2018

Published 10/18

EXECUTIVE SUMMARY

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

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

During GDA Step 2 my work has focused on the assessment of the Fault Studies 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.

The standards I have used to judge the adequacy of the RP's submissions in the area of Fault Studies have been primarily ONR's Safety Assessment Principles (SAPs), in particular SAPs FA.1 to FA.9 and ONR's Technical Assessment Guides NS-TAST-GD-034 (Transient analysis for DBAs in Nuclear Reactors) NS-TAST-GD-003 (Safety Systems) and NS-TAST-GD-094 (Categorisation of Safety Functions and Categorisation of Structures, Systems and Components).

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

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

- All initiating faults with the potential to lead to significant radiation exposure or release of radioactive material will be identified in the Fault Schedule;
- The design basis analysis (DBA) will provide a robust demonstration of the fault tolerance of the engineering design and effectiveness of the safety measures;
- The UK HPR1000 design will be developed in an evolutionary manner using robust design processes, building on relevant good international practice, to achieve a strong safety and environmental performance;
- Design Extension Conditions (DEC-A events) that have the potential to lead to severe accidents will be systematically analysed.

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

- The development of a logical method and auditable trail for the list of Postulated Initiating Events (PIEs) for UK HPR1000;
- The PSR considers operating conditions in all possible conditions from full power operation to cold shutdown;

- The RP claims to have undertaken transient analysis for UK HPR1000 reference plant (FCG3) with two sets of computer codes and that both demonstrate appropriate margins to relevant success criteria, in line with Chinese regulatory requirements;
- The RP appears to have a reasonable basis for the development of a safety case for Fuel Handling and Storage Operations;
- The RP intends to conduct deterministic analysis of DEC-A sequences but using more realistic assumptions than the conservative assumptions using in DBA, to show that the plant is tolerant without significant fault escalation and unacceptable consequences;
- The fault schedule template appears to be a sound basis for the RP to develop a suitable fault schedule which will contain the information expected by ONR's SAPs;
- The RP's approach to the categorisation of safety functions and classification of systems, structures and components is based upon guidance given in IAEA Safety Guide SSG-30, amended to recognise and address UK expectations.

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

- Fault identification for support systems;
- Spurious Control and Instrumentation systems actuation;
- The demonstration of diverse protection against frequent faults;
- Treatment of maintenance assumptions within the design basis;
- Development of appropriate acceptance criteria for the DBA for fuel handling and storage operations;
- Scope of the fuel handling and storage operations safety case and the interfaces with the proposed spent fuel interim storage solution;
- Fault identification for fuel handling and fuel storage, particularly with respect to the identification of worker exposure (on-site risks);
- The list of DEC-A sequences and confirmation that these have been assessed using appropriate methods. I will also consider the demonstration of the adequacy of the provisions made in the design to protect against these sequences;
- I intend to commission some independent confirmatory analysis of a sample of UK HPR1000 fault sequences. I will use the results of this analysis to inform my judgement on the adequacy of the RP's analysis codes and key assumptions;
- The validation and verification of the analysis codes that will be used in the UK HPR1000 safety case;
- The maturity of information within the fault schedule and links to supporting analysis within the safety case;
- The breakdown of safety functions to an appropriate level such that SSCs can be suitably classified;
- The application of the Categorisation and Classification methodology to the reactor systems and protective safety measures;
- The application of the Categorisation and Classification methodology to areas away from the primary or front line reactor systems, such as the supporting systems and fuel route and fuel handling equipment.

Overall, during my GDA Step 2 assessment, I have not identified any fundamental safety shortfalls in the area of Fault Studies 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
AOSs	Abnormal Operating States
ASP [SPHRS]	Secondary Passive Heat Removal System
BSL	Basic Safety Level (in SAPs)
BSO	Basic Safety Objective (in SAPs)
CCF	Common Cause Failures
CGN	China General Nuclear Power Corporation
DAC	Design Acceptance Confirmation
DAS	Diverse Actuation System
DBA	Design Basis Analysis
DBC	Design Basis Condition
DEC	Design Extension Condition
DEC-A	Design Extension Condition – A
DEC-B	Design Extension Condition – B
DNB	Departure from Nucleate Boiling
EA	Environment Agency
ECS [ECS]	Extra Cooling System
EDF	Électricité de France
FCG3	Fangchenggang Unit 3
FMEA	Failure Modes and Effects Analysis
GNI	General Nuclear International
GNS	General Nuclear System Ltd
EHR [CHRS]	Containment Heat Removal System
IAEA	International Atomic Energy Agency
C&I	Control and Instrumentation
JPO	(Regulators') Joint Programme Office

LOOP	Loss of Off Site Power
NNSA	National Nuclear Safety Administration (the Chinese Nuclear Regulator)
NPP	Nuclear Power Plant
ONR	Office for Nuclear Regulation
OECD NEA	Organisation for Economic Co-operation and Development Nuclear Energy Agency
PCSR	Pre-construction Safety Report
PIE	Postulated Initiating Event
PSA	Probabilistic Safety Assessment
PSR	Preliminary Safety Report (includes security and environment)
PTR [FPCTS]	Fuel Pool Cooling and Treatment System
RGP	Relevant Good Practice
RHWG	Reactor Harmonization Working Group (of WENRA)
RI	Regulatory Issue
RO	Regulatory Observation
ROA	Regulatory Observation Action
RP	Requesting Party
RPS	Reactor Protection System
RQ	Regulatory Query
SAP(s)	Safety Assessment Principle(s)
SBO	Station Black-Out
SFAIRP	So far as is reasonably practicable
SFIS	Spent Fuel Interim Storage
SSC	System, Structure and Components
TAG	Technical Assessment Guide(s)
TSC	Technical Support Contractor
TSF	Technical Support Framework
WENRA	Western European Nuclear Regulators' Association

TABLE OF CONTENTS

Tables

1 INTRODUCTION

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

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

3. Step 2 commenced in November 2017. Step 2 of GDA is an overview of the acceptability, in accordance with the regulatory regime of Great Britain, of the 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.

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

5. This report presents the results of my Fault Studies assessment of the UK HPR1000 as presented in the UK HPR1000 Preliminary Safety Report (PSR) Chapters 4, 12 and 13 (Ref. 2) and its supporting documentation (Refs 3, 4, 5, 6 and 7).

2 ASSESSMENT STRATEGY

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

2.1 Scope of the Step 2 Fault Studies Assessment

7. ONR's Safety Assessment Principles (SAPs, Ref. 8) (see Section 2.2) require the risks arising from nuclear facilities during fault conditions to be assessed using three techniques: design basis analysis (DBA), probabilistic safety analysis (PSA), and severe accident analysis (SAA). This GDA Step 2 Fault Studies assessment for the UK HPR1000 focuses on DBA, with the adequacy of the RP's PSA and SAA assessed elsewhere (Ref. 9).

8. The purpose of DBA is to provide a robust demonstration of the fault tolerance of a nuclear facility and the effectiveness of its safety measures. Its principal aims are to guide the engineering requirements of the design, including modifications, and to determine limits to safe operation, so that safety functions can be delivered reliably during all modes of operation and under reasonably foreseeable faults. In DBA, any uncertainties in the fault progression and consequence analyses are addressed by the use of appropriate conservatism.

9. In addition to the DBA, it is increasingly considered international Relevant Good Practice (RGP) to consider deterministically events outside of the traditional design basis, to show that the plant is tolerant to these events without significant fault escalation and unacceptable consequences. In light water reactors, the approach set out by the International Atomic Energy Agency (IAEA, Ref. 12) and Western European Nuclear Regulators' Association (WENRA, Ref. 13) is to divide such events, commonly known as Design Extension Conditions (DECs) into events with and without major fuel damage. For DEC-A, best-estimate analysis should be showing no, or very limited fuel damage, by crediting features included within the design.

10. My Fault Studies assessment of the safety claims has not been restricted to faults associated with the reactor operating at full power. The scope of this assessment includes all operating modes and operations of the reactor (including low power and shutdown operations) and fuel route operations (including the safe storage of spent fuel in the spent fuel pool, refuelling operations, the import and export of fuel into the spent fuel pool). The RP's safety case for the UK HPR1000 will eventually need to address faults across the whole facility which have the potential for radiological consequences (for example, the radiological waste treatment and storage systems) however this assessment of the high level claims has been targeted at the larger hazards contained within the reactor and the fuel route systems.

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

- Familiarisation with the HPR1000 design;
- The RP's approach to identifying all initiating faults with the potential to lead to significant radiation exposure or release of radioactive material;
- The methods and approaches to be used in DBA to provide a robust demonstration of the fault tolerance of the engineering design and effectiveness of the safety measures;
- The development of a safety case for fuel route operations, including the safe storage of spent fuel in the spent fuel pool, refuelling operation and the import and export of fuel into the spent fuel pool;

- The identification of Design Extension Condition (DEC) events.

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

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

- Discussed with the RP the scope and delivery of submissions likely to be required to support my Step 3 assessment; and
- Development of a strategy for using Technical Support Contracts (TSCs) for independent confirmatory analysis during later Steps.

2.2 Standards and Criteria

14. 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. 10).

15. In addition, the SAPs (Ref. 8) constitute the regulatory principles against which duty holders' and RP's safety cases are judged. Consequently the SAPs are the basis for ONR's nuclear safety assessment and have therefore been used for the GDA Step 2 assessment of the UK HPR1000. The SAPs 2014 Edition are aligned with the IAEA standards and guidance.

16. Furthermore, ONR is a member of WENRA. WENRA has developed Reference Levels, which represent good practices for existing nuclear power plants, and Safety Objectives for new reactors.

17. The relevant SAPs, IAEA standards and WENRA reference levels are embodied and expanded on in the Technical Assessment Guides (TAGs) (Ref. 11). These guides provide the principal means for assessing the Fault Studies aspects in practice.

2.2.1 Safety Assessment Principles

18. The key SAPs (Ref.8) applied within my assessment are SAPs FA.1 to FA.9 (see also Table 1 for further details).

2.2.2 Technical Assessment Guides

19. The following Technical Assessment Guides have been used as part of this assessment (Ref. 11):

- NS-TAST-GD-003 – Safety Systems
- NS-TAST-GD-034 – Transient analysis for DBAs in nuclear reactors.
- NS-TAST-GD-094 – Categorisation of Safety Functions and Classification of Structures, Systems and Components

2.2.3 National and International Standards and Guidance

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

- Relevant IAEA standards (Ref. 12)

- IAEA Safety Standards Series – Safety of Nuclear Power Plants: Design, Specific Safety Requirements (SSR) 2/1, IAEA 2012
- IAEA Safety Standards Series – General Safety Requirements (GSR) Part 4: Safety Assessment for Facilities and Activities IAEA 2016
- IAEA Safety Standards Series – Safety Classification of Structures, Systems and Components in Nuclear Power Plants Specific Safety Guide No SSG-30

- WENRA references (Ref. 13)

  - Western European Nuclear Regulators' Association. Reactor Safety Reference Levels WENRA January 2008
  - Reactor Harmonization Working Group Report on Safety of new NPP designs, August 2013
  - WENRA statement on safety objectives for new nuclear power plants, November 2010

2.3 Use of Technical Support Contractors

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

2.4 Integration with Other Assessment Topics

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

23. The key interactions I have identified are:

- Fuel and Core: this area provides input to the acceptance criteria chosen by the RP for the deterministic analysis undertaken for the safety case. This formal interaction has commenced during GDA Step 2. This work is being led by the Fuel and Core Inspector.
- Initiating event frequencies: these provide input to the fault frequencies of the identified fault sequences that I will consider in my Fault Studies assessment. This formal interaction has not yet commenced during GDA Step 2. This work will be led by the PSA Inspector.
- The Fault Studies assessment provides input to the performance requirements for Systems, Structures and Components (SSC). The substantiation of these SSCs will be the focus of the assessment by the various Engineering Inspectors (including Mechanical engineering, Electrical Engineering, Control & Instrumentation). This formal interaction has not commenced during GDA Step 2.

3 REQUESTING PARTY'S SAFETY CASE

24. 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. This section presents a summary of the RP's preliminary safety case in the area of Fault Studies. It also identifies the documents submitted by the RP which have formed the basis of my Fault Studies assessment of the UK HPR1000 during GDA Step 2.

3.1 Summary of the RP's Preliminary Safety Case in the Area of Fault Studies

25. The aspects covered by the UK HPR1000 preliminary safety case in the area of Fault Studies can be broadly grouped under 6 headings which can be summarised as follows:

- Reactor Faults:

26. The PSR is based upon the existing deterministic safety analysis of Fangchengang Unit 3 (FCG3), which is the reference plant for the UK HPR1000. The RP intends to develop this analysis in line with UK requirements. The HPR1000 design has 3 cooling loops and physically separate safety systems to respond to fault conditions and prevent damage to the reactor core. The safety systems include two diverse Control and Instrumentation (C&I) systems, 3 trains of cooling water injection (comprising medium and low pressure injection functions), 3 trains of emergency feedwater and a containment isolation function. There is also an emergency boration system and an atmospheric steam dump system to discharge steam from the Steam Generators to atmosphere. An overview of the safety systems is provided in Chapter 2 of the PSR (Ref. 2) with more detailed descriptions within Chapter 7 of the PSR (Ref. 2).

27. The RP states that the design of FCG3 has identified a comprehensive set of postulated initiating events (PIEs) which consider all foreseeable events during all operating states with the potential for serious consequences. From this set, the RP has grouped the PIEs into a list of Design Basis Conditions (DBCs), termed DBC1 to DBC4 depending on their frequency of occurrence. Analysis (in the form of transient analysis using computer codes) has been undertaken for FCG3 to demonstrate that the engineered safety measures are sufficient to protect against these DBCs and that the consequences meet the defined acceptance criteria.

28. The RP has recognised that UK requirements are different to those in China and has produced a strategy document (Ref. 3) to summarise the additional work that is being undertaken for the development of the UK DBA. This work relates to the completeness of the list of PIEs and DBC list, the development of the radiological consequences modelling and the production of a fault schedule (see paragraphs 35 and 36 below). The RP will identify diverse means of protection against frequent faults, in accordance with UK expectations, and will undertake new transient analysis as required to demonstrate that the diverse protection can meet relevant acceptance criteria.

- Fuel Handling and Storage Operations:

29. Chapter 23 of the PSR (Radioactive Waste Management & Fuel Storage) presents a description of the spent fuel pool and the fuel route but, in contrast to the reactor faults there is not the same depth of information within Chapter 12 on how faults associated with these areas of the plant will be analysed by the RP. In response to RQ-HPR1000-0099 (Ref. 7) the RP has described the parts of the Pre-Construction Safety Report (PCSR) that will be submitted at the start of Step 3 and a number of supporting documents that will provide a comprehensive safety case for Fuel Handling and Storage Operations.

30. Reference 7 also provides an indicative list of faults that may be considered within the Fuel Handling and Storage Operations safety case and the protection measures that are in place. Fault types within Reference 7 include:

- Loss of cooling faults;
- Loss of water inventory faults;
- Loss of power faults;
- Criticality faults;
- Over-raise faults and;
- Internal and External hazards (including dropped loads and collisions).

31. The design provides for redundant means to provide cooling to the spent fuel pool in the event of a fault condition, including the use of the Secondary Passive Heat Removal System ASP [SPHRS]) as a source of make-up water in the event of a loss of 3 trains of Fuel Pool Cooling and Treatment System (PTR [FPCTS]).

■ Design Extension Conditions:

32. In the PSR Chapter 13 (Ref. 2) the RP has described the approach to the analysis of fault sequences which are just beyond the frequency of occurrence typically considered within the design basis. Whilst this analysis uses similar codes to those used for the analysis of DBCs, these sequences are not considered in the same way (using conservative methods and assumptions) but are instead analysed using a best-estimate methodology. The RP uses the terminology of Design Extension Conditions (DEC) to describe these fault sequences; sequences that do not lead to fuel melt are referred to as DEC-A sequences, while those sequences with fuel melt are referred to as DEC-B sequences. DEC-B sequences are also addressed within Chapter 13 of the PSR and are considered by ONR's Severe Accident assessment (Ref. 9).

33. A number of specific systems are included within the HPR1000 design to protect or mitigate against DEC-A events. These include the Secondary Passive Heat Removal System (ASP [SPHRS]), the Extra Cooling System (ECS [ECS]), the Containment Heat Removal System (EHR [CHRS]) and the Station Black-Out (SBO) diesel generators.

■ Analysis Codes:

34. At the time of writing this Assessment Report the RP has not declared which computer codes will be used for the transient analysis that will be presented in support of the DBC and DEC-A analysis. There is the possibility that the RP could use the third-party codes that have been used for FCG3 and other Chinese domestic nuclear plant, or in-house codes developed by the reactor vendor. The RP has shared basic descriptions of the two sets of codes (Ref. 7) with ONR. Further information, including validation evidence for these codes, will be provided as a support reference to the Step 3 PCSR.

■ Fault Schedule:

35. The RP has prepared a template fault schedule (Ref. 5) for the UK HPR1000 which will summarise the initiating events identified within the design basis and the protections systems provided to safely manage such events should they occur. The single page template illustrates the format and approach that will be adopted.

36. The RP has stated that an initial version of the fault schedule will be submitted early in Step 3, based on FCG3. However, this fault schedule will not be complete until later in GDA when the underlying analysis (such as the analysis of the diverse protection claimed against frequent faults) has concluded.

- Classification and Categorisation of Systems, Structures and Components:

37. During Step 2 the RP has submitted a methodology for the categorisation of safety functions and the classification of SSCs (Ref. 6). Within this methodology the RP is proposing a scheme based upon IAEA SSG-30 (Ref.12) that has been modified to take into account UK regulatory expectations. In this scheme SSCs are classified either through a functional categorisation process or, for design provisions (generally, but not restricted to, passive components that deliver their safety function under normal operating conditions), classified directly based on their consequences of failure.

38. The process describes a 3 tier classification system with FC1, 2 and 3 to indicate Category 1, 2 and 3 safety functions. SSCs are classified separately with F-SC1, F-SC2 and F-SC3 indicating Functional Class 1, 2 and 3, and B-SC1, B-SC 2 and B-SC3 indicating Design Provisions Class 1, 2 and 3.

3.2 Basis of Assessment: RP's Documentation

39. The RP's documentation that has formed the basis for my GDA Step 2 assessment of the safety claims related to the Fault Studies aspects of the UK HPR1000 is presented in the following documents:

- PSR Chapter 4 General Safety and Design Principles (Ref. 2);

This Chapter provides a summary of the design process followed in the development of the HPR1000 (FCG3) design that will form the basis of the processes to be followed in the development of UK HPR1000 design.

- PSR Chapter 12 Design Basis Conditions Analysis (Ref. 2);

This Chapter provides a description of the fault identification and grouping for FCG3, the DBA methodology and assumptions and a brief summary of the DBA results.

- PSR Chapter 13 Design Extension Conditions and Severe Accident Analysis (Ref. 2);

This Chapter presents the analysis of low frequency fault sequences to identify the margins present in the design.

- Fault Studies strategy document (Ref. 3);

This document presents the work that was planned to be carried out for Fault Studies during Step 2 of GDA.

- Methodology of Postulated Initiating Event identification (Ref. 4);

This purpose of this document is to provide a systematic, auditable and comprehensive methodology of PIE identification for the UK HPR1000.

- Fault Schedule production methodology (Ref. 5);

This document presents the methodology for the production of a fault schedule for the UK HPR1000.

- Methodology of Safety Categorisation and Classification (Ref. 6);

This document presents the principles for the categorisation of safety functions and classification of systems, structures and components for the UK HPR1000.

- Responses to RQs (Schedule of RQs Ref. 7).

40. In addition, during April 2018 the RP submitted to ONR, for information, an advance copy of the UK HPR1000 Pre-Construction Safety Report (PCSR). Chapters, 4, 12 and 13 (Ref. 14) are relevant to Fault Studies. Having early visibility of the scope and content of these chapters has been useful in the planning and preparation of my GDA Step 3 assessment work.

4 ONR ASSESSMENT

41. This assessment has been carried out in accordance with HOW2 guide NS-PER-GD-014, “Purpose and Scope of Permissioning” (Ref. 10).

42. My Step 2 assessment work has involved regular engagement with the RP’s Fault Studies specialists, including one technical exchange workshop in China and routine progress meetings. I have also visited the Fuqing Unit 5 construction site where I could tour the reactor building (noting that while this reactor is not the same as the UK HPR1000 reference plant, it does share many similarities).

43. 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 normally lead to Regulatory Queries (RQs) being issued. At the time of writing my assessment report, in Fault Studies, during Step 2, I have raised 11 RQs to facilitate my assessment.

44. Details of my GDA Step 2 assessment of the UK HPR1000 preliminary safety case in the area of Fault Studies, 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 UK HPR1000.

4.1 Reactor Faults

4.1.1 Assessment

45. The majority of the information presented by the RP in Chapter 12 of the PSR is focussed on reactor faults, and given that these are the most significant fault types my assessment has focussed on the RP’s consideration of these faults. The terminology used by the RP (PIEs and DBCs) in the PSR is different to that used in the SAPs, however I am content that the submissions are self-consistent and achieve the same purposes as the SAPs terminology. It is my expectation that this terminology will be applied to the UK HPR1000 safety case.

46. As described in my Step 2 assessment plan (Ref. 1) I have sought to gain confidence in the fault identification processes that have been described by the RP and the completeness of the list of DBCs that will be submitted. I have discussed with the RP their approach to fault identification and the gaps that they have identified between the safety submission for FCG3 and the UK HPR1000. I have requested information on the specific fault types of Loss of Off-Site Power (LOOP) scenarios to understand the approach to these faults in FCG3 and for the UK HPR1000. I have not however conducted a thorough assessment of the list of DBCs as this will be a focus of my Step 3 assessment.

47. I have also sought to understand the RP’s approach to DBA fault sequence development and to gain confidence that appropriate analysis methods will be used. SAPs FA.5 and FA.6 present ONR’s expectations for the identification and development of fault sequences within DBA and the types of penalising assumptions that should be made. Through RQs (Ref. 7) I have gained confidence that the RP will have considered these assumptions in the development of the fault sequences, however I will be considering in detail what assumptions have been made in my assessment of a sample of fault sequences in Step 3 of GDA.

- Fault Identification

48. SAPs Principle FA.2 (Ref. 8) requires that fault analysis should identify all initiating faults with the potential to lead to any person receiving a significant dose of radiation or

to a significant quantity of radioactive material escaping from its designated place of residence or confinement. FA.5 then requires that the safety case should list all initiating faults that are included within the DBA, giving criteria for which faults should be included. The SAPs also require (paragraph 101) that the safety case should identify the failure modes by a thorough and systematic fault and fault sequence identification process.

49. The RP has therefore undertaken a fault identification exercise to supplement the FCG3 PIE list and aimed at providing a logical method and auditable trail for the list of PIEs for UK HPR1000. This exercise is described in a PIE identification methodology (Ref. 4). The RP has developed a Master Logic Diagram to identify Abnormal Operating States (AOSs), from which functional failures can be identified. This has been supplemented with Failure Modes and Effects Analysis (FMEA) of specific systems and components. Based on the information that I have reviewed so far I am content that this is appropriate for Step 2. The results of this work will be presented as supporting references to the PCSR to be submitted during Step 3.

50. The DBCs for FCG3 are presented in Chapter 12 of the PSR (Ref. 2). Whilst the frequencies of the DBC categories do not exactly match with the frequent and infrequent fault categories that is common practice in GB nuclear facilities and described in the SAPs (para. 727, Ref. 8), I am content that they are consistent with IAEA terminology and cover the UK expectations for the design basis and faults that lie just outside of the design basis region. I also note that the assumed operating conditions cover all the possible conditions from full power operation to cold shutdown. This is consistent with ONR's expectation that the DBA should include faults in all operating states, including shutdown and refueling states. Chapter 12 of the PSR (Ref. 2) describes the definitions of the plant states used at FCG3 and I anticipate that similar states will be used in the UK HPR1000 safety case.

- Fault identification for support systems

51. ONR's SAPs set the expectation that the licensee will identify all potential faults and that those with a frequency of greater than $1x10^{-5}$ per annum will be assessed within the DBA. The PSR presents a list of faults that has been considered within the DBA for FCG3. This is list is broadly consistent with my expectations and is based upon the experience of other reactor plants in China and around the world. The list however considers only failures of "frontline" systems as initiating faults. In addition to failures of "frontline" systems and components, faults can also arise within supporting systems.

52. The RP has recognised that their fault identification method requires further development and a methodology for identifying support system failures is presented within Reference 4. The RP intends to complete this work and confirm the PIE and DBC list during Step 3. I have reviewed this methodology and I consider that, at a high level it provides a reasonable basis for the RP to progress the fault identification work. The development and application of this methodology will be a focus of my assessment during later steps of GDA.

- Spurious Control & Instrumentation systems actuation

53. ONR's expectation is that, due to the complex nature of the technologies and architecture of C&I within reactor designs, spurious actuation of systems due to C&I faults should be considered within the safety analysis (NS-TAST-GD-034 , Ref. 11). ONR expects that such analysis needs to identify the functional outputs of the C&I systems and develop bounding fault conditions. The RP is, at the time of writing this report, developing a methodology for the identification of faults arising from spurious actuation of C&I systems. I will work closely with ONR's specialist C&I inspector to gain confidence that the methodology is robust and I will seek a demonstration that all

relevant design basis faults have been appropriately identified and assessed, and the plant shown to be robust.

- Fault sequence development

54. Within Chapter 12 of the PSR (Ref. 2) the RP has outlined the methodology for the analysis of DBCs and the main assumptions that will be applied. Key points include:

- Initial conditions for each DBC are defined as a particular steady state and conservative steady state uncertainties are added to nominal values;
- The first manual actions assumed from main control room are not considered until at least 30 mins after the first significant signal received;
- Only FC1 and FC2 safety systems are considered in the deterministic analysis. Other safety systems are considered if their operation is conservative;
- Only FC1 and FC2 C&I signals are considered in the deterministic analysis. Other C&I signals are considered if their operation is conservative;
- Conservative assumptions are made on uncertainties associated with C&I set points and time delays for signals.

55. Chapter 12 of the PSR (Ref. 2) states that the analysis rules are sufficiently conservative to demonstrate that an appropriate design margin remains following the limiting faults. Noting the general guidance given within NS-TAST-GD-034 (Ref. 11) on the development of fault sequences I am content that these assumptions are appropriate for the analysis of the DBCs at this stage; I will look to the PCSR submissions to develop these further and assure myself that the RP has appropriately applied them in the DBC analysis.

56. The DBA will seek to demonstrate that appropriate acceptance criteria are met following the limiting faults and Chapter 12 of the PSR (Ref. 2) outlines the criteria that have been used in FCG3 based on Chinese regulatory requirements. These acceptance criteria include limits for Departure from Nucleate Boiling (DNB) and clad temperature and oxidation. These criteria have been considered by ONR's fuel and core specialist inspector who is content that the criteria are sufficiently defined for Step 2 and acceptable in principle, noting that the proposed limits of tolerable fuel damage and their numerical values will be considered in later steps of GDA.

- Diversity and Redundancy

57. EDR.2 requires that appropriate diversity should be incorporated as appropriate into the designs of SSCs, and that it should be demonstrated that the required level of reliability for their intended nuclear safety function has been achieved. ONR requires (EDR.3) that common cause failures (CCFs) should be addressed explicitly and, in general, claims for CCFs should not be better than one failure per 100 000 demands . It is therefore RGP in the UK for frequent faults (i.e. more frequent than 10^{-3} per annum) to consider the failure of a major protection system and demonstrate that an alternative (diverse) system can operate successfully and that appropriate acceptance criteria can be met.

58. The RP has recognised the need to identify which of the DBCs need to be considered as frequent faults and for which it will need to demonstrate diverse protection. The RP intends (Ref. 3) to identify appropriate diverse lines of protection and to provide transient analysis to demonstrate that the claimed diverse protection systems will meet appropriate acceptance criteria.

59. The transient analysis for the operation of these diverse protection systems may already exist for FCG3, using the less onerous best estimate requirements of DEC- A analysis (see sections 4.3 below). In this case, the RP will need to review and

potentially repeat this analysis using conservative assumptions and judge the adequacy of the margins to appropriate DBA acceptance criteria. The evidence that is provided to demonstrate such margins will be a focus of my assessment in later steps of GDA.

60. If there are any shortfalls against the requirement for diverse protection for frequent faults, the RP has stated that design changes will be considered and an assessment will be carried out, in accordance with the principles of reducing risks As Low As Reasonably Practicable (ALARP). I am content that this is an acceptable statement for Step 2. In advance of the RP completing its assessment of diverse protection, RO-UKHPR1000-0001 has been raised by ONR which requires the RP to address specific shortfalls in the design of the Diverse Actuation System (DAS). This system is provided as a diverse means to trip the reactor and to initiate post trip cooling in the event of a failure of the Reactor Protection System (RPS). ONR considers that the design is not consistent with relevant good practice in this areas as it is designed to address Nuclear C&I Class 3 requirements, is not designed to meet the single failure criteria and is based on complex programmable hardware. The resolution of RO-UKHPR1000-0001 is being led by ONR's C&I specialist inspector.

61. SAP EDR.2 also requires that appropriate use should be made of redundancy within the designs of SSCs important to safety while SAP EDR.4 requires that 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. SAP FA.6 requires that design basis fault sequences should include consideration of single failures. In response to RQ-UKHPR1000-0073 (Ref.7) the RP has described a systematic method for identifying the most onerous single failure to be considered within the DBA. In line with Chinese practice the RP will apply active single failures at the start of the transient with passive single failures considered 24 hours after the initial event. I have confirmed with the RP that the passive failures considered at FCG3 relate to a leak in a pipe within the system. I have also confirmed that the specific fault types of non-return valve failures and safety relief valves failing to re-seat are considered by the RP as active failures, in line with ONR's expectations. I will look to future submissions to demonstrate that such unrevealed passive failures have been considered by the RP in the application of the single failure criteria.

- Common Cause Failures

62. EDR.3 sets the expectations that where redundant or diverse components are employed to provide high reliability, CCFs should be addressed explicitly. The RP has recognised (para 58 above) that CCF of the primary safety measures needs to be considered and diverse protection provided against frequent faults. The RP has also committed to identifying and considering CCFs within the fault identification methodologies for support systems and spurious failures in the C&I systems (Further discussion is provided in the response to RQ-UKHPR1000-0095, Ref. 7). I will be looking to Step 3 submissions to demonstrate that the RP has identified potential CCFs and provided adequate analysis and safety arguments to demonstrate that appropriate safety criteria are met.

- Treatment of maintenance assumptions within the Design Basis

63. In response to RQ-UKHPR1000-0084 (Ref. 7) the RP claims that, to ensure that the single failure criteria (SAPs EDR.4) is met maintenance activities on these safety trains will be controlled so that sufficient protection is always available for design basis fault conditions. NS-TAST-GD-034 (Ref. 11) notes that this is particularly important where safety systems have 3 trains. I have not assessed this claim in detail during Step 2 but it will form part of my assessment of the analysis of fault sequences by the RP in later steps, noting the requirement of the SAPs that the analysis should include the worst

normally permitted configuration of equipment outages for maintenance, test or repair (SAPs FA.6).

4.1.2 Strengths

64. During my GDA Step 2 assessment of Reactor Faults I have noted the following areas of strength:

- The development of a logical method and auditable trail for the list of PIEs for UK HPR1000;
- The PSR considers operating conditions in all possible conditions from full power operation to cold shutdown.

4.1.3 Items that Require Follow-up

65. During my GDA Step 2 assessment of Reactor Faults I have identified the following areas that I will follow-up during Step 3 of GDA:

- Fault Identification for support systems;
- Spurious Instrumentation and Control systems actuation;
- The demonstration of diverse protection against frequent faults;
- Treatment of maintenance assumptions within the Design Basis.

4.1.4 Conclusions

66. Based on the outcome of my Step 2 assessment of reactor faults, I have concluded that the RP has a reasonable basis for the approach to DBA. The list of DBCs from FCG3 will be supplemented by additional fault identification methods and the RP has committed to conducting new analysis for any new DBCs as required. The RP has also committed to conducting new analysis for the demonstration of diverse lines of protection for frequent faults.

67. I will look to future submissions to demonstrate that suitable and sufficient safety measures are provided in the design against the identified DBCs and that the RP has demonstrated adequate margins to the relevant acceptance criteria, thereby demonstrating the fault tolerance of the engineering design. I am content that the RP has recognised the areas where further analysis work is required and has adequate plans to address them.

4.2 Fuel Handling and Storage Operations

4.2.1 Assessment

68. ONR requires that a demonstration that hazards posed by a site or facility are understood and controlled (FP.4) and a safety case should be accurate, objective and demonstrably complete for its intended purpose (SC.4). It has been ONR's experience that reactor vendors have often concentrated their safety demonstrations on the reactor itself. However, it is the expectation in the UK that an RP will consider all potential sources of radioactivity and ONR therefore expects that the safety case should also include appropriate consideration of the spent fuel pool, fuel route and any other significant sources of radioactivity.

69. The PSR contains chapters on Radioactive Waste Management and Spent Fuel Storage (Chapter 23), Design Basis Conditions Analysis (Chapter 12) and Probabilistic Safety Analysis (Chapter 14), (Ref 2). Each of these chapters (and others) contains information relevant to the demonstration of safety of the HPR1000 fuel route and spent fuel storage. During Step 2 I have sought, via RQ-UKHPR1000-0099 (Ref. 7), to

understand how these elements will be used to support the production of a safety case for the fuel route and spent fuel storage (or any other sources of radioactivity).

70. The response to RQ-UKHPR1000-0099 (Ref. 7) clearly describes the scope of fuel handling and storage operations that will be considered during GDA, from receipt of new fuel to the transfer of used fuel to the spent fuel pool. However, the RP has not yet chosen a Spent Fuel Interim Storage (SFIS) solution and has declared (Ref. 7) that the scope of GDA is limited to operations within the spent fuel pool. ONR will look to the safety case produced for GDA to demonstrate that future SFIS options are not precluded by operations undertaken within the spent fuel pool.

71. The response to RQ-UKHPR1000-0099 (Ref. 7) also provides an indicative list of faults that may be considered within the Fuel Handling and Storage Operations safety case and the protection measures that are in place. To demonstrate the successful operation of the protection measures, the RP will need to develop appropriate acceptance criteria. A number of examples of acceptance criteria are described within the response to RQ-UKHPR1000-0099 (Ref. 7), including criticality limits and pool water temperatures. The RP will need to develop these limits to ensure that they are appropriate for UK regulatory expectations.

72. In response to RQ-UKHPR1000-0133 (Ref. 7) the RP has outlined a proposed methodology for identifying faults that result only in radiation exposure (i.e. faults that do not result in a significant off-site release and affect workers rather than the public). This methodology appears reasonable at this stage but will be submitted formally as an update to Methodology of PIE Identification (Ref. 4) and I will consider the methodology and identified faults during later stages of GDA.

4.2.2 Strengths

73. During my GDA Step 2 assessment of Fuel Handling and Storage Operations I have noted the following areas of strength:

- I am content that the RP has a reasonable basis for the development of a safety case for Fuel Handling and Storage Operations.

4.2.3 Items that Require Follow-up

74. During my GDA Step 2 assessment of fuel handling and storage operations I have identified the following areas that I will follow-up during Step 3 of GDA:

- Development of appropriate acceptance criteria for the DBA;
- Scope of the safety case and the interfaces with the proposed Spent Fuel Interim Storage solution;
- Fault identification for fuel handling and fuel storage, particularly with respect to the identification of worker faults.

4.2.4 Conclusions

75. Based on the outcome of my Step 2 assessment of fuel handling and fuel storage faults, I have concluded that the RP has a credible approach to the development of a safety case for this area.

4.3 Design Extension Conditions

4.3.1 Assessment

76. Consistent with the approach described in paragraphs 9 and 32 above, the RP has identified some DEC-A sequences for FCG3 from the Level 1 PSA. These are

presented within Chapter 13 of the PSR (Ref. 2) and the RP will develop this list for the UK context. As part of my assessment of later submissions I will form a judgement on the claim that DECs have been systematically analysed and that the analysis has been used to identify further preventative or mitigating measures.

77. The PSR Chapter 13 provides a good overview of the DEC-A analysis methodology. The RP intends to conduct deterministic analysis of DEC-A sequences but using more realistic assumptions than the conservative assumptions using in DBA. Chapter 13 also provides a list of DEC-A sequences analysed for FCG3, which will be the basis for the list of sequences for UK HPR1000. Some of the sequences in this list may need to be re-assessed using design basis assumptions as a result of the RP's consideration of CCFs within the design basis (as they describe the diverse protection against frequent faults (paragraph 58 above)). The RP recognises this and intends to provide new analysis as appropriate.

78. During my Step 3 assessment I will confirm that the list of DEC-A sequences is appropriate and that the sequences have been assessed using appropriate methods. The majority of DEC-A sequences considered within the PSR are for the reactor at power but there is the possibility that DEC-A sequences could arise in the spent fuel pool or elsewhere, or at other operating conditions. I therefore intend to explore whether there are any additional sequences that should be considered, as the safety case develops. I will look to future submissions for a complete list of DEC-A sequences and a demonstration that sufficient measures are provided for in the design to ensure that appropriate success criteria have been met. As part of my assessment I will consider (amongst other aspects) whether these measures are automatic or manually actuated, any novelty aspects, their safety classification and performance claims.

4.3.2 Strengths

79. During my GDA Step 2 assessment of Design Extension Conditions I have noted the following areas of strength:

- The RP intends to conduct deterministic analysis of DEC-A sequences but using more realistic assumptions than the conservative assumptions used in DBA, to show that the plant is tolerant without significant fault escalation and unacceptable consequences.

4.3.3 Items that Require Follow-up

80. During my GDA Step 2 assessment of Design Extension Conditions I have identified the following areas that I will follow-up during Step 3 of GDA:

- The list of DEC-A sequences and confirmation that these have been assessed using appropriate methods. I will also consider the demonstration of the adequacy of the provisions made in the design to protect against these sequences.

4.3.4 Conclusions

81. Based on the outcome of my Step 2 assessment of Design Extension Conditions, I have concluded that the RP's intended approach to DEC-A faults appears reasonable. The list of DEC-A faults and the supporting analysis that demonstrates that appropriate acceptance criteria are met will be subject to formal assessment in later steps of GDA.

4.4 Analysis Codes

4.4.1 Assessment

82. An integral part of DBA for a reactor is undertaking of transient analysis of fault sequences using computer models of the reactor design in question. This is a major component of the work required by the RP to demonstrate the adequacy of the design and the suitability and sufficiency of the safety measures. The results of these computer models (usually predictions of physical parameters e.g. temperatures, masses of steam/water losses, radioactive releases, etc.) are assessed against deterministic targets.

83. ONR does not mandate the computer codes that are to be used in the transient analysis for DBA. Instead, SAP FA.7 (Ref. 8) requires that analysis of design basis fault sequences should use appropriate tools and techniques.

84. The PSR states only that codes approved by the NNSA (the National Nuclear Safety Administration, the Chinese Nuclear Regulator) have been used for the transient analysis at FCG3 and that similar codes will be used for the UK HPR1000 analysis. I have therefore sought information from the RP on the computer codes that will be used for the UK HPR1000 safety case, to give me confidence that adequate analysis can be provided later in GDA.

85. In response to RQ-UKHPR1000-0067 (Ref. 7) the RP has stated that there are two potential options available for the computer codes to be used for UK HPR1000. These are:

- third party, internationally recognised computer codes, used in FCG3 and other domestic Chinese plant; or
- in-house computer codes, developed since 2010 for the analysis of transients in Pressurised Water Reactors.

86. At the time of writing the RP has not yet stated which set of computer codes it intends to use to support the UK HPR1000 safety case. The transient analysis is key evidence to demonstrate that the plant is tolerant to normal operational transients, that appropriate parameters have been chosen for the initiation of protection systems and to demonstrate that the operation of installed protection systems will prevent significant consequences.

87. In response to RQ-UKHPR1000-0067 (Ref. 7) the RP has supplied a basic description of the two sets of codes, with a brief history and, for the in-house codes, a summary of their verification and validation. I understand that the RP has undertaken transient analysis for FCG3 with both sets of codes and that both demonstrate appropriate margins to relevant success criteria, in line with Chinese regulatory requirements. Chapter 12 of the PSR (Ref. 2) contains summaries of two fault sequences that have been analysed for FCG3 and states that for all DBC the relevant acceptance criteria have been met. This provides me with some confidence that adequate transient analysis can be provided in the UK HPR1000 safety case to demonstrate the adequacy of the safety systems.

88. To gain confidence in the results of the transient analysis performed with these computer codes I intend to commission some independent confirmatory analysis of a sample of UK HPR1000 fault sequences. I will use the results of this analysis to inform my judgement on the adequacy of the RP's analysis codes and key assumptions.

89. I also intend to examine the validation and verification of the analysis codes that will be used in the UK HPR1000 safety case and this will form a key part of my assessment activity in later steps of GDA.

4.4.2 Strengths

90. During my GDA Step 2 assessment of analysis codes I have noted the following areas of strength:

- I understand that the RP has undertaken transient analysis for FCG3 with both sets of codes and that both demonstrate appropriate margins to relevant success criteria, in line with Chinese regulatory requirements.

4.4.3 Items that Require Follow-up

91. During my GDA Step 2 assessment of Analysis Codes I have identified the following areas that I will follow-up during Step 3 of GDA:

- I intend to commission some independent confirmatory analysis of a sample of UK HPR1000 fault sequences. I will use the results of this analysis to inform my judgement on the adequacy of the RP's analysis codes and key assumptions;
- The validation and verification of the analysis codes that will be used in the UK HPR1000 safety case.

4.4.4 Conclusions

92. The RP needs to declare which suite of computer codes will be used for the UK HPR1000 analysis. I am however content that the RP will be able to present suitable transient analysis for reactor fault sequences, noting that Chinese regulatory acceptance criteria have been met for FCG3 using both sets of codes. This analysis will need to be reviewed by the RP against UK requirements.

4.5 Fault Schedule

4.5.1 Assessment

93. During Step 2 I have sought to gain confidence that the RP has a plan to develop a fault schedule for the UK HPR1000 that will meet the expectations of ONR's SAPs FA.8 and ESS.11 (Ref. 8). A fault schedule is a key part of the safety case that demonstrates that all design basis faults are addressed, that safety functions and performance requirements for safety measures have been identified and that suitable and sufficient safety measures are provided.

94. Following discussions with the RP a fault schedule methodology (Ref. 5) has been submitted that outlines the intended scope and content of the fault schedule. The template appears to be a sound basis for the RP to develop a suitable fault schedule which will contain the information expected by the SAPs. The RP intends to include information on initiating event frequencies and relevant safety functions that are affected by the fault, along with details of the main and diverse protection lines. These details will include the required signals and C&I platform, the safety class of the SSC and a link to supporting studies. This should provide a clear link between the faults and the claimed protection.

95. The RP intends to deliver an early version of the fault schedule to ONR at the beginning of Step 3, with a complete fault schedule being developed during Step 3. The early version will contain the FCG3 DBCs with primary protection measures and diverse protection for frequent faults identified. The RP will update the fault schedule throughout Step 3 with any new DBCs identified for the UK HPR1000, with UK specific classification of SSC and the confirmed diverse protection for frequent faults (once the relevant transient analysis has been completed). I intend to review the fault schedule as it develops to confirm that it contains appropriate information and links to supporting analysis within the safety case.

4.5.2 Strengths

96. During my GDA Step 2 assessment of the RP's methodology for the development of a fault schedule I have noted the following areas of strength:

- The fault schedule template appears to be a sound basis for the RP to develop a suitable fault schedule which will contain the information expected by ONR's SAPs.

4.5.3 Items that Require Follow-up

97. During my GDA Step 2 assessment of the RP's methodology for the development of a fault schedule I have identified the following additional potential shortfalls that I will follow-up during Step 3 of GDA:

- The maturity of information within the fault schedule and links to supporting analysis within the safety case.

4.5.4 Conclusions

98. Based on the outcome of my Step 2 assessment of the methodology for the development of a fault schedule, I have concluded that the proposed scope and format of the fault schedule is consistent with my expectations. I expect that the fault schedule will develop over the course of GDA as underpinning work is completed and I expect the fault schedule to become a key document for my assessment (and the assessments undertaken by other inspectors) during Step 3 and 4.

4.6 Categorisation and Classification of Systems, Structures and Components

4.6.1 Assessment

99. ESC.1 to ESC.3 (Ref. 8) set ONR's expectations that safety functions will be identified and categorised based on their significance to safety, that SSCs that deliver the functions will be classified and that the SSCs are managed to appropriate codes and standards. These expectations are further developed in ONR's TAG NS-TAST-GD-094 (Ref. 11). During Step 2 I have sought to gain confidence that the RP's proposed method for the categorisation of safety functions and classification of SSCs (Ref. 6) is appropriate and consistent with the approach to DBA.

100. The RP's approach to Categorisation and Classification (Ref. 6) is based upon guidance given in IAEA Safety Guide SSG-30, amended to recognise and address UK expectations. In my opinion, this gives a sound foundation to the process and, at a high level can be seen to be consistent with the expectations of ECS.1 and ECS.2. I consider that the most important UK specific changes include the development of radiological criteria, the enhanced focus on on-site risks and the expansion of the guidance to apply to non-reactor faults. The RP also intends to classify human actions, consistent with the categorisation of safety functions.

101. The codes and standards to be applied to the SSCs will be considered by the relevant engineering specialist inspectors within ONR, noting the expectations of NS-TAST-GD-003 (Ref. 11).

102. The application of the Categorisation and Classification methodology will be a focus of my assessment during later stages of GDA. My priority will be to gain confidence in the classification of the reactor systems and protective safety measures. To do this I will consider the consequences of SSC failure assumed by the RP and whether appropriately conservative assumptions have been used. I will also be seeking to gain confidence that the methodology has been appropriately applied to areas away from

the primary or front line reactor systems, such as the supporting systems and fuel route and fuel handling equipment.

103. The RP's process described in Reference 6 is based upon an identification of safety functions, with the safety category being assigned depending on the level of Defence-in-Depth that the function is supporting and the severity of the consequences if the function is not performed:

- Functions that are required to reach a controlled state under DBC-2, 3 and 4 conditions are Category 1 for the highest consequences.
- Functions that are required to reach and maintain a safe state under DBC-2, 3 and 4 conditions are Category 2 for the highest consequences.
- Functions which provide a diverse backup to a Category 1 function in a frequent fault are Category 2.

104. Having defined the Function Category the SSC Class is equivalent to the category i.e. a Category 1 Function is delivered by a Class 1 system. This scheme places emphasis on the definition and breakdown of safety functions such that each safety function is delivered by a single SSC, rather than identifying multiple SSCs of different classes to deliver a higher level safety function.

105. The definition of the key safety functions and their breakdown into system and component level functions will therefore be important to the successful application of the categorisation and classification methodology described in Reference 6. I will look to future submissions to demonstrate that such a breakdown has been undertaken logically and to an appropriate level such that SSCs can be suitably classified.

106. ONR's guidance on Categorisation and Classification (NS-TAST-GD-094, Ref. 11) describes the factors that should be considered in the categorisation of safety functions, expanding on the general requirements of SAPs Principle ECS.1 (Ref. 8). I am satisfied that Reference 6 adequately describes how these factors have been considered by the intended scheme. NS-TAST-GD-094 (Ref. 11) does recommend that the safety function categorisation and SSC classification should be distinct to avoid confusion. Notwithstanding this advice, given that there is a direct relationship between the Functional Categorisation and the Safety Classification I do not foresee any significant confusion at this stage.

107. The RP also describes an approach to the direct classification of Design Provisions. This is IAEA terminology and Reference 6 states that categorisation of the functions provided by Design Provisions is not necessary because the safety significance of the SSC can be directly derived from the consequences of its failure. Nevertheless, Table T-6-2 of Reference 6 describes the two types of safety functions that are delivered by Design Provisions:

- Design Provisions whose failure could lead directly to radiological release during normal operation;
- Design provision whose failure could lead to radiological release during a fault due to loss of containment of radioactive material.

108. From examination of the examples of Design Provisions given in Reference 6 these are generally associated with pressure retaining SSCs such as pipework and vessels. Reference 6 links to a specific document on the methods and requirements of Structural Integrity Classification and the application of these methods will be the focus of ONR's structural integrity inspector during later steps of GDA. I have not identified any specific concerns with the adequacy of the approach to the classification of Design Provisions at this stage, noting that relevant ONR guidance (Ref. 11) does not prescribe the approach to Categorisation and Classification.

109. The RP recognises that there are some potential changes to the classification of systems arising from UK specific requirements. Notably, systems that deliver DEC-A functions are F-SC3 but if they are claimed within the design basis as a diverse backup to a F-SC1 function in a frequent fault then Reference 6 states the expectation that they should be F-SC2. It is not yet clear which systems may be affected by this and the RP is working to identify and assess the diverse lines of protection for frequent faults. I will look to future submissions for evidence that the safety classification of systems has been appropriately derived and I will engage with Inspectors in other technical disciplines to gain assurance that the required safety classification can be delivered by the engineered systems.

4.6.2 Strengths

110. During my GDA Step 2 assessment of the RP's methodology for Categorisation of Safety Functions and Classification of SSCs I have noted the following areas of strength:

- The RP's approach to Categorisation and Classification is based upon guidance given in IAEA Safety Guide SSG-30, amended to recognise and address UK expectations.

4.6.3 Items that Require Follow-up

111. During my GDA Step 2 assessment of the RP's methodology for Categorisation of Safety Functions and Classification of SSCs I have identified the following areas that I will follow-up during Step 3 of GDA:

- The breakdown of safety functions to an appropriate level such that SSCs can be suitably classified;
- The application of the Categorisation and Classification methodology to the reactor systems and protective safety measures;
- The application of the Categorisation and Classification methodology to areas away from the primary or front line reactor systems, such as the supporting systems and fuel route and fuel handling equipment.

4.6.4 Conclusions

112. Based on the outcome of my Step 2 assessment I have concluded that the RP's categorisation and classification methodology should provide an adequate basis for the classification of SSCs. I will seek to gain confidence that the functional breakdown has been conducted logically and that the consequences used within the methodology have been derived using appropriately conservative assumptions.

4.7 ALARP Considerations

113. There is no specific mention of ALARP within either Chapter 12 (Design Basis Conditions Analysis) or Chapter 13 (Design Extension Conditions and SAA) of the PSR (Ref. 2). The RP has however produced an ALARP strategy (Ref. 17) which sets out the approach to assessing the generic design of the UK HPR1000 to determine whether the nuclear safety risks of the construction, operation and decommissioning are ALARP. The RP has also stated that any potential design changes as a result of applying UK expectations to the fault analysis (see paragraph 60 above) will be considered in accordance with the principles of ALARP.

114. In my opinion, the RP has undertaken significant work to identify gaps in the approach to deterministic fault analysis at FCG3 and UK expectations of RGP, and to develop a programme of work to address these gaps. I consider that the intention to meet UK RGP and the consideration of international guidance (such as the approach to DEC-A

analysis) provides a good starting point for the demonstration that risks of operation of the UK HPR1000 will be ALARP.

115. I expect that the RP will use the results of its DBC analysis to provide context for the demonstration of ALARP, both for the general demonstration that UK RGP has been met and in the consideration of potential design changes. As the DBC analysis will aim to demonstrate adequate margins to relevant success criteria it can be used to judge the potential benefits of any identified changes to the design. The demonstration of ALARP will be a focus of my assessment during later stages of GDA, I intend to look for a demonstration that the design has been optimised and that margins to safety criteria are adequate.

4.8 Out of Scope Items

116. No items from my Step 2 assessment plan (Ref. 1) have been left outside the scope of my GDA Step 2 assessment of the UK HPR1000 Fault Studies.

4.9 Comparison with Standards, Guidance and Relevant Good Practice

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

- SAPs: I am satisfied that the RP has demonstrated an understanding of the expectations of the SAPs and is working towards the demonstration that they can be met. Table 1 provides further details.
- TAGs: I have considered the RP's submissions against the expectations of the TAGs described in Section 2.2. I am generally content that the submissions recognise these expectations and, that where there are differences between ONR's expectations and Chinese practice, these have been considered and additional work will be progressed.

4.10 Interactions with Other Regulators

118. ONR has formal information exchange agreements with a number of international nuclear safety regulators, and collaborates through the work of the IAEA and the Organisation for Economic Co-operation and Development Nuclear Energy Agency (OECD-NEA). This enables ONR to utilise overseas regulatory assessments of reactor technologies, where they are relevant to the UK. It also enables the sharing of regulatory assessment findings, which can expedite assessment and helps promote consistency.

119. During Step 2 a technology specific working group for the HPR1000 has been set up as part of the Multi-national Design Evaluation Programme (MDEP) of the OECD-NEA. I attended the first meeting of the MDEP HPR1000 Working Group on the 26 - 29 March 2018 in Beijing. The interactions included discussions on:

- Various design features for the HPR1000;
- Programme of key NNSA milestones for all HPR1000 reactors under construction in China;
- Design changes to FCG Units 3 & 4 and FQ Units 5 & 6 since the start of construction.

120. Of particular interest to Fault Studies is NNSA's use of confirmatory analysis of fault sequences and the regulatory assessment of active and passive safety systems. I will look to share information on these topics during future MDEP engagements in later GDA steps.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

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

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

- The RP has identified the UK requirement for robust, auditable fault identification and the need to demonstrate diverse protection against frequent faults.
- The RP needs to declare which suite of computer codes will be used for the UK HPR1000 analysis. I am however content that the RP will be able to present suitable transient analysis for reactor fault sequences, noting that the RP claims that the RP claims to have undertaken transient analysis for FCG3 with two sets of computer codes and that both demonstrate appropriate margins to relevant acceptance criteria, in line with Chinese regulatory requirements. This analysis will need to be reviewed against UK requirements.
- I am content that the RP understands the requirements for deterministic analysis of non-reactor faults and intend to produce a safety case for these aspects;
- The fault schedule template appears to be a sound basis for the RP to develop a suitable fault schedule which will contain the information expected by ONR's SAPs.
- The RP's approach to Categorisation and Classification is based upon guidance given in IAEA Safety Guide SSG-30, amended to recognise and address UK expectations.
- In Section 4 of this report I have reflected a number of potential shortfalls against regulatory expectations or areas of further work that is required by the RP to develop an adequate deterministic case. In many areas these have been identified by the RP as differences in approach to the assessment of potential faults between China and the UK. However I have no reason to believe that these areas cannot be addressed by the RP during GDA.
- I am satisfied that I have gained sufficient knowledge of the reactor design for my assessment during Step 2. This will develop through detailed assessment as GDA progresses.
- I have gained confidence from the submissions to date and the response to RQs that the RP understands the scope of further work that is required to develop adequate arguments and evidence later in GDA. The detailed examination of the quality and depth of these arguments and evidence will be the main part of my assessment in later stages of GDA.

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

5.2 Recommendations

124. 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 Fault Studies Assessment Plan for the UK HPR1000.

6 REFERENCES

1. *Generic Design Assessment of GNS's UK HPR1000 - Step 2 Assessment Plan for Fault Studies*, ONR-GDA-AP-17-010, Revision 0, ONR, November 2017. TRIM 2017/353800

2. *Preliminary Safety Report Chapter 2 General Plant Description*, HPR-GDA-PSR-0002, Rev. 000, GNS, 26 October 2017. TRIM Ref. 2017/401346.

   Preliminary Safety Report Chapter 4 General Safety and Design Principles, HPR-GDA-PSR-0004, Rev. 000, GNS, 26 October 2017. TRIM Ref. 2017/401351.

   Preliminary Safety Report Chapter 7 Safety Systems, HPR-GDA-PSR-0007, Rev. 000, GNS, 26 October 2017. TRIM Ref. 2017/401356.

   Preliminary Safety Report Chapter 12 Design Basis Conditions Analysis, HPR-GDA-PSR-0012, Rev. 000, GNS, 26 October 2017. TRIM Ref. 2017/401363.

   Preliminary Safety Report Chapter 13 Design Extension Conditions and Severe Accident Analysis, HPR-GDA-PSR-0013, Rev. 000, GNS, 26 October 2017. TRIM Ref.2017/401365.

   Preliminary Safety Report Chapter 14 Probabilistic Safety Assessment, HPR-GDA-PSR-0013, Rev. 000, GNS, 26 October 2017. TRIM Ref. 2017/401374.

   Preliminary Safety Report Chapter 23 Radioactive Waste Management & Fuel Storage, HPR-GDA-PSR-0013, Rev. 000, GNS, 26 October 2017. TRIM Ref. 2017/401394.

3. *Strategy Document for Fault Studies,* GH-X-00600-136-DRAF-02-TR, Rev. A, CGN, January 2018. TRIM Ref. 2018/24118.

4. *Methodology of PIE Identification,* GH-X-00100-008-DOZJ-03-GN, Rev D, CGN, May 2018. TRIM Ref. 2018/181952.

5. *Fault Schedule Production Methodology,* GH-X-00600-172-DRAF-02-GN, Rev B, CGN, June 2018. TRIM Ref. 2018/190525.

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

7. *UK HPR1000 – Regulatory Query (RQ) Tracking Sheet*, ONR, 2 November 2017. TRIM Ref. 2017/407871.

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

9. *Severe Accident Analysis Assessment Report,* ONR-GDA-UKHPR1000-AR-18-011, ONR, October 2018. TRIM Ref.2018/265777

10. *ONR HOW2 Guide Purpose and Scope of Permissioning*, NS-PER-GD-014 Revision 6, ONR, November 2016. http://www.onr.org.uk/operational/assessment/index.htm

11. ONR Technical Assessment Guides

    Transient Analysis for DBAs in Nuclear Reactors NS-TAST-GD-034, Revision 3, ONR, July 2016.
    Safety Systems NS-TAST-GD-003, Revision 8, ONR, March 2018.

Categorisation of Safety Functions and Classification of Structures, Systems and Components NS-TAST-GD-094, Revision 1, ONR, November 2015.
http://www.onr.org.uk/operational/tech_asst_guides/index.htm

12. IAEA guidance

International Atomic Energy Agency (IAEA) Safety Standards Series – Safety of Nuclear Power Plants: Design, Specific Safety Requirements, (SSR) 2/1, IAEA, 2012.

International Atomic Energy Agency (IAEA) Safety Standards Series – General Safety Requirements (GSR) Part 4: Safety Assessment for Facilities and Activities, IAEA, 2016.

International Atomic Energy Agency (IAEA) Safety Standards Series – Safety Classification of Structures, Systems and Components in Nuclear Power Plants Specific Safety Guide, No. SSG-30, IAEA, 2014.

www.iaea.org.

13. Western European Nuclear Regulators' Association.

Western European Nuclear Regulators' Association. Reactor Safety Reference Levels WENRA January 2008

Reactor Harmonization Working Group Report on Safety of new NPP designs, August 2013

WENRA statement on safety objectives for new nuclear power plants, November 2010

http://www.wenra.org/

14. *Pre-Construction Safety Report Chapter 4 General Safety and Design Principles,* GH-X-00620-004-KPGB-02-GN, Rev. B, GNS, February 2018. TRIM Ref.2018/105341.

Pre-Construction Safety Report Chapter 12 Design Basis Condition, GH-X-00620-012-KPGB-02GN, Rev. B, GNS, February 2018. TRIM Ref.2018/105328.

Pre-Construction Safety Report – Chapter 13 Design Extension Conditions and Severe Accident Analysis,GH-X-00620-013KPGB-02-GN, Rev. B, GNS, February 2018. TRIM Ref.2018/105325.

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. *Regulatory Observation (RO) Tracking Sheet,* ONR, 18 December 2017. TRIM Ref.2017/465031.

17. *ALARP Methodology,*GH-X-00100-051-DOZJ-03-GN, Rev. B, CGN, April 2018. TRIM Ref.2018/181415.

Table 1

Relevant Safety Assessment Principles Considered During the Assessment

SAP No and Title	Description	Interpretation	Comment
FA.1 Fault analysis: general Design basis analysis, PSA and severe accident analysis	Fault analysis should be carried out comprising suitable and sufficient design basis analysis, PSA and severe accident analysis to demonstrate that risks are ALARP.	This principle sets the general expectation for the range of fault analysis that should be carried out, and the role of this analysis in demonstrating that the risks are ALARP.	The RP has recognised the need for DBA, PSA and SAA within the UK HPR1000 safety case from the outset. How the DBA will be used to support the demonstration of ALARP will be a consideration during the later steps of GDA.
FA.2 Fault analysis: general Identification of initiating faults	Fault analysis should identify all initiating faults having the potential to lead to any person receiving a significant dose of radiation, or to a significant quantity of radioactive material escaping from its designated place of residence or confinement.	This principle sets the expectation that the RP should identify all potential faults and that the process should be systematic, auditable and comprehensive. The supporting text to this principle provides guidance on to the radiological consequences that should be considered when considering faults.	The RP has produced a methodology to provide a systematic, auditable and comprehensive process for the identification of faults to confirm and supplement those identified for FCG3. This methodology requires some development during GDA to ensure that all spurious C&I actuation faults, support system faults and worker faults are identified.
FA.3 Fault analysis: general Fault sequences	Fault sequences should be developed from the initiating faults and their potential consequences analysed.	This principle sets the expectation that fault sequences are developed and that there should be a clear relation between the sequences used in the DBA, the sequences in the PSA and the scenarios used in SAA.	The RP has presented principles for grouping the identified faults into DBCs (and also for grouping the faults for PSA). The PSR describes the assumptions that are made for the development of the DBCs that are subject to transient analysis.
FA.4 Fault analysis: design basis analysis 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.	This principle sets out the purpose of the DBA and the expectation that this is carried out as part of the engineering design.	The RP claims that the transient analysis of the DBCs demonstrates fault tolerance and that the relevant acceptance criteria are met for the identified faults. The assessment of the analysis that underpins this claim will be a major part of the later assessment steps of GDA.

SAP No and Title	Description	Interpretation	Comment
FA.5 Fault analysis: design basis analysis Initiating faults	The safety case should list all initiating faults that are included within the design basis analysis of the facility.	This principle and the supporting text set the criteria for which faults should be included within the DBA.	The DBC categories established by the RP include fault conditions to 1 x 10^{-5} per annum, consistent with the expectations of the SAPs. The list of DBCs for UK HPR1000 will be confirmed by the RP during GDA Step 3.
FA.6 Fault analysis: design basis analysis Fault sequences	For each initiating fault within the design basis, the relevant design basis fault sequences should be identified.	The supporting paragraphs to this principle detail the assumptions that should be made in the development of fault sequences in DBA. It also sets the expectation that fault sequences will be considered down to a frequency of 1 x 10^{-7} per annum.	DBC Analysis Methodology and Assumptions are presented in the PSR. The PCSR to be submitted at the start of Step 3 will contain the analysis of the DBCs and I will look for evidence that the design basis assumptions have been considered appropriately.
FA.7 Fault analysis: design basis analysis Consequences	Analysis of design basis fault sequences should use appropriate tools and techniques, and be performed on a conservative basis to demonstrate that consequences are ALARP.	The design basis analysis should use appropriate tools and techniques and should seek to demonstrate that the correct performance of the claimed safety systems ensure that the consequences of potential faults are acceptable.	The RP has not yet chosen which computer codes will be used for the DBA transient analysis. Information has been supplied on the potential codes and this information gives me confidence that suitable analysis can be presented at the start of Step 3.
FA.8 Fault analysis: design basis analysis Linking of initiating faults, fault sequences and safety measures	Linking of initiating faults, fault sequences and safety measures	This principle sets the expectation that the DBA should demonstrate that: all design basis initiating faults are addressed; that appropriate safety functions have been identified; that performance requirements for the safety measures have been identified and that suitable and sufficient safety measures are provided.	The RP has presented a methodology for the development of a fault schedule that will provide the links between the DBA and the engineering substantiation, and demonstrate that all faults have adequate safety measures.

SAP No and Title	Description	Interpretation	Comment
FA.9 Fault analysis: design basis analysis Further use of DBA	DBA should provide an input into the safety classification and the engineering requirements for systems, structures and components performing a safety function; the limits and conditions for safe operation; and the identification of requirements for operator actions.	This principle requires that the DBA is linked to the categorisation and classification scheme and that it provides the basis for performance requirements and safety settings for safety systems. It should also provide the basis for conditions governing permitted plant configurations and the availability of safety systems and safety-related equipment.	The RP has presented a scheme for the categorisation of safety functions and the classification of systems, structure and components.