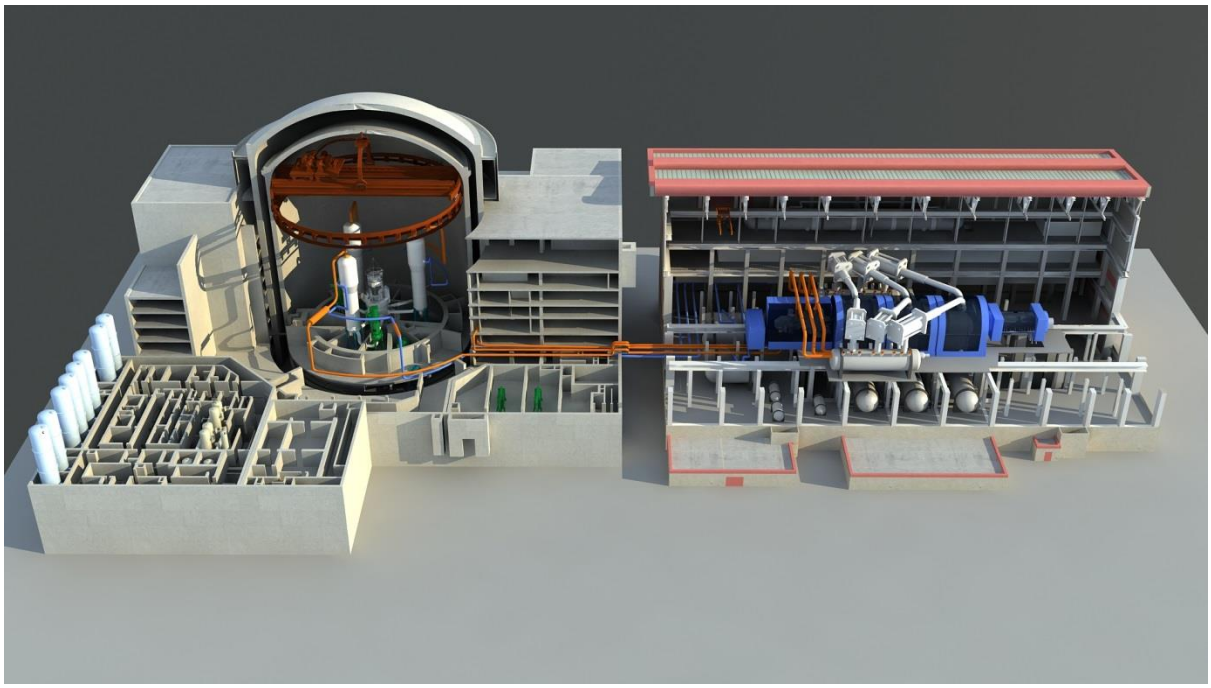
Office for Nuclear Regulation

New Reactor Division – Generic Design Assessment

Summary of the Step 3 Assessment of the UK HPR1000 Reactor



(Picture courtesy of CGN)

Assessment Report ONR-NR-AR-19-001
Revision 1
February 2020

Published 02/20

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

The mission of the Office for Nuclear Regulation (ONR) is to "provide efficient and effective regulation of the nuclear industry, holding it to account on behalf of the public". In the context of new nuclear build in the UK, regulation is initially undertaken via the Generic Design Assessment (GDA) process. ONR and the Environment Agency (EA) developed the GDA process in 2006 in order to allow the nuclear regulators to assess reactor designs on a 'generic' basis, i.e. before a site has been determined, or an operating organisation or prospective licensee has been proposed. In essence it considers the viability of reactor technologies ahead of any financial decisions or commencement of construction. This upfront process enables resolution of technical issues, and hence early identification of required design changes, which reduces regulatory uncertainty for developers.

GDA is a voluntary process and not a legal requirement of Great Britain's licensing regime for new power stations. However, the UK Government recognises that the approach is more efficient than the approach used prior to the existence of GDA and therefore expects reactor designers to follow the GDA process.

It is important to note that successful completion of GDA does not guarantee that regulatory permission will be granted to commence construction or operation of a new nuclear power plant. A prospective operator will have to obtain a nuclear site licence (NSL), and there is on-going regulation under the NSL throughout the life cycle of the plant.

To date, three reactor designs have been assessed under the GDA process and received Design Acceptance Confirmations (DAC) from ONR and Statements of Design Acceptability (SoDA) from the EA; the UK EPR™ received its DAC and SoDA in December 2012, the AP1000® in March 2017 and UK ABWR in December 2017. ONR's assessment reports on these technologies are published on the GDA joint regulators website.

In January 2017 the UK Government formally asked ONR and EA to begin the GDA of the UK HPR1000. The UK HPR1000 is a reactor design proposed for deployment at Bradwell-on-Sea, Essex. General Nuclear System Limited is a UK-registered company that was established to implement the GDA on the UK HPR1000 reactor on behalf of three joint requesting parties (RP), i.e. China General Nuclear Power Corporation (CGN), EDF SA and General Nuclear International (GNI).

The GDA process calls for a step-wise assessment of the RP's safety and security submissions with the assessments increasing in detail as the project progresses. The preparatory step, Step 1, of the UK HPR1000 GDA commenced in January 2017 and finished in November 2017. Technical assessment of the design commenced at the start of Step 2 of GDA in November 2017 and was focused on understanding and assessing the fundamental safety and security claims, and acceptability, of the UK HPR1000 within the UK regulatory regime. Step 2 of GDA finished in November 2018 and marked the commencement of Step 3 of GDA, which continued the assessment work of the previous step with increased emphasis on the arguments that underpin the safety and security claims. This is ONR's third report on the UK HPR1000 design and it summarises the progress made with our assessment during the 15 month duration of Step 3.

Overall, the interactions with the RP throughout Step 3 have been constructive. Its organisational arrangements have matured during this step, with clear evidence of General Nuclear System Limited, CGN, and EDF SA capturing, and acting upon, learning from Step 2. Working arrangements have generally become embedded and coordination between the three organisations has improved. The structure and organisation of the HPR1000 GDA RP is complex and some organisational issues still remain, such as lack of agility in decision-making mechanisms. However, we have seen strong commitment from General Nuclear

System Limited, CGN and EDF SA to learn lessons from Steps 1, 2 and 3 of GDA and to improve their working arrangements in the final step of GDA. We expect to see the increased involvement of the Bradwell Power Generation Company, the prospective future licensee for the Bradwell B Nuclear Power Plant, during Step 4.

During Step 3 of GDA we have undertaken assessment work across 19 technical disciplines and we have also covered topics of a cross-cutting nature. Our assessment conducted to date has not identified any fundamental safety or security shortfalls that might prevent the issue of a DAC for the UK HPR1000 design. We have however identified a number of potential regulatory shortfalls and have raised Regulatory Observations to address those.

There is a considerable amount of work to be undertaken by the RP going forward, requiring significant resource across all of the topic areas. ONR will continue to rigorously assess the safety and security submissions throughout Step 4 of GDA, and will address potential issues should they arise.

LIST OF ABBREVIATIONS

AD	Automatic Diagnosis
ALARP	As Low As Reasonably Practicable
ARN	(Argentina's) Autoridad Regulatoria Nuclear
AoF	Allocation of Function
BAT	Best Available Techniques
BEIS	Department for Business, Energy and Industrial Strategy
BSI	British Standards Institution
BSL	Basic Safety Level (in SAPs)
BSO	Basic Safety Objective (in SAPs)
C&I	Control and Instrumentation
CAE	Claims-Arguments-Evidence
CBSIS	Computer Based Systems Important to Safety
CCF	Common Cause Failure
CDM	Construction, Design and Management
CGN	China General Nuclear Power Corporation Ltd
CoO	Concept of Operations
COMAH	Control of Major Accident Hazards
CSRA	Cyber Security Risk Assessment
DAC	Design Acceptance Confirmation
DBA	Design Basis Analysis
DBC	Design Basis Condition
DCH	Direct Containment Heating
DEC	Design Extension Condition
DG	Diesel Generator
DMGL	Delivery Management Group Lead
DNB	Departure from Nucleate Boiling
DRR	Design Risk Register
DRP	Design Reference Point
EA	Environment Agency
EBA	Enriched Boric Acid
ECC	Emergency Control Centre
EDG	Emergency Diesel Generator
EMI	Electromagnetic Interference
EMIT	Examination. Maintenance, Inspection and Testing
ENIQ	European Network for Inspection and Qualification
FA	Fuel Assembly

FEA	Finite Element Analysis
FR	Fuel Rod
GDA	Generic Design Assessment
GNI	General Nuclear International Ltd
GSR	Generic Security Report
HBSC	Human Based Safety Claims
HF	Human Factors
HFI	Human Factors Integration
HIC	High Integrity Component
HLW	High-Level Waste
HMI	Human-Machine Interface
HPR1000WG	HPR1000 Design Specific Working Group (within MDEP)
HRA	Human Reliability Analysis
HSBC	Human Based Safety Claims
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
ICIA	In-Core Instrumentation Assembly
iDAC	Interim Design Acceptance Confirmation
IDT	Integrated Delivery Tool
IE	Initiating Event
ILW	Intermediate Level Waste
ISF	Interim Storage Facility
ISO	International Organisation for Standardisation
IVR	In-vessel Retention
IWS	Integrated Waste Strategy
JPO	(Regulators') Joint Programme Office
KDS [DAS]	Diverse Actuation System
LLW	Low Level Waste
MCR	Main Control Room
MCCI	Molten Core Concrete Interaction
MDEP	Multinational Design Evaluation Programme (within OECD-NEA)
MDSL	Master Document Submission List
MSQA	Management for Safety and Quality Assurance
MW	Megawatts
NDT	Non-Destructive Testing
NEA	Nuclear Energy Agency (within OECD)
NNR	(South Africa's) National Nuclear Regulator

NNSA	National Nuclear Safety Administration
NPP	Nuclear Power Plant
NSL	Nuclear Site Licence
NT	Numerical Target
OECD	Organisation for Economic Cooperation and Development
ONR	Office for Nuclear Regulation
OpEx	Operational Experience
PCD	Project Correspondent Department
PCER	Pre-construction Environmental Report
PCI	Pellet-Cladding Interaction
PCMI	Pellet-Cladding Mechanical Interaction
PCSR	Pre-construction Safety Report
PIE	Postulated Initiating Event
PSA	Probabilistic Safety Analysis
PSAS	Plant Standard Automation System
PSR	Preliminary Safety Report (includes security and environment)
PTI	Project Technical Inspector
PWR	Pressurised Water Reactor
QA	Quality Assurance
RCCA	Rod Cluster Control Assembly
RCP	Reactor Coolant Pump
RGP	Relevant Good Practice
RHWG	Reactor Harmonization Working Group (of WENRA)
RI	Regulatory Issue
RMI	Reflective Metal Insulation
RO	Regulatory Observation
RP	Requesting Party
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RSS	Remote Shutdown Station
RQ	Regulatory Query
SAA	Severe Accident Analysis
SAP(s)	Safety Assessment Principle(s)
SBO	Station Blackout
SDM	System Design Manual
SFAIRP	So Far As Is Reasonably Practicable

SFIS	Spent Fuel Interim Storage
SFP	Spent Fuel Pool
SFR	Safety Functional Requirement
SG	Steam Generator
SoDA	(Environment Agency's) Statement of Design Acceptability
SQEP	Suitably Qualified and Experienced Personnel
SSC	Structures, Systems and Components
SyAP(s)	Security Assessment Principle(s)
TAG	Technical Assessment Guide(s)
TAD	Target Audience Description
TESG	Technical Expert Subgroup
WENRA	Western European Nuclear Regulators' Association
V&V	Verification and Validation

TABLE OF CONTENTS

1 CONTEXT OF THIS ASSESSMENT REPORT 10
2 BACKGROUND 10
3 INTRODUCTION 11
4 ASSESSMENT STRATEGY 13
5 ASSESSMENT STANDARDS 14
6 MAIN FEATURES OF THE DESIGN AND SAFETY SYSTEMS 15
6.1 General Description 15
6.2 Safety Systems 17
6.3 ONR's Familiarity with the Technology Used in UK HPR1000 18
7 THE GDA REQUESTING PARTY 18
7.1 Organisation 18
7.2 Interactions with the Requesting Party 19
8 COLLABORATION WITH OVERSEAS REGULATORS 19
9 GDA COMMENTS PROCESS 21
10 SUMMARY OF ONR'S ASSESSMENT OUTCOMES 21
10.1 Chemistry 22
10.2 Civil Engineering 24
10.3 Control and Instrumentation 25
10.4 Conventional Fire Safety 28
10.5 Conventional Health and Safety 29
10.6 Electrical Engineering 30
10.7 External Hazards 32
10.8 Fault Studies 34
10.9 Fuel and Core 36
10.10 Human Factors 38
10.11 Internal Hazards 40
10.12 Management for Safety and Quality Assurance 43
10.13 Mechanical Engineering 45
10.14 Probabilistic Safety Analysis 47
10.15 Radiological Protection 49
10.16 Radioactive Waste Management, Decommissioning and Spent Fuel Management . 51
10.17 Security 55
10.18 Severe Accident Analysis 57
10.19 Structural Integrity 59
10.20 Cross-Cutting Topics 61
11 CONCLUSIONS 64
12 REFERENCES 66

Annexes

Annex 1: Step 3: Overall Design, Safety Case and Security Arguments Review
Annex 2: Regulatory Observations Issued

1 CONTEXT OF THIS ASSESSMENT REPORT

1. In November 2018 the Office for Nuclear Regulation (ONR) and the Environment Agency (EA) announced that we were progressing to Step 3 of the Generic Design Assessment (GDA) of the UK HPR1000 reactor.

2. During the last 15 months ONR has undertaken assessment across 19 technical disciplines.

3. Noting that the regulators will only progress to Step 4 of the GDA following satisfactory outcomes from a series of readiness reviews undertaken by the regulators and the GDA Requesting Party (RP), this assessment report has been prepared as an input to ONR's decision on whether to progress to Step 4 of the UK HPR1000 GDA.

2 BACKGROUND

4. In 2005 the UK Government requested the nuclear regulators to develop a new design assessment process in preparation for anticipated applications for new reactor construction in the UK. In response to this request ONR and EA developed the GDA process in 2006. GDA allows the nuclear regulators to assess reactor designs on a 'generic' basis, i.e. before a site has been determined, or an operating organisation or prospective licensee has been proposed. In essence it considers the viability of reactor technologies ahead of any financial decisions or commencement of construction. This upfront process enables resolution of technical issues, and hence early identification of required design changes, which reduces regulatory uncertainty for developers.

5. It is important to note that GDA is a voluntary process and not a legal requirement of Great Britain's licensing regime for new power stations. However, the UK Government recognises that the approach is more efficient than the approach used prior to the existence of GDA and therefore expects reactor designers to follow the GDA process.

6. Three reactor designs have been assessed under the GDA process and received Design Acceptance Confirmations (DAC) from ONR and Statements of Design Acceptability (SoDA) from the EA; the UK EPR™ received its DAC and SoDA in December 2012, the AP1000® in March 2017 and UK ABWR in December 2017.

7. In October 2016 General Nuclear System Limited wrote to ONR and the EA requesting entry to the GDA process for the UK HPR1000 reactor design (Chinese Hualong technology). ONR and the EA considered the request and concluded that the project appeared viable and warranted the deployment of regulatory resource (Ref. 1). In January 2017 the Government formally asked ONR and the EA to begin the GDA of the UK HPR1000 (Ref. 2). The UK HPR1000 is a reactor design proposed for construction on the Bradwell-on-Sea site in Essex.

8. General Nuclear System Limited is a UK-registered company that was established to implement the GDA of the UK HPR1000 reactor on behalf of three joint requesting parties, i.e. China General Nuclear Power Corporation (CGN), EDF SA and General Nuclear International (GNI). Although for practical purposes we have often referred to General Nuclear System Limited as the UK HPR1000 GDA RP, it is important for the reader of this report to have a clear understanding of the actual composition and identity of the UK HPR1000 GDA RP.

9. During Step 1 of the UK HPR1000 GDA the RP set up its project management and technical teams and arrangements for GDA, and prepared submissions for Step 2, including the Preliminary Safety, Security, and Environmental Report (PSR). The RP also established a UK HPR1000 website (Ref. 3) containing the PSR and the means for the public to raise comments. The RP completed Step 1 of the GDA process in November 2017 and we immediately began the technical assessment work – Step 2 of GDA.

10. During Step 2, we focused on understanding and assessing the fundamental safety and security claims, and acceptability, of the UK HPR1000 within the UK regulatory regime. Our assessment (Ref. 4) did not identify any fundamental safety or security shortfalls that might prevent the issue of a DAC for the UK HPR1000 design, and so we commenced Step 3 in November 2018.

3 INTRODUCTION

11. The GDA process calls for a step-wise assessment of the RP's safety and security submissions with the assessments increasing in detail as the project progresses.

12. Step 1 of the UK HPR1000 GDA commenced in January 2017 and finished in November 2017. Step 1 of GDA is the preparatory step and ONR did not undertake any technical assessment, however, the regulators did engage with the RP to ensure that regulatory expectations were understood. Thus, during Step 1 of the UK HPR1000 GDA ONR held extensive discussions with the RP (including technical discussions both in the UK and in China) to enable the RP's understanding of the requirements and processes that would be applied, and for our inspectors to start familiarising themselves with the HPR1000 technology. In November 2017 we announced on our website that we were progressing to Step 2 of the UK HPR1000 GDA (Ref. 5).

13. Step 2 of the UK HPR1000 GDA commenced in November 2017 and marked the commencement of technical assessment. This step was focused on understanding and assessing the fundamental safety and security claims, and the acceptability of the UK HPR1000 within the UK regulatory regime. Safety and security claims, or assertions, are those statements that describe the design and explain why the facility is safe and secure; they are normally presented within the Preliminary Safety Report (PSR) and its supporting references. Step 2 ended in November 2018 and culminated in the production of a summary assessment report (Ref. 4), underpinned by 19 technical assessment reports which were published on our joint regulators' GDA website (Ref. 6). The assessment did not identify any fundamental safety or security issues that might prevent the issue of a DAC.

14. During Step 3 ONR has increased its regulatory scrutiny and undertaken a more detailed assessment of the design focusing on the methods and approaches used by the RP to meet the safety and security claims. Step 3 is primarily a review by ONR of the arguments (or 'reasoning') supporting the RP's claims regarding the safety and security related aspects of the proposed design.

15. The intention in this step was to move from the fundamentals of the previous step to an appraisal of the design, including at a system level, and by assessment of the RP's arguments that support the safety and security claims.

16. The specific aims of this step were to:

- improve ONR's knowledge of the design;
- assess the safety and security arguments;

- progress the resolution of issues identified during Step 2;
- identify whether any significant design or safety case changes may be needed;
- identify major issues that may prevent ONR issuing a DAC and attempt to resolve them; and thereby
- achieve a significant reduction in regulatory uncertainty.

17. The safety and security cases are summarised within the (generic) Pre-construction Safety Report (PCSR), and Generic Security Report (GSR) which are published on the RP's website (Ref. 3).

18. During Step 4 of GDA ONR conducts in-depth assessment of the evidence presented by the RP to support and form the basis of the safety and security cases. At the end of Step 4 ONR judges whether a DAC should be issued for the design. If there are generic technical issues that remain outstanding, and depending on their significance, ONR may issue an interim DAC (iDAC), or may judge that neither a DAC, nor an iDAC, are warranted. ONR publishes its Step 4 assessment reports and a summary assessment report on our joint regulators' GDA website (Ref. 6). The RP's target duration for Step 4 of the UK HPR1000 GDA is 23 months.

19. It is important to note that successful completion of GDA does not guarantee that regulatory permission will be granted to commence construction or operation of a new nuclear power plant. A prospective operator will have to obtain a nuclear site licence (NSL), and there is on-going regulation under the NSL throughout the life cycle of the plant. In particular, a licensee will require ONR's formal consent before nuclear safety related construction can commence, for which it will need to develop and submit for regulatory assessment a site specific pre-construction safety case and a site security plan and demonstrate compliance in accordance with Nuclear Industry Security Regulations 2003 (as amended) (Ref. 8). To enable these processes, our regulatory philosophy is that after obtaining a DAC, the RP should transfer the outputs from the GDA (including arrangements for ensuring and assuring that safety and security claims and assumptions will be realised in the final as-built design, and arrangements for moving the safety case to the operating regime), to the licensee to be used to support the development of the site specific safety case and the site security plan. ONR's assessment, ahead of permissioning the start of nuclear safety related construction under the NSL, will then focus on site-specific and licensee-specific aspects, any modifications to the design since the DAC was issued, and/or further developments of the design, rather than conducting a full reassessment of the design and safety and security cases.

20. In addition, we encourage RPs to seek involvement of prospective licensees in GDA to ensure that operational considerations are included in the development of the safety and security cases, and to commence transfer of knowledge regarding the design and safety and security cases to the future operator. A prospective licensee would also use information coming from GDA to develop the site suitability justification, which is an essential part of the NSL application dossier.

21. It is relevant to note, and the readers of this report may be aware, that as part of our continuous improvement, in 2018/19 ONR made modifications to the GDA process taking account of learning from previous and on-going GDAs and by introducing greater flexibility to better support future assessments of Small Modular Reactors and other Advanced Nuclear Technologies. New GDA Guidance to RPs reflecting the modernised process was published in October 2019 (Ref. 9). It is important to clarify that the modernised process and new guidance are not being, and will not be,

applied to the UK HPR1000 GDA, which from its inception followed the extant GDA Guidance in Ref. 10.

4 ASSESSMENT STRATEGY

22. ONR's assessment of the RP's Step 3 safety and security submissions has been undertaken by specialist inspectors covering 19 technical disciplines. During Step 3 of GDA the inspectors working on the 19 topic areas were distributed in three groups reporting to three delivery management group leads (DMGLs) who have coordinated the assessments and provided strategic oversight.

23. The GDA project technical inspector (PTI) is responsible for leading the assessment of the RP's arrangements for developing the safety and security cases and also for matters of a cross-cutting nature, which impact all disciplines and require coordination to ensure a consistent approach.

24. The DMGLs and PTI report to ONR's Head of HPR1000 Regulation who leads the regulatory activities related to HPR1000 within ONR's New Reactors Division.

25. ONR undertook thorough preparations for Step 3 during Step 2 of the GDA. As part of these preparations ONR's inspectors developed Step 3 assessment plans for their own disciplines. The objective of developing assessment plans was to provide a consistent assessment framework across all technical areas. Each assessment plan:

- Outlined the specific aspects on which the inspector would focus assessment during Step 3.
- Identified the assessment standards that would be used.
- Identified the key documentation that the RP had planned to provide to supplement the specific chapter(s) of the PCSR to serve as the basis for ONR's assessment.
- Delineated the Step 3 timeline tailored for each specific area, including planned activity that would enable timely completion and documentation of the assessment in each technical area (eg, meetings and workshops with the RP's specialists, or the Management for Safety and Quality Assurance (MSQA) Step 3 inspections, as appropriate).

The Step 3 assessment plans were shared with the RP to provide transparency.

26. Technical oversight and assurance throughout Step 3 have been provided by ONR's Professional Leads.

27. During our assessment we use standard GDA tools to request further information or raise shortfalls; these are:

- Regulatory Queries (RQ). RQs are raised to request clarification and additional information and are not necessarily indicative of any perceived shortfall.
- Regulatory Observations (RO). ROs are raised when we identify potential regulatory shortfalls requiring action and new work by the RP for them to be resolved.
- Regulatory Issues (RI). RIs are raised when we identify serious regulatory shortfalls which have the potential to prevent provision of a DAC, and require action and new work by the RP for them to be resolved.

28. ONR works closely and coordinates its assessment activities with the EA which considers the environmental acceptability of the design. In particular, in Step 3 we

have worked jointly with EA in the area of MSQA and we have maintained very close coordination in the areas of Radioactive Waste Management, Decommissioning and Spent Fuel Management. The EA reports its findings from GDA separately on its website (Ref. 11).

5 ASSESSMENT STANDARDS

29. ONR expects new nuclear reactors to be robust facilities that are designed to provide protection against those faults and hazards which, if inadequately controlled, could give rise to societal consequences and serious radiological health effects to workers and the public. In order to demonstrate this, a GDA RP will need to develop and provide for ONR's assessment, generic safety and security cases. As indicated above, the UK HPR1000 GDA RP has provided, for regulatory assessment during Step 3, safety and security cases in the form of PCSR and GSR with numerous associated references.

30. The overriding legal requirement for any nuclear facility proposed for construction in Great Britain is that the level of risk is demonstrated to be as low as reasonably practicable (ALARP). In simple terms ALARP is a requirement to take all measures to reduce risk where it is reasonable to do so. Often, this is not done through explicit comparisons of costs and benefits, but rather by applying established relevant good practice (RGP).

31. We expect the RP's ALARP demonstration to consider first and foremost the factors related to engineering, operations and the management of safety, which constitute RGP. Sources of RGP include Approved Codes of Practice and standards produced by organisations such as the British Standards Institution (BSI), the International Organisation for Standardisation (ISO), or the International Atomic Energy Agency (IAEA), as well as the safety reference levels developed by the Western European Nuclear Regulators Association (WENRA). Well defined established standard practice adopted by an industrial sector can also be considered RGP. ONR's guidance including our Safety Assessment Principles (SAPs) (Ref. 12) and Technical Assessment Guides (TAGs) (Ref. 13) inform our view of RGP.

32. For the overall demonstration that the level of risk is ALARP, within GDA we expect the RP's safety case to address four key aspects (Refs 14 and 15):

- The rationale for the evolution of the proposed design from its forerunners and how a safer design was achieved.
- How RGP has been incorporated into all aspects of the design.
- Use of risk assessment to identify potential engineering and/or operational improvements in addition to confirming the numerical levels of safety achieved.
- A clear conclusion that there are no further reasonably practicable improvements that could be implemented, and therefore the level of risk has been reduced to ALARP. The RP should therefore implement measures to the point where the costs of any additional measures (in terms of money, time or trouble) would be grossly disproportionate to the further risk reduction that would be achieved.

33. During Step 2 of GDA the RP provided its approach to ALARP, i.e. a description of the process which has been adopted to ensure that the risks to human health arising from the operation of a power station based on the proposed design are reduced to ALARP. Step 3 has been focussed on the adequacy of the implementation of these arrangements, determining whether ALARP arguments are suitable and sufficient.

34. Our inspectors use ONR's SAPs (Ref. 12) and Security Assessment Principles (SyAPs) (Ref. 16) as the primary guidance for their assessment. The SAPs and SyAPs provide a framework for consistent regulatory judgements on the acceptability of the RP's safety and security cases. The SAPs also include numerical targets, including basic safety levels (BSL) and basic safety objectives (BSO), to be used by inspectors as an aid to judgement when considering whether radiological hazards are being adequately controlled and risks reduced to ALARP. However, it is important that the RP understands that neither the SAPs nor the SyAPs are intended, or sufficient, to be used as design standards.

35. Both the SAPs and the SyAPs are consistent with IAEA standards and guidance, and are supported by more detailed TAGs (Ref. 13).

36. Our expectations for GDA are detailed in ONR's GDA Guidance to RPs (Ref. 10). For clarity, the requirements for Step 3 of GDA are repeated in Annex 1 of this report.

6 MAIN FEATURES OF THE DESIGN AND SAFETY SYSTEMS

6.1 General Description

37. The HPR1000 technology is described in the UK HPR1000 PCSR (Ref 7). The UK HPR1000 is a pressurised water reactor (PWR) designed by CGN using the Chinese Hualong technology. Its electric output is approximately 1180MW.

38. The UK HPR1000 has evolved from a sequence of reactors which have been constructed and operated in China since the late 80s, including the M310 design used at Daya Bay and Ling'ao (Units 1 and 2), the CPR1000, the CPR1000^{+} and the more recent ACPR1000. The first two units of CGN's HPR1000, Fangchenggang Nuclear Power Plant (NPP) Units 3 and 4, are under construction in China. Fangchenggang NPP Unit 3 is the reference plant for the UK HPR1000. Ref. 3 indicates that the UK HPR1000 is designed to have a lifetime of at least 60 years.

39. The UK HPR1000 is a three-loop PWR. Each loop consists of primary pipes going in and out of the reactor pressure vessel (RPV) (referred to as cold and hot leg respectively), one reactor coolant pump (RCP) in the cold leg, and one steam generator (SG). One of the loops contains a pressuriser connected to the hot leg. The pressuriser is a vertical vessel the function of which is to maintain high pressure within the primary reactor circuit and to avoid boiling of the reactor coolant. The operational pressure of the primary circuit is 15.5 MPa abs, which is equivalent to approximately 150 times the atmospheric pressure.

40. Light water is used as coolant to extract the heat from the reactor. This water is also necessary to maintain the nuclear reaction in the core. Hot water from the reactor moves along the hot legs and enters the primary side of each SG (bottom plenum first and then the tubes) where it transfers the heat to the water, at much lower pressure in the secondary side of the SGs, and produces steam. The primary coolant leaving the SGs, which is now at lower temperature, is then pumped back into the reactor via the cold legs. The steam produced in the SGs drives a turbine that, ultimately, via a generator produces electricity.

41. The RPV is a cylindrical steel vessel designed to withstand high temperatures and pressures. The RP's documentation indicates that the number of welds between parts of the RPV is minimised as far as possible. The RPV hemispherical upper head is removable to allow refuelling of the reactor every 18 months. The RPV houses the reactor core and in-core instrumentation, and the reactor internals. The reactor core is made up of 177 fuel assemblies and 68 control rod assemblies; each fuel

assembly contains 264 fuel rods, 24 guide tubes and one gauge pipe arranged 17x17. Each fuel rod consists of a metallic cladding made of a zirconium alloy housing the nuclear fuel, which is in the form of small ceramic pellets, made of uranium dioxide, stacked up inside the cladding.

42. The reactor building houses key equipment such as the RPV, RCPs, SGs, pressuriser, primary and secondary circuit piping and the safety injection system accumulators. The reactor building is based on a double-walled containment with large free volume. There is ventilation in the annulus between the two walls to reduce the risk of uncontrolled radioactive releases to the environment in case of accidents. A large tank of water located inside the containment (in-containment refuelling water storage tank) provides the source water for the low and medium head safety injection systems.

43. Three safeguard buildings adjacent to the reactor building house key safety systems. The main control room is located in one of the safeguard buildings. The fuel building is also adjacent to the reactor. It contains the fuel handling and short term storage facilities.

44. The UK HPR1000 PCSR (Ref. 7) indicates that the reactor building, the fuel building and all three safeguard buildings are designed using the EUR spectra to withstand an earthquake of magnitude 0.3g. The PCSR also indicates that the containment, the fuel building and one of the safeguard buildings are resistant to the crash of a large commercial aircraft. The containment building, safeguard buildings, fuel building and nuclear auxiliary building are key facilities in the area generally referred to as the nuclear island (Figure 1). The turbine building is the central part of the so called conventional island.

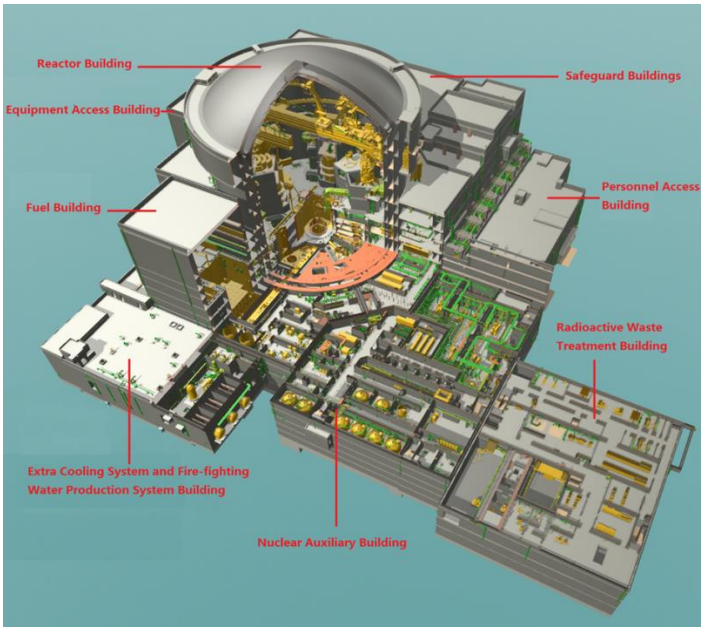


Figure 1: Nuclear Island
(Picture courtesy of CGN)

6.2 Safety Systems

45. In case of events that take the reactor out of its normal operating regime there are safety systems to shutdown the reactor and maintain it in a shutdown state, to cool down the reactor and to prevent the release of radioactive material, i.e. to take the reactor to a safe and stable condition. Brief introductions to the UK HPR1000 safety systems can be found in chapter 2 of the PCSR (Ref. 7) and are described in more detail in chapter 7, and therefore, not repeated here. It is however worth highlighting a few key features related to the safety of the UK HPR1000.

46. The design philosophy underpinning the UK HPR1000 reactor cooling safety function is based on three independent trains of engineered safety features physically separated in the three safeguard buildings discussed above. This arrangement offers 3x100% redundancy. Each safeguard building houses:

- One train of the (motor-pump driven) emergency feedwater system to feed water into the SGs in case of loss of normal feedwater.
- One train of the safety injection system. The safety injection system has three sub-systems, ie, the low head safety injection (also used for residual heat removal during normal shutdown), the medium head safety injection, and the accumulators (note that the accumulators are located inside the reactor building).

47. Although the safety philosophy for the UK HPR1000 is mainly based on active systems, the UK HPR1000 includes additional passive features of importance to safety. These are the passive secondary residual heat removal system, and the passive reactor cavity injection system:

- The passive secondary residual heat removal system has been designed to remove heat from the SGs (and thus from the reactor) in the event of complete loss of both normal and emergency feedwater. It consists of a large water tank located surrounding the upper part of the outer containment wall, and associated piping and connections to the SGs. It is designed to condense the steam from the SGs using natural circulation, in the event of total loss of normal and emergency feedwater. (See Figure 2)
- The passive reactor cavity injection system supports the in-vessel retention function.

It is worth noting that the accumulators in the safety injection system, which have also been a safety feature in PWRs of previous generations, are passive as well.

48. It is important to mention that, for the UK HPR1000, the design choice to manage severe accident scenarios where there is core degradation is based on retention of the molten debris inside the RPV via engineered means to externally flood the RPV. This strategy is called in-vessel retention (IVR).

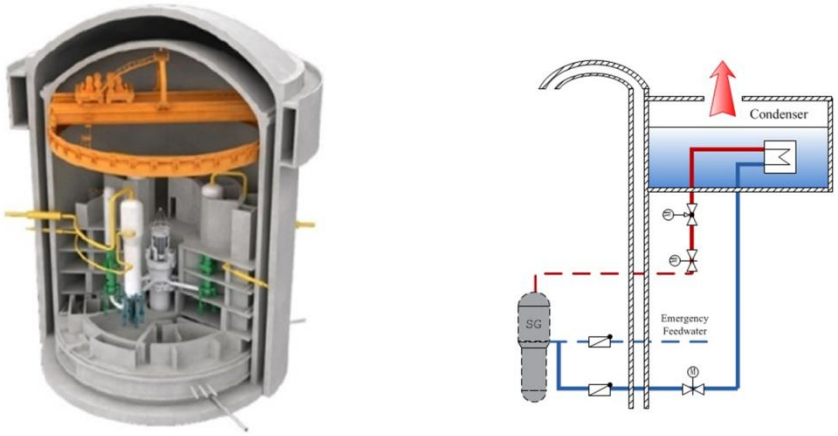


Figure 2: Secondary Passive Residual Heat Removal System
(Pictures courtesy of CGN)

6.3 ONR's Familiarity with the Technology Used in UK HPR1000

ONR has extensive experience assessing PWR designs and is therefore familiar with the technologies presented. Our knowledge of the design has been further increased during Step 3, achieving one of the key objectives of Step 3. Our assessment, while addressing all aspects of the design, is paying particular attention to the safety aspects that are unique to the UK HPR1000, such as the passive secondary heat removal system and how its effectiveness is demonstrated by the RP.

7 THE GDA REQUESTING PARTY

7.1 Organisation

49. CGN and EDF SA created General Nuclear System Limited as a joint venture company to undertake the GDA for the UK HPR1000 reactor. General Nuclear System Limited is owned by GNI (66.5%) and EDF Energy Holdings Limited (33.5%), the UK subsidiaries of CGN and EDF SA respectively. General Nuclear System Limited acts on behalf of the three joint requesting parties, CGN, EDF SA and GNI. For practical purposes we have referred to General Nuclear System Limited as the RP. However, our understanding of General Nuclear System Limited's role has become clearer over the duration of these steps. This is discussed hereafter.

50. General Nuclear System Limited is supported by its parent organisations, which have defined their roles in the PCSR (Ref. 7):

- CGN is the 'designer', responsible for undertaking technical aspects of the design and adaptation of the Hualong technology into the UK HPR1000 whilst considering UK context. Production of safety and environmental GDA submissions is primarily performed by CGN with support from EDF SA.
- EDF SA provides technical expertise to support the UK HPR1000 GDA project. This includes reviewing technical documentation, providing experience of constructing and operating plants in France and the UK, as well as the knowledge of international good practice applied to the existing nuclear fleet and in past GDA projects, in particular the UK EPR™ GDA.

51. In instances where the UK context is particularly relevant (for example in the production of security submissions), the RP recognises that wider collaborative effort is required. Where appropriate, General Nuclear System Limited is supported by third party contract partners, based on their technical competencies relevant to the project.

52. It is important to summarise, and note, that while CGN and EDF SA are two of the parties requesting the GDA, they are also formal service providers to General Nuclear System Limited, making the structure of, and logistics within, the RP complex. This is discussed further below.

7.2 Interactions with the Requesting Party

53. CGN and EDF SA bring a wealth of experience to the UK HPR1000 GDA both as designers and operators of nuclear power stations. During our interactions with both organisations we have observed on multiple occasions the extensive technical expertise that resides within both organisations. Therefore, the partnership between these organisations brings important benefits to the GDA, particularly when considering the knowledge of the UK regulatory environment that EDF SA can offer.

54. The RP's arrangements have matured during this step, with clear evidence of General Nuclear System Limited, CGN, and EDF SA capturing and acting upon learning from Step 2. Procedures have generally become embedded and coordination between the three organisations has improved. However, the structure and organisation of the UK HPR1000 GDA RP is complex and some organisational issues still remain, such as lack of agility in decision-making mechanisms. Section 10.12 discusses organisational matters further.

55. Early in Step 3, the RP made the decision to change the UK HPR1000 fuel from a Chinese to a Framatome design. This may simplify ONR's assessment of the safety case for this fuel because of our familiarity with it, but the impact on the RP's submission programme was substantial and required a high level of communication and negotiation to ensure that deliverables will be available for assessment during acceptable GDA timescales. We recognise the amount of effort that the RP expended to achieve this position and it underpins the improvement in the coordination between the organisations involved.

56. We have found the RP to be willing to engage with ONR and have had a high level of technical engagement across all assessment topics. We have also had the opportunity to engage directly with CGN's design teams in China. Our interactions have also included informative visits to several Chinese NPPs and a range of research and manufacturing facilities that support the Chinese nuclear power industry.

57. During previous GDAs, RPs whose design teams are based overseas found it a challenge to understand some requirements that are specific to the UK regulatory regime; CGN has also recognised some of these challenges in its understanding of ALARP and UK safety cases (as discussed in Section 10.20). However, we have found CGN to be highly receptive to guidance from ONR, often with resulting improvements in submissions. CGN may need to increase the input of expert advice from those with UK context experience in Step 4 in order to ensure that its safety case will meet regulatory expectations.

8 COLLABORATION WITH OVERSEAS REGULATORS

58. ONR considers international cooperation important for successful delivery of regulation of new reactors. Thus, in our GDA projects, we seek and welcome

opportunities for collaboration with overseas regulators dealing with the same reactor designs.

59. When assessing new reactors we aim to take into account international good practice, international standards and the assessment undertaken by overseas regulators, and we also aim to work with overseas regulators to benefit from their work and experience where appropriate.

60. It is important to stress, however, that any cooperation with other nuclear regulators does not replace ONR conducting our own independent assessment, but can help to supplement it with additional valuable information and insights, making our own work more efficient. The benefits of this international collaboration include obtaining access to independent analyses and audits, sharing of technical opinion, early insights into construction and commissioning issues and promotion of a more consistent and harmonised international approach.

61. UK HPR1000 uses Chinese Hualong technology. The reference plant for the UK HPR1000 is Fangchenggang NPP Unit 3, which is under construction in China. Therefore establishing and maintaining collaboration with the Chinese nuclear regulator, the National Nuclear Safety Administration (NNSA) was, and is, a priority for ONR in the UK HPR1000 GDA.

62. In September 2017 NNSA and ONR / EA launched a bilateral China / UK regulatory working group with two key objectives:

- To share information and experience.
- To identify opportunities for joint visits and inspections.

63. A two-year work plan was established based on bilateral workshops covering the following topics:

- Safety review standards – held in September 2018.
- UK / China civil nuclear security requirements – held in September 2018.
- Safety analysis for HPR1000 – held in March 2019.
- Environmental assessment and radioactive waste management – held in November 2019.

64. The senior bilateral steering group held its third annual meeting in the UK in November 2019. All parties concurred on the usefulness of the work done so far and agreed a work plan for 2020-2021. The work plan calls for a programme of bilateral workshops to be established covering the following topics:

- Computer codes and confirmatory analyses for HPR1000.
- Regulatory expectations for nuclear pressure equipment.
- Strengthening mutual understanding of each other's nuclear safety regulatory systems and regulatory concepts.
- Licensing of new NPPs: regulatory requirements and expectations in China and UK.
- Regulatory approaches to assessing / inspecting how assumptions and requirements in safety cases are developed, captured and tracked through to their implementation in the as built / operated plant / design.
- PWR commissioning - lessons from Chinese experience.

65. In addition, in September 2017 the Policy Group of the OECD-NEA Multinational Design Evaluation Programme (MDEP) approved the creation of the HPR1000 design specific working group (HPR1000WG). The members of this working group

are NNSA, ONR, Argentina's Autoridad Regulatoria Nuclear (ARN) and South Africa's National Nuclear Regulator (NNR). The first meeting of the HPR1000WG took place in March 2018 in China, with subsequent meetings held in September 2018 in France, March 2019 in the UK, and September 2019 in China. Two technical expert subgroups (TESGs) within the HPR1000WG have been created as follow:

- Severe accidents.
- Treatment of external and internal hazards.

The programme of work of the HPR1000WG includes development of common positions and technical reports on a variety of key topics of interest such as Fukushima lessons learnt, regulatory approaches to severe accident analyses, post loss-of-coolant-accident strainer performance, hydrogen management, and regulatory positions on internal and external hazards.

66. We will use the outputs from our international work to inform our Step 4 assessment.

9 GDA COMMENTS PROCESS

67. ONR's mission includes holding the nuclear industry to account on behalf of the public and places great importance on being open and transparent to ensure the public is informed of its work and its regulatory decisions, which will in turn improve and maintain their trust. Within GDA ONR does this by publishing, on the joint regulators GDA website (Ref. 6), our GDA guidance, the ROs and RIs raised during our assessment and corresponding RP's resolution plans, and our assessment reports documenting the outcomes of our assessment.

68. As part of the GDA process General Nuclear System Limited publishes information on the reactor design as well as the technical submissions that we receive as part of the assessment process. General Nuclear System Limited's website (Ref. 3) includes a comments process where the public can comment on any aspect of the UK HPR1000 reactor technology, design, safety, security and environmental features via the website or by post.

69. During this step, General Nuclear System Limited has received a total of 13 comments (November 2018 – January 2020). Of the 10 comments that are in scope:

- Five comments relate to technical aspects of the reactor technology, design, safety, security and environmental features.
- Five comments relate to other aspects not directly related to the reactor design or GDA process such as format of the submissions, siting, policy and aesthetics of the design.

70. The RP has responded to all of the comments. Three comments were deemed to be out of scope of the public comments process and one of these was passed to the Bradwell B project team. All comments and responses have been shared with the regulators for consideration in the assessment process as appropriate. All of the technical matters raised via the public comments received so far are or will be covered by our assessment.

10 SUMMARY OF ONR's ASSESSMENT OUTCOMES

71. The following subsections summarise the assessment we have conducted during Step 3 of GDA across 19 technical disciplines. The sections are structured consistently; for each topic we first outline the key relevant aspects within the safety or security cases, we then present our conclusions from Step 3, and those matters

that require follow-up during Step 4. A final conclusion on whether any fundamental safety or security shortfalls have been found is also included for each technical topic.

72. In addition to the 19 assessment summaries below, subsection 10.20 describes the regulatory activity in relation to matters of a cross-cutting nature that we have undertaken during Step 3 of GDA, and the key outcomes.

73. Our assessment conducted so far has not identified any fundamental safety or security shortfalls that might prevent the issue of a DAC for the UK HPR1000 design. We have however identified a number of potential regulatory shortfalls that require action and new work by the RP for them to be resolved. We have issued or are in the process of issuing ROs to address those shortfalls. At the time of writing this report, we have issued, in total, 31 ROs, 19 of which have been published on our GDA joint regulators website (Ref. 6) together with the RP's resolution plans. The remainder will be published in due course once resolution plans are agreed. For the purpose of traceability and transparency all the ROs issued so far in GDA are listed in Annex 2.

74. At the time of writing this report we have also raised over 600 RQs in total, requesting the RP to provide clarification or additional information on safety and security matters. So far we have not raised an RI.

10.1 Chemistry

75. Key aspects of the UK HPR1000 safety case related to Chemistry, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- Primary circuit operating chemistry, design aspects and material choices.
- Secondary circuit operating chemistry, design aspects and material choices.
- Auxiliary systems operating chemistry, design aspects and material choices.
- The approach and methodologies adopted by the RP in development of its safety case relating to chemistry behaviour and effects during accidents.
- The overall Chemistry safety case strategy and architecture.

76. During Step 3 ONR had intended to sample a number of other aspects of the UK HPR1000 safety case relating to Chemistry including those relating to ancillary systems of the primary circuit, sampling and monitoring systems, commissioning chemistry and the adequacy of chemistry control in the treatment of radioactive wastes. These omissions do not invalidate the conclusions of the assessment, and will be followed-up as appropriate during Step 4.

77. ONR's assessment of Chemistry was also supplemented by contractor support to provide an independent review of a selection of the RP's documentation relating to chemistry during accidents and aspects of primary circuit chemistry. The outputs from this work were considered during ONR's assessment.

78. The main conclusions of the Step 3 assessment in the area of Chemistry can be summarised as follows:

- The RP's chosen primary circuit operating chemistry largely follows industry RGP, in adopting an alkaline chemistry, using enriched lithium hydroxide, and dosing hydrogen in order to maintain a reducing environment. Enriched Boric Acid (EBA) is chosen for reactivity control. Throughout Step 3 the RP was considering whether to adopt zinc injection as an ALARP measure, which, encouragingly, it has now confirmed its intention to do. The main material choices for the primary circuit and associated systems are consistent with

similar plants, and the RP should be able to provide suitable justifications. However, the safety case relating to the primary circuit chemistry is immature when compared to a number of our expectations for Step 3 and the RP will need to address these as a matter of urgency throughout the remainder of GDA. While improvements and progress have been made throughout Step 3, this will need to accelerate further.

- The RP has started to develop its safety case relating to the operating chemistry, materials and design aspects of the secondary circuit. In general, this will need to develop further during Step 4 and be supplemented with evidence, but the claims and arguments appear reasonable at this stage. Consistent with the primary circuit aspects, a significant improvement in the depth and quality of information will be necessary.
- In the other aspects assessed, the RP's approaches at this stage are generally aligned with ONR's expectations and RGP. There are no significant gaps apparent in the information submitted to date but, given the limited information submitted by the RP to date, the expectation is that further evidence will be needed to confirm this position during Step 4.
- During Step 3 the assessment identified three distinct gaps in the safety case against expectations. In all of these areas the RP has not provided sufficient information during Step 3. These relate to:
  - Justification that radioactivity in UK HPR1000 has been reduced ALARP, including the impact of the operating chemistry, material choices and operating practices.
  - A demonstration that boron can be adequately controlled in UK HPR1000, including consideration of the impact of using EBA and a demonstration that boron dilution faults are prevented or mitigated.
  - Provision of a safety justification for the risks associated with fuel crud to demonstrate these are reduced ALARP.
- When considering the overall chemistry safety case strategy and architecture, it is evident that this will require significant attention from the RP going forwards. While the safety case includes the topics that we would expect to see, the level of detail and the maturity of the case will require numerous improvements. Significant work is required in all areas to develop the safety case to a sufficient level and enable a meaningful assessment to be completed. This will be a particular focus during Step 4.

79. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- Demonstration that the risks associated with fuel deposits are reduced ALARP.
- Minimisation of radioactivity and demonstration that it is reduced ALARP.
- A demonstration that all aspects of boron chemistry are controlled appropriately, including during normal operations, and considering the prevention of boron dilution faults during both normal operations and in fault conditions.
- Improvements in the availability and depth of evidence presented as part of the safety case, including the underlying narrative and clarity on the chemistry related claims and arguments.

80. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of Chemistry that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.2 Civil Engineering

81. Key aspects of the UK HPR1000 safety case related to Civil Engineering, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- The sufficiency of the safety case and design principles and methodologies contained in the design method statements, basis of safety case documents, basis of design documents and other supplementary documentation.
- The following sample areas were selected to gain confidence in the RP's application of the design methodologies and to ensure adequate assessment coverage of the safety significant design methodologies applied within civil engineering:
  - The common raft.
  - Inner containment.
  - The fuel building.
  - Aircraft impact protection.

82. In order to deliver the assessment scope, an engagement plan was implemented that centred on a series of level 4 workshops that would allow ONR to assess in detail the RP's safety case arguments. These workshops were supported by a number of routine level 4 meetings.

83. The ONR assessment of the RP's Civil Engineering design and safety case was also supplemented by a technical support contractor to provide specialist support where necessary. The outputs from this work were considered during ONR's assessment.

84. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- The overall safety case framework for civil engineering follows a claims-arguments-evidence (CAE) based safety report structure in line with ONR's expectations.
- Although further work is required in Step 4, ONR is encouraged by proactive improvements to the safety case 'golden thread' and the adoption of safety functional requirements (SFR) schedules through Step 3.
- The Civil Engineering design adopts a relatively conventional form whilst applying RGP in the form of internationally recognised codes of practice.
- The RP has utilised standard seismic and static analysis processes using widely accepted finite element analysis (FEA) codes.
- Overall, ONR concludes that the underlying design principles and methodologies for the Civil Engineering aspects of the UK HPR1000 are adequate.
- Furthermore, ONR considers it important to acknowledge the RP's proactive response to ONR's comments and queries during Step 3, and the willingness to engage a technical support contractor familiar with the UK context. An example where this has been particularly successful has been the comprehensive resolution plan agreed for RO-UKHPR1000-0009.
- Notwithstanding the comments above, the RP's current Civil Engineering safety case documentation requires further work to achieve the level of maturity expected by the regulator. The RP is aware of this and has made satisfactory commitments to update the extant documents during Step 4.

85. Based upon this assessment a number of areas have been identified that will require follow-up during Step 4, these include:

- The RP should continue to improve the SFR schedules to:
  - Address comments provided by ONR during Step 3 workshops.
  - Improve clarity regarding what fault conditions remain once all hazard scenarios are removed, and what structural requirements apply in such conditions.
  - Demonstrate how the different civil engineering SFRs, design requirements and performance criteria that relate to various hazard conditions are defined and communicated into the SFR schedules.
  - Provide further clarification with respect to the definition and substantiation of SFRs for secondary structures.
- Improved clarity is required regarding the differences in design approach for structures of different safety classification.
- Improved clarity and consistency should be provided between the Internal Hazards structures, systems and components (SSC) definition, and the SSC definition process, the Civil Engineering SSC definition and the associated SFRs.
- The cross referencing between safety case documents should continue to be improved during Step 4.
- The safety case ‘golden thread’ for layout requirements should be made visible within the civil engineering safety case documentation.
- The RP should provide a more detailed narrative within the safety case documentation regarding the beyond design basis approach.
- The RP should provide more clarity regarding the aircraft impact assessment fire strategy.
- The RP should address potential risks to the spatial configuration and layout associated with the Control & Instrumentation (C&I) and Mechanical Engineering disciplines; see RO-UKHPR1000-0017 Action 4, and RO-UKHPR1000-0014.
- More generally, the RP should continue to improve the level of detail in submissions.

86. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of Civil Engineering that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.3 Control and Instrumentation

87. Key aspects of the UK HPR1000 safety case related to C&I, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- Structure and clarity of the C&I safety case.
- Categorisation, classification and reliability claims.
- Design of overall C&I architecture.
- Spurious actuation of C&I systems.
- Design of the principal C&I systems (focussing on the design of the reactor protection system (RPS) and diverse actuation system (KDS [DAS]) as the systems of the highest safety significance providing the main and diverse defence lines against frequent faults).
- Cyber security of C&I systems (working jointly with ONR Security inspectors).
- Assessment of smart devices.
- Use of human machine interface equipment.

- Arrangements for commissioning and maintenance of C&I equipment.

88. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- The C&I safety case is logically structured around a set of high level claims which are decomposed into a series of sub-claims and arguments, but there are shortfalls in the completeness and consistency of the safety case. Arguments are often high-level statements that do not cogently describe how the claims are satisfied, and the relevance of evidential submissions to the overall case is not always clear.
- The RP's methodology for categorisation of safety functions and classification of C&I systems important to safety is aligned with RGP. However, there is no clear link between the fault analysis and the reliability targets assigned to C&I systems. In particular, it is not clear how frequency of initiating events has been considered in the derivation of reliability targets. There is a risk that reliability targets for C&I systems are too onerous which could make their substantiation more difficult than is necessary. The RP has also not presented a complete and coherent methodology for the modelling of computer based system reliability in the Probabilistic Safety Analysis (PSA).
- The C&I architecture comprises a divisional structure and voting logic to provide resilience against spurious actuation, but there are shortfalls in the level of independence between systems which present a risk that common cause failure could simultaneously affect multiple systems across different levels of defence in depth.
- The RP has adopted a methodical approach to the analysis of spurious actuation of C&I systems which is proportionate and pragmatic, but the RP has yet to complete the bounding case analysis of postulated initiating events (PIEs) caused by spurious C&I actuation.
- The development of the reactor protection system follows a structured, multi-stage lifecycle that aligns at a high level with RGP. Furthermore, the RP has assigned an appropriate classification to the KDS [DAS] and has made reasonable progress in demonstrating that the design of the system can meet UK regulatory expectations. However, the following areas for improvement were identified:
  - The RP has not provided an adequate plan for the demonstration of production excellence and conducting independent confidence building for computer based safety systems.
  - The use of programmable technology to carry out monitoring and diagnostic functions for the KDS [DAS] potentially compromises diversity arguments and increases the risk of coincident failures.
  - The primary and secondary protection systems will be supplied by the same organisation. The RP should provide a comprehensive justification of diversity throughout the development lifecycles of both systems.
  - The RP has not provided a comprehensive justification that the design of the C&I systems complies with relevant codes and standards.
- The RP has developed a suitable methodology for the assessment of cyber security risk which is aligned with RGP. During Step 4 the RP should implement the cyber risk assessment methodology for each of the centralised C&I systems and identify any design changes required to address vulnerabilities. The RP will need to ensure that the risk assessments are completed in sufficient time to allow the identification and specification of design modifications to address security vulnerabilities during GDA.

- The RP has proposed an overall methodology for the justification of smart devices that is broadly aligned with regulatory expectations. There is however a risk that the detailed safety justification of smart devices may not adopt the tools and techniques that are considered RGP in the UK. In Step 4 we expect the RP to provide evidence of the implementation of its smart device substantiation methodology through the justification of sample devices.
- The RP has not provided adequate justification that suitable and sufficient user interfaces will be provided for control of the UK HPR1000.
- The requirements for commissioning and maintenance of C&I systems are not defined in the safety case.

89. Based upon this assessment the following areas have been identified that will require follow-up during Step 4:

- The RP should provide a suitable and sufficient demonstration that the UK HPR1000 generic C&I design is compliant with RGP. This matter has been captured in RO-UKHPR1000-0016.
- The RP should clearly demonstrate the link between the fault analysis and the reliability targets assigned to C&I systems, in particular how frequency of initiating events has been considered in the derivation of reliability targets.
- The RP should provide a suitable and sufficient demonstration that the level of independence between systems reduces the risk of common cause failure simultaneously affecting multiple systems ALARP. This matter has been captured in RO-UKHPR1000-0017.
- The RP should complete the bounding case analysis of PIEs caused by spurious C&I actuation and identify any design changes required to provide protection against faults.
- The RP should ensure that full requirements traceability through the C&I system lifecycle is provided, and that inconsistencies between documents are addressed.
- The RP should provide overall verification and validation (V&V) plans for C&I systems, particularly the RPS, that describe and govern system level testing including both hardware and software.
- The RP should provide an adequate plan for the demonstration of production excellence and conducting independent confidence building for each of the principal computer based C&I systems.
- The RP should provide a robust demonstration that the programmable elements the KDS [DAS] cannot interfere with delivery of safety functions and that the integrity claims for the KDS [DAS] are not reliant on those elements.
- The RP should provide a comprehensive justification of diversity for all aspects of the development lifecycles of the RPS and KDS [DAS].
- The RP should complete the assessment of cyber security risks for each of the centralised C&I systems and identify any design changes required to address vulnerabilities.
- The RP should provide robust safety justifications of example smart devices that align with RGP and meet regulatory expectations.
- The RP should provide an adequate justification of the adequacy of user interfaces for the generic UK HPR1000 design.
- The RP should define the strategy and requirements for commissioning and maintenance of C&I systems and demonstrate how these are derived in the safety case.

90. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of C&I that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.4 Conventional Fire Safety

91. Key aspects of the UK HPR1000 safety case related to Conventional Fire Safety, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 were related to the fire safety design of the following buildings:

- Reactor building.
- Fuel building.
- Safeguard buildings.

92. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- The Step 3 assessment of the fire safety design for the reactor, fuel and safeguard buildings, indicates that the design satisfies UK legal requirements for the protection of people from the danger of fire.
- Fire safety arrangements within the reactor, fuel and safeguard buildings do not conform to expectations for traditional buildings, however the RP has demonstrated that alternative fire engineered methods achieve an adequate level of fire safety.
- The claims and arguments, supporting the fire engineering to reduce risk ALARP, are broadly convincing and complete. In limited instances, further work is required in Step 4, but credible solutions are proposed for any outstanding issues to achieve compliance with UK expectations for fire safety.
- Our Step 3 assessment focused on buildings perceived as presenting greatest potential for structural modification necessary to achieve adequate fire protection for people. Optioneering to improve fire protection for life safety has proposed minor structural alterations, however significant design alterations are not identified.
- In Step 4, the combination of fire strategy reports and gap management reports, for each of the remaining significant buildings on the nuclear island, will be assessed to determine whether they provide adequate evidence to complete the GDA for Conventional Fire Safety.

93. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- Whilst the fire strategy for the reactor building fulfilled its purpose of demonstrating how the UK HPR1000 will meet UK legal expectations for protection of people from the danger of fire, the focus of the document should be improved when the strategy is updated. Greater emphasis should be given to ‘means of escape’ to recognise priority for life safety protection in the strategy and less importance attributed to the enhanced standards of structural fire resistance.
- The RP has provided a strategy to protect vertical escape routes within the reactor building from the ingress of smoke. However, further detail is required, in Step 4, regarding airflow rates and pressure differentials between the staircases and compartments within the facility.
- The fuel building gap management report originally submitted to ONR contained references to basic principles of means of escape that would not be effective in that building. Discussions at a level 4 workshop in September 2019 indicated that the level of subject matter expertise in this area has increased. The RP has reconsidered the original fire engineering, identified

improvements to means of escape and committed to submission of an updated gap management report, which will be followed-up in Step 4.

- A perceived difficulty in providing firefighting lifts in the safeguard buildings arose due to unfamiliarity with the detailed application of the applicable British Standard. The RP should continue to develop expertise in the comprehensive guidance associated with UK good practice in design of buildings for fire safety.

94. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of Conventional Fire Safety that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.5 Conventional Health and Safety

95. Key aspects of the UK HPR1000 safety case related to Conventional Health and Safety, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- That all reasonable steps are taken to eliminate, reduce or control foreseeable conventional health and safety risks that may arise during construction (including decommissioning), maintenance and use of the nuclear plant and that appropriate information is prepared to inform others about the management of remaining significant risks.
- That the RP's and designer's understanding of relevant GB health and safety regulatory requirements, and appropriate reference to authoritative, documented RGP is adequate to determine control measures to reduce risk ALARP.
- The RP's management and monitoring of the plant designer's identification, elimination and control of foreseeable risks to health and safety outcomes. This includes the UK HPR1000 design risk recording protocols.

96. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- The RP provided a number of topic reports throughout Step 3 that present their understanding of relevant UK health and safety legislation. These include topic reports considering health risks, working at height, lifting operations, confined spaces and Control of Major Accident Hazards (COMAH). The content of these submissions proved adequate to conduct a meaningful assessment during this step and the RP demonstrated broad compliance with UK statutory requirements.
- The RP compiled a balanced and representative selection of risk examples for assessment, within the design constraints of GDA. The inclusion of examples that were 'out of scope' of GDA in recognition of areas of significant health risk to be reviewed during detailed site specific design is a welcome addition. The reports also demonstrate a general understanding of UK legal requirements and expectations.
- Throughout the topic reports, the RP's design risk register (DRR) is a core feature of the RP's arrangements to comply with Construction Design Management (CDM) (Ref. 18) requirements. The RP presented examples across the various topic reports to illustrate the intended content. There were a number of examples where the RP demonstrated a good understanding of UK RGP in controlling risks. However, the example DRR entries presented within the topic reports are early phase first version designer summaries,

which will require review to expand essential hazard content and risk mitigation information. This will be a focus during Step 4.

- Of particular note are the concerns raised regarding the layout and configuration of the spent fuel pool and associated lifting equipment design and operation. The assessment of these gaps to UK expectations is being led by the Mechanical Engineering topic, which will be followed-up during Step 4.
- There is also a lack of information on conventional health and safety associated with decommissioning activities throughout the submission made during Step 3. This will need to be considered by the RP during the remainder of GDA.

97. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- A CDM designer must do as much as is reasonable at the time when the design is prepared to eliminate, reduce or control foreseeable risks so that harm is unlikely or potential consequences are less serious. The DRR is an essential tool to record hazard information, risk management decisions and information needed to manage remaining risks. DRR examples considered in Step 3 lacked consistency in content, scope of review and remaining risk details. Our Step 4 assessment will be based upon more extensive and detailed review of the DRR content, of the designer's approach, and of associated CDM Work Instruction procedure delivery.

98. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of Conventional Health and Safety that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.6 Electrical Engineering

99. Key aspects of the UK HPR1000 safety case related to Electrical Engineering, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- The integrity of the electrical system complies with the functional safety requirements of the systems it supports.
- The suitability of the electrical system is based on strong deterministic principles.
- The electrical system can withstand internal and external events through an architecture based on defence in depth.
- The electrical system supports the operators in fulfilling their safety roles.
- The strategy on the use and assessment of smart devices.
- The electrical system will continue to meet its functional safety requirements throughout its operational life.
- Assessment of common cause failure.
- Categorisation and classification of Electrical Engineering.
- Response of lighting systems to the loss of electrical systems.
- Communication systems.

100. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- Whilst there are evident shortfalls in the approach to the determination of the functional safety requirements for Electrical Engineering, and the application

of deterministic principles as outlined in the current Step 3 version of the PCSR, the RP is improving its approach and understands ONR's expectations in this regard. This, based on evidence provided in the most recent Step 3 submissions, should ensure that an improved case is presented in Step 4.

- The RP has revised its CAE structure. Claims and arguments should be more explicitly described in respect of the requirement or expectation that is being presented and how this will be demonstrated.
- The RP has applied the principles of categorisation and classification appropriately to the electrical power system of the UK HPR1000, with the result that the system generally meets the UK expectations for classification set out in the ONR SAPs whilst maintaining an architecture consistent with IAEA guidance.
- The 'golden thread' between safety function requirement and electrical switchboard allocation will need to be fully demonstrated when the hazard and diverse line analysis in support of the fault schedule is complete.
- The RP has processes in place for the consideration of internal and external hazards in the design of the electrical power system, setting out its general design principles, which in turn are generally consistent with international guidance and practice.
- The RP has presented its design schemes for lighting and communications systems. The approach being taken to both is adequate. It is noted however that the RP is still to complete its review of human based safety claims and the potential for some actions to be safety categorised in a UK context. Until this work is completed in Step 4 it is noted that the classification of these systems is subject to change.
- With regard to smart devices:
  - The assessment has been coordinated with C&I to ensure that the RP is developing a smart device assessment process that it is suitable for all such programmable devices.
  - The RP has a stated aim to minimise the use of smart devices, which we consider appropriate. During Step 4, we intend to assess how such assertions are represented in the revised CAE structure and ultimately reflected in the system design manuals and technical specifications.
- Engagements with the RP on understanding how design life, equipment margins and qualification are defined and considered in the design and safety case have provided confidence that the concepts are embedded in the approach taken by the RP. However, the expectation for such principles and their delivery is not currently reflected in the safety case. The RP's revised approach to the presentation of CAE should address this matter.
- The RP has recognised the importance of analysing common cause failure in the overall design, is taking input from other disciplines including fault studies and PSA, and has developed a process to systematically analyse options to reduce the risk from common cause failure, focused on safety benefit and technological achievement rather than cost. However, the RP still has significant supporting work outstanding, such as diverse line and loss of support system analyses (including C&I and heating, ventilation and air conditioning (HVAC)) to ensure a comprehensive study.

101. Based upon this assessment the following areas have been identified that will require follow-up during Step 4:

- Revised claims and arguments structure and linkage to the evidence that demonstrates them.

- The link between safety functional requirements and electrical switchboard allocation, ensuring that it takes into account hazard and diverse line analysis.
- The Electrical Engineering assessment will coordinate with ONR's Internal and External Hazard assessments to ensure that hazards are characterised early during Step 4 to enable completion of the assessment of the adequacy of the design to fulfil the safety functions.
- During Step 4, the mission times of the emergency diesel generators (EDGs) and station blackout diesel generators (SBO DGs) will be assessed to provide confidence that there are no cliff-edges in the capabilities of the equipment to deliver the required safety functions.
- During Step 4, the Electrical Engineering assessment will coordinate with ONR's Human Factors assessment to ensure that where any operator actions of electrical equipment are required, both the action and the equipment are appropriately classified.
- The identification of safety significant operator actions that involve or benefit from the operation of electrical support systems.
- Assurance that qualification requirements for electrical SSCs consider the design basis environmental conditions and potential failures of support SSCs, such as HVAC, C&I and component cooling.
- The demonstration of smart device identification and assessment process on electrical equipment.
- The demonstration of how design life is identified and reflected in the equipment requirements for all electrical equipment important to safety.
- How appropriate margins in equipment performance are identified to take into account uncertainty and reasonable lifetime modifications and then considered in the analysis, design requirements and specifications of electrical SSCs.
- The inclusion of supporting analysis work, including electrical diverse line and electrical support system failure analysis in the common cause failure analysis to demonstrate that the design is ALARP.

102. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of Electrical Engineering that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.7 External Hazards

103. Key aspects of the UK HPR1000 safety case related to External Hazards, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- The RP's safety submissions to confirm whether the arguments related to External Hazards that underpin the safety claims for the UK HPR1000 are complete and reasonable in the light of our understanding of the reactor technology.
- Identification and screening of hazards and combinations of hazards.
- Definition of the generic site characteristics.
- Deterministic analysis of external hazards and combinations of hazards including the response of SSCs to the external hazard loads.
- Beyond design basis events and cliff-edge effects.
- The link between external hazards and the deterministic and probabilistic aspects of the overall safety case via the hazard schedule.

104. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- There are shortfalls in the completeness of the hazard combinations considered in GDA. As such, the safety arguments in PCSR Chapter 18 are not fully substantiated by the supporting safety case documentation at the current time.
- The RP's arguments relating to the development of the generic site envelope are appropriate and generally, suitably substantiated by the supporting documentation and hazards derivation, although some areas for improvement remain.
- The safety case arguments are not fully demonstrated with regards to protection of the design against external hazards, cliff-edge effects and performance beyond the design basis. This position is not unreasonable or to be unexpected at this point of GDA, and the RP is working to address some of our concerns, including optioneering to address the vulnerabilities identified by the deterministic analysis of the design.
- It is not possible to close the RO-UKHPR1000-0002 at the current time. Whilst the RP has identified the gaps between the reference plant and the generic site envelope further justification and substantiation of the design against external hazards is needed.
- Additional work is required by the RP to develop a complete safety case for the aircraft crash hazard. Whilst the safety case arguments are logical, the current safety case for aircraft crash is incomplete and does not demonstrate how safety arguments presented in PCSR Chapter 18 will deliver the over-arching claims. Nonetheless, the RP has made good progress in Step 3 with regards to defining adequate threats for use in the forthcoming analysis. The RP has also responded well to our expectations and made efforts to de-risk Step 4.

105. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- Justification that the external hazards identification, characterisation and screening process has identified credible combinations of hazards.
- Analysis of the effects of climate change on relevant external hazards and justification of the generic site envelope.
- Continuation of the substantiation of the design against external hazards and justification of the adequacy of the external hazard design bases.
- Justification of the completeness of the deterministic analysis of the design against external hazards for GDA.
- Provision of optioneering for vulnerabilities identified by the deterministic analysis and justification of any design modifications.
- Clarification in the safety case of the approach to beyond design basis analysis, demonstration of margins to failure and that cliff-edge effects do not exist for external hazards just beyond the design basis.
- Improvement of the presentation of the External Hazards safety case, including the underlying narrative and links to the engineering SFRs via the hazards schedule.
- Development of the safety case for the aircraft crash hazard.

106. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of External Hazards that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.8 Fault Studies

107. Key aspects of the UK HPR1000 safety case related to Fault Studies, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- The completeness of the list of PIEs for the UK HPR1000 (including fault identification for support systems, non-reactor faults and spurious C&I actuation faults).
- The completeness of the list of design basis conditions (DBCs) and design extension conditions - A (DEC-A) sequences.
- The demonstration of diverse protection against frequent faults.
- The treatment of maintenance assumptions within the design basis.
- The adequacy of the RP's analysis of DBCs and DEC-A sequences.
- The demonstration of margins to relevant acceptance criteria for the analysis of DBCs and DEC-A sequences.
- The verification and validation of computer codes that will be used in the analysis of DBCs and DEC-A sequences.
- The maturity of information within the fault schedule.
- The identification and breakdown of safety functions, and the application of the categorisation and classification methodology to reactor systems, support systems and fuel route systems.
- The development by the RP of a UK specific method for the calculation of off-site radiological consequences for comparison against Target 4 in ONR's SAPs.

108. During Step 3 ONR had intended to gain confidence in the adequacy of the deterministic analysis conducted as part of the safety case supporting non-reactor operations, including fuel handling and storage. However, these faults are not included in the latest list of UK HPR1000 design basis faults but will be identified for the start of Step 4, and a specific submission is expected that will provide analysis of these faults.

109. ONR's assessment of Fault Studies was also supplemented by contractor support. Two contracts were let during Step 3 to provide an independent review of the verification and validation of the design basis analysis computer codes and to develop thermal hydraulics and core physics computer models to undertake independent confirmatory analysis of a number of fault sequences. The outputs from this work were considered during ONR's assessment.

110. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- The RP has undertaken a programme of work to provide a logical, auditable process for identifying faults for the UK HPR1000, including consideration of support systems, spurious C&I faults and fuel route faults. The documents that have been submitted demonstrate that the RP has undertaken a considerable amount of work to underpin the extant list of DBCs and identify any new PIEs. However the final list of DBCs is yet to be submitted and the implications of any new DBCs for the design or safety case are not yet clear.
- The list of DEC-A conditions has been developed from that for the reference plant and is consistent with ONR's expectations that the safety case demonstrates that there are no significant increase in consequences for sequences just outside the design basis. The list of DEC-A conditions will be updated and the completeness of this list will be a focus during Step 4.

- The RP is making progress with its work to examine the levels of diversity present within the support system design and describe the tolerance against fault conditions. The assessment of any new DBCs or design changes arising from this work will be a significant part of the assessment effort for Step 4.
- To gain confidence that the design basis analysis has been carried out in accordance with the RP's rules and on a conservative basis in accordance with ONR's expectations, the assessment reviewed a sample of transient analysis reports covering a range of fault types. In general, the analysis appears appropriate and broadly consistent with ONR's expectations, albeit that a number of detailed matters will require further evidence and assessment going forward. Importantly, the current submissions will need to be supplemented with additional evidence to provide a more complete description of the faults analysed and justify the choice of analysis parameters. This is necessary to demonstrate that the claimed safety measures are appropriately sized to protect against the design basis faults and that the safety system actuation settings have been appropriately derived. Improvements in this area will be a focus during Step 4.
- The RP's methodology for the categorisation of safety functions and the classification of SSCs was submitted early in GDA. The assessment effort during Step 3 has therefore been focussed on the way in which this methodology is applied in the UK HPR1000 safety case. While the RP has shown a willingness to consider engineering solutions and safety case changes to address any shortfalls identified against its methodology, the linkages between safety case documents that present safety functions and the engineering requirements will need to be improved.
- A fault schedule has been submitted which identifies frequent faults and the diverse means of protection for each safety function, consistent with RGP in the UK. This aims to demonstrate that the plant has diverse protection against failure of the primary C&I signal, C&I system or mechanical system. This work remains on-going but based on the RP's progress to date it appears that the design is broadly consistent with ONR's expectations for frequent faults. Some shortfalls have been identified by the RP and these will need to be addressed. Furthermore, evidence will need to be provided to demonstrate the capability of the diverse safety measures and a demonstration that residual risks are ALARP.
- The design basis transient analysis that has been submitted by the RP has been undertaken without consideration of examination, maintenance, inspection and testing (EMIT) activities (i.e. assumes that all trains of all safety systems are available). Information has yet to be provided to demonstrate that EMIT activities can be carried out consistent with these limitations. Additional design basis analysis may be required if the RP chooses to undertake some EMIT activities which reduce the availability or redundancy of safety systems.
- The transient analysis for UK HPR1000 GDA has been undertaken using the RP's in-house computer codes which have not been used for the licensing activities for the reference plant in China and have not previously been used outside of China. The focus of the Step 3 assessment has therefore been on the verification and validation of these codes. To date, the RP has provided some initial submissions and we have not found any fundamental reasons why these codes cannot be used in the UK HPR1000 safety case, subject to suitable and sufficient evidence being submitted in Step 4. However, this area remains challenging and further information will be required in order for ONR to make a judgement on this aspect. In addition to direct contractor support on this aspect, we intend to also use ONR's independent confirmatory

analysis to gain further insights into the codes' capabilities and validation evidence.

- For radiological consequences the RP has used standards and practices which are consistent with Chinese regulations, but a number of specific differences to UK regulatory expectations exist and a UK methodology for off-site radiological consequences needs to be developed by the RP and applied to design basis faults.

111. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- A demonstration that the UK HPR1000 is tolerant to faults originating within the support systems.
- A demonstration of diverse protection for frequent faults.
- A demonstration that operation of secondary passive heat removal system will not prejudice operation of feed and bleed.
- An adequate safety case for inadvertent initiation of IVR.
- An adequate safety case for debris effects on safety injection system and containment heat removal system performance.
- Adequate validation and verification of the computer codes used in the UK HPR1000 fault studies safety case.
- An adequate methodology for the calculation of off-site radiological consequences to allow a comparison against relevant targets.
- Improvements in the presentation of the Fault Studies safety case, including the underlying narrative and links to the plant design and engineering.

112. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of Fault Studies that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.9 Fuel and Core

113. The UK HPR1000 core design was initially based on the STEP-12 fuel designed by CGN, but early in Step 3 the RP decided to replace this with the AFA3G™AA fuel designed by Framatome. This latter fuel is used in a number of plants in China, as well as in the Fangchenggang NPP Unit 3 reactor, which is currently under construction and is the reference plant for UK HPR1000. It is also similar to the fuel used in Sizewell B in the UK, as well as the fuel design proposed for Hinkley Point C. The RP presented arguments to demonstrate that the two fuels have very similar characteristics; hence the impact of the change on the core design would not erode safety margins.

114. Therefore, while this change in fuel design has limited impact on the UK HPR1000 design, it did require the RP to undertake a significant amount of rework of its safety case, including submissions that had previously been made and assessed during Step 2. This had an important impact on the scope of the Step 3 assessment in the Fuel and Core topic, which had to be changed from that originally envisaged. The revised approach was informed by ONR's previous experience with this fuel design and the impact of the change on the revised safety justifications for UK HPR1000. On this basis ONR were able to agree a schedule of submissions with the RP which allowed for a meaningful assessment to be undertaken during the Step.

115. Key aspects of the UK HPR1000 safety case related to Fuel and Core, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- Criteria, limits and conditions applied within the fuel and core design, including:
  - Design of the reactor core.
  - Design of the fuel rod (FR) and fuel assembly (FA).
  - Design of the rod cluster control assembly (RCCA).
  - Design of the spent fuel interim storage (SFIS).
- Standards and methods applied in the above, including the RP's ALARP demonstration.
- Adequacy of the computer codes used in the design, including their verification and validation.

116. During Step 3 ONR commissioned external contractor support to review the verification and validation of the computer codes used by the RP. This work remains on-going, but the initial outputs from this work were considered during ONR's assessment.

117. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- Based on ONR's SAPs and the relevant IAEA standards, ONR's expectation is that the fuel should be able to withstand normal operation and anticipated operational occurrences such as frequent faults, and fission products release in all design-basis faults should be limited. The assessment focused on the RP's safety case arguments, which support the fuel design compliance with these expectations. In general, the RP presented a reasonable set of criteria, limits and conditions that support these arguments; however the assessment identified a number of aspects which will require further clarification and justification in Step 4. Importantly, the RP will need to provide explicit demonstration that UK expectations can be met regarding aspects such as no fuel failures for frequent faults and that the risk of any failures is reduced ALARP.
- The RP has indicated that the use of dry storage of spent fuel in the long term is anticipated. This is assessed further under the Radioactive Waste, Decommissioning & Spent Fuel Management topic, but it is noticeable that this choice is justified by a systematic review of the available options, and with due consideration of applicable UK standards. The Fuel and Core assessment considered the relevant criteria, limits and conditions identified by the RP. From a Fuel and Core perspective, the arguments presented during Step 3 are largely reasonable, but significant further work will be required of the RP in Step 4 to identify SFIS related design criteria for fuel corrosion, hydrogen pick-up, mechanical impact, amongst others and analysis of the SFIS operating conditions, degradation mechanisms and challenges to fuel integrity.
- The RP's applied standards and methods for the fuel design meet the requirements of the relevant SAPs, as they will ensure delivery of the fundamental safety functions and stability in normal operation. The methods also appear to take account of the sensitivity to fault conditions and in-service degradation. However, further work will be necessary to determine the adequacy of the applied software packages.
- The overall ALARP justification for the fuel system provides reasonable arguments that the risk related to the UK HPR1000 fuel design is ALARP. The RP will need to provide robust supporting evidence for this during Step 4, including how any relevant matters from previous GDA assessments have been considered for UK HPR1000.

- As with Fault Studies, the UK HPR1000 Fuel and Core design and safety analyses are mostly based on the use of a set of CGN proprietary computer codes, instead of the Framatome codes used for the Fangchenggang NPP Unit 3 reference plant. Work remains on-going by the RP to provide the full suite of information, but the limited information provided to date has not highlighted any concerns to suggest that this cannot be completed during GDA. The RP still has to provide a large amount of detailed information to convince ONR that the results, produced with the RP's codes are valid and reliable for use in the UK HPR1000 safety case. This will be a particular focus for Step 4 assessment, in coordination with Fault Studies.
- In coordination with Chemistry, the insufficient safety justification for the risks associated with fuel crud, including a demonstration that these are reduced ALARP, was identified as a gap. This will be followed up during Step 4.

118. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- Appropriately substantiated criteria for fuel design and safety analysis, including SFIS, and demonstration of overall consistency between the fuel design limits and the relevant core design limits.
- Demonstration that UK expectations can be met by the UK HPR1000 design, including no fuel failure at frequent faults, the ALARP level of risk for fuel failure at infrequent faults and adequacy of protection system set points to prevent departure from nucleate boiling (DNB).
- Demonstration that the safety margins are larger than the estimated uncertainty.
- Analysis of the SFIS operating conditions, degradation mechanisms and challenges to fuel integrity.
- Information on the type and characteristics of in-core detectors.
- Adequate validation and verification of the computer codes used in the UK HPR1000 fault studies safety case.
- Demonstration that the risks associated with fuel deposits are reduced ALARP.
- Completion of updates to the safety case to reflect the change in fuel design.

119. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of Fuel and Core that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.10 Human Factors

120. Key aspects of the UK HPR1000 safety case related to Human Factors (HF), as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- Organisational capability.
- Human factors integration (HFI).
- Identification and substantiation of important human based safety claims (HBSC).
- Allocation of function (AoF).
- Human-machine interface (HMI) design.
- Design input to SSCs and EMIT.

121. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- At the close of Step 2, the RP faced significant challenges in developing the HF capability necessary to deliver a HF programme suitable to support a meaningful GDA. Throughout Step 3 the RP has worked hard to increase its capacity and capability and is to be commended on the progress made to date. At the end of Step 3, the RP is in a much stronger position to deliver a high quality design and safety case which adequately considers HF aspects. Importantly, the RP appears to understand clearly the challenges it will face during Step 4. This aspect will be closely scrutinised for the remainder of GDA, but the overall position is much improved.
- Fundamental to the effective and proportionate consideration of the limitations and capabilities of the human within the design, is a credible HFI programme. While closely linked to organisational capability, ONR's assessment of HFI concluded that the RP has significantly improved its capability and has introduced wide-ranging and positive improvements to all areas that underpin effective HFI. However, the RP continues to fall short in relation to identifying suitable operational experience (OpEx) and implementing learning. The RP's approach to OpEx will therefore be a key interest early within Step 4.
- The RP has developed a concept of operations (CoO) report which is a well-written and scoped report, providing a key summary of the UK HPR1000 reactor design and the proposed concept for how it will be operated. The CoO is underpinned by a target audience description (TAD). The TAD will require updating to ensure that the UK HPR1000 design takes account of the characteristics of the UK workforce for the planned operational life of the plant. The utility of the document also needs improving to ensure that it has the best opportunity of positively influencing the UKHPR1000 design. This needs to be completed early within Step 4 to maximise its impact.
- The RP has faced some significant challenges in the area of human reliability analysis (HRA) in GDA to date. The UK expectations in this area require a significantly greater burden of proof than the RP appears to be used to. Consequently, the RP has had to develop rapidly the capability to deliver this evidence base. Despite this the RP's approach to the identification of HBSC has a suitably wide scope, drawing from design basis analysis (DBA), PSA, severe accident analysis (SAA), and conventional health and safety sources. It is also appropriately linked to the wider HFI process to ensure that HBSC are suitably substantiated, either through HRA or through approaches such as verification and validation trials. Whilst the RP is likely to continue to face some significant programme challenges during Step 4 to deliver modern standards HRA, the progress during Step 3 provides confidence that this can be achieved.
- For the HF in the design area of the assessment, the focus was primarily on the RP's integration of HF into those areas of plant outside of the main control locations. Whilst the focus was not on the principal control locations for Step 3, the assessment identified a gap in the safety case in relation to the automatic diagnosis (AD) system. This system could offer significant safety benefits, but could also in itself lead to problems for the operator. The RP has yet to provide a cogent and coherent safety case for this system, and has argued that one is not needed. We will progress this topic further during Step 4 as part of the wider main control room (MCR) and related HMIs assessment.
- Regarding the other aspect of HF in design considered during the assessment, positively, the RP undertook an appropriately scoped and self-critical review of the Fangchenggang NPP Unit 3 baseline HFI programme

and design, which helped to develop an appropriate understanding of the necessary HFI scope for UK HPR1000. This identified a number of gaps against UK expectations that the RP continues to prioritise and progress. The RP's AoF method is not easy to apply and fails to integrate with the wider project functional classification systems. This stand-alone approach actively prevents integration of HF on the project. The application of this method, and the subsequent validation of AoF for the design, is late in GDA. This is somewhat mitigated by the fact that AoF has been driven by evolutionary development rather than first principles. Nevertheless, it is something the RP will need to progress quickly during the early stages of Step 4 to de-risk foreclosing on design options.

122. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- Continued development of the RP's HF capacity and capability and its impact on the HFI.
- Improvements in OpEx reviews to remove the limitations in scope seen to date.
- A lack of a suitable and sufficient safety case for the AD system.
- Updates to the TAD to reflect UK context and influence necessary design improvements.
- Enhancements to the approach to HF design reviews, beyond the current simple comparison against principles and standards, to include a more safety-function driven approach.
- Justification that suitable and sufficient fault analysis has been undertaken to underpin the HBSC.
- Optimism within the HRA approach.
- Provision of adequate evidence for HF aspects of the control locations including the MCR, technical support centre, remote shutdown station (RSS) and emergency control centre (ECC).
- Demonstration of the impact of failure of the HVAC on both the MCR personnel and C&I systems.
- Updates to the AoF based on the review performed by the RP.

123. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of Human Factors that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.11 Internal Hazards

124. Key aspects of the UK HPR1000 safety case related to Internal Hazards, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- The claims and arguments for each internal hazard and the identification of the safety measures presented in the internal hazards safety assessment reports for the safeguard buildings, reactor building and fuel building.
- Hazard analysis methodologies.
- Analysis of the bounding scenarios and consequences assessment for all internal hazards (internal fire, internal explosions, internal flooding, internal missiles, high energy pipe failure, dropped loads, electromagnetic interference (EMI), toxic, corrosive materials and gases, and vehicle impacts.

In addition, the PCSR considered claims and arguments against combined hazards) for the safeguard buildings, reactor building and fuel building.

- The substantiation of the structural barriers identified against the bounding internal hazard scenarios covering the application of the assessment methodology.
- The validation and verification of the analytical models used in the consequences analysis.

125. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- We are broadly satisfied with the overall progress made in the development of specific internal hazards safety evaluation methodology reports, reflecting RGP.
- The selection of bounding scenarios lacks the requisite justification and evidence (and associated narrative) as to why the selected bounding scenarios are fully representative of all other initiating events (including events that have been screened out) for each internal hazard. In particular, there is a need for transparency for all relevant data used, location of hazard sources and affected SSCs, description of how the scenarios developed, and the assumptions used in the selection of bounding scenarios.
- The RP made progress with the assessment of the bounding scenarios in the area of exceptions to segregation. However, there is a need for clarity on how the bounding scenarios identified and assessed would bound all exceptions to segregation areas and for all applicable internal hazards.
- The RP made progress with the assessment of the impact of the bounding scenarios on high integrity components (HIC). Clarity is required, however, on how the identified bounding consequences on a HIC item in one location would bound other HIC items in different locations, noting that not all HIC items have been confirmed.
- The consequences analysis undertaken in Step 3 lacks sufficient narrative and transparency of key assumptions, input data, analytical techniques and formulas used in the analysis, including sensitivity analysis, in demonstrating that the results are bounding and conservative.
- There is a need to demonstrate that, initially, the worst case unmitigated scenarios have been assessed for all internal hazards to allow appropriate categorisation and classification of the engineering safety measures in place (eg, detection and alarm systems, ventilation or pipe restraints), or actions by operatives. For example, in the area of high energy pipe failures, impact with barriers in a number of locations has been eliminated by restraints; however, no formal claim on restraints has been made and their substantiation is yet to be provided.
- Areas where segregation of SSCs delivering the fundamental safety functions by divisional barriers is not feasible (eg, exceptions to segregation areas), there is a need to identify and present all areas for all relevant buildings and for all systems (mechanical, electrical or control and instrumentation) and assess each area individually for all internal hazards including combined hazards.
- The RP's fire analysis has demonstrated the application of fire engineering methodologies and approaches in line with RGP; this has included review of fire sources, assessment of combustible loads and identification of bounding scenarios. However, the analysis undertaken to date has not fully demonstrated that all the identified fire sources are bounded by the scenarios identified.

- For the high energy pipe failure the identification of bounding scenarios should be based on the worst case unmitigated scenario. For the UK HPR1000 it appears that the hazard severity has been generally based on the failure of a single pipe and an individual consequential effect. In many cases several pipes exist without any clear segregation or protection measures to prevent multiple pipe failure; the RP will need to demonstrate that the risks from pipe failures are as low as reasonably practicable.
- In the area of dropped loads the selection of bounding scenarios for the fuel building and reactor building have been principally based on operational constraints, rather than the maximum heights that could be achieved by the lifting equipment. As a result, there is a gap in the analysis of those fault sequences that could result in drop loads exceeding the operational constraint.
- The RP has commenced its work on the identification of combined hazards by identifying potential consequential internal hazards across a number of its individual internal hazards safety assessment reports. At this stage, it is not clear how these potential scenarios will be addressed, but we recognise that the work in this area is ongoing and will be completed in Step 4.
- The claims and arguments presented in PCSR are reasonable and we are satisfied with the progress made in Step 3 in the identification of specific safety measures to support the claims and arguments presented in the PCSR. However, there is a need to formally identify all safety measures and their associated SFRs to deliver the claims and arguments. These SSCs should subsequently be allocated an appropriate safety classification and be substantiated. These should be listed in the hazard schedule in each safety assessment report.

126. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- The requisite narrative including transparency, evidence and justification of the bounding scenarios selected. All other initiating events bounded by the bounding scenarios, identified in Step 3, should be explicitly stated and justified.
- The requisite narrative, evidence and transparency of all key assumptions, input data and analytical techniques used in the analysis including sensitivity analysis in demonstrating that the consequences analysis results are bounding and conservative.
- The consequence analysis for all initiating faults, as necessary and appropriate, for all internal hazards and all relevant buildings. These should be presented in a coherent manner in the safety assessment reports and in the hazard schedules.
- The totality of safety measures delivering safety functions to protect against internal hazards, and their safety classification, should be identified.
- Full application of all methodologies including for those internal hazards not submitted in Step 3, combined hazards and barriers' substantiation.
- Demonstration that the design is robust against internal hazards especially in exception to segregation areas.
- The withstand capability of HIC and other SSC should be supported by the requisite evidence.
- Substantiation of all safety measures providing protection against internal hazards to a level of detail appropriate for GDA.
- The design specification for barriers penetrations.
- The consequences analysis in support of RO-UKHPR1000-0008 and RO-UKHPR1000-0014.

- The validation and verification of models used in the analysis of steam release.
- The adequacy of the models used in fire and explosions consequences analysis.
- The progress made with all the design gaps identified including the optioneering studies.
- The ALARP demonstration.

127. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of Internal Hazards that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.12 Management for Safety and Quality Assurance

128. Key aspects of the UK HPR1000 safety case related to MSQA, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- Project and safety case management arrangements, including:
  - Programme and oversight for development and delivery of submissions.
  - Quality control of submissions.
  - Commitments management process.
  - Project management / control (Master Document Submission List, project planning, management of project / technical risks, coordination of input from technical reviews).
  - RP's capacity and capability.
  - Management of third party contractors.

- Design control arrangements, including:
  - The RP's arrangements for design change control, including the categorisation of potential design changes initiated by their service provider and how these changes were assessed and implemented in the design.
  - The RP's design change control oversight, including its role in the review and approval of modifications to the UK HPR1000 reactor design.
  - The RP's technical decision making role for addressing technical issues relating to safety (nuclear, conventional and environmental).
  - Arrangements for design and safety case interfacing.

129. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- RP Organisation:
  - The RP organisation has matured, putting in additional organisational arrangements and updating their existing management procedures, to assist in meeting the requirements of the GDA process.
  - The organisational changes included the creation of the new role in General Nuclear System Limited called the 'Head of Project Correspondent Department (PCD)'. The role is to maintain a technical overview of the GDA project and ensure that effective interactions occur between different work areas and the UK regulators on project-wide and strategic issues.

- General Nuclear System Limited also established a safety case working group whose role is to provide oversight to the safety case activities within the organisation; it also interacts between the (joint) requesting parties to coordinate, control and deliver safety case tasks.
- The RP has a full suite of procedures to manage the GDA process and has rationalised and updated them to ensure they meet the business need, reflecting its current working arrangements. For the most part these were being applied adequately, with the exception of modification control and commitments management procedures described hereafter.
- CGN demonstrated the level of priority it placed on the GDA project, ensuring that sufficient resource was available, drawing in resource from other CGN entities to obtain operational experience. This also included the appointment of a safety case manager to work with the safety case working group, improving the sharing of information on safety case topics. The regulators noted the high levels of expertise, professionalism and commitment of those personnel we encountered during the MSQA inspections. To complement this, CGN continued to demonstrate a strong determination to develop an understanding of UK context in its organisation by providing training on safety case and ALARP and by obtaining support from the UK supply chain.
- Although the degree of coordination between General Nuclear System Limited, CGN and EDF SA has improved markedly during this step, there have been instances where the complexity of the organisational design has challenged the RPs ability to meet regulatory expectations. These have included issues with the sharing of design and safety case information, issues with the submission of quality and timely deliverables, and issues with the timeliness of decision-making. Consequently, we have raised concerns over the agility of the RP to respond to the challenging timescales for delivery in Step 4.

- Quality control of the safety case:
  - The quality of submissions to ONR has been variable, with many documents received early in Step 3 lacking in detail, whilst others were not coherent or had technical issues. This situation has improved during the step as regulatory feedback has been provided and acted upon by the RP. Nonetheless, ONR has suggested to the RP that it should improve the arrangements for specifying and communicating the required scope, content and purpose of documents at the point that the work is commissioned in order to ensure that ONR, CGN, EDF SA and third party suppliers share a consistent understanding of future submissions.
  - The arrangements that the RP had put in place for managing commitments to update the safety case were found to be inadequate, with CGN failing to capture commitments made to ONR to deliver new or updated documents. To its credit, CGN acted swiftly to address this issue and has appeared to capture historic commitments and ensured that new commitments are adequately identified and logged.

- Design management:
  - The RP is required to have in place arrangements for establishing, reviewing, categorising and approving changes impacting the Design Reference, which constitutes a record of the main documents that set out the UK HPR1000 design. The RP had established arrangements for controlling and categorising design changes, which the regulators

considered to be appropriate. However the regulators determined that these arrangements were not consistently applied. Consequently, and to ensure that all design changes made after the Design Reference Point (DRP) are adequately controlled by the RP, we raised RO-UKHPR1000-0024.
    - When assessing the RP's technical decision-making process used for the GDA project, the regulators found that there was a lack of alignment, within related procedures, of the criteria to identify a technical issue or how significant technical issues were resolved. This meant that General Nuclear System Limited's Technical Committee might not be sighted on all decisions that are important to safety.

- Programme management:
    - In Step 2 ONR had concerns over the level of oversight and control General Nuclear System Limited had over the programme of submissions for GDA. Consequently this matter was captured in RO-UKHPR1000-0004. During Step 3 the RP struggled to implement suitable arrangements for managing the programme and delivery schedule that allowed sufficient oversight by General Nuclear System Limited (and visibility to ONR) of all the documentation intended for GDA. However, the RP has now developed and implemented an Integrated Delivery Tool to capture, control and report the progress of all GDA documents, including those held by CGN that are not planned for submission but may be sampled by ONR.

130. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- Project oversight and control arrangements of the RP for the GDA process.
- Work planning – production of adequate specifications and improved communication between General Nuclear System Limited and CGN.
- Safety case management – adequate capturing of commitments and requirements management.
- Design management - design change control and technical decision-making.
- Arrangements for aligning the safety case, Design Reference, GDA scope and Master Document Submission List.
- Coordination with the future licensee.

131. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of MSQA that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.13 Mechanical Engineering

132. Key aspects of the UK HPR1000 safety case related to Mechanical Engineering, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- Mechanical Engineering GDA scope.
- Mechanical Engineering safety case architecture.
- The alignment of the Mechanical Engineering design with the generic site envelope.
- The development of the engineering schedule for the alignment of the safety analysis with the SSCs.

- The application of ALARP principles for aligning the UK HPR1000 with RGP.
- The approach for Mechanical Engineering design assurance.
- The asset management approach for Mechanical Engineering (i.e. safeguarding safety of Mechanical Engineering assets through life).
- Justification of Mechanical Engineering related codes, standards and regulations.
- ALARP justification of the insulation of primary circuit components.
- Justification of the design of the HVAC systems.
- ALARP justification of the approach to undertaking nuclear lifts.
- The safety categorisation and classification methodology, and its application to Mechanical Engineering.

133. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- The RP's Production Strategy for the Mechanical Engineering aspects of the safety case provides a reasonable overview of the safety case architecture. However, further evidence is required to explain how the SSCs deliver nuclear and radiological safety. The 'golden thread' of safety functional requirements should be clearly visible and defined within the generic UK HPR1000 safety case.
- With regard to the alignment of the Mechanical Engineering design with the generic site envelope, the extreme high temperature predicted for the UK HPR1000, taking account of predicted climate change is greater than that for the Fangchenggang NPP Unit 3 reference plant. The RP's analysis of the temperature differences has not identified any design changes resulting from extreme high temperature differences. The RP has not justified this adequately and further scrutiny will be required in Step 4. In particular, further justification is required to demonstrate that the UK HPR1000 HVAC systems can adequately deliver their safety functions during the UK generic site extreme external air temperature event.
- The RP has produced a draft example of part of the engineering schedule indicating how the schedule will be developed. Whilst this is reasonable for Step 3, greater priority needs to be given to developing a comprehensive engineering schedule. This needs to be delivered early in GDA Step 4 to support a meaningful assessment.
- The RP has not considered all sources of RGP in the UK context. This resulted in RO-UKHPR1000-0012. Further evidence is required, during Step 4, to demonstrate that the UK HPR1000 design will satisfy UK statutory requirements and RGP (including the identification and application of codes and standards).
- The design assurance arrangements, relating to Mechanical Engineering equipment, require more substantive evidence. Also, during Step 4, the RP's approach to design analysis requires further justification.
- During Step 4, further evidence is required to demonstrate that the UK HPR1000 asset management arrangements are adequate. This will include the methodology for equipment qualification. A cross-cutting RO (RO-UKHPR1000-0021) has been raised, led by Fault Studies - Demonstration of the adequacy of EMIT of structures, systems and components important to safety. Through this RO, ONR is seeking evidence that EMIT adequately supports the UK HPR1000 safety case.
- The RP produced an optioneering study considering the method of insulating the primary circuit components and the RP proposes that reflective metal insulation (RMI) should be used in preference to fibrous insulation. The benefits of this are considered to be reduced operator dose (during EMIT)

and eliminating the risk of fibrous material blocking coolant flow. The arguments and evidence supporting the change to RMI need to be reviewed and robustly supported. The nuclear safety impact on other systems (eg, ventilation systems that remove heat) requires consideration.

- The fuel building fuel handling and storage system design requires further justification. It does not currently appear to follow UK RGP. Hence, it does not adequately demonstrate that nuclear and conventional health and safety risks are reduced ALARP.
- With regard to safety categorisation and classification:
  - The RP's use of NC (none categorised / none classified) safety designation for some SSCs that deliver a nuclear and/or radiological safety function is not appropriate for a UK context safety case.
  - Specifically with respect to nuclear lifting operations and the assessment of dropped loads, the RP's use of normal operating limits to determine the severity of fault consequences is not considered RGP in the UK nuclear industry. An appropriate safety function category and SSC classification, based on unmitigated (worst case) conditions is required.
  - Whilst the RP's system design manuals (SDMs) contain safety functional descriptions, these are not adequately linked to the high level safety functions in the RP's decomposition of safety functions.
  - Further work is required to ensure that nuclear safety functions are correctly safety categorised and SSCs correctly safety classified.

134. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- Adequacy of the UK HPR1000 HVAC design substantiation.
- Adequacy of the engineering schedule (including implementation of safety functional categorisation and safety classification).
- Closure of gaps relating to the identification and application of RGP applicable to Mechanical Engineering for the UK HPR1000 design.
- Application of the ALARP principle when considering design changes.
- Adequacy and application of the design assurance arrangements.
- Demonstration of the adequacy of EMIT of SSCs important to safety.
- Adequacy of equipment qualification arrangements.
- Approach to reducing the hazards from fibrous material within the UK HPR1000 loss of coolant accident zone of influence.
- Approach to demonstrating that nuclear lifts reduce risks ALARP.
- Adequacy of the design of the fuel building, relating to the design of nuclear lifting operations to demonstrate that relevant risks are reduced to ALARP.

135. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of Mechanical Engineering that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.14 Probabilistic Safety Analysis

136. Key aspects of the UK HPR1000 safety case related to PSA, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- The identification, screening and grouping of initiating events (IEs).
- The screening and bounding of internal and external hazards.
- The reliability data used in the PSA, such as:

  - Data for IE frequencies.
  - Component failure probability / unavailability.
  - Common cause failure (CCF) probability.
  - HRA.
  - C&I component and system failure probability / unavailability.
  - Electrical component and system failure probability / unavailability.

- The Level 1 PSA and Level 2 PSA models for logic, comprehensiveness, quality and adequacy.
- The scope of the success criteria analysis for Level 1 PSA, Level 2 PSA, spent fuel pool (SFP) PSA, internal fire PSA, internal flooding PSA and external hazards PSA (excluding seismic PSA which will be addressed later in GDA).
- The RP's intended approach for Level 3 PSA, seismic PSA and to assess worker risk to address ONR's SAPs numerical targets (NTs) 5 and 6.

137. The original intention during Step 3 was to perform a detailed review of the seismic PSA for the reference plant. The RP has instead chosen to submit a report discussing the key important information learned in the Fangchenggang NPP Unit 3 report and how it applies to the UK HPR1000 design. We will follow up this aspect during Step 4.

138. ONR's assessment of PSA was also supplemented by contractor support to perform an independent review of the methodologies, PSA models and reports during Step 3. The outputs from this work were considered in our assessment.

139. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- The IEs that the RP selected for analysis in the PSA are broadly aligned with ONR's expectations and the process to select the IEs is clear and transparent. However, the IE list did not include some IEs that were expected to be included and the frequencies assigned to the IEs were not adequately substantiated to demonstrate that they were appropriate. The traceability of the IE frequencies to the underlying analysis was also not clear. The RP now understands these gaps and is working to address them in a timely manner.
- The RP has submitted PSA models for internal fire PSA, internal flooding PSA and external hazards PSA. The RP has also submitted summary reports for each of these which show the dominant areas of risk contribution from these hazards. The internal flooding PSA is comprehensive and generally follows expected good practices and the insights are adequately documented. The internal fire PSA report is inadequate in the depth and comprehensiveness that would be expected in a mature internal fire PSA model. Although gaps were identified against UK expectations, the RP understands, and is working to bridge them during GDA timescales. The seismic risk report and the update of the internal fire PSA will be key items of interest during Step 4.
- The PSA reliability database is comprehensive and includes the relevant data for all of the components that are modelled in the PSA. The data itself is derived from a combination of American and Chinese generic sources and appears optimistic compared with other generic sources. This will require further justification during GDA.
- Based upon the assessment of the Level 1 and Level 2 PSA models and reports it is clear that, in general, although there are some limitations regarding the scope, the PSA models that are included are comprehensive,

logical and cover most expected accident sequences well. However a number of specific gaps against expectations have been identified. The RP is working to resolve these concerns in future revisions of the PSA which will be followed-up during Step 4. The most significant of these are:
    - Lack of consideration of software and computer based systems in the PSA.
    - Inadequate substantiation and documentation of approaches and inputs to HRA modelling in the PSA.
    - Lack of documentation and substantiation of assumptions for the EMIT included in the PSA models and reports.
    - Limited scope of the SFP PSA.
- The RP will need to further develop its approach to Level 3 PSA and deliver the Level 3 PSA during Step 4. While the progress during Step 3 is sufficient, further assessment will be needed during Step 4.
- Similarly, the RP's proposed methodology to address worker risks against NTs 5 and 6 is a reasonable starting point but further development is needed. The basic framework and approach is logical and should enable the RP to be able to assess worker risk in a rigorous and probabilistic manner during Step 4.
- Overall, the RP has continued to make good progress with the PSA for UK HPR1000 and the basic approaches are sound. A number of gaps against UK expectations have been found, but the RP is confident that they can be resolved within GDA timescales.

140. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- Substantiation and documentation of inputs to HRA.
- Substantiation and documentation of EMIT.
- Consideration of software and computer-based systems in the PSA.
- Substantiation and documentation of PSA reliability database.
- Substantiation and documentation of inputs to IE frequencies and comprehensiveness of IE list.
- Immaturity of fire PSA modelling.

141. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of PSA that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.15 Radiological Protection

142. Key aspects of the UK HPR1000 safety case related to Radiological Protection, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- The RP's substantiation that the design complies with the Ionising Radiations Regulations 2017 (Ref. 17). Including arrangements for:
    - Restriction of exposure.
    - Designation of controlled or supervised areas.
    - Monitoring of designated areas.
    - Radiation and contamination zoning.
    - Radiation and contamination monitoring.
- The strategy for ensuring that exposure is ALARP.

- Management of normal operations source term (Radiological Protection led the multi-disciplinary assessment for this topic).
- Dose assessment for workers and the public.
- Arrangements for post-accident accessibility.
- Radiation shielding.

143. Detailed documentation covering radiation and contamination zoning layout of the UK HPR1000 designated areas was received relatively late in Step 3 and will be assessed during Step 4. This will include application of appropriate ventilation controls to these areas and the appropriateness of access controls.

144. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- The RP's documentation presents a systematic and thorough examination of UK legislative requirements and provides a route map that shows how compliance will be demonstrated in the UK HPR1000 safety case.
- Whilst some good examples of ALARP improvements in the design of UK HPR1000 compared to the CPR1000 are given in the worker dose assessment report, there are concerns with the RP's approach to identifying and assessing different options. The optioneering process is heavily reliant on a numerical scoring system that is not robustly underpinned and there is inadequate narrative accompanying optioneering decisions.
- The RP is taking a reasonable approach to source term definition. A logical documentation structure has been defined. Significant radionuclides have been defined covering corrosion products, activation products, fission products and actinides. An approach is proposed that should provide appropriate source terms for all plant conditions including transients. However, the RP has provided only limited evidence to support the claims and arguments that justify the radiochemistry of the primary circuit. In addition, operational controls including limits and conditions that ensure radioactivity in the primary circuit is minimised have not been identified.
- Worker dose was calculated in a systematic and conservative way, using adjusted data from operational plants, but making corrections for known changes in the design. The calculation was based on a ten year average, reflecting all types of outages to give a full and accurate calculation. However, the dose data presented does not compare favourably with other PWRs worldwide and so the RP will have to demonstrate that worker doses have been optimised. There is a detailed breakdown of dose activities which will provide a good basis for detailed optimisation studies.
- Doses to members of the public due to direct shine are based on calculation and are deemed to be lower than the ONR SAPs target 3 BSO of 20 µSv per year. Dose measurements from an operational site will need to be provided to support this claim.
- A credible methodology for devising the doses to workers in a post-accident response role has been defined. Doses will be calculated during Step 4. The adequacy of the methodology will be assessed in Step 4.
- Detailed shielding reports will be produced for Step 4 and will be assessed to ascertain that shielding codes used by the RP are subject to verification and validation. This particularly applies to a Monte Carlo code which is of Chinese origin and is not used in the UK nuclear industry. Our assessment will also determine whether the codes are properly applied and whether shielding is used in a way that ensures that doses to workers and members of the public are reduced so far as is reasonably practicable (SFAIRP).

145. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- The detailed proposals for designation of radiation areas will be reviewed to ensure consistency with IRR 17 (Ref.17) and will be used to inform the radiation shielding assessment.
- Further evidence will be sought from the RP to demonstrate that a systematic approach to option identification has been employed as part of the ALARP process for radiological protection.
- Further evidence will be sought from the RP on the ALARP demonstration for source term, including application of numerical scoring system for optioneering. This will apply particularly to the minimisation of cobalt and silver in the primary circuit.
- Related to the previous bullet point is the effective application of OpEx in support of source term characterisation and the demonstration of ALARP. Evidence will be sought from the RP to demonstrate that French OpEx is being used effectively to inform the UK HPR1000 design and safety case.
- The RP will be expected to refine the occupational exposure dose estimate to reflect any changes in design, specification or proposed operational controls that affect source term or any other factors that impact occupational exposure. It should be noted that predicted doses are currently in excess of the average for PWRs worldwide. This matter will be addressed in a manner consistent with ONR's cross-cutting assessment of the RP's demonstration of ALARP.
- Further evidence will be sought from the RP to support the claims made regarding public exposure from direct shine.
- We will assess the doses to workers employed in post-accident response and the demonstration that they are ALARP and compliant with legislative requirements.
- ONR will engage a contractor to support our assessment of the RP's approach to shielding design and to determine whether the use of shielding reduces occupational and public exposures SFAIRP.

146. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of Radiological Protection that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.16 Radioactive Waste Management, Decommissioning and Spent Fuel Management

147. Key aspects of the UK HPR1000 safety case related to Radioactive Waste Management, Decommissioning and Spent Fuel Management, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- Radioactive Waste Management aspects:
  - The overarching strategy for management of radioactive waste.
  - An account of how radioactive waste arisings (solid, liquid and gaseous) are minimised in the design of the UK HPR1000.
  - The management of non-fuel core components.
  - The adequacy of systems required for the management (collection, storage, treatment) of solid, liquid and gaseous radioactive wastes, including the conceptual proposal for the interim storage facility (ISF) for intermediate level wastes (ILW).
  - The ALARP demonstration for radioactive waste management.

- Decommissioning aspects:
  - Decommissioning strategy and plan.
  - Design for decommissioning.
  - Management of decommissioning wastes, including waste inventories, categories and activated structures.
  - Decontamination processes and techniques.

- Spent Fuel Management aspects:
  - Technology optioneering for SFIS.
  - The outline design of the SFIS facility.
  - The compatibility of the selected SFIS technology with the current UK HPR1000 design.
  - The preliminary safety evaluation for the SFIS facility.

148. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

Radioactive Waste Management

- The arguments presented have been organised to support the claims and sub-claims made in the relevant PCSR chapter. They are relevant and for the most part, appear to have been mapped to evidence, which we will assess in detail during Step 4.
- The expected range of radioactive wastes arising from a PWR-type reactor have been covered. A waste inventory and source terms have been provided to underpin the quantities, volumes and activities of these wastes, which can have an effect on the management options chosen.
- An integrated waste strategy (IWS) has been provided. It has been written in a clear and intelligible way, demonstrating that relevant UK legislation, policy and standards have been considered in the development of the radioactive waste management systems for UK HPR1000.
- A range of supporting documents have been provided covering commissioning, periodic testing, system design and sizing to substantiate the design of the radioactive waste management systems for UK HPR1000 and the sub-claims made in the generic safety case, relating to the identification of system functional design requirements and how they are satisfied.
- Evidence has been provided to demonstrate that the RP is actively pursuing avenues to open up waste routes for the UK HPR1000, as to support their claim that the accumulation of waste is minimised for the design.
- In a limited number of cases, some claims and arguments, for example, those related to the minimisation of radioactive waste, either appear incomplete, or are yet to be adequately substantiated at this stage of GDA.
- The RP's approach to optioneering and its presentation in the corresponding safety case submissions is variable and in some cases does not appear to follow their own processes and procedures. The RP has recognised this issue and responded positively to ONR's challenges, by committing to review, update and re-submit these reports to the regulators for further assessment during Step 4.
- The RP is proposing to size the ISF for solid ILW to cover operational waste arisings for 30 years, compared to the UK HPR1000 design life of 60 years. The RP's supporting justification has received enhanced regulatory scrutiny during Step 3 and will continue to do so moving into Step 4 of GDA. Furthermore, the RP is also yet to provide suitable optioneering which underpins the conceptual design of the ISF. A conceptual design has not been provided for the interim storage of low level waste (LLW). Despite there

being some important work for the RP still to complete, it is reasonable to expect this to be carried out during Step 4. Adequate progress has been made during Step 3 on the more fundamental aspects / principles associated with the interim storage of solid ILW.

- The RP's submissions describing the management and treatment of a number of ILW waste streams, namely: ion-exchange resins, sludges and concentrates and the in-core instrumentation assembly (ICIA) winding system, contain insufficient detail to be able to adequately understand the associated nuclear safety hazards and risks, and to be able to judge whether the necessary SFRs can be met.
- The ALARP demonstration for radioactive waste management is not yet complete. It does not include a consideration of: waste minimisation, reactor design innovations, nor any future opportunities for risk reduction. An adequate, holistic ALARP demonstration for radioactive waste management will need to be provided during Step 4.

Decommissioning

- The decommissioning strategy of immediate dismantling is consistent with UK policy and is based on comparison of options for the timing of decommissioning. The RP has demonstrated an understanding of the principles of design for decommissioning, and has identified a number of good practices which are broadly consistent with those identified in the independent review of RGP and OpEx undertaken by a technical support contractor during Step 3.
- Decommissioning has been mainly focused on the reactor and its key components. Whilst this focus is appropriate there are some gaps such as the approach to decommissioning of the spent fuel pool / fuel building and the segregation of highly activated concrete.
- Step 3 is intended to be a review of the arguments underpinning the claims. In the case of the Decommissioning topic area the RP has decided not to apply the CAE approach but has not explained the reasoning for this decision. Whilst it is not mandatory to apply this approach the submissions assessed indicate that the RP has in some cases not adequately linked the information presented as evidence to substantiate the claims.
- The RP has set out how the safety case will be structured for entry to Step 4, discussing the 'golden thread' of how the various documents produced link together. There does not seem to be a similar thread for the information within and between documents which would aid substantiation of the claims and sub-claims.
- It is not clear how decommissioning considerations have been balanced against other factors (eg, operational safety) in the overall demonstration of ALARP (and best available techniques (BAT)), for example in aspects such as material selection.
- The basis for the RP's statement that the risks of decommissioning can be demonstrated to be ALARP is unclear and not yet adequately supported by referenced evidence.

Spent Fuel Management:

- The RP has demonstrated good awareness of national and international practices in the long-term management of spent fuel. They have taken account of some Chinese OpEx in the selection of their preferred option of dry storage in sealed canisters in concrete casks, and in the initial design of the SFIS facility. The RP has demonstrated a good understanding of the key safety aspects of SFIS. It has undertaken an analysis of the interfaces between the SFIS facility and the SSCs in the fuel building in the existing

design. This indicates the existing SSCs are capable of supporting SFIS operational requirements, noting the design of SFIS is at a conceptual stage of development.

- ONR's Fuel and Core specialist inspector considered the RP's selection of the technology option of dry storage in casks as justified by a systematic review of the available options, taking due consideration of applicable UK standards. The RP also considered the experience of dry fuel storage at Sizewell B, as well as the planned dry fuel storage facility at Hinkley Point C. The spent fuel equipment design includes passive safety features.
- The RP undertook a systematic optioneering process in compliance with its own relevant procedure, which is consistent with ONR's guidance on demonstration of ALARP. It has also been recognised by the RP that further work is needed to make an adequate ALARP demonstration for SFIS during GDA.
- Some non-fuel core components, which will be initially classified as high level waste (HLW), due to high levels of activation, are planned to be stored in the SFIS facility. The scope of the safety case does not include consideration of these wastes so it does not appear to be complete for all the materials that are planned to be stored there. This gap will need to be addressed in an integrated manner during Step 4.
- The proposed two-phase approach to the construction of SFIS capacity needs to be considered in the context of the expectation in SAP RW.5 that the safety case justifies the continued safe storage for the entire planned storage period.
- The RP's scope for SFIS explicitly excludes failed fuel. There needs to be sufficient information to confirm that the safe management of failed fuel is not foreclosed as a result of the design of SFIS, recognising that at the GDA stage the design of this facility is conceptual. This needs further consideration in Step 4, noting that it was within scope in previous GDAs.
- The preliminary safety evaluation does not contain limits and conditions relevant to meeting the expectations of RW.5 / ENM.6 on passive safe storage, for example information on environmental controls.
- Further work is needed with regard to the systematic analysis of the hazards associated with spent fuel sentencing, transfer, storage, inspection and retrieval, which would enable definition of SFIS specific safety functions and relevant SFRs. Furthermore, the RP has not yet demonstrated that the thermal design criteria proposed for fuel during SFIS and related operations are adequate. It also needs to identify SFIS-related design criteria for fuel corrosion, hydrogen pick-up or mechanical impact.
- There appears to be a number of gaps in the preliminary safety evaluation relevant to other topic areas, for example the absence of information on radiation shielding requirements for the SFIS building and the assessment of radiation doses to members of the public. These aspects will need to be addressed during Step 4, but are outside the scope of this report.

149. The only item not assessed during Step 3 was the disposability of spent fuel, owing to delay in the provision of the necessary information. This omission does not invalidate the conclusions of the assessment and the matter will be addressed during Step 4. It should also be noted that disposability assessment is largely a matter to be addressed by the Environment Agency and Radioactive Waste Management (RWM).

150. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

Radioactive Waste Management

- Ensuring the RP's overall case for the safe interim storage of radioactive wastes, including the concept designs developed to date (and the adequacy of the proposed sizing of the stores), is supported by suitable and sufficient information and underpinned by robust optioneering.
- The RP will need make a number of key improvements to their current case to be able to robustly demonstrate that the design minimises radioactive waste.
- Further information is required on the ICIA winding system.
- For 'mobile' ILW such as: ion-exchange resin de-watering, sludge and concentrates retrieval, the RP will need to provide better system-level and process descriptions to ensure that the relevant nuclear safety hazards and risks have been identified and their magnitude properly understood.
- Identification of, and the management arrangements for, radioactive wastes arising in the event of an accident were excluded by the RP from the scope of their submissions. Identification of the waste types arising from reasonably foreseeable accidents is required, together with conceptual design information which gives assurance that the design incorporates an adequate allocation of space for the management of these wastes.
- The overall demonstration of ALARP for radioactive waste management.

Decommissioning

- The RP will need to improve the evidence, including referencing, to support the key claims in this topic area, with focus on design for safe decommissioning. This will take account of the final outcome of our technical support contractor's work to conduct a review of good practices for design for decommissioning.
- The demonstration of ALARP, including how decommissioning is balanced against other factors (eg, operational safety).

Spent Fuel Management

- The apparent lack of completeness of the preliminary safety evaluation for the SFIS facility with respect to consideration of non-fuel core components, noting that this issue is also relevant to radioactive waste management.
- Ensuring the scope of work on SFIS is sufficient to ensure that the safe management of failed fuel after removal from the spent fuel pool is not foreclosed by the design of SFIS.
- The need to define SFIS SFRs, design criteria and operational limits and conditions.

151. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of Radioactive Waste Management, Decommissioning and Spent Fuel Management that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.17 Security

152. Key aspects of the UK HPR1000 safety case related to Security, as presented in the GSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- UK HPR1000 GSR.
- UK HPR1000 vital area identification and categorisation with related methodology.

- UK HPR1000 cyber security risk assessment (CSRA) and related methodology.

153. The main conclusions of the Step 3 assessment in the area of Security can be summarised as follows:

- During Step 3 the RP has developed their GSR and importantly the supporting documents that describe how they will meet the expectations and outcomes within the SyAPs. Their current GSR provides an adequate description of their chosen methodology, how it will be applied and subsequently used to inform a security regime for the buildings in scope thereby meeting SyAPs expectations as they apply to GDA. While further work will be needed to update and complete these during the remainder of GDA, this should be achievable. This will remain a focus for assessment during Step 4.
- Delivery during Step 3 has been an on-going concern for the RP, mainly due to refinements of their approaches and methodologies and the need to manage personnel and organisational changes with their security team. However, towards the end of Step 3, the RP has adopted a more balanced approach, re-engaged suitably qualified and experienced personnel (SQEP) resources and addressed the gaps in team capacity and capability. We are now more confident that the RP has the capacity and capability to deliver against expectations in Step 4 subject to stability in the Security team and access to expertise from SQEP contractors.
- The documentation produced so far for the cyber security aspects and the framework upon which the RP bases its CSRA is adequate and aligned with RGP and relevant standards. Importantly, the RP has identified some security and safety architectural issues relating to the plant standard automation system (PSAS) at an early stage, giving time to resolve these during the remainder of GDA. The RP will need to continue to refine the CSRA as currently, elements of the report are weak with regards to presenting underpinning evidence. To allow a full assessment of this topic during GDA the RP will need to refine its methodology, and apply this to all the identified computer based systems important to safety (CBSIS), meeting expectations within SyAPs (FSyP 7).
- During this Step the RP has delivered the first iteration of its vital area identification and categorisation methodology for the UK HPR1000 design. This was one aspect where the RP was unable to fully deliver its intended scope during the Step. While sufficient information was still provided to allow ONR's assessment, delivery of further updates to these submissions has been raised as an RO (RO-UKHPR1000-0025). Notwithstanding the delivery issues, the submissions made during Step 3 represent a good foundation for further development as these could, given the appropriate development and application, provide a basis for an acceptable security case meeting ONR's expectations based on the SyAPs. The RP has also shown an understanding of our expectations and has the capacity to deliver an adequate review in sufficient time to inform their Security Concept of Operations, and potentially 'design-out' security vulnerabilities.

154. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- The lack of alignment between the CSRA methodology and the CSRA report will need to be addressed by the RP. The RP is aware that re-working the methodology will enable it to address weaknesses in its case contained in

their developing CSRA report. This work requires to be addressed early in Step 4 in order to inform the protection measures that should be explained in their Security Concept of Operations and related infrastructure within the evolving GSR.

- The RP will need to deliver a complete and detailed identification and categorisation of vital areas for plant state A (operating). Thereafter, to carry out such analysis for the remaining plant states sufficient to inform a Security Concept of Operations and related infrastructure expected in Step 4.

155. Overall, based upon the Step 3 assessment, no fundamental shortfalls in the area of Security that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.18 Severe Accident Analysis

156. Key aspects of the UK HPR1000 safety case related to SAA, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- Review of RP's SAA models and SAA results for the reference plant.
- Review of the RP's training and expertise for the SAA computer code ASTEC.
- Review of the applicability and capability of ASTEC for the UK HPR1000.
- Review of the adequacy of ASTEC code verification and validation.
- RP's overall methodology for SAA.
- Demonstration of practical elimination of accident sequences leading to early or large radioactive releases.
- RP's assessment of the five SAA engineered measures.
- Detailed technical review of the selection of SAA sequences.
- Detailed technical review of the first group of SAA calculation models and reports.

157. Early in Step 3 the RP changed the analysis codes for the SAA of UK HPR1000 from MAAP to ASTEC. This impacted on the focus of ONR's Step 3 assessment, requiring more effort to be placed on understanding the impact of this change. This is reflected in the assessment scope described above.

158. ONR's assessment of SAA was also supplemented by contractor support. Two contracts were let to provide input to the Step 3 assessment: ASTEC familiarisation training to provide an overview of the ASTEC codes strengths and weaknesses and an independent review of the verification and validation of the SAA computer codes. Outputs from this work were considered during ONR's assessment. A contract has also been let to independently verify the credibility of the UK HPR1000 IVR design using independent calculation tools. This contract remains on-going and will deliver during Step 4.

159. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- The RP has identified relevant severe accident phenomena that can lead to early and late containment failure in a PWR and has justified the exclusion of some phenomena for UK HPR1000. However, while the UKHPR1000 is designed to prevent molten core concrete interaction (MCCI), direct containment heating (DCH) and ex-vessel steam explosions there is benefit in the RP undertaking further analyses of these phenomena in order to identify reasonable practicable measures to mitigate severe accidents. Positively, the

RP has committed to perform such analysis of ex-vessel steam explosions, but it is unclear if similar effort will be undertaken for MCCI or DCH.

- The methodology for identifying the most limiting severe accident scenarios to analyse is based on the Level 1 PSA and makes for a well-structured, auditable and repeatable methodology that ensures that a variety of fault types are captured in the process. Further work will be needed during GDA to demonstrate that this does not exclude important claims or different plant states from consideration.
- The RP has submitted a summary of why it considers that situations that can lead to a large or early release have been practically eliminated, in accordance with IAEA and WENRA expectations. However, we have identified some concerns with the current case that has been put forward by the RP which mainly relate to the arguments made on the highest integrity components and severe accidents when the containment is open. There is no reason to suggest that the RP should not be able to address these aspects adequately during the remainder of GDA.
- The assessment considered both the analysis and design of the five dedicated severe accident safety measures identified for UK HPR1000, with a particular focus on IVR during Step 3. In general, our assessment did not identify any significant concerns, but a number of specific aspects will be followed up during Step 4. In addition, the approach to the safety case will need to be improved, in terms of both the quality and quantity of supporting evidence provided. Further confidence will also be sought by completion of ONR's independent confirmatory analysis.
- As with the other safety analysis topics, part of Step 3 has focused on verification and validation of the computer codes used for the SAA. The majority of the codes used for the SAA are third party with publicly available information. Therefore the approach was to focus on the analysis methodologies, sensitivity analyses, user effects and user proficiency. The RP still has to provide a large amount of information during Step 4 and this will remain a focus for Step 4 assessment.
- The RP has continued to progress the resolution of RO-UKHPR1000-0003 during Step 3, including the notable submission of the response to Action 3. The response exemplified a number of concerns over the RP's approach to severe accident. The current case appears only to provide evidence that the design is adequate, rather than derive functional requirements or seek ALARP solutions, and links to the wider safety case need improving. However, comprehensive guidance to the RP has been provided and further work is planned in the short term to improve these matters.

160. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- Analyses to determine the likelihood of re-criticality during the late re-flood stage.
- Analyses of ex-vessel steam explosions to determine the potential mechanical load on the containment structure.
- Further justification for the severe accident scenario selection methodology, to demonstrate that the methodology does not unduly influence the safety case to concentrate on safety functions credited for at-power severe accident scenarios.
- Presentation of the severe accident analyses and associated verification and validation, mainly relating to understanding remaining uncertainties in the analysis and their potential impact.

- Further details regarding the design of the severe accident safety measures, in particular regarding IVR.
- The RP's approach to demonstrating practical elimination of accident sequences leading to early or large radioactive releases, especially the case for open containment configurations and the presentation of the case.
- The production of an overall holistic safety case for severe accident for UK HPR1000. This relates directly to actions 3 and 4 of RO-UKHPR1000-0003. Currently the severe accident safety case is mainly a report of the results of the SAA, and does not adequately relate to the wider safety case for the design.
- Improvement to the overall quality of the safety case including referencing of scientific evidence and previous work performed for the reference plant. The RP could be more forthcoming with existing evidence to strengthen its safety case.

161. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of SAA that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.19 Structural Integrity

162. Key aspects of the UK HPR1000 safety case related to Structural Integrity, as presented in the PCSR, its supporting references and the supplementary documents submitted by the RP, that were sampled during Step 3 can be summarised as follows:

- Structural Integrity classification.
- Avoidance of fracture demonstration.
- Structural integrity provisions including design philosophy, design features / specifications.
- Material selection, specifications and manufacture methods for a sample of SSCs.
- Material testing and surveillance strategies.
- Application of design for inspectablity in the UK HPR1000.
- Description of compliance with appropriate design codes and standards.
- Specific areas that required follow-up as identified in the Structural Integrity Step 2 assessment report.

163. During Step 3 ONR had intended to sample a number of other aspects of the UK HPR1000 safety case relating to structural integrity including those relating to third party surveillance and the material selection of the containment liner. These omissions do not invalidate the conclusions of the assessment, and will be followed-up as appropriate during Step 4.

164. The main conclusions of the Step 3 assessment in this area can be summarised as follows:

- The RP has demonstrated that it is evolving and taking on board UK expectations with respect to structural integrity and nuclear safety. It is important that this development is continued within Step 4.
- It is clear that the RP has continued to develop the claims and arguments that underpin the structural integrity safety case. The structure of these claims appears appropriate at high level. Further clarity is required as to the structure for lower classification components but this can be provided within Step 4.

- The majority of the methods to produce the evidence to underpin the safety case within the structural integrity areas have been presented within Step 3. Our assessment has identified areas for improvement but in general the methods considered appear appropriate. However, the final test will be when these methods are deployed. Based on the sampling in Step 3, it is considered appropriate to now review the results of these methods.
- The RP now has a robust structural integrity classification methodology. The application on a wider basis should be sampled in Step 4.
- The RP's identification of HIC candidate SSCs is now based on a rational consideration of the UK HPR1000 design. Nonetheless the SI classification of several components needs to be resolved as a matter of priority with multi-discipline consideration of the RP's consequence analyses.
- The RP is making adequate progress in justifying the use of applicable codes and standards.
- The RP is progressing the overall ALARP demonstration for structural integrity. There are gaps to address but based on the evidence provided so far there is a reasonable expectation that an adequate ALARP demonstration can be provided.
- The RP has made progress in developing the avoidance of fracture demonstration methodology but the application of this process is immature at this stage. However this is to be expected at this stage within GDA and further engagement will be made within Step 4.
- Engagements with the RP to discuss the ALARP basis of certain design features have highlighted that the basis / supporting justification for them is not clear. To be able to make a demonstrably robust ALARP demonstration in these areas, the technical feasibility and reasonable practicability of alternative design options will need to be appropriately considered. This may lead to potential design modifications being judged to be necessary by the RP. This will be addressed as a matter of priority to mitigate the risks for GDA.
- The RP's process for materials selection was developed and is broadly satisfactory and aligns with ONR's expectations. In addition the RP has considered a satisfactory range of relevant and applicable ageing and degradation mechanisms for the RPV. In Step 4, the assessment of the application of the RP's material selection methodology will be broadened.

165. Based upon this assessment the following specific areas have been identified that will require follow-up during Step 4:

- The RP has not yet provided confidence that their approach to the avoidance of fracture aspects of the structural integrity safety case, and more specifically reconciliation, is demonstrably robust, and appropriately integrated into the wider UK HPR1000 generic safety case. This is being addressed as part of the RP's resolution of RO-UKHPR1000-0006.
- Review the RP's evidence to justify the Structural Integrity classification of the main coolant loop. This will be followed up as part of the resolution of RO-UKHPR1000-0008.
- The RP has not been able to communicate adequately that the risk of using the ASME design code and RSE-M in-service inspection code for the UK HPR1000 SG is being appropriately managed and is ALARP. A RO to capture this shortfall and manage its resolution has been raised.
- The RP has not demonstrated that it has considered sufficient options for improving the design of structures and components in terms of design for inspectability. In addition, the RP has not explained why some potential

improvements had not been considered. This will be followed up as part of the resolution of RO-UKHPR1000-0022.

- The RP has presented the ALARP justification for a number of design features which in our view do not currently provide enough confidence that the relevant risks have been reduced to ALARP. The ALARP basis will be explored further within Step 4 of GDA.
- Consideration of what is meant by 'adequate strength' during a severe accident is needed to ensure that safety claims on the RPV performance during a severe accident are reasonable.
- The RP has developed what appears to be a comprehensive approach to selecting materials based on the safety case requirements. The application of this methodology will be tested to ensure it is robust for a broad application.
- Detailed assessment of the SG and RCP (eg, design features and material selections).

166. Overall, based upon the Step 3 assessment, no fundamental safety shortfalls in the area of Structural Integrity that might prevent the issue of a DAC for the UK HPR1000 design were identified.

10.20 Cross-Cutting Topics

167. ONR considers cross-cutting topics to be those matters that relate to technical processes and have a substantive impact on the development of the safety case across all technical disciplines. Within ONR, assessment of these topics is coordinated by the PTI to ensure that a consistent approach is taken by both the RP in its development of submissions and ONR in its undertaking of assessments.

168. During Step 3, we have identified several matters as cross-cutting topics:

- Methodology for optioneering and decision making for ALARP.
- Methodology for categorisation of safety functions and classification of SSCs.
- Scope of GDA.
- Development of the UK HPR1000 safety case.

169. With regard to ALARP substantiation, safety categorisation and classification, and the scope of GDA, during Step 2 we reported that ONR was satisfied with the RP's approaches. However, we recognised that they were high-level strategy documents which needed to be supported by working-level procedures and training to provide detailed guidance to RP staff involved in the production of the UK HPR1000 safety case. Consequently, during Step 3 we have focussed our attention on how the arrangements are being applied in practice; we have assessed the quality of safety submissions to confirm that the approaches are applied adequately and consistently by the RP.

170. As has been the case with previous RPs who were not familiar with the UK regulatory context, CGN's safety case and design personnel have at times had difficulties providing suitable and sufficient ALARP arguments to substantiate their safety claims. The main issues we have observed in the submissions and during our interactions with the RP include:

- The requirement to undertake ALARP assessments has, in some areas, been largely driven by ONR. The RP needs to recognise gaps independently.
- Some ALARP optioneering workshops have not included all the technical disciplines that we would expect to see represented, and have also suffered from lack of input from those with UK context experience.

- When selecting options for consideration in an ALARP study, some viable options have been excluded.
- There has been inconsistency in the selection and application of OpEx, which can be used to determine RGP in an ALARP assessment.
- There has been an over-reliance on quantitative arguments for identifying ALARP options, without supporting explanation.

171. Feedback from our assessment team was consolidated and communicated to CGN's design and safety case teams in October 2019 to promote improvement. However, it is important to recognise that throughout Step 3 CGN's personnel have been highly receptive to regulatory comments and guidance and there were indications in the second half of Step 3 of improvements in many ALARP submissions, particularly where RP's safety case authors have maintained regular contact with ONR and there has been UK context input to decision making (either from General Nuclear System Limited, EDF SA or from third party consultants). The issue of the identification and application of OpEx is ongoing and at the time of writing this report ONR is giving this matter a degree of enhanced regulatory scrutiny.

172. The RP's methodology for the categorisation of safety functions and the classification of SSCs was submitted during Step 2 and we concluded that this methodology provided a sound basis for the development of the UK HPR1000 safety case. During Step 3 we have focussed attention on the manner in which this methodology is applied in the UK HPR1000 safety case.

173. During Step 3 ONR has received a number of submissions that outline the preliminary categorisation of safety functions and the classification of SSCs. The most significant submission was an early version of the fault schedule, which the RP submitted at the start of Step 3. This provided the categorisation of safety functions but was based on the list of design basis faults established for Fangchenggang NPP Unit 3 and contained only a preliminary indication of the diverse means of delivering safety functions for frequent faults. The RP provided a commitment to update the information to align with the UK HPR1000 fault analysis. An updated fault schedule, which will also consider any design changes for UK HPR1000, was provided at the end of 2019 and we will consider this as part of our Step 4 assessment.

174. Several topics, such as C&I, Electrical Engineering and Mechanical Engineering have also sought information on the application of the methodology and the resulting classification of SSCs, and findings can be found in sections 10.3, 10.6 and 10.13 respectively. As a priority in Step 4 we will be seeking confirmation, via our assessment of the evidence, that the methodology is being applied consistently across all areas, and that the outputs are being properly captured in the safety case. This matter is also closely associated to other safety case issues described hereafter such as the articulation of the 'golden thread' and the management of requirements and assumptions.

175. With regard to the scope of GDA, for the most part, ONR has been satisfied with the scope report provided by the RP. However, as the level of detail of our assessment increases and we continue to enhance our knowledge of the design, further refinements of the GDA scope document may be necessary during Step 4. Also, as indicated in section 10.12, our MSQA work during Step 4 will look at the RP's arrangements (and their implementation) to maintain alignment between the GDA scope, the Design Reference, the safety case and the Master Document Submission List.

176. One of the biggest challenges facing the RP during Step 3 has been the improvement of its arrangements for developing the UK HPR1000 safety case. Step 2 identified several issues with the RP's arrangements which, without resolution, would have meant that the safety case would have been unlikely to be coherent, cogent, consistent and complete. Consequently, we raised RO-UKHPR1000-0004 to drive improvement. The RO focuses on four aspects of safety case development:

- Safety case development strategy.
- Safety case delivery programme.
- Safety case development organisation.
- Capturing assumptions, requirements and commitments from the safety case.

177. The RP has made progress on all aspects of RO-UKHPR1000-0004, including:

- Using PCSR and GSR strategies, supported by topic specific production strategies that set out the approach to develop the UK HPR1000 safety case throughout GDA, describing what the safety case is expected to contain and the approach that is being taken to manage its production.
- Establishing an integrated delivery tool (IDT) to consolidate a programme of safety case documentation that is intended to be submitted or will be available for sampling. This system will provide General Nuclear System Limited, CGN, EDF SA and the regulators with a consistent understanding of GDA submissions and their intended submission dates.
- Developing the safety case organisation, with the appointment of a CGN safety case manager to provide authority and accountability for the authoring of an adequate safety case, and the establishment of safety case control and working groups to ensure consistency and share expertise (including UK context).
- Setting out a preferred option for managing assumptions, requirements and commitments so that the safety case will be realised in the construction, commissioning, operation, and decommissioning of the UK HPR1000. This option will involve the further development and integration of the fault, engineering and hazards schedules, which ONR recognises as good practice.

178. One of the main challenges we have faced in Step 3 has been influencing the RP to identify the documents that comprise the totality of the safety case. During Step 2 and early Step 3, the RP's list of documents that it planned to submit was limited to those that were being produced specifically for GDA, and so were being largely driven by ONR's assessment. We had little visibility of design and safety documents produced for the reference plant, Fangchenggang NPP Unit 3, and had concerns that the RP would be unable to produce detailed supporting evidence to underpin its safety case within GDA timescales. We engaged with CGN and helped them to understand and recognise the importance of making use of existing Fangchenggang NPP Unit 3 documentation to underpin the UK HPR1000 assessment. The RP has now provided a list of documents that are either planned to be submitted to ONR or will be available upon request for sampling (after translation to English). This has been a vital development that has provided increased confidence that the RP can deliver detailed design information within the challenging timescales of GDA.

179. During Step 3, our inspectors have at times struggled to follow the 'golden thread' within the safety case, which relates to the traceability of the fault analysis, through to the SFRs, and into the design of the SSCs that deliver them. This problem has been alleviated somewhat by the submission of the topic specific production strategies, which provide an overview of how the safety case is structured for each discipline. However, there remain gaps in several important areas that will need to be

addressed in Step 4. Indications are that the RP's proposed solution to address the RO-UKHPR1000-0004 action on the management of requirements and assumptions in the safety case, should largely address this by using the fault, engineering and hazards schedules to 'map' the linkages between the fault analysis and the design of SSCs. However, it is uncertain how far the RP will be able to develop the solution within the timescales of Step 4, we have advised the RP of the importance of articulating the 'golden thread' to ensure successful conclusion of GDA.

180. As discussed in Section 10.12, the quality of submissions, particularly early in Step 3, has been variable. The constrained duration of Step 4 and the many remaining matters for ONR to follow up, as summarised in the previous subsections, mean that the RP will need to deliver at pace whilst ensuring that submissions are of sufficient quality to enable us to undertake a meaningful assessment. This is likely to be a significant challenge to the RP and will have implications on resource demand.

181. In addition to the above cross-cutting matters, an additional area of concern identified during Step 3, which impacts on a wide range of topic areas, is the presentation of arrangements for EMIT of SSCs in the safety case. ONR is not confident that EMIT is considered consistently across the safety case and associated engineering. We have concluded from current submissions that insufficient information is provided to explain what EMIT activities are required and whether these activities can be carried out consistently with the limits and conditions resulting from the safety analysis. The RP has provided an overview of EMIT and some general principles that are proposed to be applied but it is unclear what scope of information will be provided as part of GDA, and what the intention is for further developing this information (either during or post-GDA). This matter has been captured in RO-UKHPR1000-0021 and the assessment is being led by our Fault Studies team.

11 CONCLUSIONS

182. This report is ONR's third public report on the UK HPR1000 and it comes at the end of Step 3. In this step we have increased our regulatory scrutiny and undertaken a more detailed assessment of the design focusing on the methods and approaches used by the RP to meet the safety and security claims for UK HPR1000 that we assessed during Step 2 of GDA.

183. Overall, the interactions with the RP throughout Step 3 have been constructive. Its organisational arrangements have matured during this step, with clear evidence of General Nuclear System Limited, CGN, and EDF SA capturing, and acting upon, learning from Step 2. Working arrangements have generally become embedded and coordination between the three organisations has improved. The structure and organisation of the UK HPR1000 GDA RP is complex and some organisational issues still remain, such as lack of agility in decision-making mechanisms. However, we have seen strong commitment from General Nuclear System Limited, CGN and EDF SA to learn lessons from Steps 1, 2 and 3 of GDA and to improve their working arrangements in the final step of GDA.

184. During Step 3 of GDA we have undertaken assessment work across 19 technical disciplines and we have also covered cross-cutting topics. Our assessment conducted to date has not identified any fundamental safety or security shortfalls that might prevent the issue of a DAC for the UK HPR1000 design. We have however identified a number of potential regulatory shortfalls requiring action and new work by the RP for them to be resolved, and have raised ROs to address those; so far we have formally issued 31 ROs.

185. Moving forward to Step 4, there is a considerable amount of work to be undertaken by the RP, requiring significant resource across all of the topic areas. The timely provision of detailed information containing the necessary evidence will be vital to ensuring that ONR has suitable and sufficient documentation to undertake a meaningful assessment. The constrained timescales of Step 4 are likely to pose a challenge to the RP, and it will have to exercise a high level of control to ensure that the quality of submissions is not challenged by the need to deliver at pace.

186. ONR will continue to rigorously assess the safety and security submissions throughout Step 4 of GDA, and will address potential issues should they arise. We will continue to assess the effectiveness of the RP's arrangements to deliver an adequate, holistic safety case. We expect to see the increased involvement of the Bradwell Power Generation Company, the prospective future licensee for the Bradwell B NPP, during Step 4.

12 REFERENCES

1. UK HPR1000 Generic Design Assessment (GDA) – Assessment of the readiness of the GDA Requesting party (RP) and ONR to commence GDA. ONR. October 2016. http://www.onr.org.uk/pars/2017/uk-hpr1000-16-005.pdf

2. UK HPR1000 Reactor: Written statement - HCWS398. BEIS. January 2017. https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2017-01-10/HCWS398/

3. UK HPR1000 Generic Design Assessment (GDA) Website. General Nuclear System Limited. http://www.ukhpr1000.co.uk/

4. Summary of the Step 2 Assessment of the UK HPR1000 Reactor, Project Assessment Report ONR-NR-PAR-18-007, ONR, November 2018. http://www.onr.org.uk/pars/2018/uk-hpr1000-18-007.pdf

5. Regulators begin Step 2 of nuclear reactor assessment. ONR and EA. November 2017. http://news.onr.org.uk/2017/11/regulators-begin-step-2-of-assessment-of-new-nuclear-reactor/

6. Generic Design Assessment Joint Regulators Website (HPR1000). ONR and EA. http://www.onr.org.uk/new-reactors/uk-hpr1000/index.htm

7. UK HPR1000 Pre-Construction Safety Report. General Nuclear System Limited. http://www.ukhpr1000.co.uk/documents-library/pre-construction-safety-report/

8. Nuclear Industry Security Regulations 2003 (as amended), www.legislation.gov.uk

9. New Nuclear Power Plants: Generic Design Assessment Guidance to Requesting Parties, ONR-GDA-GD-006 Revision 0, ONR, October 2019. http://www.onr.org.uk/new-reactors/guidance-assessment.htm

10. Generic Design Assessment Guidance to Requesting Parties for the UK HPR1000, ONR-GDA-GD-001 Revision 4. ONR. October 2019. http://www.onr.org.uk/new-reactors/ngn03.pdf

11. Environmental management – Nuclear regulation. EA. https://www.gov.uk/topic/environmental-management/nuclear-regulation

12. Safety Assessment Principles for Nuclear Facilities. ONR. 2014 Edition Revision 1. ONR. January 2020. http://www.onr.org.uk/saps/saps2014.pdf

13. Office for Nuclear Regulation (ONR) Permissioning Inspection – Technical Assessment Guides. http://www.onr.org.uk/operational/tech_asst_guides/index.htm

14. Risk Informed Regulatory Decision Making. ONR. June 2017. http://www.onr.org.uk/documents/2017/risk-informed-regulatory-decision-making.pdf

15. Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable). ONR. December 2019. http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-005.pdf

16. Security Assessment Principles for the Civil Nuclear Industry. 2017 Edition. ONR. March 2017. http://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf

17. The Ionising Radiations Regulations 2017 and Approved Code of Practice (ACOP) and guidance, L121, second edition. HSE. 2018. www.legislation.gov.uk

18. Construction (Design and Management) Regulations 2015, www.legislation.gov.uk

Annex 1

STEP 3: OVERALL DESIGN, SAFETY CASE AND SECURITY ARGUMENTS REVIEW
http://www.onr.org.uk/new-reactors/ngn03.pdf

Description and aims

Step 3 is primarily a review by ONR of the arguments (or 'reasoning') supporting the RP's claims regarding the safety and related security aspects of the proposed design.

The intention in this Step is to move from the fundamentals of the previous step to an analysis of the design, primarily at the system level, and by analysis of the RP's arguments that support the safety and security claims.

The specific aims of this step are to:

- improve ONR knowledge of the design;
- assess the safety and security arguments;
- progress the resolution of issues identified during Step 2;
- identify whether any significant design or safety case changes may be needed;
- identify major issues that may prevent ONR issuing a DAC and attempt to resolve them; and thereby
- achieve a significant reduction in regulatory uncertainty.

The exact scope and focus of step 3 will depend on the design and on the outcome of Step 2.

This step may take around 12 months, assuming that the RP is able to provide quality and timely submissions and responses to regulatory concerns.

Exceptionally, in the event that the RP is not able to provide the information necessary for ONR to complete the step in the indicative time period, there is scope for the step to be extended for an agreed, limited period to allow the requisite documentation to be submitted and assessed. Agreement to such an extension would be dependent on the confirmed availability of ONR's specialist resources during the proposed extension period. ONR will still aim to achieve the original planned overall timescale for completing GDA, for instance by seeking to shorten the next step.

The RP is required to:

Provide, at the start of Step 3, sufficient safety and security documentation to allow ONR to proceed with assessment across all technical areas. Where full documentation cannot be provided at the start of the step, ONR and the RP will need to agree a schedule of submissions. The documentation should include the following:

- Responses to any matters outstanding from Step 2.
- Explanation of how the decisions regarding the achievement of safety functions ensure that the overall risk to workers and public will be ALARP.
- Sufficient information to substantiate the claims made in the Safety and Security Reports.
- Sufficient information to enable ONR to assess the design against all relevant SAPs.
- A demonstration that the detailed design will meet the safety and security objectives before construction or installation commences, and that sufficient analysis and engineering substantiation has been performed to prove that the operational plant will be adequately safe and secure.
- Detailed descriptions of system architectures, their safety or security functions, and reliability and availability requirements.

- Confirmation and justification of the design codes and standards that have been used and where they have been applied, non-compliances and their justification.
- Fault analyses including DBA, Severe Accident Analysis and PSA.
- Safety function categorisation and the safety classification of structures, systems and components (SSC) - with a demonstration of how this is reflected in the design.
- Justification of the safety and security of the design throughout the plant's life cycle, from construction through operation to decommissioning and including on-site spent fuel and radioactive waste management features.
- Identification of potentially significant safety and security issues that have been raised in assessments of the design by overseas regulators, and explanations of how they have been (or will be) resolved.
- Identification of the safe operating envelope and the operating regime that maintains the integrity of that envelope.
- Definition of the technical and documentary scope of GDA, including definition of the safety and security submission, definition of a Design Reference, and Design Reference Point, and implementation of GDA submission configuration control arrangements. This should also include confirmation of:
    - those aspects of the design, safety case and supporting documentation that are complete and are intended to be covered by the DAC;
    - any aspects that are still under development; and
    - identification of outstanding confirmatory work that will be addressed during Step 4.
- Confirmation of the proposals for:
    - updating the Master Document Submission List;
    - the Design Reference;
    - the management of design changes during GDA; and
    - the safety submission freeze.
- Towards the end of Step 3, undertake a review of its readiness to move to Step 4 and report on the outcome of this review to ONR
- Provide a list of Vital Areas and provide an example(s) of how the VAI methodology has been applied.

The above documentation may be in the form of a draft Pre-Construction Safety Report (PCSR) or Generic Security Report (GSR). Where necessary, the RP should update the safety documentation on their website (removing commercial information, and security sensitive information) to reflect additional details provided during step 3.

The RP will also be required to respond to questions and points of clarification raised by ONR during its assessment, and to relevant issues arising from public comments.

Step 3: ONR will:

Undertake an assessment of the RP’s submission, on a sampling basis, primarily directed at the system level, focussing on the RP's supporting arguments. The scope of ONR’s assessment will be partly defined by experience in step 2 and the issues arising in that step, and also by experience in previous GDAs.

This will include:

- Considering whether the design is likely to meet the RP's design safety criteria and that these ensure risks will be ALARP.
- Undertaking an initial assessment of the scope and extent of the arguments in each of the technical areas, including the generic site envelope.
- Assessing the safety case development process scope and extent.

- Reviewing what overseas regulators have done and how ONR can make use of it.
- Deciding on scope of, and plan for, further assessment.
- Assessing the quality assurance (QA) arrangements, including safety case and design change control arrangements.
- Assessing the RP's independent verification process.
- Identifying the need for additional regulatory verification / analysis.
- Judging whether the design is balanced in terms of the different contributors to the overall risk from the plant.
- Reviewing the RP proposals for spent fuel management, radioactive waste management and decommissioning.
- Identifying any research needs and setting up of longer-term research or contract support to complement Step 4.
- Considering security proposals and undertaking a detailed review of the security architecture of the plant including assessment of how those areas requiring protection have been identified and categorised.
- Considering issues identified through the public involvement process.
- Undertaking a review of ONR's own readiness to move to Step 4.

Step 3: ONR output

ONR will publish:

- a statement on the progress of ONR's assessment of the design, safety case and security arguments;
- a summary report describing any outstanding safety or security issues which have the potential to require significant design or safety case changes, or which may prevent ONR issuing a DAC; and
- a statement on whether the design assessment can move to Step 4.

Annex 2

REGULATORY OBSERVATIONS ISSUED

(Refer to http://www.onr.org.uk/new-reactors/uk-hpr1000/ro-res-plan.htm for further details)

RO-UKHPR1000-0001	Diverse Actuation System Design Shortfalls
RO-UKHPR1000-0002	Demonstration that the UK HPR1000 Design is Suitably Aligned with the Generic Site Envelope
RO-UKHPR1000-0003	Suitable and Sufficient Severe Accident Analysis Safety Case
RO-UKHPR1000-0004	Development of a Suitable and Sufficient Safety Case
RO-UKHPR1000-0005	Demonstration that the UK HPR1000 Design Reduces the Risks Associated with Radioactive Waste Management, So Far As Is Reasonably Practicable
RO-UKHPR1000-0006	Avoidance of Fracture Demonstration
RO-UKHPR1000-0007	Aircraft Impact Safety Case for UK HPR1000
RO-UKHPR1000-0008	Justification of the Structural Integrity Classification of the Main Coolant Loop
RO-UKHPR1000-0009	Geotechnical Design Parameters
RO-UKHPR1000-0010	Discharge Estimates and Limits
RO-UKHPR1000-0011	Human Factors Capability and Integration to Deliver the GDA of UK HPR1000
RO-UKHPR1000-0012	Identification and Application of Relevant Good Practice Applicable to Mechanical Engineering for the UK HPR1000 Design
RO-UKHPR1000-0013	Modelling of Computer Based System Reliability in the PSA
RO-UKHPR1000-0014	Spent Fuel Building – Design of Nuclear Lifting Operations to Demonstrate Relevant Risks are Reduced to ALARP
RO-UKHPR1000-0015	Demonstration that Risks Associated with Fuel Deposits are Reduced So Far As Is Reasonably Practicable (SFAIRP)
RO-UKHPR1000-0016	Demonstration of Compliance with Relevant Good Practice for Control and Instrumentation
RO-UKHPR1000-0017	Demonstration of Independence between C&I Systems
RO-UKHPR1000-0018	Substantiation of HRA Inputs in PSA Model
RO-UKHPR1000-0019	Substantiation of Initiating Event Frequencies in the PSA
RO-UKHPR1000-0020	Veracity of PSA Data

RO-UKHPR1000-0021	Demonstration of the Adequacy of Examination, Maintenance, Inspection and Testing (EMIT) of Structures, Systems and Components Important to Safety
RO-UKHPR1000-0022	Design for Access and Inspectability
RO-UKHPR1000-0023	Demonstration of Diverse Protection for Frequent Faults
RO-UKHPR1000-0024	Control of Changes to the UK HPR1000 Design
RO-UKHPR1000-0025	Vital Area Identification and Categorisation
RO-UKHPR1000-0026	Demonstration that Radioactivity has been Reduced So Far As is Reasonably Practicable (SFAIRP)
RO-UKHPR1000-0027	Debris Effects on Safety Injection System and Containment Heat Removal System Performance
RO-UKHPR1000-0028	Adequate Justification of Estimated Public Doses for UK HPR1000
RO-UKHPR1000-0029	Internal Fire PSA
RO-UKHPR1000-0030	Justification for the Use of Automatic Diagnosis
RO-UKHPR1000-0031	Control of Boron during Normal Operations and Faults