Office for Nuclear Regulation

An agency of HSE

# Generic Design Assessment – New Civil Reactor Build

# Step 4 Internal Hazards Assessment of the EDF and AREVA UK EPR™ Reactor

Assessment Report: ONR-GDA-AR-11-017
Revision 0
11 November 2011

## COPYRIGHT



First published December 2011

## PREFACE

The Office for Nuclear Regulation (ONR) was created on 1st April 2011 as an Agency of the Health and Safety Executive (HSE). It was formed from HSE's Nuclear Directorate (ND) and has the same role. Any references in this document to the Nuclear Directorate (ND) or the Nuclear Installations Inspectorate (NII) should be taken as references to ONR.

The assessments supporting this report, undertaken as part of our Generic Design Assessment (GDA) process and the submissions made by EDF and AREVA relating to the UK EPR™ reactor design, were established prior to the events at Fukushima, Japan. Therefore, this report makes no reference to Fukushima in any of its findings or conclusions. However, ONR has raised a GDA Issue which requires EDF and AREVA to demonstrate how they will be taking account of the lessons learnt from the events at Fukushima, including those lessons and recommendations that are identified in the ONR Chief Inspector's interim and final reports. The details of this GDA Issue can be found on the Joint Regulators' new build website www.hse.gov.uk/newreactors and in ONR's Step 4 Cross-cutting Topics Assessment of the EDF and AREVA UK EPR™ reactor.

## EXECUTIVE SUMMARY

This report presents the findings of the Internal Hazards Assessment of the UK EPR™ reactor undertaken as part of Step 4 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA). The assessment has been carried out on the Pre-construction Safety Report (PCSR) and supporting documentation submitted by Electricité de France SA (EDF) and AREVA NP SAS (AREVA) during Step 4.

This assessment has followed a step-wise-approach in a claims-argument-evidence hierarchy. In Step 2 the claims made by the EDF and AREVA were examined and in Step 3 the arguments that underpin those claims were examined.

The scope of the Step 4 assessment was to review the safety aspects of the UK EPR reactor in greater detail, by examining the evidence, supporting the claims and arguments made in the safety documentation, building on the assessments already carried out for Steps 2 and 3, and to make a judgement on the adequacy of the internal hazards information contained within the PCSR and supporting documentation.

It is seldom possible, or necessary, to assess a safety case in its entirety, therefore sampling is used to limit the areas scrutinised, and to improve the overall efficiency of the assessment process. Sampling is done in a focused, targeted and structured manner with a view to revealing any topic-specific, or generic, weaknesses in the safety case. To identify the sampling for internal hazards an Assessment Plan for Step 4 was set-out in advance.

My safety assessment within this topic includes hazards such as fire, explosion, flood, dropped loads, pressure part failure, and steam release etc. within the reactor buildings. I have considered the adequacy of: the identification of hazards; prevention of hazards; and the protective barriers, segregation, separation, and active protection systems that are included within the design to provide mitigation in the unlikely event that such internal hazards should occur.

For GDA Step 3 my assessment sample covered internal hazards elements of the PCSR and supporting documentation that focused on an examination of the principal claims and arguments presented by EDF and AREVA for redundancy and segregation of plant and equipment important to nuclear safety. Redundancy is achieved through four segregated 'trains' of protection, with each train able to provide 100% of the safety duty required to enable safe shutdown and post trip cooling. A 'train' of protection includes all the elements necessary to perform the safety function, for example water source, pumps, pipes, electrical supplies etc.

My assessment has focussed on:

- Ensuring that any areas required for further assessment during Step 4, identified within the Step 4 Internal Hazards Assessment Plan of the EDF and AREVA UK EPR, have been adequately captured either within this assessment or are captured as part of assessment done in other related technical assessment areas.
- The requisite evidence relating to internal hazards in the areas of dropped loads and impact, high energy line break, internal missile, fire, steam release, internal flooding, and internal explosion.
- Undertaking deep slice sampling of the evidence for a number of areas, including, common cause failure and hydrogen generation.
- Assessment and close out of Regulatory Observations raised during Step 3 that were not subject to detailed assessment within the Step 3 Internal Hazards Assessment of the EDF and AREVA UK EPR.

No items have been identified as being outside the scope of the GDA process.

From my assessment, I have concluded that:

- EDF and AREVA have been proactive in addressing observations made within Step 4 of the GDA and this has resulted in positive improvements in the design of the UK EPR, specifically, door control measures for doors performing nuclear safety functions and fire modelling. These are examples that provide confidence and strength in the robustness of the safety case for internal hazards. Furthermore a great deal of work has been undertaken by EDF and AREVA relating to detailed analysis of potential internal hazards which has arisen from a thorough understanding of both the safety case and the design.
- The design of the UK EPR is broadly in line with my expectations in relation to current national and international standards, guidance and relevant good practice. There are a number of areas where further internal hazards substantiation is required in order to ensure that the safety case for these specific hazards areas is robust. In addition, concerns have arisen over the approach taken to safety case for internal flooding and the lack of a detailed consequence analysis associated with dropped loads and missile impact.
- Overall, I believe that, in the majority of areas, there is a clear philosophy and logic associated with design and that the UK EPR PCSR has been developed utilising a thorough and robust analysis of the threats posed by internal hazards.

In some areas there has been a lack of detailed information which has limited the extent of my assessment. As a result the ND will need additional information in the longer term to underpin my conclusions and I have identified these areas as Assessment Findings that will be carried forward as part of normal regulatory business. Examples where such information will be required include design changes identified within analyses undertaken that have not been captured within the safety case, evidence associated with door design and cable specifications and protection in relation to steam release.

Some of the observations identified within this report are of particular significance and will require resolution before the HSE would agree to the commencement of nuclear safety related construction of a UK EPR reactor in the UK. These are identified in this report as GDA Issues and are listed in Annex 2. In summary these relate to:

- Substantiation and analysis of the consequences of dropped loads and impact from lifting equipment included within the EPR design. This is due to inconsistencies between the approach stated and my expectations detailed within our Safety Assessment Principles and our interpretation of national and international standards and guidance.
- Outstanding internal hazards substantiation for internal flooding, cable routing, high energy line break and missiles form part of the requisite evidence and will be required in order to demonstrate an adequate internal hazards safety case.
- The internal flooding claims stated within the PCSR appear inconsistent with our expectations in terms of the deterministic approach to the analysis of potential sources of internal flooding.
- Substantiation of the claims made within the PCSR associated with the consequences of missile generation arising from failure of RCC-M Components.

Overall, based on the sample undertaken in accordance with ND procedures, I am broadly satisfied that the claims, arguments and evidence laid down within the PCSR and supporting documentation submitted as part of the GDA process present an adequate safety case for the generic UK EPR reactor design. The UK EPR reactor is therefore suitable for construction in the UK, subject to satisfactory progression and resolution of GDA Issues to be addressed during the forward programme for this reactor and assessment of additional information that

becomes available as the GDA Design Reference is supplemented with additional details on a site-by-site basis.

## LIST OF ABBREVIATIONS

| | |
|---|---|
| AC | Alternating Current |
| ALARP | As Low As Reasonably Practicable |
| AREVA | AREVA NP SAS |
| ASN | Autorité de Sûreté Nucléaire (French nuclear safety authority) |
| BMS | (Nuclear Directorate) Business Management System |
| BSL | Basic Safety Level (in SAPs) |
| BSO | Basic Safety Objective (in SAPs) |
| CCWS | Component Cooling Water System |
| CHRS | Containment Heat Removal System |
| C&I | Control and Instrumentation |
| CNSC | Canadian Nuclear Safety Commission |
| CRF | Circulating Water System |
| CVCS | Chemical and Volume Control System |
| DECC | Department of Energy and Climate Change |
| DFL | Smoke Control and Extract System |
| DfT | Department for Transport |
| EBS | Extra Borating System |
| EDF | Electricité de France SA |
| EFWS | Emergency Feed Water System |
| EMI | Electromagnetic Interference |
| ESWS | Essential Service Water System |
| FA3 | Flamanville 3 Nuclear Power Station |
| FDS | Fire Dynamics Simulator |
| FPCS | Fuel Pool Cooling System |
| GDA | Generic Design Assessment |
| GSI | Generic Safety Issue |
| GWPS | Gaseous Waste Processing System |
| HELB | High Energy Line Break |
| HSE | The Health and Safety Executive |
| HRR | Heat Release Rate |
| HVAC | Heating, Ventilation, and Air-Conditioning |
| IAEA | The International Atomic Energy Agency |
| IRWST | In-containment Refuelling Water Storage Tank |

## LIST OF ABBREVIATIONS

| | |
|---|---|
| JAC | Fire Fighting Water Supply |
| JPI | Fire Fighting Hydrant System |
| LEL | Lower Explosive Limit |
| LFL | Lower Flammability Limit |
| LOCA | Loss Of Coolant Accident |
| LOOP | Loss Of Offsite Power |
| MDEP | Multi-national Design Evaluation Programme |
| MFWS | Main Feed Water System |
| MSRT | Main Steam Relief Train |
| MSSS | Main Steam Supply System |
| MW | Megawatt |
| NCB | Non Classified Building |
| ND | The (HSE) Nuclear Directorate |
| NDA | Nuclear Decommissioning Authority |
| NPSH | Net Positive Suction Head |
| NTG | Nuclear Topic Group |
| OCNS | Office for Civil Nuclear Security |
| OECD | Organisation for Economic Co-operation and Development |
| PCC | Plant Condition Category |
| PCSR | Pre-construction Safety Report |
| PID | Project Initiation Document |
| PSA | Probabilistic Safety Analysis |
| PSR | Preliminary Safety Report |
| PWR | Pressurised Water Reactor |
| RB | Reactor Building |
| RCP | Reactor Coolant Pump |
| RCS | Reactor Coolant System |
| RGP | Relevant Good Practice |
| RHR | Residual Heat Removal |
| RO | Regulatory Observation |
| ROA | Regulatory Observation Action |
| RRC | Risk Reduction Category |
| SAB | Safeguards Auxiliary Building |
| SAPs | HSE Safety Assessment Principles |

## LIST OF ABBREVIATIONS

| | |
|---|---|
| SFA | Access Fire Compartment |
| SFC | Fire Containment Compartment |
| SFE | Environment Fire Compartment |
| SFI | Intervention Fire Compartment |
| SFS | Safety Fire Compartment |
| SGBS | Steam Generator Blowdown System |
| SIS | Safety Injection System |
| SSC | System, Structure and Component |
| SSER | Safety, Security and Environmental Report |
| STUK | Säteilyturvakeskus (The Finish Nuclear Safety Authority) |
| TAG | (Nuclear Directorate) Technical Assessment Guide |
| TQ | Technical Query |
| TSC | Technical Support Contractor |
| UCWS | Ultimate Cooling Water System |
| US NRC | Nuclear Regulatory Commission (United States of America) |
| WENRA | Western European Nuclear Regulators' Association |

## TABLE OF CONTENTS

**Tables**



**Annexes**

# 1 INTRODUCTION

1 This report presents the findings of the Step 4 Internal Hazards Assessment of the UK EPR™ reactor Pre-construction Safety Report (PCSR) (Ref. 17) and supporting documentation provided by Electricité de France SA (EDF) and AREVA NP SAS (AREVA) under the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process. Assessment was undertaken of the PCSR and the supporting evidence derived from the Submission Master List (Ref. 18). The approach taken was to assess the principal submission, i.e. the PCSR, and then undertake assessment of the relevant documentation sourced from the Master Submission List on a sampling basis in accordance with the requirements of the (HSE) Nuclear Directorate (ND) Business Management System (BMS) procedure AST/001 (Ref. 2). The Safety Assessment Principles (SAPs) (Ref. 4) have been used as the basis for this assessment. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

2 During the assessment a number of Technical Queries (TQ) and Regulatory Observations (RO) were issued and the responses made by EDF and AREVA assessed. Where relevant, detailed design information from specific projects for this reactor type has been assessed to build confidence and assist in forming a view as to whether the design intent proposed within the GDA process can be realised.

# 2 NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR INTERNAL HAZARDS

3 The intended assessment strategy for Step 4 for the internal hazards topic area was set out in an assessment plan that identified the intended scope of the assessment and the standards and criteria that would be applied. This is summarised below:

## 2.1 Assessment Plan

4 The Step 4 Internal Hazards Assessment Plan for UK EPR (Ref. 21) identified that the objective of the Step 4 assessment was to review the safety aspects of the proposed reactor designs in a more detailed way by examining the evidence supporting arguments and claims made in the EDF and AREVA safety documentation. The Step 4 was intended to build on the assessment already undertaken for Steps 2 and 3 and make a judgement on the adequacy of the internal hazards safety case within the PCSR and supporting documents.

5 The overall bases for the start of assessment in GDA Step 4 were the internal hazards elements of :

- (i) the update to the Submission / PCSR / Supporting Documentation, (ii) the Design Reference that relates to the Submission / PCSR as set out in UK EPR GDA Project Instruction UK EPR/I/002; These submissions should fulfil the requirements of the GDA Guidance to Requesting Parties (Ref. 5).
- Design Change Submissions proposed by EDF and AREVA which have been incorporated within the GDA scope with agreement of Assessment Unit Heads.

6 To allow time for consideration of the consolidated PCSR (Ref. 22) before the end of Step 4, delivery to ND of the final version of the aforementioned submission was required to be issued to ND by end of March 2011. This then allowed the Step 4 assessment to be reviewed against the consolidated PCSR to ensure all matters that have been raised as a result of the Step 4 assessment have been captured.

7 Within the Step 4 Plan the following generic HSE Commitments were required to be taken into consideration as part of the Step 4 Internal Hazards Assessment.

- Consideration of issues identified in Step 3.
- Judging the design against SAPs and judging whether the proposed design reduces risks to as low as reasonably practicable (ALARP).
- Inspections of the Requesting Party's procedures and records.
- Independent verification analyses.
- Reviewing details of the design controls, procurement and quality control arrangements to secure compliance with the design intent.
- Establishing whether the system performance and reliability requirements are substantiated by the detailed engineering design.
- Assessing arrangements for moving the safety case to an operating regime.
- Assessing arrangements for ensuring and assuring that safety claims and assumptions are realised in the final design, building and construction.
- Judging whether significant site parameters are appropriately defined in the generic site envelope.
- Reviewing overseas progress and issues raised by Overseas Regulators.
- Considering unresolved issues raised through the public involvement process.
- Resolution of identified nuclear safety issues, or identifying paths for resolution.

## 2.2 Standards and Criteria

8 The relevant standards and criteria adopted within this Step 4 assessment are primarily the Safety Assessment Principles, internal technical assessment guides, relevant national and international standards and relevant good practice informed from existing practices adopted on UK nuclear licensed sites. The key SAPs and relevant (Nuclear Directorate) Technical Assessment Guides (TAGs) have been detailed within this section. National and international standards and guidance have been referenced where appropriate within the assessment report. Relevant good practice, where applicable, has also been cited within the body of the assessment.

### 2.2.1 Safety Assessment Principles

9 The key SAPs applied within the internal hazards assessment of the EDF and AREVA UK EPR are included within Table 6 of this report.

### 2.2.2 Technical Assessment Guides

10 The following technical assessment guides have been used as part of this assessment:

1. Technical Assessment Guide - Internal Hazards, T/AST/014 Issue 02 (Ref. 6)
2. Technical Assessment Guide – Diversity, Redundancy, Segregation and Layout of Mechanical Plant, T/AST/036 Issue 02 (Ref. 7)

3. Technical Assessment Guide – Guidance on the Purpose, Scope and Content of Nuclear Safety Cases, T/AST/051 Issue 01 (Ref. 8)

### 2.2.3 National and International Standards and Guidance

11 The following international standards and guidance have been used as part of this assessment:

1. *Safety of Nuclear Power Plants: Design. Safety Requirements*, NS.R.1(Ref. 9)
2. *Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants. Safety Guide*, NS.G.1.7 (Ref. 10)
3. *Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants. Safety Guide*, NS.G.1.11 (Ref. 11)
4. *Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA Reactor Reference Safety Levels. Issue S: Protection Against Internal Fires*, (Ref. 12)

## 2.3 Assessment Scope

12 The intended assessment strategy for Step 4 for the internal hazards topic area was set out in an assessment plan that identified the intended scope of the assessment and the standards and criteria that would be applied. This is summarised below:

### 2.3.1 Findings from GDA Step 3

13 A number of areas were identified during Step 3 which warranted further assessment within Step 4, some of which were related to a lack of detail relating to claims and arguments that would have been expected as part of the scope of the PCSR submitted in support of Step 3 and a general assessment task associated with a need to analyse the evidence as part of Step 4. In addition, due to resource and time implications, areas have been identified for assessment arising from the limited sampling undertaken by ND during Step 3. The areas identified for further assessment are detailed within Table 1, below.

**Table 1:** Areas for Further Assessment Identified Within Step 3

| Assessment Area | Description |
|---|---|
| Dropped Loads and Internal Missile Methodologies | Assessment of the methods applied in the production of the claims, arguments and evidence associated with dropped loads and internal missiles. |
| Fuel Building | Internal hazards assessment of the Fuel Building to determine whether there are any specific nuclear safety claims associated with the buildings themselves. |

| Assessment Area | Description |
|---|---|
| Fire Protection System – Random Failures | Further assessment of the claims made on the fire protection systems when the system is required to perform an F1 function e.g. pond water make-up.<br><br>Note: The function of an F1 system is to either attain a controlled shutdown state (F1A) or to secure safe shutdown after the controlled state has been reached (F1B). |
| RO-UKEPR-30 – Fire Barriers | Complete assessment of RO-UKEPR-30 relating to the MAGIC Fire Modelling that was undertaken to support the claims associated with total burnout of fire compartments. |
| RO-UKEPR-35 – Door Control Measures | The response to this RO was received after the Step 3 report had been produced and will be subject to assessment within Step 4. |
| Cable Routing and Segregation | Further assessment of the arguments coupled with assessment of the evidence associated with the provision of segregated cable routes. |
| Internal Flooding | Arguments associated with internal flooding are to be assessed during Step 4 due to the limited assessment undertaken at Step 3. |
| Dropped Loads and Impact | Arguments associated with dropped loads and impact (including crane zoning and interlocks) is to be assessed during Step 4 due to the limited assessment undertaken at Step 3. |
| Internal Missile Generation | Arguments associated with internally generated missiles are to be assessed during Step 4 due to the limited assessment undertaken at Step 3. |
| Internal Explosion | Arguments associated with intern explosion are to be assessed during Step 4 due to the limited assessment undertaken at Step 3. |
| Internal Hazards - General | Sampling of the evidence provided to support the claims and arguments made during Step 3. |

14 All issues identified specifically within the Step 3 Internal Hazards Assessment (Ref. 13) have been captured and included within this Step 4 report explicitly. In addition, there are some areas where information has yet to be produced for the reference design Flamanville 3 (FA3) and as a result have not been submitted to ND for assessment; however, such areas are captured as either Assessment Findings or GDA Issues depending upon the nuclear safety significance of the outstanding information.

### 2.3.2 Additional Areas for Step 4 Internal Hazards Assessment

15 The areas for assessment during Step 4 were identified as a result of the follow on assessment of the areas identified within Step 3. In addition, there was assessment of the evidence associated with the following internal hazards areas:

- Protection of plant and equipment important to safety against the effects of internally generated missiles.

- Internal hazards substantiation of the FA3 design associated with Internal Flooding including operator actions.
- Substantiation of the consequences associated with dropped loads and impact from RS1 and RS2 lifting equipment.
- Internal hazards substantiation associated with the cable routing and segregation in place for the reference design, FA3.
- Deep slice sample of the analysis undertaken associated with common mode failure in the event of fire.

### 2.3.3 Use of Technical Support Contractors

16 Atkins was used to provide technical support throughout the assessment phase of the UK EPR Step 4 Internal Hazards Assessment.

### 2.3.4 Cross-cutting Topics

17 There were a number of areas during the Step 4 assessment when there was a need to consult with other assessors. These areas have been overseen by ND to ensure that all potential interactions are captured and that nugatory duplicate assessment work is prevented. The cross-cutting subjects within the Internal Hazards assessment of UK EPR were:

- Categorisation and classification
- Operator Actions
- Hydrogen Evolution within Containment
- Cable Routing
- Spurious Actuation
- Dropped Loads and Impact
- Failure of pressure vessels, tanks and pipework
- Fault Schedule and Deterministic Analysis

### 2.3.5 Integration with Other Assessment Topics

18 Table 2 identifies the key assessment areas involved in an integrated approach taken to the cross-cutting subjects associated with internal hazards (other technical areas were consulted during the assessment process when required):

**Table 2:** Integration with other Assessment Topics

| Cross-cutting Subject | Specific Assessment Area | Technical Assessment Area |
|---|---|---|
| Categorisation and Classification | Internal Hazards | All assessment disciplines overseen by Unit Heads |
| Operator Actions | Internal Flooding | Human Factors |

| Cross-cutting Subject | Specific Assessment Area | Technical Assessment Area |
|---|---|---|
| | Dropped Loads and Impact | |
| Hydrogen Evolution within Containment | Internal Explosion | Severe Accident Analysis<br>Reactor Chemistry |
| Cable Routing and Segregation | Internal Fire | Electrical Assessment |
| Spurious Operation | Electro-Magnetic Interference | Electrical Assessment<br>Control and Instrumentation Assessment |
| RS1 and RS2 Lifting Equipment | Dropped Loads and Impact | Mechanical Engineering Assessment<br>Civil Engineering Assessment<br>Control and Instrumentation Assessment |
| Failure of pressure vessels, tanks and pipework | In-Containment Missiles and Pipewhip | Structural Integrity Assessment<br>Civil Engineering Assessment |
| Fault Schedule and Deterministic Analysis | Redundancy, diversity and segregation for internal hazards. | Deterministic Safety Assessment |

### 2.3.6 Out of Scope Items

19 No items have been identified as being out of scope of GDA.

## 3 REQUESTING PARTY'S SAFETY CASE

20 The internal hazards safety case for the UK EPR is set out in the PCSR and the relevant parts are summarised in this section. The safety case is based upon a deterministic analysis of internal hazards utilising a combination of active and passive means to the prevention of hazard escalation beyond an individual train of protection. There are four redundant divisions each capable of fulfilling the three basic nuclear safety functions; control of reactivity, removal of heat from the core, and containment of radioactive substances. Internal hazards are postulated to occur in two different types of safety classified building, these two types being:

- Type 1 Buildings; buildings which are separated into divisions, for example the Safeguard Buildings and the Diesel Generator Buildings.
- Type 2 Buildings; buildings or parts of buildings which are not separated into divisions, for example the Containment Building.

21 If an internal hazard occurs in a Type 1 Building, the design must ensure that the consequences of the hazard are limited to the affected division. This means that the building structures necessary to prevent the propagation of an internal hazard (fire, flood, steam release etc.) must be designed to withstand the consequences of the internal hazard. The approach also requires that any penetrations or interlinking of the divisions be minimised.

22 If an internal hazard occurs in a Type 2 Building, the installation rules or the design must ensure that not more than one redundant F1 system is affected. The function of an F1 system is to either attain a controlled shutdown state (F1A) or to secure safe shutdown after the controlled state has been reached (F1B). As part of the design there is a distinction drawn between local and global effects of the hazard:

- Local effects are those limited to the immediate area where the hazard occurs e.g. pipewhip, jet impingement and fire.
- Global effects are those which may have an impact on larger areas of the building e.g. increase in the ambient temperature, moisture, or flooding. These global effects must be limited to the affected building.

23 The PCSR identifies the following internal hazards and addresses them within Section 13.2 of the PCSR:

- Pipework leaks and breaks (including tanks, pumps and valves).
- Internally generated missiles.
- Dropped loads.
- Internal explosions.
- Fire.
- Internal flooding.

24 Electro-Magnetic Interference (EMI) is not addressed within Section 13.2 as it is included in Section 7.2 of the PCSR relating to Control and Instrumentation (C&I).

25 The design and installation of classified or non-classified mechanical, electrical and control systems must, where reasonably practicable, be such that an internal hazard cannot trigger a Plant Condition Category (PCC), PCC-3 / PCC-4 event. The PCSR

states that if a PCC-3 / PCC-4 event is caused by an internal hazard, an adequate number of safety classified systems / redundancies, designed to mitigate the effects of a PCC-3 / PCC-4 event, must remain operational taking into account the single failure principle. PCC events are graded from 1 to 4 and are defined within the PCSR as:

- PCC-1 which includes all normal operating conditions characterised by initiating events whose estimated frequency of occurrence is greater than 1 per year.
- PCC-2 which includes design basis transients, characterised by initiating events with an estimated frequency of occurrence in the range of $10^{-2}$ to 1 per year.
- PCC-3 which includes all design basis incidents, characterised by initiating events with an estimated frequency of occurrence within the range of $10^{-4}$ to $10^{-2}$ per year.
- PCC-4 which includes all design basis accidents, characterised by initiating events with a frequency of occurrence within the range of $10^{-6}$ to $10^{-4}$ per year.

26 Internal hazards within the Nuclear Auxiliaries Building, the Turbine Hall and other non-safety classified buildings must be analysed to show that inadmissible consequences to safety-classified buildings are avoided.

27 The other aspect relating to the assessment of internal hazards is associated with the potential internal hazards arising from a PCC-3 / PCC-4 or Risk Reduction Category (RRC) RRC-A event. These are addressed within the safety analysis for the individual events. However, in all cases non-redundant safety classified Structures, Systems and Components (SSCs) must be designed to withstand the impact of internal hazards. In the case of redundant safety classified SSCs, internal hazard-induced failure of redundant elements that are not required to achieve a safe state is an acceptable consequence.

28 The SSCs required in the event of an RRC-B event (core meltdown accidents) should be designed to withstand the effects of any associated internal hazards. The single failure principle is not applied, however, the following must be shown:

- The containment remains leak-tight.
- Where necessary, the containment internal structures maintain their load bearing capability.
- The functionality of the containment support systems (e.g. hydrogen control system, Containment Residual Heat Removal System (CHRS) and the necessary instrumentation is ensured.
- The generation of missiles that could threaten the containment function or its support systems is avoided.
- Habitability of the control room is ensured.

29 By demonstrating the above requirements, it follows that the systems required to control the RRC-B event are not unacceptably affected by the hazard.

### 3.1 Dropped Load and Impact

30 A dropped load occurs if, during a manoeuvre, the lifting device can no longer control the load on the hook.

31 A dropped load may lead to mechanical damage to the equipment or structures located near the lifting area. This is dependent on the weight of the load and the resistance of the impacted equipment or structure.

32 The impact may also cause the load to be damaged and this event must be taken into consideration, particularly if the load contains radioactive substances e.g. fuel assemblies.

33 The approach for protection against dropped loads is essentially deterministic.

34 According to this deterministic approach:

- A dropped load is postulated from any lifting device which does not have sufficient classification but only for one item of equipment at a time.
- The dropped load occurs during normal plant operating conditions (power or shutdown conditions).

### 3.1.1 Design Basis for Dropped Loads and Impact

35 Protection against dropped loads is based on the following measures:

- Classification of the lifting devices and associated requirements.
- Installation or design rules for potential targets.
- Operational rules for lifting devices.

36 Lifting devices are classified in accordance with the results of a simplified hazard analysis. This analysis evaluates the consequences of a postulated dropped load from the associated lifting device.

37 The consequences of a postulated dropped load are considered to be unacceptable if it could lead to:

- A criticality accident.
- A loss of decay heat removal function.
- A release of radioactivity leading to radiation exposure in the vicinity of the unit which exceeds PCC-4 limits.

38 Lifting devices, failure of which could lead to potential unacceptable consequences are then classified as having 'higher requirements'. These requirements enable the possibility of damage due to the dropped load to be discounted for design basis considerations.

39 The consequences are considered to be serious if it could lead to:

- A non-isolatable release of primary coolant into the containment.
- A failure which leads to consequential failure of an F1 system.
- A release of radioactivity leading to increased radiation levels inside the area which affects the classification of radiological zones.

40 The associated lifting device is then classified as having 'additional requirements'.

41 All other lifting devices are not safety classified.

42 For lifting devices which are classified as having 'higher requirements', the lifting system and operations are designed such that the frequency of unacceptable consequences is adequately low.

43 The possibility of small loads being dropped e.g. valves and small motors, must be taken into account during the normal design of buildings through consideration of maximum admissible temporary loads.

44 In order to minimise the effects from a dropped load, the design and layout of the site and its facilities are such that they:

- Minimise the direct effects of dropped loads on SSCs.
- Minimise any interactions between a failed SSC and other safety-related SSCs.
- Ensure site personnel are physically protected from direct or indirect effects of incidents.
- Facilitate access for necessary recovery actions following an event.

45 In addition to the measures applied to lifting devices to enable the probability of dropped loads occurring to be reduced or discounted, further measures are applied to minimise the risk. These measures are achieved by the application of administrative controls on the operation of the lifting devices in terms of:

- Restriction of operating periods.
- Limitation of lift heights.
- Use of prescribed routes for transporting heavy loads.

46 The following rules are applied in order to plan the transport routes for heavy loads which are fixed to lifting devices:

- Use of the shortest possible routes.
- Duration of the lifting operation to be optimised.

47 The transport routes must be chosen so that:

- Stoppage times above critical locations (e.g. reactor pit) are as short as possible.
- The reactor pit should only be crossed during periods of approved maintenance.

### 3.1.2 Design Verification for Dropped Loads and Impact

48 As part of the design verification, it must be demonstrated that:

- The classification is appropriate.
- The consequences of any postulated dropped load are acceptable.

49 The assessment of dropped loads takes into account simultaneous effects, common cause failure, defence in depth and consequential effects. To achieve this, the analysis takes into account that:

- A hazard (i.e. dropped load) may occur simultaneously with a facility fault or when plant is unavailable due to maintenance.
- There is a significant potential for hazards to act as initiators of common cause failure, including loss of off-site power and other services.

- Dropped loads have the potential to threaten more than one level of defence in depth at once.
- Dropped loads can arise as a consequence of events external to the site and should be included in the relevant fault sequences.

50 Assessments are also made against the most onerous plant conditions within the normal operating envelope. Sensitivity studies are also performed for certain initiating events in order to show the absence of any cliff-edge effects in terms of radiological consequences.

### 3.2 Missile Generation

51 The missile safety analysis is the deterministic demonstration that the unit has acceptable protection against such a risk.

52 There are two general sources of postulated missiles:

- Failure of rotating equipment e.g. pumps, fans, compressors and turbines.
- Failure of pressurised components e.g. high energy components.

53 Breaks in safety classified components (vessels, tanks, pumps and valves) are discounted, consequently no missiles are postulated for this class of component. This also applies to welded flanges. Non-safety classified components within safety classified buildings is limited where reasonably practicable. When this is not possible, the potential for missile ejection must be considered.

54 In the case of pipework breaks, the generation of missiles is not considered due to the type of materials used and based upon experience; however, effects due to pipewhip are analysed.

55 Missiles resulting from ejection of the pressure heaters, or rod cluster control assembly, are discounted on technical grounds, as their pressure retaining parts form part of the reactor coolant system pressure boundary and the ejection of control rods is considered as a limiting accident (PCC-4).

56 In the nuclear power plant design stage, provision is made for risks due to missiles generated inside containment or other structures, in rooms outside of the containment containing safety equipment, and missiles generated from on-site locations outside of the buildings.

57 Due to their importance to plant safety, missile protection measures are taken for the Reactor Building (including the internal structures), the Safeguard Buildings, the Fuel Building, the Diesel Generator Building and the Pumping Station.

58 The approach applied for protection against internally generated missiles is spatial separation of the different F1 system trains into different building divisions, including the associated auxiliary and power and fluid supply systems. The divisions are structurally separated by partition walls. In addition to these structural walls, there are further concrete structures provided around individual redundant equipment items to provide additional shielding against the effects of missiles e.g. partition walls between different reactor coolant system loops in the containment, missile protection zones in the containment, where appropriate, and the separation of individual components. These barriers ensure that any missiles generated in one division do not affect redundant plant and equipment in adjacent divisions.

59 In addition to the measures taken inside the containment to prevent the effects of missiles on other redundant equipment, it must be ensured that the equipment inside the containment which contains radioactive material, and the containment itself, are not damaged simultaneously by a missile. This is achieved primarily by the partition walls provided between the individual reactor coolant system loops, or by the arrangement of the reactor coolant system within the missile protection zone or specific valve and steam generator compartments.

60 Based on the concept of defence in depth, the mechanical and structural measures described above ensure overall protection against missiles. In addition, the probability of internally generated missiles is reduced by the consistent application of safety orientated design and engineering principles e.g. the use of over-speed trip devices, equipment restraints and valve stem threads which securely retain the valve in the event of mechanical failure.

61 In addition, the high level of quality assurance applied during the design, manufacture, installation, inspection pre-service and in-service in accordance with the relevant codes and standards, and the regular maintenance regime, ensures that the probability of missile generation will be extremely low.

62 The multiple measures described within the PCSR ensure that the generation of missiles and the unacceptable consequences of missile effects, given the probability of generation, impact and possible damage, are so improbable that further detailed analyses are not necessary. Whilst it is not considered necessary to perform an analysis of each individual missile source, worst case scenario analyses are performed considering certain representative internal missiles.

63 Safety classified buildings are analysed to demonstrate that the thickness of the missile resistant barriers are adequate. In order to demonstrate that the thicknesses of the barriers are adequate for the worst case scenario, various containment missiles are analysed.

64 Whilst a systematic functional analysis is not performed for missile protection, it is confirmed that the design features e.g. thicknesses of walls and raft, are sufficient to protect against representative missiles.

65 For the UK EPR, it is intended that the alignment of buildings will ensure that the SSCs relevant to nuclear safety will be located outside the region vulnerable to missiles produced by turbine disintegration. The turbo-alternator unit design will also ensure a very low probability of energetic missiles being produced in the event of turbine disintegration.

66 The PCSR provides further detailed analysis of the potential missile threats within specific buildings and also to specific items of plant.

### 3.3 Pipework Leaks and Breaks

67 The PCSR describes high energy pipework as components containing water or steam at pressures ≥ 20 bar (absolute), or temperatures ≥ 100ºC, under normal operating conditions. Components containing gas at a pressure above atmospheric pressure are always considered to be high energy components. All other components are considered to be moderate energy components.

68 For small diameter pipework ≤ 50mm nominal bore, there is no restriction in the assumed break location, i.e. breaks are assumed to occur at any place on the pipe.

69 For pipework with a diameter > 50mm nominal bore, failure effects are considered for all leaks and breaks, other than those covered by the break preclusion assumption (below).

70 If certain specific requirements are adhered to, catastrophic failures of pressurised pipework may be discounted in the deterministic approach used during the design of the equipment and surrounding structures. The concept is based upon the following requirements:

- The break (rupture) preclusion involves integrity claims on pipework associated with the reactor coolant system pipework and the main steam lines between the steam generator and the fixed points downstream of the main isolation valves.
- The 2% criterion is a criterion which allows pipe breaks to be excluded from the design basis if pipework is in operation under high energy conditions for a period of less than 2% of the plant lifetime. The 2% criterion is applicable only to safety classified pipework of more than 50mm nominal bore that is designed in accordance with mechanical codes.

71 The PCSR focuses on the integrity claims associated with pipework claimed as part of the break (rupture) preclusion demonstration as well as providing information relating to the claims made on plant and equipment to prevent high energy line breaks.

72 During the design of the safety classified SSCs, the effects of the following on the consequences of leaks and breaks are to be considered for high energy pipework:

- Jet impingement forces.
- Pipewhip.
- Reaction forces.
- Compression wave forces.
- Flow forces.
- Differential pressure forces.
- Pressure build-up.
- Humidity.
- Temperature.
- Radiation.
- Flooding.

73 For moderate energy pipework:

- Flooding.
- Radiation.

74 Each of these potential hazards is to be considered as part of the detailed design of the UK EPR. The principles for preventing such hazards to take place are included within the PCSR.

### 3.3.1 Design Verification for Pipework Leaks and Breaks

75 Sensitivity studies are performed for certain initiating events in order to show the absence of any cliff-edge effects in terms of radiological consequences.

#### 3.3.1.1 Local Effects

76 The local effects are divided into compression wave forces and the effects on the systems caused by an increase in flow within the affected system and effects acting in the vicinity of the system:

- **Compression wave forces and increased flow forces** are only significant in the event of sudden breaks or breaks of a large cross section, and analysis is limited to these potential events. This analysis must calculate the forces on the internal structures of components connected to the fluid system. In addition, compression waves generate forces on the piping supports which are considered in the context of the reaction force analysis.
- **Jet impact forces** are considered in case of leaks and breaks that have the potential for consequential effects on adjacent SSCs. The resulting loads must be taken into consideration by ensuring that the loads are covered by the design or by providing appropriate protection measures, e.g. restraints or additional supports.
- **Reaction forces** due to leaks or breaks acting on the relevant pipework supports must be taken into consideration in the calculations required for these supports.
- **Pipe whip** must be considered, in the case of breaks with respect to possible impact on adjacent SSCs.

77 In addition spray effects from failures in low energy systems are considered for electrical components and Control and Instrumentation (C&I) components, where unacceptable consequences could occur. Protective measures for these components are provided in accordance with equipment qualification guidelines.

78 The local effects of failures of high energy lines in the following safety classified buildings must be analysed:

- Reactor Building.
- Safeguard Buildings, including the main steam and feedwater valve components.
- Fuel Building.

79 Protection requirements must be defined to determine the maximum acceptable effect on adjacent systems in case of failures of high energy pipework and are based upon the following rules:

- In case of loss of the reactor coolant, the integrity of the containment building including the pipework sections near the containment penetrations, as well as the operability of the containment isolation valves must be ensured in order to prevent the release of radioactivity outside the containment.
- Systems required to shutdown the reactor, maintain sub-criticality, and remove residual heat, must not be adversely affected by pipework failures.
- A consequential failure in the small diameter impulse lines and cables of safety classified components is admissible if the resulting actions are not detrimental to safety or if the component is fail safe. If this is not the case, detailed failure analysis must be performed.

- As a general rule, the same protection requirements must be applied to the safety classified supporting systems as are applied to the safety classified systems themselves.

80 The protection requirements are important in case of high energy line failures. In certain instances, exemption from these protection requirements is acceptable, where an appropriate justification is provided.

81 In supporting the above rules, there are a number of installation requirements which adopt the principle of segregation by division, or by concrete structures, in order to ensure redundancy in the safety functions. Some specific installation requirements associated with the protection against internal hazards are detailed below:

- In order to comply with the single failure criterion for the required Safety Injection System (SIS) trains, the Loss of Coolant Accident (LOCA) must be limited to one leg (hot or cold) of one reactor coolant system loop. In addition, the SIS lines which do not inject into the break must remain intact. This also concerns consequential damage to the pressuriser spray lines (connected to the cold leg of Loop 2 or 3). However, a break in a spray line may result in a simultaneous LOCA via the hot leg and the cold leg. These cases are covered by the analysis of cold leg leaks and breaks.
- As a general rule, the pipework installation must be performed in a way which prevents consequential failures of the secondary system in case of a failure in the primary system and vice-versa.
- The isolating function of the secondary side must be ensured in a way which isolates the affected steam generator in case of failure in the main steam or feedwater system and all other secondary side leaks which cannot be isolated.
- Isolation of the affected pipework in case of a failure which can be isolated in the lines connected to the steam generators must be ensured (e.g. by fixed points which protect the isolation valves).
- A failure of secondary side pipework must not lead to simultaneous depressurisation of two steam generators, unless it is possible to demonstrate that this is acceptable from a safety perspective.
- Consequential failures between steam and feedwater lines of the same steam generator must be avoided.
- Unacceptable consequential failures of the Containment Heat Removal System (CHRS) must be ruled out by using suitable installation (layout) provisions.
- In case of pipework failures with consequential damage to other pipework, the total fluid loss must remain within the limits of the global effects analysis.

#### 3.3.1.2 Wider Effects

82 Failure of pipework carrying hot water (Temperature ≥ 100ºC) or steam must be analysed taking into consideration the environmental conditions in the safety classified buildings. Representative cases must be determined for the Reactor Building (RB), Safeguard Auxiliary Building (SAB) (including the main steam and feedwater valve compartments) and the Fuel Building (FB).

83 The systems and components of one division in the Diesel Generator Buildings and the pumping station may be subject to failures caused by harsh environmental conditions, if the systems which cause these conditions are located therein.

84 The propagation of the harsh environmental conditions from the non-safety classified buildings or from the Nuclear Auxiliaries Building towards the safety classified buildings must be prevented.

### 3.4 Nuclear Fire Safety

85 The safety case for nuclear fire safety in the context of the UK EPR is contained within the PCSR, Sub-Chapter 13.2 Section 7, however, an overview of the key claims and design principles are contained within this section of the assessment report.

86 A key reference of the PCSR for the fire safety design is the EPR Technical Code for Fire Protection (ETC-F) (Ref. 19). This document details the design requirements for fire protection with respect to nuclear and industrial risk, personnel safety and the environment as well as design requirements for explosion prevention. The code provides specific design requirements relating to the use of fire protection systems, fire resistance requirements for barriers, requirements and methodologies for calculating cable protection, segregation requirements etc. Many of the principles and requirements detailed within the PCSR are derived from this main design code.

87 The safety objective for fire protection is to ensure that the safety functions are performed in the event of a fire inside the installation.

88 This objective implies that:

- A fire must not cause the loss of more than one set of redundant equipment in an F1 system.
- The non-redundant systems and equipment, which perform the required safety functions must be protected against the effects of a fire in order to ensure continuous operation.
- A fire must not compromise the habitability of the control room. In the event that the control room cannot be accessed the accessibility and the habitability of the remote shutdown station must be assured.

89 Fire is normally assumed to occur in any room which contains combustible materials and ignition sources. Coincidental occurrence of two or more fires, from independent causes, is not considered.

90 Fires could also occur as a consequence of other internal or external hazards e.g. fire induced Loss of Coolant Accident (LOCA), severe accidents, and earthquakes.

91 In the case of an earthquake, buildings designed to resist external hazards must not contain equipment, which is likely to release combustible materials or to create a source of ignition. An exception is made for the Nuclear Auxiliary Building and the Effluent Treatment Building where only the buildings themselves are seismically classified. If the equipment inside a building is not designed to resist an earthquake, fire protection measures must be provided to resist the effects of these hazards.

92 An independent fire is only assumed to occur during the post-accident phase and after a controlled condition has been reached following a PCC-2 to PCC-4 event. Nevertheless, the fire protection measures are available for the full duration of the post-accident phase.

93 The possibility of a fire in the Main Control Room during the post-accident phase following a PCC-2 to PCC-4 event is discounted in the design. This is justified by the availability of sufficient fire protection measures and the presence of operating staff who would be able to rapidly extinguish any fire.

94 RRC type events are very infrequent. As a result, the combination of an RRC event with an independent fire is assumed to occur only during the post-accident phase and no earlier than two weeks after the event.

### 3.4.1 Fire Consequences

95 It is conservatively assumed that all equipment (apart from that protected by fire barrier devices or able to withstand the fire effects) present in the fire compartment where the fire is assumed to exist, can no longer perform its normal function due to the fire.

96 A fire must not cause the loss of non-redundant safety equipment, otherwise this equipment must be protected or the potential for a fire must be eliminated.

97 A fire could lead to an additional PCC-2 event. In this instance, adequate system redundancies must remain available to control the event.

98 Where possible a fire must not lead to an additional PCC-3 / PCC-4 event.

### 3.4.2 Principles of the Fire Protection Approach

99 The main approach for protection against fire is deterministic which is complemented by a probabilistic safety assessment.

100 The principles are as follows:

- The fire is assumed to occur in any plant room, which contains combustible materials and an ignition source.
- Coincidental occurrence of two or more fires from independent causes, affecting rooms in the same or different plant is not taken into consideration.
- The ignition of any combustible material present in buildings must be considered, except for low and very low voltage electrical cables and equipment or materials protected by a housing or cabinet.
- Limitations of fire spreading using either the fire containment approach (fire compartments) in buildings separated into divisions or the fire influence approach (fire cells) in buildings or parts of buildings without divisional separation.
- A fire is assumed to occur during normal plant conditions (from full power to shutdown condition) or in a post-accident condition once a controlled condition has been achieved.
- In order to be able to set up the suitable protective measures, the fire load for each room must be calculated and kept up to date.
- The temporary or permanent storage of fire loads during the various states of the plant as well as workshops with fixed, hot working stations, must be identified and subject to risk analysis.
- The fire protection provisions must be optimised in order to limit the discharge of toxic or radioactive materials.

- The random failure of an active equipment item of the fire protection systems must not lead to a common mode failure on the systems needed to perform the F1 safety functions, even if these functions are not needed following such an event. The redundancy requirement (whether functional or not) due to this principle being taken into account must be implemented within the train separation principles.
- A check on the robustness to a random failure must be applied on a deterministic basis in the event of:
  i) A fire independently of the accidents, liable to impair the integrity of the fire barriers.
  ii) A fire leading to PCC-2 events.
  iii) A fire resulting from a PCC-3 / PCC-4 event.
- The random failure must be applied on a deterministic basis:
  i) To the active equipment of the fire protection mechanical systems.
  ii) To all the components of the fire protection electrical systems.
- A localised loss of integrity of the fire safety barriers may be accepted insofar as the failure of an active equipment item of the fire protections system does not lead to a common mode failure on the systems required to perform F1 safety functions.

### 3.4.3 Design Basis for Nuclear Fire Safety

101 There are three key principles in the approach taken for the design for nuclear fire safety for the UK EPR design, prevention, detection and extinguishing. The measures taken in the design in order to address these three principles are to prevent fires occurring, and to contain and control any fires that do occur.

102 The measures associated with fire prevention (or reducing the likelihood of fire) are minimising combustible material inventory, separating or shielding them (enclosure or cabinet) and preventing potential ignition sources being placed near combustible materials. Wherever possible, preference must be given to the use of non-combustible materials.

103 If a fire does start, despite the preventative measures in place, measures must be taken to limit fire spread and prevent:

- Impact on the function of the F1 systems. Fire damage must be restricted to one redundant train in a given F1 system.
- Spreading to other rooms and into emergency exits and disrupting fire-fighting provisions.
- Environmental impact contravening applicable UK Regulations.

104 Limiting the spread of a fire is achieved by dividing the buildings into fire compartments and fire cells, which use physical or geographical separation principles.

105 Any installed fire barrier must contain the fire so that only one of the redundant trains in a given F1 system may be endangered by fire, for cases where different redundant systems are installed in different areas, fire compartments or fire cells. The requirements for separation are as follows:

- All safety classified buildings (Type 1 and 2) must be separated from other buildings using a 2 hour rated fire barrier wall (R) EI 120 where R denotes load bearing capacity, E is the fire integrity requirement and I is the fire insulation requirement.
- Priority must be given to physical separation. In the same way, priority must be given to structural measures (fire resistance of the structures) rather than to reliance on fire protection devices.
- In case of fire, the redundant elements in an F1 system must be protected so that failure is limited to a single train.
- Random failure is only to be considered for active equipment items such as fire stop check valves and servo controlled doors. Fire doors themselves, smoke extraction ducts and floor drains are considered as passive equipment items that are not subject to the random failure requirement.
- The following table summarises the different types of fire compartments:

**Table 3:** Fire Compartments Used Within UK EPR Design

| Objective | Fire Compartment |
|---|---|
| Radioactivity containment | Type 1a/1b |
| Safety | Type 2 |
| Protected evacuation route | Type 3 |
| Facilitation of the intervention and limiting the unavailability | Type 4 |
| Storage | Type 5 |

106 Where geographical separation is used a vulnerability analysis is undertaken to demonstrate adequate fire safety provision.

107 There are five compartment types adopted as part of the UK EPR PCSR:

- **Fire Containment Compartment** (CCO/SFC) (Type 1a). These compartments are created when a fire in any safety classified building could lead to the release of radioactive or toxic material which, in the absence of any dispersion measures outside of the relevant compartment, causes deviation from acceptable release levels. In addition to containing the fire, they ensure the control of the released radioactive or toxic materials. The partitions of these fire and containment compartments must have a fire resistance rating of (R)EI 120 and smoke doors classified at 200 degrees C (S200C5). They must also be fitted with a fixed automatic fire-extinguishing system capable of accomplishing its function in the event of a random failure.
- **Fire Environment Compartment** (CEO/SFE) (Type 1b). These compartments are created when a fire inside a non safety building could lead to the release of radioactive or toxic materials which, in the absence of any dispersion measures outside of the relevant fire compartment, causes deviation from acceptable releases. In addition to containing the fire, they ensure the control of the released radioactive or toxic materials. The partitions of these fire and containment compartments must have

a fire resistance of (R)EI 120 and S200C5 classified doors. They must also be fitted with a fixed automatic fire-extinguishing system.

- **The Safety Fire Compartment** (SCO/SFS) (Type 2). These compartments are created to protect safety trains from common mode failure. The partitions of these safety fire compartments must have a fire resistance (R)EI 120 and S200C5 classified doors. Active or passive means of fire protection must be established if necessary to ensure their integrity after this time has passed.
- **Access Compartment** (RCO/SFA) (Type 3). These compartments are intended to enable the personnel to be evacuated in full safety in the event of fire, and to provide access for fire-fighting teams. These compartments form the protected escape routes within the buildings. The partitions of these compartments must have a fire resistance rating equal to the fire resistance of the adjacent fire area - (R)EI 60 and the doors must be classified S200WC5 (smoke tightness, limited radiation, durability in accordance with NF EN 13501-2). These compartments must not contain safety equipment or combustibles.
- **Intervention fire Compartment** (IFC/SFI) (Type 4). These compartments are created when the installation conditions result in the possibility of a flash-over fire (PFG), to facilitate the intervention of fire fighting crews and limit the unavailability of the unit. The partitions of these fire compartments must have a fire resistance rating suited to the consequences of the fire in the area without being less than (R)EI 60.
- **Fire Cells** – in some buildings and in the reactor building in particular, division into fire compartments may be limited due to construction or process factors, e.g.

  i) Compact nature of the installation.

  ii) Hydrogen concentrations.

  iii) Steam releases in the case of pipe break.

  In this instance, some sections of the buildings may be divided into fire cells, where equipment is protected by spatial separation rather than physical barriers. Evidence of non-propagation of fire and avoidance of failures of safety classified equipment, must be established by assessing all possible modes of fire propagation and combustion products. Fire cells are only used in exceptional circumstances and their effectiveness is demonstrated on both the fire propagation and the radioactive or toxic waste release level.

108 Detection and suppression systems are installed in a number of areas to control the fire as quickly as possible. The control requirements are:

- The purpose of the detection system is to quickly detect the start of a fire, to locate the fire, to trigger an alarm, and in some instances to initiate the automatic fire fighting systems.
- The fire detection system must be operational in all cases where a fire is assumed to occur.
- Fire fighting devices, which are fixed or portable depending on the nature of the fire and the type of equipment to be protected, must be provided where a fire is likely to affect redundant equipment performing the same safety function.

109 A vulnerability analysis is carried out as part of the safety case that either demonstrates that common mode failures due to fire have been eliminated, or show that the consequences of postulated fire are tolerable. The analysis considers the effects of fire

on a single compartment or division, and for cells considers those cells adjoining the area.

### 3.5 Internal Flooding

110 The safety case for internal flooding in the context of the UK EPR is contained within the PCSR Sub-Chapter 13.2 Section 8. However, an overview of the key claims and design principles are contained within this section of the assessment report.

111 Internal flooding is considered as part of the PCSR for UK EPR and potential for flooding to damage essential equipment or civil structures resulting in the potential threat to safety-related plant and equipment. The following potential initiators have been considered within the assessment of internal flooding:

- Leaks and cracks in pressurised systems.
- Incorrect system configuration.
- Flooding by water from neighbouring buildings.
- Spurious operation of the fire extinguishing system, and use of mobile fire fighting equipment.
- Overfilling of tanks.
- Consequences of failure of isolation devices.
- Operator error.

112 External flooding associated with snow, rain, tsunami, and tidal changes are not considered within this section, however, sources of flooding on the site are addressed as they constitute an internal hazard, these are:

- Deterioration of water channel structures, such as reservoir ponds and cooling tower basins.
- Breaks in systems or equipment including breaches in the Circulating Water System (CRF) in the Turbine Building or breaches in non-seismically qualified site tanks in the event of a seismic event.
- The sudden trip of the CRF pumps is an on-site event. However because the impact of this event is governed by the heat sink water levels which are site-specific, this specific flooding hazard is assessed together with external flooding as a site specific issue.

113 In line with the deterministic approach taken for the other internal hazards considered within the UK EPR design, only one of the potential internal flooding initiators is postulated to occur at any one time, unless two or more initiators have a common identified cause and this initiator is expected to occur during normal operation of the reactor (during power operation or during shutdown).

114 The systems and structures which are liable to fail during flooding are:

- All electrical and C&I equipment, with the exception of cables whose terminals are not flooded and where the equipment is protected against water ingress.
- Certain civil structures that are not qualified to resist the floodwater pressure or its temperature.

- All non-watertight mechanical equipment.

115 Each of the potential internal flooding initiators is considered within the Section 13.8 of the PCSR. A number of these measures are to be addressed at a future stage of the design, hence only high level requirements / principles are provided within the PCSR.

116 The PCSR does provide criteria for leak duration:

- If the breach can be detected by C&I systems, and if provision has been made for automatic isolation, the release time is determined by the time taken to detect the leak plus the time taken to actuate the automatic isolation.
- If the breach can be detected by signals in the main control room, and if provision is made for manual isolation from the main control room, the release time comprises the time taken for the first alarm to be received in the control room plus a nominal 30-minute period allocated to manual actions in the main control room.
- If the breach can be detected by signals in the main control room, and if provision is made for isolation using local actions, the release time comprises the time taken for the first alarm to be received in the control room plus the time allocated to the operators performing the local action, for example for manual isolation of a valve it is assumed that the time allocated to a local action is 1 hour.
- If the breach cannot be detected or if isolation is not possible, the release of the full inventory of the failed system is assumed, if the leakage is not limited in any other way.

117 If isolation of a breach is assumed, only the volume of water released during the period up to isolation is considered. The content of the part of the system which cannot be isolated is assumed to be released. The PCSR considers that any leakage is assumed to be at maximum operational pressure and any released steam is considered to be fully condensed.

118 The design of the facility includes adequate provision for the collection and discharge of water reaching the site from any design basis internal flooding hazard. Where this is not achievable, the Systems, Structures and Components (SSCs) important to safety will be adequately protected against the effects of water with examples of measures being:

- The water may flow to the lower levels via the stair wells, lift wells, the building's drainage system or other openings.
- The sump pumps of the building drainage system are pessimistically considered as unavailable.
- It is assumed that the level of water is equally distributed in all of the zones concerned, at the lowest level.
- With regard to the room in which water is released, the level may be higher in the case of high flows. It must only be considered for specific instances where the systems / equipment to be protected are located in these rooms.
- The doors at the interfaces of the buildings and divisions are resistant to the maximum water column resulting from the main initiating event or the initiating event used for the sizing of the civil works. These doors are qualified for the resulting requirements. Similarly, the materials used for caulking, to close the openings and the joins in the walls between the divisions, are qualified against the water column height of the main initiating event..

- The flood barriers for safety-classified equipment are taken into consideration.

119 In order to minimise the effects from an internal flooding event, the design and layout of the site and its facilities are such that they:

- Minimise the direct effects of internal flooding on SSCs.
- Minimise any interactions between a failed SSC and other safety related SSCs.
- Ensure site personnel are physically protected from direct and indirect effects of incidents.
- Facilitate access for necessary recovery actions following an event.

120 Supporting facilities and services important to the safe operation of the reactor are designed and routed so that, in the event of incidents, sufficient capability to perform their emergency functions will remain. Support facilities and services include access roads, water supplies, fire mains and site communications.

121 In buildings which are split into divisions, the complete loss of a division does not prevent fulfilment of the essential safety functions. Therefore, the main safety objective is to ensure that an internal flood cannot extend to another safety classified building or another safety classified division. However, certain other additional measures may be necessary, for example:

- Isolation of the Safety Injection System (SIS) sump valves in case of failure in the SIS pipework, in order to protect the In-containment Refuelling Water Storage Tank (IRWST) supply.
- Protection of the main control room against flooding originating from the chilled water system located above.

122 In the other buildings (Reactor Building, Fuel Building) flooding must be prevented from causing failure in redundant F1 systems (including support systems). If necessary, mitigation measures must be taken, such as:

- The construction of local partition walls between the system's redundant section in the non-divided areas.
- Locating the components at higher levels.
- Reducing the level of flooding using measures such as drains.

123 In case of internal flooding in the non-classified buildings or flooding anywhere else on site, water must be prevented from entering the safety classified buildings.

### 3.5.1 Design Verification for Internal Flooding

124 The design verification for internal flooding is the deterministic demonstration that the unit has acceptable protection against such a hazard. It is carried out according to the methodology described below.

125 The analysis takes into account simultaneous effects, common cause failure, defence in depth and consequential effects. To achieve this, the analysis takes into account that:

- Certain hazards may not be independent of internal flooding and may occur simultaneously or in a combination that can be reasonably expected.

- An internal or external hazard may occur simultaneously with an internal fault, or when plant is unavailable due to maintenance.
- There is a significant potential for internal or external hazards to act as initiators of common cause failure, including loss of off-site power and other services.
- Internal flooding events have the potential to threaten more than one level of defence in depth at once.
- Internal flooding can arise as a consequence of faults internal or external to the site and should be included in the relevant fault sequences.
- The severity of the effects of the internal or external flooding experienced by the facility may be affected by the facility layout, interaction, and building size and shape.

126 The verification is performed at the end of the detailed studies for each safety-classified building. The onset of a flood will be postulated for each room, for each applicable type of initiator and the consequences assessed.

127 For each building the following aspects are assessed:

- The possible sources of flooding.
- The water paths between various rooms.
- Safety related equipment that can be affected by the consequences of internal flooding including the effects of water spray and loss of a supporting system due to flood.
- Identification of possible common mode failures.
- The risk of groundwater pollution / release of radioactive waste.

128 Sensitivity studies are performed for certain initiating events in order to show the absence of any cliff-edge effects.

### 3.6 Internal Explosion

129 In considering risk from internal explosions, potential dependencies are considered with the following hazards:

- Earthquakes; this dependency is examined in particular for pipework at risk located in the nuclear island and the associated risk of explosive gases. (Including the earthquake event; risk of falling object in the case of earthquakes)
- Pipewhip effects following break of high energy pipework.
- Fire potential of piping carrying explosive gases or pressure tanks.
- Risk of projectiles due to high winds.
- Lightning.

130 No combination of an external or internal hazard or of an initiating event, with an independent internal explosion, is considered; in particular, two independent explosions are not considered.

131 The requirements and combined hazards taken into consideration are reflected by the following safety objectives:

- An explosion should not adversely affect more than one element of a redundant F1 system.
- As far as is reasonably practicable, an explosion should not trigger a PCC-3 or PCC-4 event.
- An explosion should not adversely affect the stability and integrity of:
  i) Safety classified buildings and fire safety barriers.
  ii) Components whose failure is excluded by design e.g. pipework satisfying the break (rupture) preclusion principle.

132 In all cases, a sufficient number of systems / redundancies enabling the plant to reach a safe state should maintain their operability. An explosion should not affect the habitability of the main control room. In the event that the main control room cannot be accessed, the habitability of the remote shutdown station should be guaranteed. In addition, there should be accessibility to perform local actions, when necessary.

133 In addition, an explosion should not challenge safety objectives specific to other nuclear installations on the nuclear site.

134 The safety functions required to cope with the internal explosion hazard are classified F2. The single failure principle and preventative maintenance are considered within the safety analysis of internal hazard scenarios.

135 The potential sources of internal explosions associated with the UK EPR design are:

- Internal explosions within systems.
- Internal explosions inside or outside buildings which may be due to a release of explosive gases from systems, processes or tanks.
- Internal explosions inside or outside buildings which may be due to failure of pressure tanks for gas or liquefied gas, explosive or not.

136 The risks of explosions in mechanical or electrical equipment (motors, circuit-breakers etc.) are generally excluded because of design provisions (use of dry transformers, circuit-breakers without oil tanks). If necessary, the risk must be considered and prevented by design, installation and operating procedures.

137 The approach for protection against explosions involves three stages:

- Prevention, which consists of:
  i) Taking constructive or organisational measures to prevent and / or control all releases.
  ii) Avoiding the formation of explosive atmospheres which may result from such releases.
  iii) Avoiding ignition of any explosive mixture formed.
  iv) Preventing the risks in pressure tanks.
- Monitoring; by providing detection systems, combined with preventive action.
- Limiting the consequences; provide means for mitigating the effects of an explosion in respect to safety related targets. The possible presence of other nuclear installations on the site also has to be considered when defining the targets.

### 3.6.1 Design Basis - Internal Explosion

138 A room or location is said to be at risk when it contains a system at risk with removable single points (valves, man holes, non-welded connections), process generated explosive gas or an explosive gas pressure tank. It is considered that a system which carries an explosive gas is at risk when, under its maximum normal operating condition, the concentration of explosive gas is equal or greater than the Lower Explosive Limit (LEL) of the gaseous mixture contained within the system. By conservative convention the LEL is considered to be equal to the Lower Flammability Limit (LFL). Liquids with a flash point lower than 55ºC, or for which the working temperature is greater than the flash point, are considered as explosive gases.

139 The following measures are incorporated into the UK EPR design requirements for systems containing explosive gases:

- Implementation of provisions at the design stage which ensure that they are leak tight.
- Design of rooms, equipment and ventilation, which do not lead to stagnation areas.
- Electrical earthing of systems and equipment.
- Appropriately classified equipment for use in potentially explosive atmospheres in line with the requirements of the European Directive.
- The detection of explosive gases provided in rooms at risk in the buildings of the nuclear island and in other areas outside the nuclear island where an explosion could threaten safety related plant and equipment.
- Periodic maintenance, inspection and testing of systems associated with explosive gases.
- The air renewal rate that should avoid the formation of explosive atmospheres, wherever possible.

140 The design verification for internal explosions in the nuclear power plant must demonstrate that the site has adequate protection against the explosion hazard. This demonstration should be performed in accordance with the following principles:

- The rooms or locations at risk should undergo an analysis of the adequacy of the preventive measures in place.
- If the risk remains, an analysis should be performed on the consequences of an explosion against the safety targets located inside or outside the buildings.

141 The PCSR provides analyses of the risks of explosion within the nuclear island, in buildings outside the nuclear island, and in external areas on the nuclear site.

# 4 GDA STEP 4 NUCLEAR DIRECTORATE ASSESSMENT FOR INTERNAL HAZARDS

142 The following sections provide the detailed assessment for each of the areas identified within Section 2.3 on Assessment Scope. The assessment sample has been limited to those areas within the report and the assessment is structured as follows:

- the background to the selected area for assessment,
- the scope of the assessment undertaken,
- the detailed assessment including comparison with national and international standards, guidance and relevant good practice, and
- assessment conclusions including any GDA Issues or Assessment Findings.

## 4.1 Dropped Loads

143 The Step 3 Assessment Report was based on information that was identified within the PCSR. This was used as the basis for the initial high level comments made. The comments related to a lack of detail in relation to the presentation of the arguments and evidence to support the claims and assertions made. The following areas were identified as requiring further assessment during Step 4:

- *"Further evidence of the adequacy of the approach to the methodology applied to the identification of dropped loads and internal missiles should be further investigated during Step 4 when the two outstanding documents are supplied"*
- *"….there are 'additional requirements', which are required if the consequences of a dropped load are considered to be serious…..However, there is very little information as to how these areas are identified and what is actually required in order to demonstrate that they provide an adequate level of nuclear safety for the potential hazards that could arise. Further substantiation and evidence will be required during Step 4 relating to dropped loads."*
- *"The PCSR also states that unintentional travel above critical areas with heavy loads is prevented by means of interlocks, yet does not mention any further detail as to how this principle will be achieved on plant."*
- *"Simultaneous effects, common cause failure, defence in depth and consequential effects are addressed within the PCSR, but only at a high level and as such further substantiation will also be required in this area during Step 4."*

144 During Step 4 I have carried out further assessment of the EDF and AREVA approach to dropped loads and impact, leading on from the initial high level information reported within the Step 3 report. The Step 4 assessment focussed on the EDF and AREVA methodology for the assessment of dropped loads and also on the analysis of the evidence available to demonstrate that the safety case for potential dropped loads and impacts was robust.

145 As part of the Step 2 assessment a request was made through a TQ (TQ-EPR-014) (Ref. 14) for EDF and AREVA to provide information on the methodology they used to identify the internal hazards. Although the full response to this TQ was not available at the time of issuing the Step 3 Internal Hazards Assessment, two methodology documents related to missiles and dropped loads respectively, were received during Step 4.. The missile methodology is assessed within Section 4.2.1. while the document, *"EPR – Load drops –*

*Methodology for risk analysis in civil engineering and building installations – Design review preparation conditions"* (Ref. 20) has been used as the basis of the dropped load and impact assessment.

### 4.1.1 Scope of Assessment Carried Out

146 The assessment involved gaining an understanding of the approach taken to the safety case substantiation of postulated load drops and impacts for the UK EPR design. It involved detailed review of the basis of the claims and arguments made within the PCSR and utilised international and UK relevant good practice for both nuclear generation and nuclear chemical plant facilities as a basis for determining the adequacy of the approach. The involvement of other assessors in support of this assessment was required, specifically, Mechanical Engineering and Civil Engineering as there were claims made on the lifting equipment itself and the preclusion of dropped loads by design as well as claims made on the civil structures in the event of dropped loads from RS2 lifting equipment.

### 4.1.2 Assessment

147 The methodology for dropped loads and impact for the UK EPR is based upon the single failure proof RS1 lifting equipment. The methodology stated that it removed the need for further consequence analysis as the potential for a dropped load was not deemed to be credible. For RS2 lifting equipment, the key claim is on the civil structures such that they are able to tolerate a dropped load and impact and the consequences of such an event are acceptable.

148 The methodology for load drops considers the consequences of a load drop as:

- *Inadmissible*, if they could lead to a critical accident, a loss of the function of control rod insertion, or a release of radioactivity leading to exposure to radiation in proximity to the plant unit and exceeding PCC4 limits. For "Inadmissible consequences", the heavy load handling equipment is classified as having advanced requirements which result in the crane being classified RS1 and permit the claim that dropped loads are precluded by design.
- *Serious*, if they could lead to a non-isolatable release of reactor coolant in the containment leakage system, consecutive failures of F1 systems (including damage or loss of barriers or systems in place to ensure segregation of those systems), or a release of radioactivity leading to exposure to radiation within the plant unit that affects environmental monitoring system zones. For "Serious consequences", the heavy load handling equipment is classified as having additional requirements which result in the crane being classified RS2 and not being claimed for preclusion of dropped loads.

149 The methodology report does identify operating and design arrangements which include:

- restriction of operating periods;
- limitations on lifting heights;
- routes prescribed for the transportation of heavy loads, and;
- the avoidance of routing lifts above classified safety equipment.

150 These provisions appear reasonable, in principle, and are in line with my expectations, however, there is no information presented to demonstrate how this is achieved, e.g. there are no details provided associated with the restriction of operating periods and the impact of using the crane at different reactor states and the potential radiological consequences associated with use at these different states. In addition, my opinion is that, the approach to avoiding the routing of lifts above classified safety equipment will not be achievable for all postulated lifts.

151 As part of the Step 4 assessment of the lifting equipment being undertaken by the Mechanical Engineering assessors, RO-UKEPR-052 (Ref. 15) relating to load path and rigging faults was produced that detailed 3 regulatory observation actions (ROAs) which required EDF and AREVA to:

- Systematically review the rigging arrangements for all lifting equipment associated with lifts of nuclear safety significance, to identify faults, and review and implement reasonably practicable improvements to either eliminate such faults by design, or limit their frequency by the provision of engineered protection systems.
- Systematically review the load path for all lifts of nuclear safety significance, to identify the potential for load interference (e.g. snagging or ledging), and review and implement reasonably practicable improvements to either eliminate such faults by design, or reduce their frequency.

  This review should also identify equipment vulnerable to load interaction, and review and implement reasonably practicable improvements to either remove this hazard by design, or reduce the consequence by appropriate protection measures.
- Review Operational Experience Feedback associated with UK nuclear lifting operations, and identify and implement any reasonably practicable improvements to their design.

152 The assessment of RO-UKEPR-052 has been undertaken across both the Mechanical Engineering and Internal Hazards assessment areas and the findings of ND are reported within the Step 4 Mechanical Engineering Assessment of the EDF and AREVA UK EPR (Ref. 65)

153 Although RO-UKEPR-052 identified the main cause of dropped load and impacts, namely load path and rigging faults, the internal hazards assessment identified that there are other factors that should be considered especially in light of the preclusion of dropped loads for single failure proof cranes.

154 TQ-EPR-669 (Ref. 14) was raised requesting information on the use of the Polar Crane (RS1 - single proof crane) during all plant states. The response stated that the Polar Crane is not used during power operation (Reactor State A) but is used during the other Reactor States as part of outage preparation at Reactor States B and C. Reactor State B is defined within Chapter 14.0 of the PCSR (Ref. 17) as:

*"Intermediate shutdown above 120°C (P < 130 bar). State B covers all shutdown states during normal plant operation, where primary heat is removed by the SG. It extends from 130 bar (inhibition of some F1-A signals) to 32 bar/120°C (connection of RIS/RRA [SIS/RHRS]) RCP [RCS] conditions. Above 120°C, the LHSI in RHR-mode (LHSI/RHR) is not connected to the RCP [RCS] in normal operation. More details on the LHSI/RHR connection conditions are provided in Sub-chapter 6.3. Note that the LHSI/RHR can be connected to the RCP [RCS] at 180°C, if necessary, but this is not an initial state corresponding to a normal operation and therefore it does not need to be considered as an initial state in the deterministic safety analysis. In this state B, some automatic reactor*

*protection functions available in state A may be deactivated (see Sub-chapter 14.1 and 14.7)."*

155 Reactor State C is defined within Chapter 14.0 of the PCSR as:

*"Intermediate and cold shutdown with LHSI/RHR. The RCP [RCS] is closed or can be rapidly reclosed, e.g. when a vent line is open, so that the SGs can be used for decay heat removal, if necessary. The RCP [RCS] is full of water or at partial loop level e.g. for SG tubes draining and for RCP [RCS] purging. Reactor state C covers the RCP [RCS] temperature range between 120°C and 55°C. Three different sub-states C1, C2 and C3 are defined depending on the different levels of RCP [RCS] water inventory, operating status of reactor coolant pumps and LHSI/RHR pumps and SG availability for heat removal:*

*State C1*

*• RCP [RCS] pressure around 30 bar (range : 24.5 – 32 bar)*

*• RCP [RCS] temperature between 120°C and 100°C*

*• RCP [RCS] water inventory corresponding to the pressuriser level at hot zero power conditions*

*• two SG participating in heat removal*

*• two reactor coolant pumps in operation*

*• RIS/RRA [SIS/RHRS] operating via two LHSI/RHR trains, the other two trains are on stand-by*

*State C2*

*• RCP [RCS] pressure around 30 bar (range : 24.5 – 32 bar)*

*• RCP [RCS] temperature between 100°C and 55°C*

*• RCP [RCS] water inventory corresponding to the pressuriser level at hot zero power conditions*

*• two SG available for heat removal*

*• one or two reactor coolant pumps in operation*

*• RIS/RRA [SIS/RHRS] operating via all 4 LHSI/RHR trains*

*State C3*

*• RCP [RCS] pressure between 32 and 1 bar*

*• RCP [RCS] temperature around 55°C*

*• RCP [RCS] water inventory between pressuriser level at hot zero power conditions and low level operation (3/4 loop)*

*• two SG available for heat removal*

*• No reactor coolant pumps in operation*

• *RIS/RRA [SIS/RHRS] operating via three LHSI/RHR trains, the other train is on standby."*

156 Table 4, details the work undertaken utilising the Polar Crane in a normal refuelling outage for reactor states B and C. This information was provided within the response to TQ-EPR-669.

**Table 4:** Use of the Polar Crane During a Normal Refuelling Outage

| Reactor State | Heat Removal | Description of Work Undertaken Utilising Polar Crane |
|---|---|---|
| B | Steam Generators | - Removal of the [redacted] missile slabs on the internals pool. |
| C | Residual Heat Removal System | - Removal of the [redacted] missile slabs above the reactor vessel.<br>- Installation of the access stairways to the pool intermediate platform.<br>- Hydrogen re-combiners removal and storage.<br>- Reactor building transfer stop gate removal<br>- Temporary installation of the thermal insulation [redacted]<br>- Installation of the multi-stud tensioning machine above the reactor vessel and de-torquing of the [redacted] studs.<br>- Removal of the multi-stud tensioning machine with studs and transfer to its stand in front of the equipment hatch. |

157 Further to the information provided within the response to the TQ-EPR-669 (Ref. 14), there was a need for EDF and AREVA to consider the limits and conditions of use of the Polar Crane and other RS1 lifting equipment as well as the consideration of the consequences of dropped loads and impacts. As a result, I requested that the consequences of load drops from all RS1 and RS2 lifting equipment be assessed through a cross-cutting RO (Ref. 15), RO-UKEPR-070. Within the RO it was stated that there was a need to demonstrate that the provisions in place to ensure that the risk to nuclear safety of a load drop or impact was ALARP and that such assessment could take into account:

- claims on civil structures
- additional physical protection
- limits and conditions on the use of the RS1 lifting equipment
- provision of detailed load path routes avoiding areas of highest nuclear significance
- measures (both system based and administratively controlled) in place to ensure the potential for impact of the load is minimised.

158 I produced 4 Regulatory Observation Actions that required EDF and AREVA to:

- Provide substantiation of the safety significant structures, systems and components vulnerable to dropped load and impact from RS1 lifting equipment. Such SSCs include civil structures as well as vessels, piping etc.

- Provide substantiation of the safety significant structures, systems and components vulnerable to dropped load and impact from RS2 lifting equipment. Such SSCs include civil structures as well as vessels, piping etc.
- Provide an inventory of all RS2 dropped loads which have been considered in the design of the civil structures and the justification of their values.
- Provide a description of the approach taken to treat dropped loads on civil structures, including design criteria and expected reliability considerations of global stability. This should include reference to the reports where each of the RS2 items identified in ROA-UKEPR-70.A3 are treated

159 At the time of writing this assessment report the response to the RO had not been received and therefore, given the significance of the concerns, a GDA Issue (**GI-UKEPR-IH-01)** and associated Actions have been raised **(GI-UKEPR-IH-01.A1 and GI-UKEPR-IH-01.A2)**.

Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

160 In terms of internationally accepted standards and guidance, operating experience and relevant good practice, it was considered important to provide an overview of the current expectations associated with dropped loads and impact from both a national and international perspective.

161 The HSE Safety Assessment Principles, SAPs, state within EHA.14:

| **Engineering principles: external and internal hazards** | **Fire, explosion, missiles, toxic gases etc – sources of harm** | **EHA.14** |
|---|---|---|
| Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed. | | |

162 The approach currently undertaken within the UK for the analysis of dropped loads associated with the lifting equipment involves the assessment of the consequences of dropped loads on safety significant SSCs which results in the determination of the limits and conditions of operation of the lifting equipment, detailed load paths, and systems and administrative controls in place. In addition, current practice employed at the existing UK PWR and within other plants internationally is for the reactor to achieve cold shutdown, with temperatures <93 degrees Celsius and pressures <30 bar, prior to undertaking operations involving the Polar Crane. This is not the approach proposed by the EDF and AREVA operating philosophy for State B and some State C operations.

163 NS-G-1.11 (Ref. 11) states, *"Structures classified as liable to affect SSCs in the event of their collapse should be designed and built so that the probability of their collapsing can be shown to be negligible; otherwise the consequences of their collapse should be evaluated. Similarly, the hazard posed to SSCs by falling objects (cranes and lifted loads) should be evaluated"*. The approach to the analysis of the consequences within NS-G-1.11 is consistent with the approach adopted within the UK currently, however, in the absence of a consequence assessment for the RS1 lifting equipment the approach taken by EDF and AREVA is not consistent with UK expectations.

164 In addition to NUREG-0554 (Ref. 23), the USNRC issued NUREG-0612 (Ref. 24), which presented an overall philosophy that provided a defence-in-depth approach for controlling the handling of heavy loads with the focus on prevention of dropped loads rather than

assessment of the consequences and it subsequently required the following approach to be adopted within existing US Nuclear Power Plant:

- Assure that there is a well designed handling system.
- Provide sufficient operator training, load handling instructions, and equipment inspection to assure reliable operation of the handling system.
- Define safe load travel paths and procedures and operator training to assure to the extent practical that heavy loads are not carried over or near irradiated fuel or safe shutdown equipment.
- Provide mechanical stops or electrical interlocks to prevent movement of heavy loads over irradiated fuel or in proximity to equipment associated with redundant shutdown paths.
- Where mechanical stops or electrical interlocks cannot be provided provide a single-failure-proof crane or perform load drop analyses to demonstrate that unacceptable consequences will not result.

165 The current design for UK EPR appears to be consistent with the philosophy stated within NUREG 0612, however, there is a lack of detailed supporting arguments and evidence to confirm that the engineered and administrative arrangements stated within NUREG-0612 have been adequately addressed within the design and hence why RO-UKEPR-070 was produced seeking further clarification of the safety case within this area. Whist it is accepted that this approach would serve to reduce the risks associated with dropped loads, it does not consider the potential consequences of dropping a load.

166 It is recognised that the design of single failure proof cranes is to a high reliability and standard and that failures associated with load drops is minimised, however, I would expect that such cranes would be subject to some form of supporting consequence analysis including both engineering and administrative controls to minimise both the probability and consequence. This analysis has not been provided.

167 The details of RO-UKEPR-070 were presented to the Mechanical Engineering Nuclear Topic Group (NTG), an internal group comprising of all ND mechanical engineering technical specialists, who have considerable experience relating to lifting equipment and of dropped loads and impact. Their advice was sought relating to this concern in order to inform this assessment of the current approach to dropped loads and impact from high integrity lifting equipment from both a UK and International Standard approach. In addition, advice from the NTG is based upon many years experience and understanding of the relevant good practice observed within the UK and overseas.

168 The Mechanical Engineering Nuclear Topic Group advice, following group discussion, was summarised by the following two statements:

*"Crane and lifting equipment reliability is determined by many factors in addition to equipment integrity. Regardless of integrity claims it is considered necessary to assess the consequences of dropped loads and other malfunctions.*

*The operating limits and conditions for cranes and lifting equipment should be determined taking account of the failure consequences assessment, and industry and regulatory guidance and engineering good practice, and operation should be demonstrated to be ALARP."*

169 Furthermore, in July 2003, USNRC issued NUREG-1774, entitled, "A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002" (Ref. 25) in

which one of the observations made stated, *"… most load drop events were the result of poor program implementation or human performance errors that led to hoist wire rope or below-the-hook failures. All three very heavy load drops were the result of rigging failures, not crane failures. Consequently, there were no very heavy load drop events that could have been prevented had only a single-failure-proof crane been employed in the lift. However, there were load or hook and block assembly drops that could have been prevented with the use of single-failure-proof cranes and lifting devices."*

### 4.1.3 Assessment Conclusions

170 Whilst the EDF and AREVA methodology provides useful information relating to the analysis of lifting equipment, operating and design arrangements, as well as the approach to the assessment of load drops on concrete structures, it lacks the requisite evidence to support the case as presented within the PCSR. The concern is specifically in relation to the consequences and associated substantiation of dropped loads for RS1 lifting equipment. In addition there is a lack of evidence associated with the arguments relating to operating and design arrangements in place to either prevent or minimise the effects of dropped loads and impact e.g. the evidence to support use of the Polar Crane at temperatures >120 degrees Celsius and pressures <130 bar.

171 To conclude, there is a compelling case, as confirmed within current guidance and standards, operating experience and relevant good practice, in support of the need to undertake a detailed quantitative analysis of the potential consequences of a dropped load or impact arising from the use of lifting equipment.

172 RO-UKEPR-052 identified the need to undertake detailed analysis of load path and rigging faults and as a result of the internal hazards assessment of dropped load and impact, the cross-cutting RO, RO-UKEPR-070 has gone a stage further and required EDF and AREVA to assess the consequences of dropped loads and impact on all RS1 and RS2 lifting equipment.

173 The GDA Issue, *"Substantiation and analysis of the consequences of dropped loads and impact from lifting equipment included within the EPR design."* includes the following GDA Issue Actions:

| | | | |
|---|---|---|---|
| **Technical Area** | **INTERNAL HAZARDS** | | |
| **Related Technical Areas** | Mechanical Engineering<br>Civil Engineering | | |
| **GDA Issue Reference** | **GI-UKEPR-IH-01** | **GDA Issue Action Reference** | **GI-UKEPR-IH-01.A1** |
| **GDA Issue** | Substantiation and analysis of the consequences of dropped loads and impact from lifting equipment included within the EPR design. | | |
| **GDA Issue Action** | Provide substantiation of the nuclear safety significant structures, systems and components vulnerable to dropped load and impact from RS1 and RS2 lifting equipment.<br>It is the expectation of ONR that dropped loads be considered for lifts that may result in nuclear significant consequences. The response should include detailed assessment of potential loads that could be dropped under such conditions and demonstrate that the provisions in place to ensure that the risk to nuclear safety of a load drop or impact is ALARP. Such assessment may include multi-legged arguments which consider the | | |

| | |
|---|---|
| | following:<br>• Claims on civil structures.<br>• Additional physical protection.<br>• Limits and conditions on the use of the RS1 and RS2 lifting equipment.<br>• Provision of detailed load path routes avoiding areas of highest nuclear significance.<br>• Measures (both system based and administratively controlled) in place to ensure the potential for impact of the load is minimised.<br>• Any further defence in depth and ALARP measures that could be implemented into the design.<br>• The impact of the changes made to the PCSR relating to the outcome of this substantiation on other safety case submissions submissions.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my expectations.<br>With agreement from the Regulator this action may be completed by alternative means. |

| | | | |
|---|---|---|---|
| **Technical Area** | **INTERNAL HAZARDS** | | |
| **Related Technical Areas** | Mechanical Engineering<br>Civil Engineering | | |
| **GDA Issue Reference** | **GI-UKEPR-IH-01** | **GDA Issue Action Reference** | **GI-UKEPR-IH-01.A2** |
| **GDA Issue Action** | Provide a description of the approach taken to treat dropped loads on civil structures, including consideration of the following:<br>• Derivation of design loads.<br>• Analysis methods.<br>• Design rules.<br>• Reliability expectations.<br>• Consistency between ECEIG070272 REV A1 “EPR- Load Drops - Methodology for risk analysis in civil engineering and building installations - Design review preparation conditions” and ETC-C in relation to consideration of Global stability.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my expectations.<br>With agreement from the Regulator this action may be completed by alternative means. | | |

## 4.2 Internal Missiles

174 The potential for internal missile generation associated with the UK EPR design was not assessed in detail during Step 3 as the supporting methodology report had not been issued in advance of reporting due to the need to translate the document from French to

English. As a result the Step 3 Internal Hazards Assessment Report identified the following areas for further assessment during Step 4:

- *"Further evidence of the adequacy of the approach to the methodology applied to the identification of dropped loads and internal missiles should be further investigated during Step 4 when the two outstanding documents are supplied."*
- *"Missile generation arising from the reactor vessel, steam generators, pressuriser, accumulators, reactor coolant pump body and other high energy tanks are considered to be sufficiently unlikely that they can be discounted as potential missile sources. The basis of this argument is that there are claims on the material characteristics, conservative design applied to each item of equipment, quality controls in manufacturing, as well as construction, maintenance, inspection and testing regimes. These claims are not addressed within this internal hazards assessment as they are associated with structural integrity, mechanical engineering and QA. Should the assessments within these areas identify that the missiles could be generated from these high integrity components further assessment would need to be undertaken to determine the nuclear safety significance associated with the generation of missiles from these components."*
- *"There are a number of different potential missiles assessed resulting from failures of valves within the reactor building. Three missiles, namely, a reactor coolant system safety valve, a CVCS isolation valve and a SIS/RHRS valve each with differing masses are analysed with a view to bounding the characteristic range of missiles. These missiles form the basis of the claim for valve generated missiles, however, there are no arguments or evidence to support their adequacy in terms of potential impact to nuclear safety should there be a valve generated missile within the Reactor Building. Further substantiation relating to the arguments and evidence associated with valve generated missiles is required during Step 4."*
- *"The PCSR identifies a number of measures to protect plant and equipment important to safety within the Reactor Building, including:*

  *Enclosure within compartments.*

  *Missile protection barriers.*

  *Use of physical restraints.*

  *Geographical separation and the use of distance.*

  *Component design and orientation.*

  *The claims above are consistent with the approach to missile protection applied within the UK and are consistent with the expectations of the HSE SAPs, EHA.14 relating to the identification of potential sources of missiles and the need for assessment, however, the PCSR does not provide arguments and evidence at this stage to support the claims made."*

175 In addition, the Step 3 Assessment Report identified the need to assess the specific barriers claimed to provide protection to SSCs within the Safeguards Building, the Fuel Building and the Diesel Buildings from the effects of internally generated missiles.

176 The approach to assessment was to undertake assessment of the Missile Methodology Report with a view to exploring the detailed arguments and evidence as required as part of the Step 4 assessment and then to review the claims made on the SSCs that are

claimed to not generate missiles either by virtue of their design or their operating limits and conditions e.g. failure of vessels, tanks and pumps.

### 4.2.1 Internal Missile Methodology

177 As mentioned within Section 4.1 of this assessment report, within the Step 2 Internal Hazards Assessment a request was made through a Technical Query, TQ-EPR-014, which requested EDF and AREVA to provide information on the methodology used to identify the internal hazards. The response to this TQ came in many parts and was incomplete at the time of issuing the Step 3 Internal Hazards Assessment, as the missile methodology had not been issued for assessment.

178 The document, *"EPR – Internal Missiles – Methodology description for analysis of layout in the buildings. Conditions for preparing design reviews."* (Ref. 27) was provided in response to the TQ and has been used as the basis of this assessment.

#### 4.2.1.1 Scope of Assessment Carried Out

179 The assessment has focussed on the arguments and evidence required to support the claims made within the PCSR as detailed previously. The approach to the assessment is to consider the claims made for each area and determine whether there are adequate arguments and evidence in place to support those claims.

#### 4.2.1.2 Assessment

180 The methodology provides information relating to the provisions in place for protection against the effects of internally generated missiles including details of the methodology for the identification and analysis of representative internal missiles. The purpose of the methodology is to demonstrate that the risk of missiles identified cannot result in deteriorating:

- More than one redundant F1 System; or
- Stability/integrity of:
  - i) The primary system barrier (except in the case of a Loss of Coolant Accident (LOCA),
  - ii) The reactor internals, including fuel elements,
  - iii) The main steam lines and steam generator (SG) feedwater supply line barriers,
  - iv) The fuel pit and its internal elements, including fuel elements,
  - v) Safety-classified buildings and fire-fighting barriers,
  - vi) Components whose fault is excluded by the design.

181 The purpose of the methodology appears reasonable and the detailed requirements for demonstrating that missiles cannot have a detrimental effect on nuclear safety are comprehensive.

182 The methodology considers the two main sources of missiles, failure of rotating equipment and failure of high energy equipment, which, as principles, I am satisfied capture all significant potential sources of missiles within the nuclear island. Missiles

generated as a result of an explosion are considered as part of the consequences associated with explosion.

183 There were a number of statements within the methodology that required further clarification and supporting arguments and evidence to be supplied. These included:

- Claims made on barriers against the effects of internal missile.
- Claims on the incredibility of failure of pump flywheels.

184 Discussions were held with EDF and AREVA relating to the unsubstantiated claims made within the methodology document. In addition to internal hazards assessment involvement, there was involvement from the structural integrity assessment area due to high integrity claims being made on SSCs in that topic area.

185 The methodology claims that some barriers are claimed to protect SSCs against the effects of missiles. The barriers claimed are not contained within the methodology report nor are they specified within the PCSR and as a result there was uncertainty over the extent of the claims made against such barriers. In addition, the PCSR states that the "Barrier Design Procedure" for internal missiles is contained within the document ETC-C (Ref. 16), however, the only reference to missile impact is associated with the impacts of heavy missiles on reinforced concrete slabs which is more associated with the dropped load and impact safety case rather than the internal missile safety case. ETC-C states, *"For the internal missile situation, calculations may be performed by special study with a penetration formula for hard missiles on a reinforced concrete slab (See appendix 1D)"*. The calculations detailed within Appendix 1D of ETC-C consider missile mass, velocity and diameter as well as considering the impacted concrete structure. This approach seems reasonable to the determination of the potential penetration depth and allows the existing wall thickness to be verified against the postulated penetration depth.

186 Further evidence associated with the claims made on barriers against the effects of internal missiles was sought through the issue of a TQ-EPR-1375 (Ref. 14) requesting EDF and AREVA to provide details of all barriers claimed within the safety case to prevent loss of more than one division due to the effects of failure of both RCC-M and non-RCC-M pipework, vessels, and tanks. At the time of writing this assessment report the response to the TQ had not been received and therefore, given the significance of the concerns, a GDA Issue (**GI-UKEPR-IH-02**) and an associated Action have been raised **(GI-UKEPR-IH-02.A4)**.

187 In the case of pump flywheels, the methodology states that there are strict requirements associated for the design, fabrication, and inspection such that the potential for failure of pump flywheels can be discounted. My expectations are such that unless there is a high integrity claim on the specific pump flywheel, then some form of consequences assessment should be undertaken. There have been discussions with EDF and AREVA together with the Structural Integrity assessment inspectors which have highlighted that the only flywheels where there are nuclear significant consequences of failure are associated with the reactor coolant pumps. The Structural Integrity assessment inspectors have considered failure of the reactor coolant pump flywheels and are content with the high integrity claims made. As a result no further assessment of failure of flywheels is undertaken given that the potential for failure has been discounted on the grounds of the aforementioned high integrity claim.

188 The methodology report then considers the potential for missiles generated from failures of high energy components such as vessels, tanks, pumps, valves and welded flanges. The potential for missiles generated from such components is precluded based upon the

RCC-M classification of the component. Further assessment of these areas has been subject to a cross discipline task and has involved assessment inspectors involved in the structural integrity assessment. This aspect of the assessment is considered specifically within Section 4.2.2.

Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

189 The Safety Assessment Principles (SAPs), state within EHA.14:

| **Engineering principles: external and internal hazards** | **Fire, explosion, missiles, toxic gases etc – sources of harm** | **EHA.14** |
|---|---|---|
| Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed. | | |

190 The International Atomic Energy Agency (IAEA) guidance NS-G-1.11 (Ref. 11) considers the need for barriers and physical separation to be adopted when there is the potential for missiles to result in loss of redundancy and that such barriers should be sited close to the source of the missiles. EDF and AREVA have claimed such protection within the design but not explicitly captured the location of the barriers that are claimed in the safety case.

191 Paragraph 3.27 of NS-G-1.11 states:

*"Evaluation of the adequacy of barriers, whether they are structures provided for other purposes or special missile barriers, necessitates the consideration of both local and general effects of missiles on the barrier. Depending upon the postulated missile's mass, velocity and impact area, the local or the general effect of the missile may dominate, but both should be evaluated. Local effects of missiles are penetration, perforation, scabbing or the ejection of concrete blocks and spalling, which are limited mainly to the area of impact on the target. General effects of missiles include buckling or structural failures in bending, tension or shear. Small missiles such as valve stems will have mainly local effects, while large, slow moving missiles such as those arising from structural collapse or falling loads will have mainly general effects."*

### 4.2.1.3 Assessment Conclusions

192 I am content with the approach taken to the assessment of potential missiles arising from failures of pump flywheels.

193 The GDA Issue, *"Outstanding internal hazards substantiation for internal flooding, cable routing, high energy line break and missiles forms part of the requisite evidence and will be required in order to demonstrate an adequate internal hazards safety case."* includes the following potential GDA Issue Action:

| | | | |
|---|---|---|---|
| **Technical Area** | **INTERNAL HAZARDS** | | |
| **Related Technical Areas** | Structural Integrity<br>Civil Engineering<br>Fault Studies<br>PSA | | |
| **GDA Issue Reference** | **GI-UKEPR-IH-02** | **GDA Issue Action Reference** | **GI-UKEPR-IH-02.A4** |

| | |
|---|---|
| **GDA Issue Action** | Provide the requisite evidence in the form of the detailed Flamanville 3 verification and validation analysis and/or other supporting documentation in support of the claims and arguments presented within Chapter 13.2 of the PCSR associated with internal missiles. The response should include analysis that supports the claims and arguments relating to:<br>• Identification of all potential sources of internal missile which could result in a threat to nuclear safety significant SSCs.<br>• Consequence analysis, where applicable.<br>• Break preclusion.<br>• Identification and qualification of physical restraints, barriers and doors.<br>• Any further defence in depth and ALARP measures that could be implemented into the design.<br>• Any identified design changes and their implementation within the PCSR.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my expectations.<br>With agreement from the Regulator this action may be completed by alternative means. |

### 4.2.2 Missiles Arising from Failure of Tanks and Vessels

194 Further to the assessment of the EPR Internal Missile Methodology as discussed within Section 4.2.1 above, the specific issue of the break preclusion claim made against RCC-M (Ref. 28) classified vessels, pumps, tanks and valves was identified as requiring further detailed assessment from both an internal hazards and structural integrity perspective.

#### 4.2.2.1 Scope of Assessment Carried Out

This assessment focussed on the validity of the claims associated with the extension of the break preclusion of RCC-M components beyond those submitted in answer to Regulatory Observation RO-UKEPR-019 (Ref. 15). The list of components generated in answer to RO-UKEPR-019 are the only ones for which the requirement of break preclusion is being claimed under the topic of Structural Integrity. The assessment involved assessment inspectors from the Structural Integrity assessment area in order to provide assistance associated with the integrity claims made within the PCSR.

195 My assessment focus within this area related to the arguments and evidence associated with the claims associated with the generation of missiles from RCC-M components.

#### 4.2.2.2 Assessment

196 The PCSR section relating to the potential for generation of internal missiles, PCSR Chapter 13.2, Section 4.2.2.1.1. (Ref. 17) states,

*"A failure within the reactor vessel, steam generators, pressuriser, accumulators, reactor coolant system primary circuit, pump casings and other high energy tanks, with sufficiently high classification (at least M3 requirements, see Sub-chapter 3.2), leading to the generation of missiles, is considered to be sufficiently unlikely for this mode of missile*

*generation to be discounted. A massive and rapid failure of these components is not considered credible due to the material characteristics, the conservative design applied to each item of equipment, the manufacturing quality controls and the construction, operation, maintenance and inspections regimes.*

*However, for these components, in accordance with the concept of defence in depth, an analysis of the failures involving generation of missiles, which could lead to unacceptable radiological releases, is performed. The components identified are then classified "High Integrity Components" and are subject to appropriate requirements. Even if the failure of a main reactor coolant system loop is considered incredible, the loops are designed so that a break in one loop could not lead to failures in the other loops.*"

197 Furthermore, the PCSR section relating to protection against failures of tanks, pumps and valves, PCSR Chapter 13.2, Section 3.2.1. on RCC-M classified equipment states,

*"Gross rapid failure of these components is not considered credible due to the material characteristics, the conservative design applied to each item of equipment, the manufacturing quality controls and the construction, operation, maintenance and inspection regimes."*

and

*"The consequences of leaks from tanks, pumps and valves are not analysed, as it is considered that the postulated leak and break size (cross sectional area) in connected pipework, including associated welds, are bounded by the following effects:*

- *System analysis e.g. over cooling transients, reactivity feedback, emergency core cooling, and redundancy in the design of the safety systems.*
- *Increased ambient conditions e.g. pressure, temperature, humidity, and radiation.*
- *Internal flooding*
- *Forces acting on safety-related SSCs e.g. jet impingement, pressure waves etc."*

198 Whilst it is accepted that undertaking a bounding consequence analysis is an appropriate method of structuring a safety case it is not clear to me that the scenarios listed above will bound all potential failures of RCC-M vessels, tanks, pump casings etc. Further evidence associated with the claims made on the preclusion of missile generation from failure of RCC-M components was raised by TQ-UKEPR-1374 which requested EDF and AREVA to provide details of the approach taken to claims made on the preclusion of missiles generated from failure of RCC-M components and provide evidence to support discounting missile generation.

199 At the time of writing the Step 4 Assessment Report, the response to the TQ had been received, however, there was insufficient time to enable assessment, and therefore, given the significance of the concerns, a GDA Issue **(GI-UKEPR-IH-04**) and associated Action has been raised **(GI-UKEPR-IH-04.A1)**.

200 The SAPs principle EHA.14 states:

| **Engineering principles: external and internal hazards** | **Fire, explosion, missiles, toxic gases etc – sources of harm** | **EHA.14** |
|---|---|---|
| Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed. | | |

201 In the absence of a consequence analysis of failure of RCC-M components, it is not possible to determine the potential source of harm to the nuclear facility.

202 NS-G-1.11 states within Section 3.2 on missiles:

*"In nuclear power plants, pressure vessels that are important to safety are designed and constructed by means of extremely comprehensive and thorough practices to ensure their safe operation. Analysis is performed to demonstrate that levels of stress are acceptable under all design conditions. All phases of design, construction, installation and testing should be monitored in accordance with approved procedures to verify that all work is carried out in accordance with the design specifications and that the final quality of the vessel is acceptable. A surveillance programme during commissioning and operation, as well as a reliable system for overpressure protection, should be used to determine whether the vessels remain within their design limits. The gross failure of such vessels (such as the reactor pressure vessel) is generally believed to be sufficiently improbable that consideration of the rupture of these vessels as a PIE [Potential Initiating Event] should not be necessary."*

203 The vessels to which the above paragraph relates are those which are so important to safety that the risk of failure must be demonstrated to be so low that it can be discounted. In the Structural Integrity Safety Case these have been termed the High Integrity Components (HIC).

204 Section 3.3 of the same document refers to other vessels which are not of such high integrity and are assumed to fail; the guidance within this area states:

*"Other vessels in nuclear power plants may not undergo such stringent design, quality assurance and surveillance. Failures of such vessels containing fluids of high internal energy should be evaluated, as they may become sources of missiles if they rupture. The failure of a pressure vessel can result in a wide variety of failure modes depending on such factors as material characteristics, the shape of the vessel, the positions of welds, the design of nozzles, construction practices and operating conditions. Metal vessels composed of materials that behave in a brittle manner are more likely to produce missiles."*

205 It is my expectation that where components are not termed as HIC then some form of consequence analysis is required and this is how I have interpreted the guidance within NS-G-1.11. This is also in line with the SAP EHA.14 discussed previously.

206 In addition, NS-G-1.11 Section 3.5 states:

*"A vessel, because of its unpredictable behaviour and the potential for severe damage, should be designed so that it cannot as a whole become a missile. If it is judged that the vessel as a whole could become a missile, an analysis should be made of the various locations of ruptures and break sizes to determine whether the resultant vessel blowdown forces would be sufficient to separate the vessel from its retaining supports (restraints). If a vessel could be separated from its restraints, the design of the vessel should be modified to prevent this type of failure."*

#### 4.2.2.3 Assessment Conclusions

207 I would expect EDF and AREVA to either substantiate the claims made associated with RCC-M components such that the potential for disruptive failure is not credible, which will require the application of the arguments used in answer to RO-UKEPR-020, or undertake detailed consequence analysis associated with failure of RCC-M vessels and tanks.

These conclusions are based upon the expectations stated within both the SAPs and the IAEA guidance which confirms the need for such analyses. Therefore, the GDA Issue, "Consequences of missile generation arising from failure of RCC-M Components" includes the following GDA Issue Action:

| | | | |
|---|---|---|---|
| **Technical Area** | | **INTERNAL HAZARDS** | |
| **Related Technical Areas** | | Structural Integrity<br>Civil Engineering<br>Fault Studies | |
| **GDA Issue Reference** | **GI-UKEPR-IH-04** | **GDA Issue Action Reference** | **GI-UKEPR-IH-04.A1** |
| **GDA Issue** | Consequences of missile generation arising from failure of RCC-M Components. | | |
| **GDA Issue Action** | Provide substantiation of the claims made within the PCSR associated with the preclusion of missile generation from failure of RCC-M components which are not designated as High Integrity Components (HIC) as defined in the consolidated PCSR. This could be undertaken through detailed analysis of the consequences of failure. The detailed analysis should include consideration of:<br>• Identification of those potential sources of internal missile which could result in a threat to nuclear safety significant SSCs.<br>• Analysis of the consequences of failure.<br>• Passive features such as barriers and restraints.<br>• Examination, maintenance, inspection, and testing as a potential part of a multi-legged safety justification for missiles.<br>• Any further defence in depth and ALARP measures that could be implemented into the design.<br>• Any identified design changes and their implementation within the PCSR.<br>• The impact of the changes made to the PCSR relating to the outcome of this substantiation on other safety case submissions such as civil engineering and mechanical engineering.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of ONR expectations.<br>With agreement from the Regulator this action may be completed by alternative means. | | |

### 4.3 High Energy Line Break

208 High energy line break (HELB) considers the potential for failures of pipework and considers the following hazards as part of this assessment:

- Part-pressure failure,
- Jet impingement

- Pipewhip

209 During Step 3, leaks and breaks were subject to a limited assessment of high level principles. The Step 3 report identified the basis for the consideration of failures of pipework based upon specific nominal bores and the principles of the safety case for pipe break were sound. As part of the Step 4 assessment, further sampling of some of the specific areas where pipe breaks are postulated have been subject to assessment in order to identify the requisite evidence to support the claims being made within the PCSR.

### 4.3.1 Scope of Assessment Carried Out

210 The scope of the assessment involved a sample of arguments and evidence to support the claims contained within the PCSR, which entailed assessment of the *"1st stage analysis: consequences of high energy line breaks - safeguard auxiliary and electrical buildings"* (Ref. 29). In addition, two areas of the Safeguards Auxiliary Building (SAB) were subject to detailed deep slice sampling assessment.

### 4.3.2 Assessment

211 The approach taken to the production of the 1st stage SAB analysis for HELB used simplified scenarios sourced from the FA3 design and considered multiple damaged pipes, greater than the amount that would be expected to fail based upon the reference information relating to failures of the pipework. The intention of the 1st stage analysis is to validate overall compliance of the facility with the requirements of the safety case prior to all the detailed design data being made available.

212 There are assumptions made within the 1st stage analysis associated with failure of the vulnerable pipework at any point along its length. This essentially results in a threat to all pipework within the room or compartment where the break occurs. Should the results identify a shortfall in the application of this approach, namely, that the bounding assumption of failure of pipework at any point is not tolerable, further analyses would be undertaken. This second stage analysis is undertaken once all completed detailed design information is available as part of the verification and validation for HELB. The 1st Stage Analysis is not due to be fully completed until March 2011 and, therefore, too late for detailed assessment and inclusion within the Step 4 Assessment Report. The 2nd Stage Analysis will follow on from the work undertaken within the 1st Stage Analysis and will also not be available prior to the end of Step 4.

213 I believe that the deterministic approach to loss of multiple equipment within areas vulnerable to HELB is an acceptable approach in the first instance as a means to identify any vulnerability associated with HELB. However, I would expect any areas identified within the 1st stage analysis to be captured and analysed at the earliest opportunity in order to ensure that the specific threats associated with HELB are designed out in the first instance.

214 As part of my deep slice sample, my assessment has focussed on the completed reports undertaken as part of the 1st Stage HELB Analysis provided for the SAB. The analysis identifies two areas of the SAB where vulnerabilities associated with the potential to lose all redundancy in the event of HELB:

- Loss of the 4 Safety Injection System (SIS) trains and 2 Containment Heat Removal System (CHRS) trains by draining the In-Containment Refuelling Water Storage Tank (IRWST) into the SAB.
- Loss of alignment functions on the Emergency Feedwater System (EFWS) pump heads and discharge suction.

215 Each of these events were assessed further and TQs (TQ-EPR1277, TQ-EPR-1278) (Ref. 14) were raised seeking further information and the plant conditions required in order to result in loss of all redundancy for the two events.

Loss of the 4 SIS trains and 2 CHRS trains resulting in drainage of the IRWST into the SAB

216 The TQ response (TQ-EPR-1277) (Ref. 14) associated with the event stated that this potential loss of all redundancy was identified during the HELB studies that were undertaken for EPR. The potential for a pipe break on the Low Head Safety Injection (LHSI) line could result in a pipewhip event resulting in a break on the CHRS line. This in turn would result in drainage of the IRWST into the SAB as the motorised valve on the line is normally in the open position. The subsequent drainage of the IRWST could then result in unavailability of all 4 SIS trains and both CHRS trains. As this event does not meet the requirements of prevention of more than one redundancy of an F1 system against the effects of an internal hazard, EDF and AREVA have proposed to implement a change to the operation configuration of the system.

217 The proposed modification involves changing the normal position of EVU1111VP within Division 1 SAB and EVU4111VP within Division 4 SAB from “open” to “closed”. The TQ states, *“There is no operational requirement for these valves to be in an open position in normal operation of the plant. The CHRS system is required during accident sequences when the containment isolation signal has already been initiated so these valves would have been closed.”* I am uncertain over the extent of analysis that has been undertaken within this area. Whilst it is accepted that changing the configuration of the valves may not have an impact on the safety case, there is no evidence provided other than the statement within the TQ response. I would expect that further analysis of the event to determine the sensitivity and impact of the change on the safety case be undertaken. As a result this has been identified as an Assessment Finding **(AF-UKEPR-IH-01)**. A GDA Issue has been raised within the area of fault studies entitled, *“EDF and AREVA to provide a design basis analysis of failures in the essential support systems”* in which there is a GDA Issue Action associated with the need to undertake a design basis analysis of loss of cooling chain faults. Completing the action should result in the Assessment Finding being addressed, however, I require this aspect of the evidence to be provided specifically rather than through the generic GDA Issue in order to close out the assessment within this area.

Loss of alignment functions on the EFWS pump heads and discharge suction

218 The EFWS comprises four separate trains comprising of a tank supplying a pump and tank header, a discharge header and isolation valves. The valves in each train feeding the tank and discharge headers are normally closed to provide the most effective separation between the divisions and opened by operator action as required providing feed to the steam generators, as necessary. Each train of the EFWS is located in a separate SAB and feeds its own steam generator.

219 The TQ response (TQ-EPR-1278) (Ref. 14) identified that realignment of the EFWS pumps is required for PCC transients such as a break in the Main Feed Water System

(MFWS), steam system piping break or steam generator tube rupture. The alignment of the EFWS considers the most onerous operating scenario and assumes one train in maintenance with simultaneous failure in another train. As a result the realignment of the EFWS pump feeding the affected steam generator to an unaffected one is necessary to ensure that there are two available for cooling the primary circuit. This realignment is undertaken downstream of the EFWS pumps at the discharge headers which are located within the lower rooms of the SAB. These lower rooms also contain a number of high energy pipes which, as a result of the 1st Stage HELB analysis, are assumed to fail. The analysis concludes that there is the potential for a HELB within one of these rooms that could result in loss of the ability to align the valves according to the requirements of the safety case. EDF and AREVA deem this to be acceptable since there is no dependency link between a HELB in the lower parts of the SAB and the PCC events associated with the requirements for realignment. Furthermore, a HELB within the areas described during a PCC event constitutes a passive single failure which is bounded by the active single failure for the PCC bounding case taking into account loss of an entire train of the EFWS.

220 I am satisfied that these particular events have been adequately addressed by EDF and AREVA, however, as the 1st and 2nd Stage analyses have yet to be completed and whilst there remains the potential for design changes, as is the case of potential drainage of the In-containment Refuelling Water Storage Tank (IRWST) detailed above, I believe it prudent to identify this area as a GDA issue as part of a broader GDA Issue relating to internal hazards substantiation **(GI-UKEPR-IH-02.A3).**

Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

221 The SAPs, state within SAP EHA.5 and SAP EHA.6:

| **Engineering principles: external and internal hazards** | **Operating conditions** | **EHA.5** |
|---|---|---|
| Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition. | | |

| **Engineering principles: external and internal hazards** | **Analysis** | **EHA.6** |
|---|---|---|
| Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects. | | |

222 This is further reinforced by SAP EHA.14:

| **Engineering principles: external and internal hazards** | **Fire, explosion, mssiles, toxic gases etc – sources of harm** | **EHA.14** |
|---|---|---|
| Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed. | | |

223 NS-G-1.11 states within paragraph 3.55:

*"The whipping pipe branches should be analysed geometrically to determine possible directions of motion that might endanger target SSCs, as well as to evaluate their kinetic energy. Any possible mechanical impact on the target should be investigated by means*

*of an appropriate dynamic analysis made on the basis of a detailed assessment of the system transient, to quantify the discharge forces and the energy of the whipping pipe as well as the fraction of the energy that would be transferred to the target (the extent of the analysis can be limited on the basis of conservative assumptions). In addition, the analysis should include an assessment of the effectiveness of the pipe whip restraints, demonstrating that pipe deflections may be kept small by the physical restraints. In the case of terminal end breaks, consideration should be given to the secondary effects on the remaining terminal ends."*

224 The SAPs and IAEA guidance detailed above, consider that detailed analysis of failures associated with HELB be analysed in detail to determine their potential impact on adjacent safety significant SSCs.

### 4.3.3 Assessment Conclusions

225 I believe that this deterministic approach to loss of multiple equipment within areas vulnerable to HELB is an acceptable approach, in the first instance, as a means to identify any vulnerability associated with HELB. However, I would expect that the 1st and 2nd Stage Analyses be provided as part of the overall evidence in order to support the claims and arguments presented within the PCSR.

226 The GDA Issue, *"Outstanding internal hazards substantiation for internal flooding, cable routing, high energy line break and missiles forms part of the requisite evidence and will be required in order to demonstrate an adequate internal hazards safety case."* includes the following GDA Issue Action:

<table>
<tr><td>Technical Area</td><td colspan="3">INTERNAL HAZARDS</td></tr>
<tr><td>Related Technical Areas</td><td colspan="3">Structural Integrity<br>Civil Engineering<br>Fault Studies<br>PSA</td></tr>
<tr><td>GDA Issue Reference</td><td>GI-UKEPR-IH-02</td><td>GDA Issue Action Reference</td><td>GI-UKEPR-IH-02.A3</td></tr>
<tr><td>GDA Issue Action</td><td colspan="3">Provide the requisite evidence in the form of the detailed Flamanville 3 verification and validation analysis, specifically, the FA3 1st Stage Pipe Break Analysis and/or other supporting documentation in support of the claims and arguments presented within Chapter 13.2 of the PCSR associated with high energy line break (HELB) within the EPR design. The response should include analysis that supports the claims and arguments relating to:<br>• Consequence analysis, where applicable.<br>• Break preclusion.<br>• Identification and qualification of physical restraints, barriers and doors.<br>• Identification and qualification of pressure relief panels/routes.<br>• Any further defence in depth and ALARP measures that could be implemented into the design.<br>• Any identified design changes and their implementation within the PCSR.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my</td></tr>
</table>

| | |
|---|---|
| | expectations.<br>With agreement from the Regulator this action may be completed by alternative means. |

227 In addition, there is a need to provide the requisite evidence associated with configuration of two valves associated with the CHRS and as a result the following Assessment Finding has been identified:

- ***AF-UKEPR-IH-01*** *– The Licensee shall provide evidence to support the design change associated with the configuration of the valves, EVU1111VP within Division 1 SAB and EVU4111VP within Division 4 SAB including a demonstration that closure of the valves during normal operations does not have a detrimental effect on the design basis analysis undertaken in support of the safety case.*

228 This Assessment Finding should be addressed as part of the following procurement and construction generic milestone for Assessment Findings:

- Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.

## 4.4 Internal Fire

229 Internal fire was subject to extensive assessment during Step 3 and the following areas were identified as requiring further assessment of the arguments and evidence during Step 4:

- F1B Functions Associated with the fire fighting water system (JPI/JAC)
- Common Mode Failure Analysis and Segregation from the Effects of Fire
- Passive Cable Protection
- DFL HVAC Smoke Control and Extract System
- Fire involving the Reactor Coolant Pumps

### 4.4.1 F1B Functions Associated with the Fire Fighting Water System (JPI/JAC)

230 During Step 3 a TQ-EPR-215 (Ref. 14) was raised seeking clarification of the functional classification for the JPI/JAC system in relation to the F1B claims being made on the system. The response to the TQ arrived too late in the process to be considered within the Step 3 Assessment Report and as a result the GDA Step 4 Plan identified a need to assess the response to the TQ.

#### 4.4.1.1 Scope of Assessment Carried Out

231 During Step 4 Issue 02 of Section 13.2 PCSR was issued, which included amendments to Issue 01 specifically associated with the claims made on the JPI/JAC system performing F1B functions. As a result Issue 02 has been used as the basis for this assessment but due cognisance has been taken of the response to TQ-EPR-215.

#### 4.4.1.2 Assessment

232 Issue 02 of the PCSR states that the JPI/JAC system has additional functions associated with decay heat removal in the case of the following events:

- PCC-3 event "isolable piping failure on a system connected to the spent fuel pool" (see Sub-chapter 14.4). In this event, capacity for storage and pumping function of the JAC system are used for achieving water makeup to the fuel pool, through JPI circuit.
- Hypothetical loss of the Fuel Pool Cooling System (FPCS). In this case, the loss of water by evaporation or boiling in the spent fuel pool may be mitigated by water makeup from the JAC system through the JPI circuit.

233 The JAC system is intended for the production of fire fighting water for the whole plant, both the conventional and nuclear islands. The system comprises of two tanks with a capacity of approximately 3600m$^3$ in total with four standard fire fighting pumps. The JPI system is the nuclear island piping system fed via two segregated lines from the JAC. In the event of requiring FPCS makeup, the JAC tanks are able to supply 330m$^3$ at the required flow rate of 150m$^3$/h through the actuation of one JAC pump. The JAC/JPI equipment necessary in this event is classified F1B, is operable after an earthquake and has backup power supplies. As a result the PCSR now identifies the following aspects of the JPI/JAC system as being F1, specifically:

- JPI containment penetrations,
- Pumps, pipes and valves of the JAC and JPI systems which provide water makeup to the spent fuel pool.

234 The report, *"Functional design relating to PCC treatment of loss of cooling and pool drainage"*, ECEF080499 (Ref. 30) provides details of the F1 functions of JPI/JAC system in the case of a PCC-3 and a PCC-4 event. The two events have been subject to assessment to determine whether the claims made upon the JPI/JAC system are adequate.

235 In the case of the PCC-3 event, *"Isolable piping failure on a system connected to the spent fuel pool"*, it is stated that in the event of a main train pipe break there would be a need to provide makeup water due to the break resulting in automatic shutdown of both main train pumps on reaching [redacted] which would then result in loss of pond cooling. Drainage through the suction and drainage lines would be halted through the provision of siphon breakers and a controlled state would be reached at [redacted] level. In order to reach a safe shutdown state there would be a need to locate and isolate the break through manual isolation of the redundant valves at the mains trains suction. At this point there would be a need to supply makeup water from the JPI lines fed from the JAC. Once a level of [redacted] is reached in the pond, the remaining main train could be restarted. The timescales in which pond makeup would be required through the initiation of a JAC pump would be over two hours for all plant states both with and without the transfer tube open.

236 For the PCC-4 event, *"Non isolable small break (<50mm) or isolable RIS [SIS] break (<250mm) in RHR mode, spent fuel pool drainage aspects (State E)"*, in which a pipe break is considered on:

- the DN250 reactor coolant cooling system (Safety Injection System (SIS) line in the Residual Heat Removal (RHR) mode),

- a pipe with a diameter of less than DN50 connected to the reactor coolant system upstream of the first isolation valve.

237 During State E, the transfer tube is open and as a result a break can affect the cooling of the spent fuel pool and lead to automatic shutdown of both main train pumps on reaching [redacted]. During the unloading/refuelling phases, the break is automatically isolated at the suction of the SIS/RHR by the closure of the redundant motor-operated valves of the SIS on detection of low level being detected in the reactor building transfer compartment. The level of the pond would be [redacted] at this point and would require makeup of [redacted] provided by the JPI/JAC system to bring the plant to a safe shutdown state of [redacted]. Once again there would be in excess of two hours in which to instigate makeup feed via the JPI/JAC system.

Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

238 The approach taken for the use of the fire fighting water supply system is consistent with the IAEA guidance document, NS.G.1.7, which states within paragraph 5.36, *"The water system for the fire extinguishing system should be used only for fire fighting. This water system should not be connected into the piping of the service water or sanitary water systems except as a source of backup supplies of fire fighting water or to perform a safety function to mitigate an accident condition. Such connections should be provided with an isolating valve that is locked in the closed position or should be provided with position monitoring during normal operation."*

239 In addition, there are many fire fighting systems currently installed across both nuclear reactor plant and nuclear chemical plant which have an additional function to provide a form of emergency water supply to mitigate against various accident conditions e.g. cooling pond make up supply systems and, in the case of high active waste storage, decay heat removal. Therefore, the approach taken through the utilisation of the fire fighting water stocks is consistent with existing UK practice.

#### 4.4.1.3 Assessment Conclusions

240 Given the infrequent nature of the event, the redundancy in the system (4 JAC pumps with interconnecting lines feeding the JPI ring main), and the time for corrective action to be taken to align and reinstate makeup water to the spent fuel pond, I am satisfied that the provisions in place and the claims made upon the use of the JPI/JAC in this event are adequate. Furthermore, as the approach taken to the provision of fire fighting water supplies is consistent with international relevant good practice and with existing practice within the UK, I am satisfied that the proposed approach to the utilisation of the fire fighting water supply is satisfactory.

241 There are no Assessment Findings or GDA Issues identified arising from this aspect of the internal hazards assessment.

### 4.4.2 Common Mode Failure Analysis and Segregation from the Effects of Fire

242 The principles associated with common mode failure and segregation have previously been subject to assessment during both Steps 2 and 3 of the GDA. The purpose of the further assessment was to consider the detailed arguments and evidence arising during the Step 4 assessment. The requirement for this assessment was identified within the Step 3 Assessment Report and within the Step 4 Assessment Plan for internal hazards.

#### 4.4.2.1 Scope of Assessment Carried Out

243 The focus of the assessment has been on the potential for common mode failure associated with multiple trains located within common areas. Consideration of the approach taken by EDF and AREVA to ensure that adequate analysis has been undertaken to ensure that the requirements for 4 train segregation are met for F1A functions and 2 train segregation for F1B functions. As part of the sample undertaken two Nuclear Island buildings were assessed; the SAB, due to the need for four train segregation for the F1A functions; and the Fuel Building, due to the need for two train segregation of the F1B functions contained therein. Fire was selected as the potential common mode failure initiating event.

#### 4.4.2.2 Assessment

244 Following on from the design requirements for fire within the PCSR, further sampling of safety submissions provided in response to TQs and through internal hazards topic meetings which has focussed on the vulnerability analysis undertaken to ensure that any potential common mode failures due to fire are identified and adequately addressed.

245 The PCSR identified the need to undertake a vulnerability analysis in order to assess the potential for common mode failures arising from fire. The analysis involves the determination of any potential common code failures arising from the application of the criterion contained within EDF report, *"Principle of Common Mode Fire Risk Analysis"*, ENSNEA090055 (Ref. 31). The criteria (a to f) are as follows:

- Criterion (a): *"Safety-class mechanical equipment or electrical connections belonging to two redundant trains from the same system performing the same safety function should not be installed in the same safety fire area"*.
- Criterion (b): *"Safety-class mechanical equipment or electrical connections belonging to a train of a system performing a safety function on the one hand, and to systems necessary for the operation of the same system of a redundant train on the other hand, must not be installed in the same safety fire area."*
- Criterion (c): *"Electrical connections that are supplied by redundant electrical switchboards, and whose number is such that the selectivity of the protection of these switchboards may be challenged, must not be present in the same safety fire area."*
- Criterion (d): *"Equipment whose failure in the event of fire is likely to lead to a PCC condition and equipment required for the management of the PCC condition under consideration must not be present in the same safety fire area."*
- Criterion (e): *"Equipment whose failure is postulated with regard to the single aggravating factor in a PCC condition and equipment required in the study of the condition under consideration from the controlled state must not be present in the same safety fire area."*
- Criterion (f): *"For all RRC A/B conditions considered, a check will be performed that a fire does not prevent to maintain the final state beyond the 15 days following the initiating event."*

246 In order to demonstrate that these criterion are met a number of analyses have been undertaken for Flamanville, 3 that will provide evidence to support UK EPR GDA, associated with the determination of fire zoning requirements based upon the high level

design requirements which are fed through into the above criterion. As part of the sample undertaken during Step 4, I undertook assessment of the following three reports:

- *"Safety Requirements for defining Safeguard Auxiliary and Electrical Building Fire Zones"*, ECEF070601 (Ref. 32)
- *"Safety Requirements for defining Fuel Building Fire Zones"*, ECEF071646 (Ref. 33)
- *"Safety Requirements for the Establishment of Fire Zoning in the Reactor Building"*, ECEF071591 (Ref. 34)

247 Criterion (a) and (b) detailed above are consistent with the approach taken to ensuring adequate segregation of SSCs against the potential effects of an internal fire within existing UK nuclear power generation facilities. Ensuring that there is adequate redundancy and segregation of the trains provides confidence that should there be a single fire within a division of the Safeguard Building it would be extremely unlikely to spread to an adjacent train. The approach taken to EPR with four train segregation ensures that there is always one train remaining to perform the required safety function – one train out on maintenance, application of a single random failure to another, and the train affected by fire, hence leaving 1 train to fulfil the 100% duty requirement. There is two train segregation provided as part of the F1B functions within the Fuel Building, with the exception of the FPCS which is three trained to allow for on-load maintenance with the third FPCS train contained within the Division 1 SAB.

248 I am satisfied with criterion (a) and (b) for the SAB and Fuel Building and the approach and assumptions made are in line with my expectations.

249 In the case of the Reactor Building, due to the open nature of the containment, separation in to different safety fire areas is not always feasible. There are some provisions in place to minimise the potential effects of fire within the Reactor Building, namely:

- It is split into two safety fire compartments: one for inside the inner containment wall and the second for the containment annulus.
- Beneath 19.5 m level the inner containment is divided into four safety fire cells, one per electrical division and includes the Reactor Coolant Pumps and the Safety Injection System, and the Residual Heat Removal System, all three of which are four train systems.
- The containment annulus is also split into four safety fire cells each containing all the cabling and connections to the corresponding Safeguard Building.

250 The analysis has considered each of the F1 systems within the Reactor Building to determine their vulnerability to a single fire. The Steam Generator Blowdown System (SGBS) has been sampled from the Reactor Building analysis to determine the adequacy of the provisions in place for meeting the requirements of criterion (a).

251 The SGBS analysis identifies that isolation after a Steam Generator tube rupture, requires a number of valves to remain available and as such requires them to be separated from the effects of a single fire. The analysis identifies the need to separate valves APGi110VL and APGi120VL from APGi130VL (where i = 1 to 4 for each of the divisions), however, it does not confirm where the segregation requirements are captured within the design. The analysis simply states that they require to be segregated and is captured as if it were a design requirement. This situation is repeated for a number of valves on this system and for other systems detailed under criterion (a).

252 In addition, there are a number of instruments that require to be separated in order to enable F1 functions to be kept available in the event of fire while also avoiding spurious actuations in the case of sensors using voting logic for the initiation of protection. Some of the instruments are used for post-accident monitoring and automatic diagnostics. The list of instruments is extensive and runs to 25 systems and over 120 instruments and valves. It is understood that these requirements are captured as part of the detailed design phase and will be subject to appropriate verification and validation. However, I have reservations associated with how the requirements identified within the Reactor Building analysis are brought forward into the PCSR given that the report does not form part of the auditable trail of the PCSR and furthermore, how such requirements are captured as part of the construction and operational phase. I have, therefore, raised an Assessment Finding to ensure that such requirements are captured **(AF-UKEPR-IH-02)**.

253 Criteria (a) to (c) are associated with the cable routes and require detailed knowledge of the specific routing of individual cables between safety significant SSCs which is undertaken as a verification and validation task at a later stage in the project. This verification and validation work for FA3 has not yet been completed and, therefore, it is difficult to state with confidence that the cable routing to and from each division has been adequately segregated either spatially or by passive fire protection from a foreign division.

254 TQ-EPR-1279 (Ref. 14) relating to the cable protection philosophy for foreign divisions coupled with a request for Report, "Identification of Protected Cable Trays", EYRT2010FR0042 A, was raised as a result of the assessment undertaken. This TQ was due to be issued by the 20th October 2010, however, the response had not been issued at the time of writing this report.

255 Information has also been provided associated with analyses that have been undertaken relating to safety requirements for the definition of fire zoning, which include assessment of PCC and RRC events to determine whether there are any potential common mode failures (with the exception of the assessment of criteria (a) to (c) relating to cable routing mentioned previously).

256 Whilst I have a degree of confidence from the specifications within the design, there remains a gap in the requisite evidence associated with the cable routing as the analysis for criterion (c) has not yet been completed for Flamanville 3 and the outstanding TQ relating to the philosophy for routing of cables within foreign divisions and the identification of protected cable routes.

257 Therefore, it is difficult to state with confidence that the cable routing to and from each division has been adequately segregated either spatially or by passive fire protection from a foreign division. As part of a broader GDA Issue relating to internal hazards substantiation, a GDA Issue Action has been produced that requires EDF and AREVA to provide detailed analysis and substantiation in support of the claims and arguments associated with the routing of electrical cables within the UK EPR design **(GI-UKEPR-IH-02.A2)**.

258 Criterion (d) considers fire initiation within a fire zone and the potential to result in a PCC condition. The approach taken involves a review of the potential impact fire would have on the PCC-2, PCC-3 and PCC-4 events detailed within the PCSR Section 14, Fault Analysis (Ref. 17). As part of the analysis undertaken there have been no PCC events identified that require further analysis for the Reactor Building. In addition there have been no PCC-4 events identified within the SAB or the Fuel Building as requiring any further transient analysis due to the design provisions inherently ensuring that fire cannot

result in a PCC-4 event. As part of my sample, two PCC-2 events and one PCC-3 event have been selected for further assessment which are:

PCC-2 Event – Loss of a FPCS Cooling Train or Support System in State A

259 This event considers fire within each of the divisional electrical supplies within the SAB and considers what FPCS pumps and support systems will be available taking into account maintenance and the application of the single failure criterion. The electrical power for the FPCS pumps and the requisite support systems is detailed within Table 5 below.

**Table 5:** Electrical Power for the FPCS Pumps and Support Systems

| | Division 1 | Division 2 | Division 3 | Division 4 |
|---|---|---|---|---|
| FPCS | Pump train 3 | Pump 1 train 1<br>Pump 2 train 1 | | Pump 1 train 2<br>Pump 2 train 2 |
| CCWS | CCWS pump div 1 | CCWS pump div 2 | CCWS pump div 3 | CCWS pump div 4 |
| ESWS | ESWS pump div 1 | ESWS pump div 2 | ESWS pump div 3 | ESWS pump div 4 |
| CHRS | Pump train 3 | | | |
| UCWS | Pump train 3 | | | |

260 From this information the analysis then went on to ascertain the impact of loss on power for each of the divisions and considered differing initial plant conditions to determine the most onerous requirements on the FPCS in the event of fire. The most onerous plant configuration coupled with a fire was:

- fire within either Division 2 or 4 with the other FPCS pumps (FPCS Main train 1 or 2 depending on whether the fire results in loss of power within Division 4 or 2) shut-off but available, and the 3rd train also shut-off but available.

261 The analysis concludes that should fire initiate and result in loss of power as detailed above, then there are at least two ways available on shutdown to cool the FPCS. If a single failure is applied to one of these methods, the other method can be started to cool the Fuel Building pool. As a result the analysis does not identify any further requirements associated with ensuring pool cooling in the event of fire within the SAB.

PCC-2 Event – Loss of a FPCS Cooling Train or support system in State A initiated by a fire in the Fuel Building.

262 This event involves the need to ensure that there is a single FPCS train available to maintain cooling to the spent fuel pit. It postulates that one of the main FPCS trains is out for maintenance and the other is affected by fire within the Fuel Building. This results in the need to utilise the third train located within Division 1 of the SAB. There are motor driven valves associated with the third train that are located within the Fuel Building, however, they are aligned such that there is no requirement for the valve position to be changed to allow the use of the 3rd train of the FPCS and they are not susceptible to movement should a fire occur.

263 The analysis states that if maintenance is not being undertaken on either of the main FPCS trains or on their associated support systems, it would be acceptable to shut down the 3rd train. The analysis of the PCC-3 event confirmed that there were no requirements arising from the assessment undertaken.

PCC-3 Event - Small break LOCA in State A or B initiated by a fire in the SAB

264 The plant configuration at the time of the fire is such that a single Chemical and Volume Control System (CVCS) pump is operational, powered by Division 1 and performing a reactor coolant pump seal injection function. In addition, the Division 1 Component Cooling Water System (CCWS) pump is operational and the Division 2 CCWS pump is not available due to maintenance.

265 This event considers the potential for a fire occurring in Switchgear Room, [redacted], located on the 8.1 metre level within the Division 1 SAB. The fire is postulated to result in loss of the 10kV AC emergency supply distribution system which consequently results in loss of the following plant and equipment:

- Division 1 CVCS Pump
- Division 1 CCWS Pump
- Electrical building HVAC system (DVL) for Division 1 as the fans contained within Division 2 are fed from the 10kV AC emergency supply distribution system board contained within Division 1.

266 The analysis then postulates the functions that would be lost taking into consideration the plant configuration at the time of the fire. There is a clear logic applied to the sequence of plant and equipment that culminates in the loss of seal injection to all four RCPs due to unavailability of power supplies in Division 2 the normal/emergency switchover will not be effective. In addition two Reactor Coolant Pumps would cease to operate (Division 1 and Division 2) due to loss of cooling for the motors, bearings, thrust bearings and thermal barriers. In order to ensure that loss of seal injection to all RCPs is prevented, the analysis recommends the following:

- *"During maintenance on a CCWS Division 1 or 2 train (or 3 or 4), the Division 4 (or 1) CVCS charging pump must be started as a precaution."*

267 From the deep slice sample into these particular PCC-2 and PCC-3 events, I am satisfied that a thorough and robust analysis has been undertaken for PCC events within the SAB and the Fuel Building. In addition, I believe that a modification to the operation of the CCWS and CVCS system during maintenance states constitutes a proactive approach to the mitigation of the unlikely event in which seal injection to all RCPs is lost due to a single fire that results in loss of the 10kV emergency supplies. As was the case for the Reactor Building, I have reservations associated with how the requirements identified within the SAB analysis are brought forward into the PCSR given that the reports do not form part of the auditable trail of the PCSR and furthermore, how such requirements are captured as part of the construction and operational phase. This has been captured within the same Assessment Finding as part of the overall approach to capturing requirements from these analyses **(AF-UKEPR-IH-02)**.

268 Criterion (e) considers the requirement to assume an aggravating factor, i.e. a redundancy requirement at the function level. In the case of the SAB the single aggravating factor is associated with loss of a FPCS pump power switchboard. The only safety function that is required in this situation would be start up of a cooling train together with any supporting systems. Should the fire occur in a fire zone where the failed switchboard is located, it would not further degrade the start-up of the other main train or the 3rd FPCS train as they are powered and controlled by another division.

269 For the Fuel Building, there are F1B functions which have been subject to analysis within reference 33 in terms of the application of potential aggravating factors, however, all the equipment that has the potential to cause a PCC condition and the respective equipment used to manage the PCC event in question is not contained within the same fire zone.

270 In the case of the Reactor Building there are a number of F1B functions used from the controlled state to the safe shutdown state performed by equipment contained within the Reactor Building. In all bar one case, criterion (e) is applied to the diesel generators as they are associated with Loss of Offsite Power (LOOP) and therefore the requirements of criterion (a) are bounding and criterion (e) would not set any further requirements. The single case where criterion (e) is applied is associated with the transfer line between Steam Generators. This has been analysed and the report concludes that in the event of Steam Generator tube rupture without LOOP and with the application of the single failure to a Main Steam Relief Train (MSRT) stuck in the open position, the position is acceptable as the MSRT and SGBS (Steam Generator Blowdown System) valves are not in the same fire area.

271 I am satisfied that the analysis undertaken in relation to potential aggravating factors has been comprehensive in the case of the SAB and the Fuel Building, and believe that it is mostly demonstrated through the application of criterion a, b and d. In the case of the Reactor Building, the Assessment Finding that is to be raised will address the need to provide further evidence to demonstrate the requirements within criterion (a) and thus criterion (e) have been met.

272 As mentioned earlier, RRC events are very infrequent ($<10^{-6}$/year) and as a result, the combination of an RRC event with an independent fire is assumed to occur only during the post-accident phase and no earlier than two weeks after the event. Criterion (f) considers the need to verify that, for RRC-A and RRC-B events, a fire does not prevent maintaining the final condition greater than 2 weeks after the event.

273 The analysis undertaken on the combination of fire and RRC-A sequences specifies all such sequences and defines the requisite corresponding functions to be undertaken immediately as well as the final state after two weeks. It is at this time an independent fire is assumed to occur. The report identifies one particular case associated with common mode failure of the emergency diesels and the need to segregate the boards associated with this system (LH boards) from the boards associated with the Station Black-Out (SBO) diesels (LJ boards) within SAB 1 and 4. The basis for requiring the boards to be in separate fire zones within each of the buildings in question arises from analysis undertaken as part of the independence demonstration for the LH and LJ switchboards under the Probabilistic Safety Analysis (PSA), which stated, *"In Divisions 1 and 4, the LH and LJ switchboards and the I&C must be located in different fire safety zones."*

274 I recognise that this measure is not a requirement of the deterministic safety case; it is associated with further risk reduction and is a proactive ALARP approach identified through the detailed analysis of the different RRC-A sequences undertaken for EPR. I am satisfied with the approach taken for the analysis of RRC-A sequences as assessed through the application of criterion (e).

275 The analysis undertaken on the combination of fire and RRC-B sequences details the functions required for a severe accident beyond two weeks. The analysis does not identify any further fire zoning requirements in the event of a severe accident due to the already segregated nature of the SAB ensuring that a single fire would not spread to

effect more than one division. In addition, there are no requirements for segregation of instrumentation relating to severe accidents.

276 I am content with the analysis undertaken as part of the analysis of RRC-B severe accidents, as the existing segregation provisions minimise the potential for fire to result in loss of more than one division.

Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

277 The ND Technical Assessment Guide, T/AST/014, on internal hazards states:

*"In order that items important to safety will have the level of reliability required to meet the safety goals, the licensee must consider the possibility of single random failures, common cause failures, simultaneous and consequential events and unavailability of SSCs due to maintenance activities. Common causes include both SSC failures and effects of internal hazards such as fire. The appropriate level of reliability of essential safety functions may be achieved by incorporating redundancy within single trains and/or segregation and diversity between trains."*

278 The SAPs, state within EHA.5 and EHA.6:

| **Engineering principles: external and internal hazards** | **Operating conditions** | **EHA.5** |
|---|---|---|
| Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition. | | |

| **Engineering principles: external and internal hazards** | **Analysis** | **EHA.6** |
|---|---|---|
| Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects. | | |

279 In addition, SAP FA.6 states:

| **Fault analysis: design basis analysis** | **Fault sequences** | **FA.6** |
|---|---|---|
| For each initiating fault in the design basis, the relevant design basis fault sequences should be identified. | | |

*"Each design basis fault sequence should include as appropriate:*

*a) failures consequential upon the initiating fault, and failures expected to occur in combination with that initiating fault arising from a common cause;*

*b) single failures in the safety measures in accordance with the single failure criterion;*

*c) the worst normally permitted configuration of equipment outages for maintenance, test or repair;*

*d) the most onerous permitted operating state within the inherent capacity of the facility;"*

280 The approach to segregation is consistent with the IAEA guidance document, NS.G.1.7, which states within the section entitled, *"General Concepts"*:

*"Structures, systems and components important to safety are required to be designed and located, consistent with other safety requirements, so as to minimize the likelihood and effects of internal fires and explosions caused by external or internal events. The*

*capability for shutdown, removal of residual heat, confinement of radioactive material and monitoring of the state of the plant is required to be maintained. These requirements should be met by the suitable incorporation of redundant parts, diverse systems, physical separation and design for fail-safe operation…"*

281 Complimenting the statements made within ND and IAEA guidance, Western European Nuclear Regulators' Association (WENRA) Reference Level S: Protection against internal fires, states within its basic design principles:

- *SSCs important to safety shall be designed and located so as to minimize the frequency and the effects of fire and to maintain capability for shutdown, residual heat removal, confinement of radioactive material and monitoring of plant state during and after a fire event.*
- *Buildings that contain equipment that is important to safety shall be designed as fire resistant, subdivided into compartments that segregate such items from fire loads and segregate redundant safety systems from each other. When a fire compartment approach is not practicable, fire cells shall be used, providing a balance between passive and active means, as justified by fire hazard analysis.*

282 The guidance also recommends:

- *A fire hazard analysis shall be carried out and kept updated to demonstrate that the fire safety objectives are met, that the fire design principles are satisfied, that the fire protection measures are appropriately designed and that any necessary administrative provisions are properly identified.*
- *The fire hazard analysis shall be developed on a deterministic basis, covering at least:*
  - *i) For all normal operating and shutdown states, a single fire and consequential spread, anywhere that there is fixed or transient combustible material;*
  - *ii) Consideration of credible combination of fire and other PIEs likely to occur independently of a fire.*

283 In addition, existing UK nuclear power generation facilities apply a similar approach to ensuring that there is adequate redundancy and segregation in place to ensure that the design basis stated above is met.

284 The approach taken for the analysis undertaken for UK EPR is broadly in line with that observed within ND guidance and relevant good practice within the UK and internationally.

#### 4.4.2.3 Assessment Conclusions

285 The approach of the PCSR in ensuring that the criterion associated with common mode failure due to fire are in line with my expectations in that the principles applied seem reasonable and it is believed that methodology taken is synonymous of a positive and proactive approach to ensuring the risk associated with fire is ALARP.

286 The outstanding cable routing verification and validation reports are a key source of supporting evidence to the claims and arguments presented as part of the analyses presented within the safety requirements reports for fire zoning. As a result, a GDA Issue has been raised to ensure that the requisite evidence contained within the verification and validation reports is provided.

287 The GDA Issue, *"Outstanding internal hazards substantiation for internal flooding, cable routing, high energy line break and missiles forms part of the requisite evidence and will be required in order to demonstrate an adequate internal hazards safety case."* includes the following GDA Issue Action:

| | | | |
|---|---|---|---|
| **Technical Area** | **INTERNAL HAZARDS** | | |
| **Related Technical Areas** | Structural Integrity<br>Civil Engineering<br>Fault Studies<br>PSA | | |
| **GDA Issue Reference** | **GI-UKEPR-IH-02** | **GDA Issue Action Reference** | **GI-UKEPR-IH-02.A2** |
| **GDA Issue Action** | Provide the requisite evidence in the form of the detailed Flamanville 3 verification and validation analysis and/or other supporting documentation in support of the claims and arguments presented within Chapter 13.2 of the PCSR associated with the routing of electrical cables within the EPR design in order to prevent a single fire resulting in loss of more than one divisional separation group.<br>The response should include analysis that supports the claims and arguments relating to:<br>• The routing and identification of protected cable trays.<br>• Justification of claims and arguments made relating to geographical separation.<br>• The provision of passive protection applied to cables and cable trays specifically.<br>• Any further defence in depth and ALARP measures that could be implemented into the design.<br>• Any identified design changes and their implementation within the PCSR.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my expectations.<br>With agreement from the Regulator this action may be completed by alternative means. | | |

288 In addition, I have reservations associated with how the requirements identified within these analyses are brought forward into the PCSR given that the reports do not form part of the auditable trail of the PCSR and furthermore, how such requirements are captured as part of the construction and operational phase. As this concern is associated with adequately capturing safety case requirements and does not directly impact on nuclear related construction, the concern is to be identified as an Assessment Finding requiring any internal hazards requirements identified outside of the auditable trail but which have an impact on the safety to be captured appropriately:

- ***AF-UKEPR-IH-02*** *– The Licensee shall provide evidence to demonstrate how the requirements from analyses associated with common mode failure in the event of fire are captured within future revisions of the safety case given the impact changes may have on the overall safety case.*

289 This Assessment Finding should be addressed as part of the following procurement and construction generic milestones for Assessment Findings:

- Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.

### 4.4.3 Passive Cable Protection

290 The Step 3 Internal Hazards Assessment identified the need to assess the cable segregation and protection as part of the assessment during Step 4. This has been partly addressed as part of the fire common mode analysis as part of criteria (a) to (c) detailed within section 4.4.2 of this report, however, consideration also needs to be applied to the provision of passive cable protection in the form of wrapping, coatings, enclosures etc., which is the focus of this section of the assessment.

#### 4.4.3.1 Scope of Assessment Carried Out

291 As part of philosophy applied within the UK EPR design there is a need for local passive protection to be applied to cabling to ensure that no single fire can result in loss of more than one division. The assessment examines the approach taken to cable routing within the UK EPR design and serves to identify the extent and adequacy of the proposed design in relation to the application of this method of passive fire protection.

292 As a means to provide confidence in the approach taken for cable protection within the UK EPR design, assessment has been undertaken on some of the design and installation requirements provided in response to following TQs:

- TQ-EPR-762 Technical Reference – Cable Fire Protection Specification (Ref. 14)
- TQ-EPR-763 Test information relating to venting of fire protected cable tray enclosures (Ref. 14).

293 The methodology and approach taken for the application of cable protection and wrapping is derived from technical references, *"Fire Resistant Cable Wraps and Cases in Thermal and Nuclear Power Plants"*, CRT 62-C-010-01 (Ref. 36), and *"Test specification for electrical cableway protection systems"*, ENGSIN040526 (Ref. 37), both of which have been considered as part of this assessment.

#### 4.4.3.2 Assessment

294 Reference 36 presents the technical rules associated with the application of cable wrapping to electrical cables and fire cases for electro-mechanical equipment, including, electrical cables, electrical boxes, sensors etc. The report defines cable wraps as, *"a heat-insulating sheath consisting of an assembly of flexible or rigid materials which have recognised intrinsic fire resistant characteristics, inside which cable raceways are arranged."* and defines fire cases as *"a set of heat-insulating walls forming a closed volume on a civil works structure consisting of an assembly of rigid materials which have recognised intrinsic fire resistance characteristics, inside which the protected equipment items are arranged."*. These definitions are in line with current UK practice for the protection of cable trays through either the use of cable wrappings or coatings and through the use of fire resistant enclosures.

295 The technical rules stipulate requirements for the cable wraps and enclosures in terms of their ability to withstand:

- fire for a predetermined period of time and maintain operability.
- water from automatic suppression systems or containment sprays.

296 There are also criteria for when cable wraps can be used e.g. for high and medium voltage cables, when wrapping is not a permitted method of providing protection and for low voltage cables there is a need to perform further analysis to determine whether cable wrapping would be an effective method of cable protection. In addition, there are further requirements associated with design, construction, installation, and verification of the cable protection installed.

297 Further assessment of the basis of the fire testing was sampled including the specific test methods and criteria adopted for the passive cable protection systems to be adopted on UK EPR to determine their adequacy.

298 Reference 37 details the requirements for fire qualification requirements for cable raceways and specifies the test conditions, specific cable tray configurations, and the qualification criteria. Any cable wrapping system or cable enclosure has to be tested in accordance with NF EN 1363 – 1 (Ref. 38) which is the French equivalent to BS EN 1363 – 1, *"Fire Resistance Tests – Part 1: General Requirements"* (Ref. 39). In addition, ETC-F states that the type of cables used throughout the UK EPR design are tested to BS EN 60332 – 3 - 23, *"Tests on Electric and optical fibre cables under fire conditions. Test for vertical flame spread of vertically mounted bunched wires or cables – Category B."* (Ref. 40) to determine their performance in fire. The test requires that within a 40 minute period the vertical flame development should not exceed 2.5 metres from the base of the burner. Although this test does not require the cables to be fire resistant, they serve to significantly reduce the potential for a large fire involving bunched cables due to their fire retardant nature and limited flame propagation characteristics.

Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

299 In addition to the European Standards discussed above, the SAPs identify the need to consider the effects of water on SSCs important to safety and the need to use non-combustible or fire retardant materials in the facility. NS-G-1.7 (Ref. 10) also identifies similar provisions for ensuring the reducing the impact from cable fires.

300 SAPs EHA.15 states:

| **Engineering principles: external and internal hazards** | **Fire, explosion, missiles, toxic gases etc – effect of water** | **EHA.15** |
|---|---|---|
| The design of the facility should prevent water from adversely affecting structures, systems and components important to safety. | | |

*"The design of the facility should include adequate provision for the collection and discharge of water reaching the site from any design basis external event or internal flooding hazard or, if this is not achievable, the structures, systems and components important to safety should be adequately protected against the effects of water."*

301 Furthermore, EHA.17 states:

| **Engineering principles: external and internal hazards** | **Fire, explosion, missiles, toxic gases etc – use of materials** | **EHA.17** |
|---|---|---|
| Non-combustible or fire-retardant and heat-resistant materials should be used throughout the facility. | | |

302 NS-G-1.7 states within Appendix IV, "*The impact of electrical cable fires on items important to safety should be determined in the fire hazard analysis*.

*IV.2. Various design approaches have been taken to limit the significant impact of cable fires. Among these approaches are: protecting electrical circuits against overload and short circuit conditions; limiting the total inventory of combustible material in cable installations; reducing the relative combustibility of cable insulation; providing fire protection to limit fire propagation; and providing separation between cables from redundant divisions of safety systems, and between power supply cables and control cables."*

303 The approach taken for passive cable protection for UK EPR is broadly in line with that observed within ND guidance and relevant good practice within the UK and internationally.

#### 4.4.3.3 Assessment Conclusion

304 The provisions in place are in line with my expectations for ensuring that the passive cable protection does not degrade and result in the spread of fire and ensuring that the cables continue to perform their required safety function under the same fire test conditions. Furthermore, the test criteria stated for the testing of cables is consistent with the approach that I would expect for type of cable used within the UK EPR design.

305 No GDA Issues or Assessment Findings have been identified within the area of passive fire protection and specification of the types of cables used within the UK EPR design.

### 4.4.4 DFL HVAC Smoke Control and Extract System

306 During the Step 4 assessment, a series of concrete ducts installed at a number of levels within the Safeguards and Fuel Buildings were identified. The ducts were associated with smoke extraction and control and appeared to pass through a number of nuclear significant hazard barriers unprotected by fire dampers. As a result TQ-EPR-766 (Ref. 14) was raised requesting substantiation of the ducts where they penetrated such barriers.

#### 4.4.4.1 Scope of Assessment Carried Out

307 The assessment focussed on the response to the TQ relating to the unprotected penetrations and determines whether such a system, installed for life safety and fire fighting purposes, is in line with the requirements set out within the PCSR for the provision of adequate segregation of divisional trains of protection for nuclear safety.

#### 4.4.4.2 Assessment

308 The response to the TQ detailed that the DFL system has two functions:

- smoke extraction system; and
- life safety provision, through the over-pressurisation of staircases and corridors.

309 The smoke extraction system is a manually operated system that is utilised by the fire authorities to remove smoke once fire has been extinguished. The system is installed in a number of rooms within the SAB, however, it is configured with fire dampers that are

closed during normal operations and only opened when required to fulfil this function. As the fire dampers are in the closed position they are not provided with redundant dampers in series as the system is a passive system and the fail safe state during normal operation is met. As a result the application of single failure protection is not applicable as the dampers are in a fail safe position. In addition, the rooms to which the extract system serve are contained within the individual divisions of the SAB and are not linked, therefore, should a damper spuriously open, the bounding claim that there would be no loss of more than one division is met. I am content with this aspect of the smoke extraction system for individual rooms within the SAB.

310 In the case of pressurisation of the escape routes for life safety, the dampers on the system are normally closed and only open in the event of fire. There are ducts that contain maintenance hatches that cross nuclear significant hazard barriers between the individual divisions of the SAB and the Fuel Building. There is, therefore, the potential for fire within one division spreading to affect others should the hatches either not be adequately protected or be used as part of the pressurisation of the escape route. The TQ response stated that all hatches would be sealed to the equivalent rating of the appropriate nuclear significant hazard barrier i.e. a two hour fire rating, with the exception of the following hatches:

- Hatches required for the installation of the DFL fire dampers, and
- Hatches required providing access to the top gap sealing.

311 These hatches will be provided with fire dampers and removable fire resistant lids meeting the 2 hour fire resistance requirements. During normal operation the dampers and associated lids will be closed, therefore, the need to apply the single failure criterion to the active components is not required due to the passive nature of the barrier. As a result the ducts are not penetrating unprotected through the nuclear significant barriers. I am satisfied that the integrity of the ducts is ensured such that a fire within one division will not spread to affect an adjacent division and the requirements of the safety case in ensuring that no single fire can result in loss of more than one division are met.

Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

312 The SAPs state within SAP EDR.2 and SAP EDR.4:

| **Engineering principles: design for reliability** | **Redundancy, diversity and segregation** | **EDR.2** |
|---|---|---|
| Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety. | | |

| **Engineering principles: design for reliability** | **Single failure criterion** | **EDR.4** |
|---|---|---|
| During any normally permissible state of plant availability no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function. | | |

313 In addition SAP EHA.6 states:

| **Engineering principles: external and internal hazards** | **Analysis** | **EHA.6** |
|---|---|---|

| |
|---|
| Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects. |

314 Paragraph 3.2 of NS-G-1.7 states:

"*Early in the design phase, the plant buildings should be subdivided into fire compartments and fire cells. The purpose is to segregate items important to safety from high fire loads and to segregate redundant safety systems from each other. The aim of segregation is to reduce the risk of fires spreading, to minimize secondary effects (Section 6) and to prevent common cause failures."*

315 The approach taken for passive cable protection for UK EPR is broadly in line with that observed within ND guidance and relevant good practice within the UK and internationally.

#### 4.4.4.3 Assessment Conclusions

316 I am satisfied with the approach taken to the design of the DFL system for both smoke extraction and pressurisation of escape routes.

317 No GDA Issues or Assessment Findings associated with this aspect of the assessment are required.

### 4.4.5 Fire Assessment of Reactor Coolant Pumps

318 During Step 3 TQ-EPR-217 (Ref. 14) was raised seeking information relating to a fire induced LOCA arising from fire threatening reactor coolant pump (RCP) seals. The response to the TQ provided analyses of the potential fire threat including details of fire modelling work that had been undertaken within this area. The initial assessment resulted in the issue of a further TQ (TQ-EPR-534) (Ref. 14) seeking clarification of the volumes of oil considered to be involved in a potential fire involving the RCPs. The response to the second TQ was provided during Step 4 which enabled the assessment to be undertaken and captured within this report.

#### 4.4.5.1 Scope of Assessment Carried Out

319 The scope of the assessment of the RCPs has focussed on the potential for a single fire resulting in a LOCA due to fire affecting the RCP seals. In addition, assessment was undertaken on the potential for a single fire to result in loss of more than one RCP.

#### 4.4.5.2 Assessment

320 The response to the original TQ (TQ-EPR-217) (Ref. 14) detailed a number of measures to ensure that a fire involving an RCP does not:

- Propagate to other divisions,
- Compromise the pressure retaining functions of the RCP,
- Prevent the fulfilment of F1 functions to ensure that the plant can be brought to a safe shutdown state.

321 One measure that the design of the UK EPR takes into consideration is the reduction in the potential quantity of oil that could be released onto the floor of the containment through the use of detection systems that provide early warning of any potential leak and oil catchment devices within the body of the RCP that retain oil from spillages due to leaks at mechanical joints. The maximum potential amount of oil that could be leaked onto the floor was stated to be [redacted]. This figure was derived from the maximum amount of oil that could be released into the lower bearing recovery pot which totalled [redacted]. The capacity of the lower bearing recovery pot is [redacted], hence the potential for leakage of [redacted] onto the floor. However, there are parts of the RCP which contain significantly greater quantities of oil, namely the oil cooler and the upper bearing, however, the oil collection devices for these two systems are capable of retaining the full quantity of oil released.

322 Further defence in depth measures are in place to minimise the potential consequences of oil leaks from the lubricating oil systems for the RCPs, which include:

- Monitoring devices. Lube oil level switches, motor bearing temperature measurement, and vibration monitoring systems alarm to the Main Control Room (MCR) which results in the RCP being manually switched off and the source of the alarm investigated.
- Floor drainage. In addition to the oil collection devices and monitoring devices, floor drainage systems are provided that direct the lube oil away from the RCP and can hold almost the entire contents of the RCPs, therefore, preventing relatively large spills beneath the RCP.
- Fire Suppression Systems. Each RCP is provided with a fire suppression system to extinguish/control any potential fire involving the RCP. As this measure is identified as a level of defence in depth, fire modelling was undertaken to demonstrate that no nuclear safety claim was required for the system.

323 In addition the TQ provided details of an analysis that had been undertaken using a fire modelling programme, Fire Dynamics Simulator (FDS). The purpose of the simulation was to provide temperature and duration profiles of an RCP oil fire in order to support the fire hazard analysis to determine that a postulated fire did not rely on the fire suppression system to extinguish/control the fire in anyway. The assumptions and input data for the fire modelling undertaken were:

- The oil inventory involved in the fire assumes [redacted] made up of the [redacted] that spills on to the floor plus the [redacted] contained within the lower bearing.
- The effects of floor drainage are not considered within the simulation.
- The high flash point ($220^{o}C$) lubricating oil flows out, adheres on to the casing of the reactor coolant pump and spreads on to the floor area.
- An ignition probability of 1 is assumed as is rapid fire growth.
- The Heat Release Rate (HRR) per unit area of the lubricating oil is conservatively taken as $1.8MW/m^2$ when normal values for this type of lubricating oil are generally around $1.1MW/m^2$.
- The maximum HRR for the casing and floor spillage are [redacted] respectively.

- There is linear fire growth up to 60 seconds at which point the fire has reached a maximum HRR of [redacted].

324 Under the above conditions, burn out of the fire occurs in approximately [redacted] and although the analysis identifies high air temperatures in the area of the affected RCP, the resulting temperatures observed outside the area of the RCPs adjacent to the Steam Generators was of the order of [redacted]. In addition, the fire simulation showed that surface temperatures of safety related compartments in adjacent loops were lower than the design temperatures of the equipment, namely a LOCA which assumes temperatures of [redacted].

325 The analysis following the fire simulation undertaken using FDS concludes:

*"The predicted temperature levels do not cause any harm to any of the Reactor Coolant System (RCS) components, therefore the integrity of the RCS is maintained. The fire hazard functional analysis supported by the results of the fire simulation demonstrates that the cooling of the shaft sealing system of the RCP in case of the oil fire is ensured and integrity of the seals is not challenged. In addition, due to the limited severity of the fire and the limited spatial area affected, the fire does not prevent the operation of systems which are necessary to transfer the plant to safe shutdown."*

326 I believe that a thorough and conservative analysis has been undertaken associated for a fire involving the total oil inventory from the bottom bearing of the RCP, however, I sought further confidence in the approach taken to the basis of selection of the oil source, given that there were other oil collection devices that held far greater quantities of oil. Therefore I raised a further TQ (TQ-EPR-534) (Ref. 14) which requested further technical information relating to the justification of the claims made on the oil retention devices preventing the release of greater quantities of oil.

327 The response to the second TQ detailed the design provisions associated with the oil retention devices for the oil cooler and the upper bearing as the previous response and the fire simulation work had assumed loss of the entire contents of the lower bearing. [redacted] and, in addition, there is a high pressure lube oil lift system which is operated during start-up and shut-down. Each of these systems (tanks and pipework) are seismically qualified SC1 and designed to remain operational in the event of a Design Basis Earthquake. The response argues that due to the robust construction of the systems the simultaneous rupture of more than one lube oil system is eliminated.

328 The oil collection device for the upper bearing has a capacity of [redacted] and has been sized based upon the maximum oil leak from the upper bearing and cooling circuit which in a worst case scenario is [redacted]. This quantity of oil is associated with pipe rupture on the oil lift system high pressure side assuming the oil lift motor continues to operate until the oil level drops below the suction pipe.

329 I am satisfied that the oil retention devices have sufficient capacity to contain the worst credible oil leak and that the measures in place to prevent and minimise the impact of oil leakage are thorough and robust.

Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

330 The SAP EHA.14 states:

| | | |
|---|---|---|
| **Engineering principles: external and internal hazards** | **Fire, explosion, missiles, toxic gases etc – sources of harm** | **EHA.14** |

| |
|---|
| Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed. |

331 The ND Technical Assessment Guide, T/AST/014, on internal hazards states:

*"All reasonably practicable means commensurate with good engineering practice should be adopted in the design and layout of the plant, and through the use of fire detection and suppression equipment of appropriate capacity and capability, to reduce the likelihood of fires and mitigate against the consequences of fires."*

332 T/AST/014 states it is necessary that:

- bunds, drip trays and flange shields etc, should be provided to control and contain any leakage of combustible or flammable liquids as well as any potential fire initiators; and
- multiple trains of systems and components required to perform essential functions should be suitably segregated either by the fire containment approach (i.e. fire barriers) or the fire influence approach (i.e. combination of distance and fire detection and suppression systems etc).

333 NS-G-1.7 states within paragraph 2.22:

*"A postulated initiating event should not lead to a fire with consequences for safety systems. Possible causes of fires, such as severe seismic events or the disintegration of a turbine, should be addressed in the fire hazard analysis, and special design provisions (e.g. use of cable wraps, detection systems and suppression systems) should be made as necessary. In the fire hazard analysis, special attention should be paid to hot equipment and/or to the potential failure of circuits conveying flammable liquids and gases."*

334 The approach taken for design and analysis of the potential consequences of a RCP fire for UK EPR is in line with that observed within ND guidance and relevant good practice within the UK and internationally.

#### 4.4.5.3 Assessment Conclusions

335 I am satisfied that the oil catchment capacity of the upper bearing and the oil cooler are sufficient to retain the worst case oil leaks from the RCP without operator intervention. Total leakage from the bottom bearing has been demonstrated, using fire simulation, to give rise to a fire which, in the most pessimistic regime, will not exceed the design temperatures required to retain the integrity of the reactor cooling system without placing a nuclear safety claim on the installed fire suppression system. This system therefore, fulfils a defence in depth role.

336 No GDA Issues or Assessment Findings associated with this aspect of the assessment are required.

### 4.4.6 Effluent Treatment Building

337 The Step 3 Internal Hazards Assessment Report identified the need to undertake assessment of internal fires within the Effluent Treatment Building. Given that there are no systems within the Effluent Treatment Building that are classified greater than F2, there are no significant nuclear safety claims made on SSCs contained therein and no requirements for redundancy and segregation. Fire within the Effluent Treatment Building

is of more relevance to conventional fire safety and means of escape provision. Therefore, no further assessment of internal fire within the Effluent Treatment Building is considered necessary as part of the GDA process.

### 4.4.7 Fire Fighting Pumphouse

338 The Step 3 Internal Hazards Assessment Report identified the need to undertake assessment of internal fires within the Fire Fighting Pumphouse. Given there are no nuclear safety significant consequences of loss of the fire fighting pumphouse as the fire fighting pumps have no role in preventing fire spread to affect more than one division (due to the demonstration supplied within RO-UKEPR-030 relating to total burnout of fire compartments) and have no further nuclear safety claims made upon them for controlling or extinguishing fires, I am satisfied that no further assessment of the Fire Fighting Pumphouse is required.

### 4.4.8 Non-Classified Buildings

339 This area was specifically identified within the Step 3 Assessment Report to determine whether a fire within a non-classified building could spread to safety classified buildings such that nuclear safety as a result of the fire could be threatened. The 2 hour fire resistance rating of the external barriers of the safety classified buildings is such that potential fires within an adjacent connecting non-classified building would not be sufficient to result in the fire compartment to the safety classified building to be exceeded. I am satisfied that no further assessment is required of the potential for fire spread from non-classified Buildings to safety classified buildings.

## 4.5 Fuel Building Internal Hazards Assessment

340 No assessment of the Fuel Building with regard to internal hazards was undertaken as part of the Step 3 Internal Hazards Assessment. The need to undertake assessment of this building was identified as a task that was required to be undertaken as part of Step 4 both within the Step 3 Assessment Report and the Step 4 Assessment Plan for internal hazards.

### 4.5.1 Scope of Assessment Carried Out

341 The internal hazards assessment of the Fuel Building included assessment already undertaken as part of the section on internal fire, specifically associated with claims made on F1B Functions of the JPI System and Common Mode Failure Analysis and Segregation detailed within Sections 4.4.1 and 4.4.2 respectively. In addition, further assessment of the Fuel Building during Step 4 involved assessment of the Extra Borating System (EBS).

342 The EBS was selected for assessment from the PCSR as it provides an F1B safety function. It penetrates containment and has been identified by EDF and AREVA within Chapter 13.2 of the PCSR as requiring protection from internal hazards.

### 4.5.2 Assessment

343 The EBS is required to provide borated water into the primary coolant following a reactor trip in order to compensate for reactivity insertion due to the cool down following

shutdown. An assessment of the system has been carried out with regard to faults due to internal hazards occurring in either of the trains which make up the system, the system pipework and the electrical supplies to the feed pumps.

344 The EBS comprises of two separate trains, each located in its own half of the Fuel Building which is separated by the central dividing barrier up to the 0.0m level. Each train comprises of a tank supplying a pump, a discharge header and motorised isolation valves on the pump discharge. The [redacted] boric acid supply tanks are interconnected through normally closed valves in order that in the event of a failure of one train, the other train can be cross connected to empty the contents of the affected tank. The EBS pumps are capable of being supplied from each of the emergency diesel generators via cross connections between the diesel generator switchboards.

345 In the event of a single internal hazard affecting either the EBS or the electrical supplies powering the system, the second train is used to supply the primary reactor coolant with borated water. For this reason, no maintenance is permitted on the EBS during operation. Periodic testing is carried out by starting the pumps against a closed injection line to circulate the fluid through the system back to the storage tanks to prove against blockage and to ensure mixing of the contents of the tank.

346 The electrical supplies for each EBS train are fed from Divisions 1 and 4 backed up by the emergency diesels. The cables from the diesels to the switchboards and the cross connections between the switchboards are adequately separated to provide protection against common cause faults. The cable routes from the switchboards to the EBS pumps and valves have not been assessed as their layouts are not yet available as the internal hazards substantiation of the cable routes is yet to be undertaken (see Section 4.4.2. associated with GDA Issue Action GI-UKEPR-IH-02.A2).

347 In the event of a flood in the fuel building, each train of the EBS is located in its segregated division protected by a claimed flood barrier capable of withstanding a 10 metre water height which extends to the 0.0 metre level (TQ-EPR-679 refers) (Ref. 14). As a result, only one train of the EBS will be affected in the event of a flood either from a failure of the EBS or another failure within the fuel building that would result in flooding. In addition, any failure of the EBS would not lead to any significant flooding due to the small size of the tanks and the low design flow of the pumps. In the event of a fire the EBS is also fully segregated by a 2 hour barrier between each train. The potential for missile impact and the potential claims made on the segregation barriers will form part of the substantiation provided as part of the provision of the requisite evidence, if the barriers do need to be claimed for this purpose.

Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

348 The SAPs, state within EHA.6:

| **Engineering principles: external and internal hazards** | **Analysis** | **EHA.6** |
|---|---|---|
| Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects. | | |

349 The consideration of internal flooding associated with loss of redundancy for the EBS is captured within SAPs EHA.15, which states:

| **Engineering principles: external and internal hazards** | **Fire, explosion, missiles, toxic gases etc – effect of water** | **EHA.15** |
|---|---|---|

| |
|---|
| The design of the facility should prevent water from adversely affecting structures, systems and components important to safety. |

*"The design of the facility should include adequate provision for the collection and discharge of water reaching the site from any design basis external event or internal flooding hazard or, if this is not achievable, the structures, systems and components important to safety should be adequately protected against the effects of water."*

350 NS-G-1.11 states within paragraph 2.41:

*"Physical separation should be provided between redundant items of safety equipment (including power supplies, instrumentation cables and any related systems) on the basis that the multiple components should be independent and their separation will help to eliminate some situations in which common external factors could result in multiple failures."*

### 4.5.3 Assessment Conclusions

351 From the assessment undertaken of the EBS, I am satisfied that the system has been adequately designed against the potential effects of internal hazards. The cable routing associated with the EBS has not been subject to assessment during Step 4 as the detailed routing information is not yet identified, however, this has been identified within the GDA Issue detailed within Section 4.4.2.

352 No GDA Issues or Assessment Findings associated with this aspect of the assessment are required.

## 4.6 Steam Release

353 The specific area of steam release was not considered within the sampling assessment undertaken during Step 3 of the GDA. The area of steam release is generally included by EDF and AREVA through the detailed HELB studies undertaken, however, I was interested in the consequences of steam and the claims made on SSCs, specifically, doors, penetrations and barriers. Therefore, during Step 4 TQ-EPR-966 (Ref. 14) was raised seeking further details of all doors, penetrations and barriers claimed within the internal hazards safety case against the effects of steam.

### 4.6.1 Scope of Assessment Carried Out

354 The assessment focussed on the response to TQ-EPR-966 (Ref. 14) and the referenced document, *"High Energy Pipe Break: Propagation of degraded ambient conditions in the Nuclear Island"*, EZLT/2010/en/0007 (Ref. 41).

### 4.6.2 Assessment

355 The response to the TQ details the specific areas in which the formation of harsh ambient conditions due to a steam release could occur:

- Steam Generator Blowdown System in HLA3403ZL,
- Main Feed Water System in HLA/D2630ZL and HLA/D3129ZL,

- Safety Injection and Residual Heat Removal System in HLA & HLD SIS/RHR compartments,
- Main Steam System in HLA & HLD MSSS compartments.

356 Reference 41 provides further information regarding the methodology applied to the assessment of steam release. In particular the identification of those High Energy systems which would result, in the event of failure, in the formation of a degraded ambient condition as a result of steam release. The approach taken is to ensure that divisional separation or the containment function of the building is not compromised.

357 The report defines a high energy system as one that operates at temperatures and pressures greater than or equal to 100$^{o}$C and 20 bar respectively. In addition, there is no consideration of leaks and breaks in pipework that are less than or equal to 50mm in diameter. The basis for this assumption is due to the low energy potential in relation to the global effects of failure. Therefore, any pipe greater than 50mm in diameter with temperatures and pressures stated previously is taken into consideration in the analysis.

358 In addition, the report states that the Reactor Building has not been subject to analysis as any degraded conditions are contained and the nuclear significant SSCs contained therein are designed to withstand the effects of a degraded environment.

359 I believe that this approach to the failure of high energy systems resulting in degraded ambient conditions is a reasonable basis for the analysis.

360 The analysis then considers each of the systems identified above and states that the consequences of failure are acceptable given their locations within the Nuclear Island.

361 Parts of the Steam Generator Blowdown System are contained within the SAB and room HLA3403ZL is identified as a compartment that has the potential to be subject to a degraded ambient condition due to failure of the flash tank. The analysis considers the consequences of this failure which would result in a pressure build up which would ultimately lead to the door, HLL3407DO opening and allowing steam into the adjacent corridor, HLA3426ZL. The steam would then be vented to atmosphere through external doors. In this scenario, the steam release would not result in further propagation of the degraded conditions nor would it result in loss of more than one division or release of any radioactive substances as the release from the flash tank is from the secondary side coolant not the primary.

362 I am content with this approach to venting the potential steam release, however, there is a need for the doors to be designed such that should this event occur they would open under the pressure of the failure and not contain the release or result in a detrimental effect to aspects of the building structure. An Assessment Finding has been identified within this area to ensure that the doors are designed to allow for the steam release path to be realised in this event **(AF-UKEPR-IH-03)**.

363 The Main Feed Water System (MFWS) is located within MFWS compartments HLK/L/M/N2601ZL, HLK/L/M/N2603ZL, HLK/L/M/N2901ZL, HLK/L/M/N2903ZL, and within corridors HLA/D2603ZL and HLA/D3129ZL of the SAB. The system operates at ≈80 bar and a maximum temperature of 230$^{o}$C. The report postulates breaks within each of the compartments and provides detailed layouts indicating the location of the blow out panels that permit steam to be discharged either into the corridor areas (then outside to the environment) or immediately to the environment from the MFWS compartment directly without compromising the other MFWS compartments within the same divisional building i.e. a failure within a MFWS compartment associated with Division 1 should not compromise the MFWS within associated with Division 2 even though both trains are

contained within Division 1 SAB. Furthermore there is geographical separation of the steam lines for the other two trains (Divisions 3 and 4) within the Division 4 SAB. There is the potential for temperatures and pressures to increase within the Cable Raceways (HLK/N3403ZL) which contain redundant cabling associated with the MFWS, however, it is claimed that the cables within this area are rated to withstand temperatures of 300$^{o}$C and a pressure of 2 bar. The report concludes that a break in a main feed water system compartment cannot lead to either an inadmissible propagation of a degraded ambient condition nor does it compromise the divisional separation or containment of radioactive substances as the release of secondary side coolant to the environment is acceptable.

364 I am satisfied that the approach to providing protection of the redundant MFWS compartments is comprehensive and robust, however, given the need for the cables within the cable raceways (HLK/N3403ZL) to withstand temperatures of 300$^{o}$C and pressures of up to 2 bar, an Assessment Finding has been identified within this area to ensure that the specification for the cables to be installed meet this criterion and that the layout ensures that such criterion can be met **(AF-UKEPR-IH-04)**.

365 The Safety Injection and Residual Heat Removal Systems (SIS and RHR) are located at the -9.0m level within each Division of the SAB, however, the systems that are utilised as part of the high energy system are contained within SAB 1 and 4; these systems are required during cold shutdown states when the reactor state is C1 with temperatures ≥100$^{o}$C. The systems within SAB 2 and 3 are only used in normal operations when temperatures are <100$^{o}$C, hence there are no parts of the SIS and RHR that require to be analysed due to the temperatures and pressures not being sufficiently high for pipework to be qualified as high energy. In addition, the SIS is required to perform a water make-up function in the event of a LOCA, and the RHR is required in order to provide a residual heat removal function once a safe state has been reached. Again, these particular events are not analysed in detail as there would be a need for multiple independent faults to occur simultaneously.

366 In the case of a break in a high energy system at Reactor State C1, the design of the SAB SIS/RHR compartments within Divisions 1 and 4 include the provision of a number of vent and pressure relief paths for the removal of the high pressure and temperature steam. The provisions in place consider the need to relieve the pressure from the -9.0m level upwards through the building rather than out into the corridor, therefore, the doors to the compartments are pressure resistant and rated to withstand an overpressure of up to [redacted]. The vents and pressure relief panels are located within the ceiling of the compartment as well as within a dedicated triangular duct; the flow paths then direct the pressure and steam out of the building via bursting membranes located above ground. The analysis considers that the potential for propagation of degraded ambient conditions to another Safeguard Building or to the Fuel Building is prevented through these design provisions.

367 I am content with this approach to venting the potential steam release upwards through the building, however, there is a need for the pressure resistant doors to be designed such that should this event occur the doors would be able to withstand the requisite [redacted] in the event of a break in the SIS or RHR and not to prevent the release passing into the corridor rather than via the dedicated engineered route. An Assessment Finding has been identified within this area to ensure that the pressure resistant doors are designed to prevent the passage of steam out of the compartment and on to the -9.0m level and potentially undermine the divisional segregation via this route **(AF-UKEPR-IH-05)**.

368 The Main Steam Lines within SAB 1 and 4 are claimed within the PCSR as "high integrity" and hence their failure is not postulated, however, there are further pipes within the Main Steam Supply System (MSSS) that are not claimed as "high integrity" but are high energy pipes e.g. the heating lines and the blow down lines. The analysis considers failure of a heating line break as this failure is deemed to be the most conservative. As is the case for the MFWS, the steam lines are located within separate compartments, two per divisional Safeguard Building (Safeguard Building 1 contains Divisions 1 and 2, and Safeguard Building 4 contains Divisions 3 and 4). Again, as with the MFWS approach there are a number of burst openings installed as part of the design that are capable of relieving the pressure within the MSSS compartments into the corridor and then through further burst panels installed within the floor of the corridor to direct the steam release to the environment. The report concludes that a break of pipework that is not claimed as "high integrity" cannot lead to either an inadmissible propagation of a degraded ambient condition nor does it compromise the divisional separation or containment of radioactive substances as the release of secondary side coolant to the environment is acceptable.

369 I am content with the approach taken to the analysis of steam release within the MSSS compartments, as the "high integrity" claims have been considered by the Structural Integrity Assessment area and they are content with the claims made relating to the pipework. I am satisfied that the basis for the analysis is sound in relation to the application of the most onerous failure.

Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

370 The SAPs, state within EHA.5 and EHA.6:

| **Engineering principles: external and internal hazards** | **Operating conditions** | **EHA.5** |
|---|---|---|
| Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition. | | |

| **Engineering principles: external and internal hazards** | **Analysis** | **EHA.6** |
|---|---|---|
| Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects. | | |

371 In addition, SAP FA.6 states:

| **Fault analysis: design basis analysis** | **Fault sequences** | **FA.6** |
|---|---|---|
| For each initiating fault in the design basis, the relevant design basis fault sequences should be identified. | | |

*"Each design basis fault sequence should include as appropriate:*

*a) failures consequential upon the initiating fault, and failures expected to occur in combination with that initiating fault arising from a common cause;*

*b) single failures in the safety measures in accordance with the single failure criterion;*

*c) the worst normally permitted configuration of equipment outages for maintenance, test or repair;*

*d) the most onerous permitted operating state within the inherent capacity of the facility;"*

372 IAEA guidance, NS-G-1.11, states within the paragraph 3.40:

*"Depending on the characteristics of the pipes under consideration (internal parameters, diameter, stress values, fatigue factors), the following types of failure should be considered as PIEs:*

*(a) For high energy pipes, except for those qualified for leak before break, for break preclusion or for low probability of failure: circumferential rupture or longitudinal through-wall crack.*

*(b) For low energy pipes: leak with limited area.*

*It is accepted to postulate only a limited leak (and not a break) if it can be demonstrated that the piping system considered is operated under 'high energy' parameters for a short period of time (e.g. less than 2% of the total operating time) or if its nominal stress is reasonably low (e.g. a pressure of less than 50 MPa)."*

373 The approach taken by EDF and AREVA is consistent to the expectations stated within IAEA guidance, including the definition of low energy pipework which it states are pipes with an operating pressure of less than 2.0MPa (20 bar) and a temperature less than 100$^{o}$C in the case of water.

### 4.6.3 Assessment Conclusions

374 The deterministic approach taken to the analysis of failures of high energy pipework including detailed analysis of the associated consequences of failure of each of the systems is in line with my expectations. The analysis appears to be robust and thorough; however, the following Assessment Findings to ensure that key aspects of the case associated with Steam Release are captured within Phase 2.

- ***AF-UKEPR-IH-03*** *– The Licensee shall provide evidence to demonstrate that the design of the doors required to open in the event of increased pressure (due to a steam release) will do so at the requisite pressure and thus allow the steam release path to be realised in accordance with the requirements of the safety case.*
- ***AF-UKEPR-IH-04*** *– The Licensee is required to provide evidence relating to the specification of cables including wrapping and layout to demonstrate that the cables within the cable raceways (HLK/N3403ZL) are able to withstand temperatures of 300$^{o}$C and pressures of up to 2 bar.*
- ***AF-UKEPR-IH-05*** *– The Licensee shall provide evidence to demonstrate that the design of the doors required to remain intact in the event of increased pressure (due to a steam release) will withstand requisite pressure and ensure that the engineered discharge routes for the steam release to be realised in accordance with the requirements of the safety case.*

375 The above Assessment Findings should be addressed as part of the following procurement and construction generic milestones for Assessment Findings:

- Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.

## 4.7 Internal Flooding

376 The Step 3 Assessment Report identified that the PCSR did not contain arguments and evidence to support the claims and assertions made. The following areas were identified requiring further assessment during Step 4:

- *"Arguments and evidence relating to specific sources of internal flooding, including operator error, are not included within the PCSR and further substantiation will, therefore, be required during Step 4."*
- *"Further assessment associated with the completed verification process [the design verification for internal flooding] is to be undertaken when this process is complete within Step 4 or Phase 2."*

377 These two areas have been subject to further assessment as part of the Step 4 Internal Hazards Assessment and are discussed further within this section of the report.

### 4.7.1 Scope of Assessment Carried Out

378 The Step 4 assessment has involved further sampling of the PCSR and supporting documentation to determine further detailed arguments and evidence to support the claims made therein. The assessment has considered the responses to a number of Technical Queries and has been informed through various meetings with EDF and AREVA.

### 4.7.2 Assessment

379 The internal flooding methodology, ECEIG040650 (Ref. 42) is of limited value to the Step 4 Assessment of the UK EPR as the document does not provide any further information relating to arguments and evidence. Both the methodology and the PCSR refer to internal flooding detailed studies and verification that has yet to be undertaken for UK EPR, however, there has been significant process with the analysis for internal flooding on the verification and validation during Step 4 for the reference plant, Flamanville 3. As a result, the detail of the arguments and evidence has yet to be presented.

380 In light of the lack of such detail, further detailed technical information relating to claims on barriers, drains and equipment susceptible to internal flooding was requested. This was done in order to gain confidence that the arguments and evidence would confirm that the claims made for UK EPR were valid.

381 TQ-EPR-679 (Ref. 14) was raised requesting the detailed layouts illustrating the barriers that have been claimed as part of the internal flooding safety case. The source of the TQ arose from assessment of PCSR Chapter 13.2 Section 8 on internal flooding, specifically, the statement within Section 8.1.3.4 which provides information relating to SSCs important to safety and the measures in place to protect them against the effects of flooding. Flood barriers are identified as one of those measures for the protection of safety classified equipment.

382 The response to the TQ provided details of the claims made upon barriers segregating each of the divisional SAB, the two way segregation of the Fuel Building, and the external barrier of the Reactor Building. In addition the external walls of the Nuclear Island were also classed as providing protection against the effects of internal flooding arising from sources of internal flood located on the site but outside of the Nuclear Island. The barriers are claimed to withstand the effects of internal flooding up to the 0.0 metre level and capable of withstanding a 10 metre head of water.

383 A further TQ (TQ-EPR-695) (Ref. 14) was raised requesting details of any nuclear safety claims made on SSCs relating to internal flooding e.g. engineered drainage/sumps and plant/equipment designed to withstand the effects of internal flooding. The source of the TQ arose from the assessment of PCSR Chapter 13.2 Section 8 which alludes to claims made on drainage systems, sumps, and the ability of specific equipment to survive the effects of internal flooding.

384 The response provided details of the following SSCs which were claimed as part of the internal flooding case:

- Water tight doors at the interfaces of the buildings and divisions are resistant to the maximum water column resulting from the main initiator or the initiator used for the sizing of civil works. These doors are qualified for this requirement.
- The materials used for caulking, to close the openings and the joins in the walls between the divisions, are qualified against the water column height of the main initiator.
- The basement of the buildings acts as a retention zone for water. It will be painted with a waterproof paint up to the maximum water column resulting from the main initiator.
- The water flow resulting from the initiator is directed towards the retention rooms of the considered building. To ensure this, the initiator flow rate is compared with the cumulative flow rate of the floor drains, openings under doors, other available openings and un-caulked sleeves within the considered rooms. Discharge valves are used where required in specific rooms to achieve a sufficient flow rate.

385 The TQ response provided further useful information in relation to the high level claims on SSCs but did not specifically identify areas where SSCs are required to be specifically claimed e.g. the PCSR discusses some examples associated with protection of specific valves for the IRWST supply and protection of the MCR from flooding originating from the chilled water system, which was the level of detail that was requested within the TQ.

During the assessment undertaken within Step 4, it became apparent that the bounding claims made associated with internal flood appeared to be dependent on operator action in order to satisfy the deterministic case rather than solely as risk mitigation. Therefore the basis of the safety case claims do not meet my expectations in relation to the approach taken to method by which the claims and arguments presented for internal flood are bounded.

386 My principal concern is related to the treatment of human factors/human reliability in the flooding analysis method. It appears that an assumption is made of complete operator success prior to deriving the resultant flooding volumes. This does not meet our expectations for deterministic safety analysis; the assessment should assume a bounding water volume loss followed by analysis/demonstration of engineered prevention/counter measures in the first instance. Only then should any requirements for operator action be proposed. This would then provide the basis for an ALARP argument. As a result I sent a letter (EPR70257R) (Ref. 43) raising this concern.

387 EDF and AREVA have responded with letter ND (NII) EPR00770N (Ref. 44) which includes a commitment to address the shortfalls with the following stepped approach:

*"Step 1: Bounding cases : Leak volumes and retention volumes*

*As explained in the full response to the TQ-EPR-679, the walls in the interface and periphery of the Nuclear Island buildings have been designed to withstand a 10.00 metre water column under the 0.00m Level.*

*A document will be produced as part of Step 1 to identify the main flooding initiator(s) in each safety classified building of the Nuclear Island, assuming that the flooding event is not mitigated by a manual action. Based on the current layout, each associated bounding leak volume will be then compared with the water volume for which the considered safety division in the building has been sized.*

*If the flooding event proves that the volume of water retention of the affected building is not sufficient, the consequences would be considered as unacceptable as they can endanger another safety division. The mitigation options for such events will be analysed in Step 2.*

*Step 1 deliverable is proposed to be issued by the 30th of April 2011.*

*Step 2: Bounding cases: Mitigation measures*

*Mitigation measures for all critical cases identified in Step 1 studies will be elaborated in an ALARP study using solutions a, b, or c outlined above and summarised in a report to support the safety case for internal flooding.*

*Step 2 deliverable is proposed to be issued by the 31st of August 2011.*

*Step 3: GDA submission update*

*The study will be included in the GDA submission for internal hazards. A proposal for the revised PCSR will be issued by the 31st of December 2011."*

388 I believe that this proposed approach is acceptable; however, there is still a requirement for a GDA Issue given the proposed timescales for resolution and, therefore, a GDA Issue (**GI-UKEPR-IH-03**) and an associated Action have been raised **(GI-UKEPR-IH-03.A1)**.

389 The second area identified within the Step 3 assessment was the need to assess the completed verification and validation of internal flooding for the UK EPR. TQ-EPR-694 (Ref. 14) was raised requesting the completed verification for the design as this should provide the requisite evidence to support the claims and the arguments made within the safety case.

390 The response to TQ-EPR-694 relating to a request for the internal flooding verification was delivered late within Step 4 and as a result there has been insufficient time to produce the assessment to allow the information to be taken into account within the Step 4 Assessment Report. Consequently the need to provide the requisite evidence in the form of the detailed analysis and substantiation in support of the claims and arguments presented within Chapter 13.2 of the PCSR associated with internal flooding has been identified as a GDA Issue **(GI-UKEPR-IH-02.A1)**.

Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

391 The SAPs, state within EKP.5:

| **Engineering principles: key principles** | **Safety measures** | **EKP.5** |
|---|---|---|
| Safety measures should be identified to deliver the required safety function(s). | | |

*"Safety should be secured by characteristics as near as possible to the top of the list below:*

*a) Passive safety measures that do not rely on control systems, active safety systems or human intervention.*

*b) Automatically initiated active engineered safety measures.*

*c) Active engineered safety measures that need to be manually brought into service in response to the fault.*

*d) Administrative safety measures (see paragraph 376 f.).*

*e) Mitigation safety measures (e.g. filtration or scrubbing).*

*Note: The hierarchy above should not be interpreted to mean that the provision of an item towards the top of the list precludes provision of other items where they can contribute to defence in depth."*

392 The SAPs, state within ERL.3:

| **Engineering principles: reliability claims** | **Engineered safety features** | **ERL.3** |
|---|---|---|
| Where reliable and rapid protective action is required, automatically initiated engineered safety features should be provided. | | |

*"For requirements that are less demanding or on a longer timescale, operator actions or administrative control may be acceptable to complement the engineered systems. The objective should be to minimise the dependence on human action to maintain a safe state."*

393 This is further reinforced by SAPs EHA.6, EHA.14 and EHA.15:

| **Engineering principles: external and internal hazards** | **Analysis** | **EHA.6** |
|---|---|---|
| Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects. | | |

| **Engineering principles: external and internal hazards** | **Fire, explosion, missiles, toxic gases etc – sources of harm** | **EHA.14** |
|---|---|---|
| Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed. | | |

| **Engineering principles: external and internal hazards** | **Fire, explosion, missiles, toxic gases etc – effect of water** | **EHA.15** |
|---|---|---|
| The design of the facility should prevent water from adversely affecting structures, systems and components important to safety. | | |

### 4.7.3 Assessment Conclusions

394 There are two GDA Issues that have been identified arising from the internal flooding assessment undertaken during Step 4.

395 The GDA Issue, *"The internal flooding claims stated within the PCSR appear inconsistent with the deterministic approach to the analysis of potential sources of internal flooding"* (**GI-UKEPR-IH-03**) contains the following GDA Issue Action.

| | | | |
|---|---|---|---|
| **Technical Area** | **INTERNAL HAZARDS** | | |
| **Related Technical Areas** | Human Factors<br>Civil Engineering<br>Environment Agency | | |
| **GDA Issue Reference** | **GI-UKEPR-IH-03** | **GDA Issue Action Reference** | **GI-UKEPR-IH-03.A1** |
| **GDA Issue** | The internal flooding claims stated within the PCSR appear inconsistent with the deterministic approach to the analysis of potential sources of internal flooding. | | |
| **GDA Issue Action** | Please provide adequate substantiation of the internal flooding safety case through a deterministic analysis that initally assumes an unmitigated flood source and applies a multi-legged argument that may include consideration of the following:<br>• Potential failure mechanisms of water based systems.<br>• Civil engineering aspects including barriers and drainage.<br>• Systems (both engineered and administrative) to ensure that the effects of an internal flooding event are limited to loss of one division.<br>• Any further defence in depth and ALARP measures that could be implemented into the design.<br>• The impact of the changes made to the PCSR relating to the outcome of this substantiation on other safety case submissions such as civil engineering and human factors.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my expectations.<br>With agreement from the Regulator this action may be completed by alternative means. | | |

396 The GDA Issue, *"Outstanding substantiation associated with internal flooding, cable routing, high energy line break and missiles forms part of the requisite evidence and will be required in order to demonstrate an adequate internal hazards safety case."* includes the following GDA Issue Action:

| | | | |
|---|---|---|---|
| **Technical Area** | **INTERNAL HAZARDS** | | |
| **Related Technical Areas** | Structural Integrity<br>Civil Engineering<br>Fault Studies<br>PSA | | |
| **GDA Issue Reference** | **GI-UKEPR-IH-02** | **GDA Issue Action Reference** | **GI-UKEPR-IH-02.A1** |
| **GDA Issue** | Outstanding Verification and Validation for internal flooding, cable routing, high energy line break and missiles forms part of the requisite evidence and will be required in order to demonstrate an adequate internal hazards safety | | |

| | |
|---|---|
| | case. |
| **GDA Issue Action** | Provide the requisite evidence in the form of the detailed Flamanville 3 verification and validation analysis and/or other supporting documentation in support of the claims and arguments presented within Chapter 13.2 of the PCSR associatedwith internal flooding. The response should include analysis that supports the claims and arguments relating to:<br>• Civil structures (including surface coatings) claimed as flood barriers.<br>• Watertight doors and penetrations including qualification data.<br>• Drains and sumps claimed to prevent damage to nuclear significant SSCs.<br>• Calculations in place to support any claims made on potential water volumes.<br>• Any further defence in depth and ALARP measures that could be implemented into the design.<br>• Any identified design changes and their implementation within the PCSR.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my expectations.<br>With agreement from the Regulator this action may be completed by alternative means. |

397 It is important to stress that in order for **GI-UKEPR-IH-02.A1** to be addressed, the resolution of the deterministic claims as detailed within **GI-UKEPR-IH-03.A1** should be satisfactorily addressed. Alternatively, it may be possible to address the issue through a robust mechanism for ensuring that any changes that impact the internal hazards substantiation are captured so that changes to the deterministic case are appropriately captured.

## 4.8 Internal Explosion

398 Due to the limited degree of assessment undertaken during Step 3, the Step 4 Internal Hazards Assessment Plan identified the need to undertake further assessment of the arguments and evidence during Step 4.

### 4.8.1 Scope of Assessment Carried Out

399 The following reports were provided during Step 3 and have been used as the basis for the assessment of internal explosion for UK EPR:

- *"Systems at risk of explosion – EPR"*, ECEF071213 (Ref. 47), and
- *"Internal explosion: analysis of rooms at risk"*, EYRL2007fr0036 (Ref. 48).

400 A number of the systems that are subject to assessment within reference 47 are associated with the primary circuit of the reactor and as such are not considered within the internal hazards assessment e.g. $H^2$ accumulation within the pressuriser and the recombiners, the aspects of which are addressed within the Reactor Chemistry Step 4 Assessment Report (Ref. 45). The assessment has focussed on the arguments and

evidence associated with the claims made within the PCSR associated with the hydrogen supply system and the battery rooms together with their associated ventilation systems.

401 External gas storage areas have not been considered in this assessment as their location, geometry and extent are considered to be Phase 2 licensing matters.

### 4.8.2 Assessment

402 The PCSR identifies a number of *"Safety Objectives"*, namely:

- An explosion shall not result in the loss of more than one redundant equipment assembly of an F1 system.
- Insofar as possible, an explosion shall not cause the loss of an item of equipment or part of equipment which could result in a PCC3 or 4 event.
- Moreover, an explosion shall especially not result in deteriorated stability/integrity of:
  - i) Safety-class buildings and fire safety barriers.
  - ii) Remote shutdown station guaranteed if control room inaccessible.
  - iii) Components whose failure is ruled out by design.

403 Furthermore, it claims that there is sufficient redundancy to enable the plant to reach a safe shutdown state and that any potential explosion should not affect habitability of the Main Control Room.

404 ECEF071213 identifies the risks and provide a hierarchy of protection against explosion within UK EPR. The hierarchy is, firstly, to prevent the formation of an explosive atmosphere, secondly, use detection to monitor any build up of the hazard and finally to limit the consequence of a subsequent explosion.

405 The main systems which are considered to be at risk from explosion are the hydrogen distribution system (SGH), the hydrogenation plant (RCV), the hydrogen recombiner (TEG) and the battery rooms and their ventilation systems. As mentioned within the scope above, this assessment focuses on the hydrogen distribution system and the battery rooms.

406 Reference 47 states that a gas circuit is at risk whenever, during normal operation, the concentration of the explosive gas is greater than or equal to the Lower Explosive Limit (LEL) and as a conservative measure the Lower Flammability Limit (LFL) is used within the analysis. Only rooms when there is the potential for this limit to be reached e.g. the LFL for hydrogen is 4% in air are considered.

407 Once the rooms at risk have been identified there are a number of design requirements considered based upon the following:

- Prevention:
  - i) The adoption at the design stage of measures guaranteeing leak tightness.
  - ii) The design of rooms, equipment, and ventilation systems that do not result in pockets of stagnant air.
  - iii) Circuit signalling.
  - iv) Grounding of all circuits and equipment.
  - v) Use of signs with standardised pictogrammes.

vi) Making provision for the risk of impact.

- The detection of explosive gases installed in specific rooms and areas.
- Categorisation of equipment within rooms identified as at risk.
- Planned inspection and maintenance.
- Ventilation either natural or forced which, where possible, should prevent the formation of an explosive atmosphere.

Hydrogen Distribution System

408 The hydrogen distribution system supplies hydrogen to the Chemical and Volume Control System (CVCS) and to the Gaseous Waste Processing System (GWPS). The internal hazards assessment considers the point at which the hydrogen enters the Nuclear Island and the routing which they take up to the point where they enter their respective systems. There is both hydrogen detection and fire detection which, if went into alarm, would automatically close the isolation valve at the site hydrogen store. There are further protection features associated with the hydrogen distribution system which include electrical earthing, impact protection, and limitation of leaks through enhanced design features e.g. the provision of a sealed hydrogen circuit with exception of the pressure reduced, flanged valves with seal lips, valves with elastomer diaphragms compatible with hydrogen and flow restrictors.

409 Reference 48 details the specific rooms at risk in which the hydrogen pipework is routed. The Safeguard Buildings and Reactor Building do not contain any pipework associated with the hydrogen distribution system as the hydrogen distribution only serves the CVCS hydrogenation station in the Fuel Building and the GWPS recombiner in the Nuclear Auxiliary Building. The routing of the pipework passes through 6 rooms within the Fuel Building and 13 rooms within the Nuclear Auxiliary Building. The rooms identified as being at risk are individually analysed and calculations performed. The CVCS valve room (HK1385) has been selected for further assessment as this was the smallest room by volume which, partially as a result, had one of the highest potential hydrogen concentrations identified.

410 Room HK1385 has a volume of approximately 39$m^3$ and the systems at risk have been identified as the hydrogen distribution system and the CVCS system. The volume of hydrogen released assumes loss of HVAC, failure to close the valve to the CVCS, and the time taken to close the valve after detection via the redundant hydrogen monitoring as 1 hour. The calculations associated with the potential volumes were checked and found to be correct. The volume percentage calculations detailed within the analysis calculate that the hydrogen concentration within the room in a worst case failure of the hydrogen feed pipework would be less than the LFL (4%).

Battery Room Hydrogen Generation

411 There are many batteries installed as part of the UK EPR design; predominantly within each of the SAB, however, there are also batteries installed within the Diesel Buildings. There are eight rooms identified within the analysis (6 within the SAB and two within the Diesel Buildings), all of which are battery rooms and have been subject to assessment as the batteries release hydrogen during normal operation. The analysis provides details of the ventilation system in place to ensure that an explosive atmosphere cannot be generated. The ventilation systems in both the SAB and Diesel Buildings are redundant systems for both supply and extract. The two supply air trains, allows for maintenance to be undertaken on the other during normal operation and the supply system serves the

entire building. The extract system is a two train independent system, one for the building and other dedicated as a battery room extract which in itself comprises two trains; one for maintenance and one for normal operation.

412 The analysis identifies that during maintenance there is the potential for an explosive atmosphere to occur due to the non-redundancy of the ventilation system. Calculations are included within the analysis which show that the time it takes the Battery Rooms to reach 25% of the LFL, namely 1% hydrogen, is at least 18 hours in the worst case and the time taken to reach the LFL is claimed to be 72 hours. In addition, there is redundant hydrogen detection installed within each of the rooms to ensure that appropriate action can be taken to terminate the battery charging.

413 The production of hydrogen calculated was [redacted] which confirms that the quoted time period of a minimum of 18 hours to reach the LFL is correct.

414 As the specification for the batteries to be installed within UK EPR is yet to be produced, the information presented within the analysis is associated with FA3, there is a need for the calculations to be undertaken taking into account the potential hydrogen accumulation rates arising from the selected batteries. In addition, there is also a need to consider the potential for a flammable atmosphere being formed during the most onerous operating conditions, such as boost charging. An Assessment Finding has been raised due to the need to confirm that, as a result of site specific aspects of the design, the potential for an explosive atmosphere has been minimised **(AF-UKEPR-IH-06)**.

Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

415 The SAPs state in SAP EHA.14:

| **Engineering principles: external and internal hazards** | **Fire, explosion, missiles, toxic gases etc – sources of harm** | **EHA.14** |
|---|---|---|
| Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed. | | |

416 The ND Internal Hazards Technical Assessment Guide, T/AST/014 provides further information relating to the need to assess facilities against the potential effects of internal explosions. Section 5.8 of the guidance states:

*"Consideration should be given to a need for redundancy and segregation in the design and layout of items important to safety to mitigate against any potential threat from explosions and missiles. The hazards should be prevented or minimised but where they are not avoidable items important to safety should be protected by spatial or physical barriers."*

417 Included within the TAG are specific matters that should be addressed in the design and safety of the plant, which include:

- Sources of possible explosions/missiles should be identified, the possible magnitude of explosions, blast waves and the likely size, frequency and trajectory of missiles estimated, and their effects on items important to safety assessed.
- The results of a hazard analysis in conjunction with the licensee's acceptance criteria should be used to verify the adequacy of protection provided by spatial segregation, protective barriers, and redundancy in safety related items and safety systems.

- Possible causes of explosions to be considered include the ignition of flammable gas, vapour or oil-mist clouds, exothermic reactions, pyrophoric materials, failure of pressure parts, and explosions associated with switchgear, high energy transformers, electrical batteries, terminal boxes and power cables.
- Hydrogen must be treated with particular care as hydrogen explosions can be very violent. Flammable and potentially explosive gases such as propane and butane are burned to supply heat for carbon dioxide and nitrogen vaporisation. In addition to the effects of blast overpressure, the hazard analysis should consider the heat and toxicity of hot or burning gases, fire, and the generation of missiles.

418 In relation to the potential for an explosive atmosphere within battery rooms associated with the production of hydrogen from the batteries during charging, BS6133:1995, *"Code of Practice: Safe operation of lead-acid stationary batteries"* (Ref. 49) states:

"The volume of hydrogen obtained can be expressed as a percentage of the total volume of the room or cabinet/cubicle, and this can be used to calculate the number of air changes per hour necessary to keep the hydrogen concentration below the recommended maximum of 1 % (V/V)."

### 4.8.3 Assessment Conclusions

419 The approach to the assessment of potential hydrogen explosions, both arising from failures of pipework and from hydrogen generation as a result of battery charging is in line with my expectations and those of international standards and guidance.

420 The following Assessment Finding has been raised due to the need to confirm that, as a result of site specific aspects of the design, the potential for an explosive atmosphere has been minimised:

- ***AF-UKEPR-IH-06*** *– The Licensee shall provide evidence to demonstrate that the potential for a hydrogen explosion within the Battery Rooms during the most onerous operating conditions has been considered within the UK EPR design.*

421 This Assessment Finding should be addressed as part of the following procurement and construction generic milestones for Assessment Findings:

- Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.

## 4.9 Electro-Magnetic Interference (EMI)

422 The Step 3 Assessment Report identified that EMI may be subject to further assessment during Step 4. EDF and AREVA consider EMI within the scope of the electrical engineering area and it has been agreed with the electrical engineering assessor that this is to be captured within the Step 4 Electrical Engineering Assessment of the EDF and AREVA UK EPR (Ref. 50) and as a result there is no further consideration within this report.

## 4.10 Threats to Recirculation from IRWST Filter Blockage

423 TQ-EPR-216 (Ref. 14) was raised during Step 3 of the GDA process in relation to the IRWST and the potential to prevent re-circulation as a result of blockage to intake filters and/or pumps due to debris. The initial TQ did not provide the requisite technical

information relating to the justification of claims made upon the SSCs in place to prevent filter blockage e.g. kerb sizing, design of the retention basket, and any bounding assumptions made relating to potential type and geometry of debris. A further TQ (TQ-EPR-533) was raised requesting this further technical information.

424 Following a LOCA, the SIS is used to make up the reactor coolant and ensure sustained core cooling. The coolant used for this purpose is stored in the IRWST and drawn by suction from the IRWST into the SIS using the SIS pumps. In addition, in selected PCC-4 events (pipe breaks outside the containment with the safety injection system (SIS) in residual heat removal mode) and RRC-A sequences and severe accidents (RRC-B sequences), the Containment Heat Removal System (CHRS) is used to both cool the IRWST and remove decay heat from the containment. The CHRS also draws the coolant that is used for these purposes from the IRWST. The volume of the IRWST is such that Net Positive Suction Head (NPSH) is sufficient for the pumps SIS/RHR and CHRS in the case of accident or severe accident.

### 4.10.1 Scope of Assessment Carried Out

425 My assessment has focussed on the specific area of IRWST blockage and used the information contained within the responses to the TQs and the reference cited as the basis for this assessment.

### 4.10.2 Assessment

426 The initial TQ (TQ-EPR-216) (Ref. 14) provided an overview of the purpose and design of the SSCs in place to prevent debris blocking the filters and preventing re-circulation. The following provisions have been included within the design to prevent blockage of the filters:

- Low kerbs are located around the heavy weight floor openings to the IRWST in order to facilitate sedimentation of the debris on the heavy weight floor.
- Debris grids covering the openings with a large mesh which are used to capture large items of debris.
- Retention baskets are located beneath the penetrations which are designed to retain the majority of the debris generated in the event of a LOCA.
- The provision of filters to both the SIS and CHRS which have a large surface area and a fine mesh to capture small particles of debris.
- The ability of the back-flushing to remove the debris bed from the filters to prevent filter clogging and efficient backflushing allowing most of the backflushed debris to settle on the IRWST floor.

427 With the provisions detailed above, the SIS and CHRS systems are able to meet the following requirements:

- Prevention of particles greater than 2mm passing through the filters.
- Prevention of a concentration of particles downstream of the filters exceeding 500 parts per million.
- Maintaining the pressure drop across the filters such that the required NPSH and available NPSH is positive over the requisite temperature range ($40^{o}C$ – $120^{o}C$ in the case of the SIS and $40^{o}C$ to $160^{o}C$ for the CHRS).

428 Determining the adequacy of the provisions is dependent upon the characteristics of the debris that could be generated in the event of a LOCA. EDF and AREVA have undertaken analysis for the SIS on the potential debris resulting from PCC and RRC-A events and included within the analysis is the consideration of 50kg of fire resistant materials. For events when the CHRS is required (PCC-4 and RRC-A/B events), there is uncertainty over the size and amount of debris that could be generated and debris arising from loss of fire resistant materials such as wrapping is not considered as EDF and AREVA state that it is not susceptible to degradation following an event such as a severe accident due to it's material properties.

429 I am satisfied with the approach taken to the design principles adopted for ensuring that the potential for filter blockages arising from debris, however, further information was sought through TQ-EPR-533 (Ref. 14), which requested further technical information relating to kerb sizes, retention basket design, and the bounding assumptions relating to potential blockages in order to provide confidence in the principles adopted.

430 The response provided clarity over the kerbs claimed to promote sedimentation and the mesh claimed to prevent large items of debris falling into the retention basket. The kerbs [redacted] and provide a passive means of not only to aid sedimentation but also to ensure that any large debris is retained on the floor. The design of the large debris grids [redacted] ensure that the returning water flow is achieved and that simultaneous blockage of all four heavy openings is not possible. The geographically separated location of the heavy weight floor openings also ensures that a single event cannot result in blockage of all four return paths.

431 Information was also provided relating to the individual compartments within the retention baskets which detailed additional return paths from the annular space in the event of failures associated with the pressuriser or breaks in the secondary side steam and feedwater lines. There are kerbs installed at the interface of the annular space to the IRWST that performs the same function as the kerbs to the heavy weight floor openings, however, in the case of the annular space the kerb is at a height of [redacted]. This is provided to ensure that large items cannot pass into the IRWST as there is no mesh provided at this interface. In addition the height of the opening is limited to approximately [redacted] which prevents larger items of debris from passing into the IRWST.

432 The TQ response provided detailed further information relating to potential IRWST depths and demonstrated that the retention basket will maintain its passive filtration function in the event of LOCA and severe accident and that the filters would remain operational. In addition, there is a one metre gap between the top of the retention basket and the base of the heavy floor above and should the retention basket become blocked there is the ability for it to overflow and thus ensure functionality of the system. Should the retention basket overflow the sump strainers for the SIS and CHRS would be able to perform their function as they are separate structures within the IRWST.

433 There are [redacted] sump strainers in total, [redacted] for the SIS and [redacted] for the CHRS. The sump strainers consist of a [redacted] wire mesh, fabricated as modules for ease of construction, installation and maintenance. There are approximately [redacted] cartridges each [redacted] high linked to ducts leading to the inlet box above the each of the sumps. Each strainer provides a filtration surface area of [redacted] and can support pressures and temperatures of [redacted] and [redacted] respectively.

434 As was mentioned previously, there is the ability to provide a back-flush function for each of the strainers. The system for the SIS is provided as defence in depth and is utilised if the pressure drop in the strainers reaches a defined maximum point, however, the CHRS

system is required due to the uncertainty involved in the potential debris that could enter the IRWST and as a result the design margin is uncertain. The provision of the back-flush system provides confidence that the filters could be cleared should they become blocked in the event of there being a need for the CHRS (PCC-4 or RRC-A/B events.)

435 Within the response to TQ-EPR-533, there was information provided relating to the provision of a test program to test the entire system as part of the validation. In addition to the information contained within the TQ response, I assessed the supporting reference, *"Test program for the qualification of the FA3 IRWST filtration system"* (Ref. 46) to assess the various conditions applied to the scale test loop and to understand the types of tests undertaken.

436 The program details six tests which examine the system to qualify its efficiency in the event of a LOCA. The aspects of the system which are subject to test include:

- the filtration efficiency of the retention basket and strainer;
- the retention capacity of the IRWST basket;
- the filtration efficiency of the IRWST strainers;
- the ability of the IRWST strainers to be back-flushed.

437 The six tests involved using a scaled mock-up and using differing types of debris of different sizes commensurate with that expected in the event of a LOCA. There is conservatism in the test procedure as the kerbs are not taken into account and as a result there is no sedimentation considered to be trapped either on the heavy floor or the annulus and a proportion of the debris used is mechanically shredded to ensure that it is less than [redacted] in size. There are detailed validation criteria that require to be met and if not, there is a need to either modify the design or produce a justification detailing why the criteria are not suitable.

438 On completion of the initial six tests (the pre-tests) there are a further six qualification tests undertaken which consider:

- Injection via the heavy floor opening into the top of the retention basket; and
- Injection via the annulus via the side of the retention basket.

439 As part of the test program there are detailed test procedures in place to ensure that the appropriate process is followed thus ensuring that the test is carried out in accordance with the procedure and hence provide validation of the test as well as to ensure consistency in the approach.

440 The response to TQ-EPR-533 states that the preliminary testing that has been done has shown:

- the retention baskets have a very good retention capacity, approximately [redacted];
- the solid content of the water of the water downstream is limited at the beginning of the test to [redacted] and decreases thereafter to below [redacted] at the steady state;
- the combination (retention basket and strainer) leads to a head loss across the strainer limited to [redacted] which provide margin to the limit of [redacted].

441 I am content that the supplementary technical information contained within the response to the TQ together with the supporting reference provides the requisite information and

confidence in the capability of the IRSWT filter system through the detailed analysis and testing program that has been undertaken.

442 Towards the latter stages of this assessment, I became aware that the US NRC had raised a Generic Safety Issue (GSI) (Ref. 61) in relation to the assessment of debris accumulation on the US EPR sump performance. A letter was subsequently sent to EDF and AREVA (Ref. 62) requesting them to explain whether failure to meet the test requirements undertaken as part of the US design certification application were applicable to the UK EPR design or provide justification why the concerns of US NRC were not applicable..

443 EDF and AREVA responded (Ref. 63) with information that detailed the differences between the design of the IRWST filtration systems for the US EPR and the UK EPR. The key differences between the two designs include:

- The UK EPR CHRS system is a two train system with the ability to back-flush the filters during a fault condition as opposed to a single train system adopted for US EPR with no ability to simultaneously back-flush due to the operational need of the system in a fault condition.
- There are differing debris sizes with the UK EPR design which take account of greater amounts of smaller debris in comparison to the US EPR. Conversely, the US EPR considers far high quantities of larger debris than the UK EPR [redacted]. However, it is recognised that the US EPR utilises Reflective Metal Insulation which serves to minimise the amount of fibrous material likely to be present within the debris. The UK EPR utilises glass wool as a means to insulate the RCS and other auxiliary pipework.
- The UK EPR considers 50% of the debris within a basket whereas the US EPR considers 100% (given that it is a single train system).
- The design of the CHRS/SIS strainer is different between the UK EPR and US EPR with the UK EPR utilising a number [redacted] cartridges and the US EPR adopting a single-box design. As a result there is a larger filter surface available for the UK EPR ([redacted] as opposed to [redacted] for the US EPR).

444 It can be noted that the detailed designs of each system vary quite significantly. There are a number of aspects of the UK EPR design which are seen as providing greater confidence in the ability of the system to perform and not be subject to blockage due to debris accumulation on the filters. Most notably that the system is a two train system with the ability to perform back-flush operations during a fault scenario and the greater surface area adopted for the strainers.

445 There are also aspects of the US EPR design that would appear reasonably practicable measures in relation to the selection of the insulation material and the method by which it is contained; this has been captured within an Assessment Finding within the Fault Studies Containment and Severe Accidents Step 4 Assessment Report (Ref. 64), which states:

*"AF-UKEPR-CSA-07 – The licensee shall, prior to inactive commissioning – containment pressure test, demonstrate that the design of insulation and the strainer structures associated with the safety injection system is such that the risk of sump blockage has been reduced to the lowest level reasonably practicable. In particular, the licensee should produce an analysis of the options and justify the choice of insulating technology."*

446 Furthermore, the Step 4 Reactor Chemistry Assessment (Ref. 45) has raised an Assessment Finding relating to the need to control the use of fibrous materials within the plant. As part of the assessment, EDF and AREVA confirmed that preference would be given to the encapsulation of insulation materials by metal cladding. The Reactor Chemistry Assessment states:

*"Should fibrous material reach the IRWST (due to the failure of cladding for instance), silicates or zeolite-forming solutes may be carried into the core and impair heat transfer during an accident. Also, other materials may be introduced into the containment building during a shutdown, and these may place an additional burden on the sump filtration system."*

447 The Assessment Finding states:

*"AF-UKEPR-RC-50 - The Licensee shall estimate the quantities of all possible chemical species that could degrade the performance of the IRWST and analyze their downstream effects on cooling and radioactive release. Possible sources from different events include; acidic fumes from radiolysis or pyrolysis, working materials introduced during shutdowns and leaching from solid materials trapped in the strainers. Each of these could reduce the quality of the water in the IRWST and impair heat transfer or iodine retention."*

448 There is also an Assessment Finding associated with the satisfactory completion of the qualification testing undertaken on the filtration system within the Mechanical Engineering Step 4 Assessment Report (Ref. 65), which states:

*"AF-UKEPR-ME-32 - The licensee shall ensure that the IRWST filtration system tests are satisfactorily completed to qualify the performance of the UK EPR design."*

449 Given the differences in design coupled with the application of detailed and comprehensive test programme for the IRWST filters, the need for satisfactory completion identified within the above Assessment Findings, I am satisfied that the concerns relating to sump blockage by the USNRC are not directly applicable to UK EPR. Nevertheless, I see the need to successfully resolve the three Assessment Findings as essential in demonstrating the overall adequacy of the system proposed for the UK EPR.

Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

450 The SAPs, state within EHA.6:

| **Engineering principles: external and internal hazards** | **Analysis** | **EHA.6** |
|---|---|---|
| Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects. | | |

451 This is further reinforced by SAP EHA.14:

| **Engineering principles: external and internal hazards** | **Fire, explosion, missiles, toxic gases etc – sources of harm** | **EHA.14** |
|---|---|---|
| Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed. | | |

452 IAEA Safety Standard, *"Safety of Nuclear Power Plants: Design – Requirements"*, NS-R-1, states within paragraph 3.7:

*"Where an unproven design or feature is introduced or there is a departure from an established engineering practice, safety shall be demonstrated to be adequate by appropriate supporting research programmes, or by examination of operational experience from other relevant applications. The development shall also be adequately tested before being brought into service and shall be monitored in service, to verify that the expected behaviour is achieved."*

453 The approach to the design of the IRWST filter system is, therefore, in line with our expectations with regard to national and international standards and guidance.

### 4.10.3 Assessment Conclusions

454 I am satisfied that the design provisions, including the physical testing, of the IRWST filter system provide confidence in the ability of the system to perform its requisite safety function for the events postulated. Furthermore, it is reassuring to see the application of such detail and rigour in the approach taken to the testing of this system.

455 There are no GDA Issues or Assessment Findings associated with this aspect of my Internal Hazards Assessment.

## 4.11 Regulatory Observations

456 There were 3 Regulatory Observations raised during GDA:

- RO-UKEPR-30 – Fire Barriers
- RO-UKEPR-35 – Door Control Measures
- RO-UKEPR-70 – Dropped Loads and Impact

457 The first two ROs were raised during Step 3, however, not all the information was available at the time to fully assess. In the case of RO-UKEPR-30, there was one remaining deliverable associated with the MAGIC computer modelling analysis to demonstrate the capability of the barriers to withstand a fire for a minimum of 2 hours which I have assessed as part of Step 4. The other deliverables as part of the RO response plan were assessed during Step 3 and the outcome of the assessment is detailed within Section 2.3.2.3 of the Step 3 Internal Hazards Assessment of the EDF and AREVA UK EPR. The response to RO-UKEPR-35 was provided by EDF and AREVA towards the end of Step 3 and was not subject to assessment, therefore, the full response to the RO has been assessed during Step 4.

458 RO-UKEPR-70 was raised during Step 4 and at the time of writing this report, a response plan has yet to be received from EDF and AREVA. The assessment that led to the issue of the RO is contained within Section 4.1 of this report and as a result is not considered further within this section.

### 4.11.1 RO-UKEPR-030 – Fire Barriers

#### 4.11.1.1 Scope of Assessment Carried Out

459 The final deliverable that EDF and AREVA committed to within the response plan to the RO, and provided during Step 4, was to:

*"Perform a MAGIC simulation for one representative safety fire compartment with the highest fire loading and compare the result with standard temperature curves. This assessment will not take credit for active fire fighting systems."*

460 In response, the report, *"UK EPR- MAGIC simulation for one representative safety fire compartment with the highest fire loading and comparison with standard resistance curves without taking credit for active fire fighting systems."*, ECEIG091608, (Ref. 51) was provided which has been used as the basis for my assessment.

#### 4.11.1.2 Assessment

461 The report provides analysis of two compartments:

- HLB1421SFI, Safety Fire Compartment encompassing cable rooms HLB1402ZL, HLB1420ZL, HLB1401ZL and HLB1806ZL; and
- HLB222SFI, Safety Fire Compartment encompassing cable rooms HLB2204ZL, HLB2205ZL, and HLB2208ZL.

462 The analysis makes a number of modelling assumptions including:

- The fire is assumed to be located within the centre of the room and is assumed to consume all combustibles.
- The fireloading has been based on the cable trays within the room being filled to capacity (100%).
- The openings within the barriers are considered within the model, with the exception of penetrations that will be fire stopped as part of the design e.g. cable penetrations.
- The dimensions of the room are associated with the volume and the height.

463 I consider that the assumptions used within the computer model are acceptable as to do further, more detailed, analysis would require far more complex programming and software. Given that the modelling is considered to be confirmatory, I am satisfied with the approach taken.

464 The analysis also takes into account the potential for random failure of the largest fire damper within the room [redacted] i.e. it is left open for the duration of the test. This is in line with my expectations associated with active single failure as there are no other components within the barrier that could be more onerous, other than a door, but this is considered more as a passive component, and measures to ensure that doors are monitored are addressed within RO-UKEPR-35.

465 The results of the testing demonstrated that all fires burnt for a duration of less than 60 minutes and that the comparison to the standard fire resistance curves demonstrated the temperatures after a period of two hours were significantly less than the limiting temperatures contained within the aforementioned curves.

466 The report concludes that the two hour fire barriers will adequately withstand the worst case for involving the highest combustible inventory and confirms the findings within the preceding actions detailed within the RO response plan.

467 I considered this to be a detailed and accurate analysis for the rooms identified within the SAB, however, I questioned why the bulk diesel storage tanks rooms were not assessed given the significantly higher combustible inventory coupled with the lower volume. I decided to address this through the issue of TQ-EPR-666 (Ref. 14) rather than raise a

further RO action as it was associated with potential claims made on the fire fighting system as an F1 system. The TQ stated:

- *"The report EYTF/2007/FR/0028 describes the JPV fire fighting system operation in the diesel generator buildings as a F1 system, "preventing propagation to safety class equipment of redundant divisions." Please confirm that the findings of RO30, with respect to the fire barriers of the Safety Fire Compartments (SCO) are able to resist a fire without reliance on active fire suppression, are applicable to the SCO compartments within the diesel buildings."*

468 The response provided some further analysis and modelling undertaken on the safety fire cell with the highest fireloading, HDA0A03ZL, which was the main fuel storage tank room and contained approximately [redacted].

469 As was the case for the SAB modelling, a single random failure of the largest damper was assumed. In addition, there is a penetration to the adjacent room which is assumed to be open to air to simplify the computer model. This is stated within the response as being conservative as the quantity of air entrained through the penetration is not limited.

470 I am satisfied with the input parameters for the model and with the assumptions made for modelling a fire within the diesel tank room.

471 The results of the MAGIC fire modelling returned a maximum temperature within the room of [redacted] due to the limited ventilation available to maintain burning. The analysis then undertakes a comparison with the standard fire resistance curves and, again, shows that the curve is not exceeded by the modelled fire. The report concludes that fire involving the bulk fuel within the diesel tank room does not compromise the safety fire compartment and confirms that there is no nuclear safety requirement for the fire fighting system.

#### 4.11.1.3 Assessment Conclusions

472 I am satisfied that this analysis provides the requisite demonstration that the fire fighting system does not require to be claimed to perform a nuclear safety function and that the barriers will withstand a fire within the area due to the limited ventilation available to maintain burning. This RO was closed out during Step 4, the confirmation of which is included within my letter to EDF and AREVA, EPR70135R (Ref. 52).

473 There are no GDA Issues or Assessment Findings associated with this aspect of my assessment.

### 4.11.2 RO-UKEPR-035 – Door Control Measures

474 During the latter part of Step 3, I was informed that, where there are doors within Safety Fire Compartments (SFO), it was not proposed to have any engineered systems in place to identify whether the door is left open. TQ-EPR-129 was raised seeking further information relating to the door controls provisions that are to be adopted as party of the UK EPR design. I was informed that the current FA3 design does not have any measures to identify whether doors have been left open other than administrative controls. Given the nuclear significance associated with potential breaches in nuclear significant hazard barriers, I did not consider that administrative controls on their own were likely to be adequate. As a result a Regulatory Observation (RO-UKEPR-035) was raised to address this shortfall, to which a response was provided during Step 4.

#### 4.11.2.1 Scope of Assessment Carried Out

475 The assessment is based on the responses to the Regulatory Observation Actions raised through the issue of RO-UKEPR-35 and provided during Step 4.

#### 4.11.2.2 Assessment

476 The first action, RO-UKEPR-035.A1, stated

*"EDF and AREVA are required to demonstrate that within the UK EPR design will have adequate door control measures for doors installed within Safety Fire Compartments. Relevant good practice already observed and in place within the UK for the provision of door control measures, operational experience observed within the current UK reactor fleet and the expectations and requirements of other overseas regulators for the installation of door control measures, lead to the expectation that adequate door control measures are required to be incorporated into the UK EPR design."*

477 The response plan (Ref. 53) to the Regulatory Observation Action provided the following tasks that were to be undertaken to address the action raised:

- *"In each building of the Nuclear Island of the UK EPR, EDF/AREVA to identify the relevant doors that constitute the fire barriers of the Safety Fire Compartments."*
- *"Description of the design process that EDF/AREVA will put forward to ensure the UK EPR design fulfils the NII's requirement for these fire doors."*

478 The submission of the full response to the RO (Ref. 54) detailed limited information relating to the identification of the barriers as it simply stated that there were 57 doors located in safety fire compartments as part of the segregation for nuclear safety. In addition, the information provided in response to the description of the process did not provide the requisite detail relating to the specific design provisions, rather, it consisted of high level principle based information.

479 Whilst it is accepted that there will be uncertainty in the detailed design of the door control measures, the information presented was insufficient to satisfy me that the modifications to be included within the UK EPR adequately addressed the concern raised within the RO. As a result, a further RO action was raised (RO-UKEPR-35.A2), which stated:

*"Further to receipt of a response to RO-UKEPR-035.A1, please could you provide further information that details the specific design provisions for the door control measures which should include the relevant design change form for the modification, the supporting submission programme and the justification of the detailed design to be incorporated as part of the UK EPR design together with any other supporting substantiation for the modification to be undertaken. Design change information submitted late may not be included in our assessment and may result in an Exclusion or out of scope item to any DAC that we may issue."*

480 The full response (Ref.55) included a technical report, *"UK EPR – Specification of the Door Monitoring System"* ECUK100261 (Ref. 56). The report provides information relating to the operational requirements of the system including both local and central alarm functions should the door not be closed properly as well as design requirements that need to be developed and implemented during construction. The structure of the system is provided within the report which identifies two sub-functions; detection of open

doors and raising the alarm function. The alarm has a number of basic functions identified, namely:

- Raise a local alarm both visually and audibly to alert staff of the need to ensure that the requisite action is taken by staff i.e. to ensure the door is closed in accordance with the safety case.
- Raise a centralised alarm to identify to staff within either the MCR or the Security Control Centre that a door is open and that action is required. This is to be done either visually or audibly.
- Management of planned breaches of fire compartments through the ability to disable the alarm to allow for authorised compartment breaches.
- Power supply of the local alarms, the role being to adapt the supply voltage of the network to a voltage compatible with the equipment.

481 There are control and instrumentation principles for the door control systems, thus ensuring that during the detailed design and construction phase that adequate consideration is taken in order to meet these requirements.

482 Finally, there is a comprehensive list of all doors within identified safety fire compartments which require door control measures to be installed.

#### 4.11.2.3 Assessment Conclusions

483 I am satisfied with the approach taken to addressing the principles of design, the approach to operation of the system and the specific identification of the doors. There are a number of areas that are yet to be developed, however, these are identified within the report and I am satisfied that the approach taken to the design and operational requirements will ensure that they are captured. This RO was closed out during Step 4, the confirmation of which is included within my letter to EDF and AREVA, EPR70222N (Ref. 57).

484 There are no GDA Issues associated with this aspect of my assessment, however, I consider it prudent to include an Assessment Finding associated with ensuring that the door control systems installed are captured and adequately specified, designed and implemented within the UK EPR. The following Assessment Finding has therefore been raised.

- ***AF-UKEPR-IH-07*** *– The Licensee shall provide evidence to demonstrate that the specification, design and implementation of the door control measures are included within the UK EPR design.*

485 This Assessment Finding should be addressed as part of the following procurement and construction generic milestones for Assessment Findings:

- Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.

### 4.12 Regulatory Issues

486 There were no Regulatory Issues raised as part of the internal hazards assessment throughout the GDA process.

### 4.13 Overseas Regulatory Interface

487 There were a number of meetings held that focussed on the internal hazards assessment during Step 4. The meetings were held as part of the Multinational Design Evaluation Programme (MDEP) and organised through the Organisation for Economic Co-operation and Development (OECD). Within the meetings was representation from:

- United States Nuclear Regulatory Commission (USNRC).
- Autorité de Sûreté Nucléaire (ASN), the French Nuclear Regulator.
- Säteilyturvakeskus (STUK), the Finnish Nuclear Regulator.
- Canadian Nuclear Safety Commission (CNSC).

488 The topics discussed within the meetings were:

- cable routing and segregation;
- dropped loads and impact;
- verification and validation;
- Reactor Coolant Pump fires;
- door control measures;
- nuclear safety claims on fire protection systems; and
- internal explosion, specifically, hydrogen concentrations.

489 In addition, I attended a meeting with STUK at their offices in Helsinki, Finland, further to a visit to the Olkiluoto 3 construction site to share information relating to the assessment of cable routing and segregation. This was undertaken jointly with the Nuclear Directorate (ND) Electrical Engineering Assessor.

### 4.14 Interface with Other Regulators

490 There has been an interface with inspectors within HSE who specialise in General Fire Precautions, Conventional Safety, and Construction (Design and Management) Regulations as there was a need to consider the layout of UK EPR relating to means of escape. A number of joint meetings were held between ourselves and EDF and AREVA to discuss the approach that was to be taken to ensure that potential conflicts between the conventional safety aspects of the UK EPR and the nuclear safety case were minimised. A workshop was held by ND to provide EDF and AREVA an overview of our expectations within this area. Further to the workshop, a letter (Ref. 60) was written to EDF and AREVA providing some high level comments on a sample of the areas within the UK EPR coupled with an offer to provide further assistance within this area.

### 4.15 Other Health and Safety Legislation

491 As mentioned above, the interface with other HSE specialists in the fields of fire and construction safety included discussion of the Regulatory Reform (Fire Safety) Order 2005 (Ref. 58) and the Construction (Design and Management) Regulations 2007 (Ref. 59).

# 5 CONCLUSIONS

492 This report presents the findings of the Step 4 Internal Hazards Assessment of the EDF and AREVA UK EPR reactor.

493 To conclude, I am broadly satisfied with the claims, arguments and evidence laid down within the PCSR (Ref. 22) and supporting documentation for internal hazards derived from the Submission Master List (Ref. 18). I consider that from an internal hazards view point, the EDF and AREVA UK EPR design is suitable for construction in the UK. However, this conclusion is subject to satisfactory progression and resolution of GDA Issues to be addressed during the forward programme for this reactor and assessment of additional information that becomes available as the GDA Design Reference is supplemented with additional details on a site-by-site basis.

## 5.1 Key Findings from the Step 4 Assessment

494 The design of the UK EPR is in line with my expectations in relation to current national and international standards, guidance and relevant good practice. There are a number of areas where further internal hazards substantiation is required in order to ensure that the safety case for these specific hazards areas is robust. In addition, concerns have arisen over the approach taken to safety case for internal flooding and the lack of a detailed consequence analysis associated with dropped loads and missile impact.

495 Overall, I believe that, in the majority of areas, the UK EPR PCSR (Ref. 22) has been informed by a thorough and robust analysis of the threats posed by internal hazards coupled with a clear philosophy and logic associated with design.

### 5.1.1 Assessment Findings

496 I conclude that the following Assessment Findings listed in Annex 1 should be programmed during the forward programme of this reactor as normal regulatory business.

### 5.1.2 GDA Issues

497 I conclude that the GDA Issues listed in Annex 2 must be satisfactorily addressed before Consent will be granted for the commencement of nuclear island safety related construction.

## 6 REFERENCES

1 Not used.

2 *ND BMS. Assessment Process.* AST/001 Issue 4. HSE. April 2010. www.hse.gov.uk/foi/internalops/nsd/assessment/ast001.htm

3 *ND BMS. Technical Reports.* AST/003 Issue 3. HSE. November 2009. www.hse.gov.uk/foi/internalops/nsd/assessment/ast003.htm

4 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition Revision 1. HSE. January 2008. TRIM Ref. 2007/44121.

5 *Nuclear power station generic design assessment – guidance to requesting parties.* Version 3. HSE. August 2008. http://www.hse.gov.uk/newreactors/guidance.htm.

*6* *ND BMS. Technical Assessment Guide. Internal Hazards.* T/AST/014 Issue 2. HSE. August 2008. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast014.htm.

7 *ND BMS. Technical Assessment Guide. Diversity, Redundancy, Segregation and Layout of Mechanical Plant.* T/AST/036 Issue 2. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast036.htm.

8 *ND BMS. Technical Assessment Guide. Guidance on the Purpose, Scope and Content of Nuclear Safety Cases.* T/AST/051 Issue 1. HSE. May 2002. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast051.pdf.

9 *Safety of Nuclear Power Plants: Design. Safety Requirements.* International Atomic Energy Agency (IAEA). Safety Standards Series No. NS-R-1. IAEA. Vienna. 2000.

10 *Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants. Safety Guide.* International Atomic Energy Agency (IAEA) Safety Standards Series No. NS-G-1.7. IAEA. Vienna. 2004.

11 *Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants. Safety Guide.* International Atomic Energy Agency (IAEA) Safety Standards Series No. NS-G-1.11. IAEA, Vienna 2004.

12 *Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA Reactor Reference Safety Levels. Issue S: Protection Against Internal Fires.* WENRA. January 2008. http://www.wenra.org.

13 *Step 3 Internal Hazards Assessment of the EDF and AREVA UK EPR*. HSE-ND Assessment Report AR 09/026. November 2009. TRIM Ref. 2009/330030.

14 *EDF and AREVA UK EPR - Schedule of Technical Queries Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600726.

15 *EDF and AREVA UK EPR - Schedule of Regulatory Observations Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600727.

16 *ETC-C (EPR Technical Code for Civil Works) Part 1.* ENGSGC050076 Revision B. EDF. April 2006. TRIM Ref. 2010/404165.

17 *UK EPR Pre-construction Safety Report – November 2009 Submission.* Submitted under cover of letter UN REG EPR00226N. 30 November 2009. TRIM Ref. 2009/481363 and as detailed in UK EPR Master Submission List. November 2009. TRIM Ref. 2011/46364.

18 *UK EPR Master Submission List.* UKEPR-0018-001, Issue 01, EDF and AREVA. November 2011. TRIM Ref. 2011/552512.

19 *EPR Technical Code for fire protection*. ENGSIN050312 Revision B. EDF. August 2009. TRIM Ref. 2010/230212.

20 *EPR – Load drops – Methodology for risk analysis in civil engineering and building installations – Design review preparation conditions.* ECEIG070272 Revision A1. EDF. February 2009. TRIM Ref. 2010/350469.

21 *Step 4 Internal Hazards Assessment Plan for the EDF and AREVA UK EPR*, AR09/054, HSE-ND, April 2010, TRIM Ref. 2009/387625

22 *UK EPR Consolidated Pre-construction Safety Report – March 2011 Submission.* Detailed in EDF and AREVA letter UN REG EPR00997N. November 2011. TRIM Ref. 2011/552663.

23 *Single-Failure Proof Cranes for Nuclear Power Plants*. NUREG-0554, U.S. Nuclear Regulatory Commission, May 1979.

24 *Control of Heavy Loads at Nuclear Power Plants Resolution of Generic Technical Activity A-36*. NUREG-0612, U.S. Nuclear Regulatory Commission, July 1980.

25 *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002*. NUREG-1774, U.S. Nuclear Regulatory Commission, July 2003.

26 Not used.

27 *EPR – Internal Missiles – Methodology description for analysis of layout in the buildings. Conditions for preparing design reviews.* ECEIG070282, Revision A1, EDF, 2006, TRIM Reference 2010/391455.

28 *RCC-M. Design and Construction Rules for Mechanical Components of PWR Nuclear Islands.* 2007 Edition. Published by the French Association for Design, Construction and In-Service Inspection Rules for Nuclear Island Components – AFCEN, Paris. ISBN.

29 *1st stage analysis: consequences of high energy line breaks - safeguard auxiliary and electrical buildings*. ECEF092042 Revision A1. EDF. February 2010. TRIM Ref. 2011/85907.

30 *Functional design relating to PCC treatment of loss of cooling and pool drainage*. ECEF080499 Revision A1. EDF. April 2008. TRIM Ref. 2011/86128.

31 *Principle of Common Mode Fire Risk Analysis,* ENSNEA090055 Revision A. EDF. June 2009. TRIM Ref. 2011/5839.

32 *Safety Requirements for defining Safeguard Auxiliary and Electrical Building Fire Zones*. ECEF070601 Revision B1. EDF. August 2009. TRIM Ref. 2011/85894.

*33* *Safety Requirements for defining Fuel Building Fire Zones*. ECEF071646 Revision B1. EDF. August 2009. TRIM Ref. 2011/85899.

*34* *Safety Requirements for the Establishment of Fire Zoning in the Reactor Building*. ECEF071591 Revision B1. EDF. August 2009. TRIM Ref. 2011/85898.

35 Not used.

36 *Fire Resistant Cable Wraps and Cases in Thermal and Nuclear Power Plants"*, CRT 62.C.010-01, EDF, 2004, TRIM Ref. 2011/93851.

37 *Test specification for electrical cableway protection systems*. ENGSIN040526 Revision A. EDF. June 2009. TRIM Ref. 2011/85568.

38 NF EN 1363 – 1. *Essais de résistance au feu - Partie 1 : exigences générales.* ISO, 2000.

39 BS EN 1363 – 1. *Fire Resistance Tests – Part 1: General Requirements.* British Standards Institution (BSI) 1999.

40 *BS EN 60332 – 3 – 23:. Tests on Electric and optical fibre cables under fire conditions. Test for vertical flame spread of vertically mounted bunched wires or cables – Category B.* British Standards Institution (BSI) 2010.

41 *High Energy Pipe Break: Propagation of degraded ambient conditions in the Nuclear Island*, EZLT/2010/en/0007, Revision B, EDF, April 2010. TRIM Ref. 2011/92982.

42 *Internal Flooding – Layout Analysis Methodology for buildings in the Nuclear Island*. ECEIG040650 Revision C1. EDF. September 2008. TRIM Ref. 2011/92107.

43 *Internal Flooding and Operator Actions*. Letter from ND to UK EPR Project Front Office. EPR70257R. 13 October 2010. TRIM Ref. 2010/516768.

44 *Internal Flooding and Operator Actions*. Letter from UK EPR Project Front Office to ONR. ND(NII) EPR00770N. 09 February 2011. TRIM Ref.2011/104841.

45 *Step 4 Reactor Chemistry Assessment of the EDF and AREVA UK EPR™Reactor*. ONR Assessment Report ONR-GDA-AR-11-024 Revision 0. TRIM Ref. 2010/581508.

46 *Test program for the qualification of the FA3 IRWST filtration system.* NESS-F DC 373 Revision C. Areva. August 2009. TRIM Ref. 2011/92269.

47 *Systems at risk of internal explosion – EPR*. ECEF071213 Revision A1. EDF. December 2007. TRIM Ref. 2011/85895.

48 *Identification of systems and rooms in the EPR nuclear island (BNI) with risk of internal explosion.* EYRL2007fr0036 Revision H1. Sofinel. September 2008. TRIM Ref. 2011/281452.

49 *BS 6133:1995. Code of Practice: Safe operation of lead-acid stationary batteries.* British Standards Institution (BSI) 1995.

50 *Step 4 Electrical Systems Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-023 Revision 0. TRIM Ref. 2010/581509.

51 *UK EPR- MAGIC simulation for one representative safety fire compartment (SCO) and comparison with standard resistance curves without taking credit for active fire protection systems.* ECEIG091608 Revision A. EDF. September 2009. TRIM Ref. 2011/86138.

52 *Regulatory Observation RO-UKEPR-30 and RO-UKEPR-30.A1 – Internal Hazards – Fire Hazard Analysis*. Letter from ND to UK EPR Project Front Office. EPR70135R. 04 January 2010. TRIM Ref. 2010/919.

53 *Internal Hazards – Action RO-UKEPR-35.A1 response plan*. Letter from UK EPR Project Front Office to ND. EPR00155N. 14 August 2009. TRIM Ref. 2009/320395.

54 *RO-UKEPR-035 – Nuclear Significant Hazard Segregation Door Control Measures.* Letter from UK EPR Project Front Office to ND. EPR00173R. 28 September 2009. TRIM Ref. 2009/381718.

55 *RO-UKEPR-035 – Nuclear Significant Hazard Segregation Door Control Measures additional Regulatory Observation Action RO-UKEPR-035.A2*. Letter from UK EPR Project Front Office to ND. EPR00416R. 11 June 2010. TRIM Ref. 2010/260875.

56 *UK EPR – Specification of the Door Monitoring System*. ECUK100261 Revision A. EDF. June 2010. TRIM Ref. 2011/45410.

57 *Closure of Regulatory Observation RO-UKEPR-35 – Internal Hazards – Nuclear Significant Hazard – Segregation Door Control Measures*. Letter from ND to UK EPR Project Front Office. EPR70222N. 28 July 2010. TRIM Ref. 2010/329736.

58 *Regulatory Reform (Fire Safety) Order 2005*. Statutory Instrument No. 1541. Regulatory Reform, England and Wales. June 2005.

59 *Construction (Design and Management) Regulations 2007*. Statutory Instrument No. 320. Health and Safety Executive. February 2007.60 *General Fire Precautions, CDM in Design, Security and Internal Hazards Workshop*. Letter from ND to UK EPR Project Front Office. EPR70274N. 16 December 2010. TRIM Ref. 2010/632420.

60 *General Fire Precautions, CDM in Design, Security and Internal Hazards Workshop*. Letter from ND to UK EPR Project Front Office. EPR70274N. 16 December 2010. TRIM Ref. 2010/632420.

61 *AREVA NP INC. – US EPR Standard Design Certification Application Review Schedule.* Letter from USNRC to AREVA NP Inc, ML 100280792. 16 February 2010. TRIM Ref. 2011/416550.

62 *US NRC Letter, ML 100280792, Resolution of Generic Safety Issue (GSI) – 191, "Assessment of Debris Accumulation on PWR Sump Performance".* Letter from ND to UK EPR Project Front Office, EPR 70295R. 28 February 2011. TRIM Ref. 2011/124941.

63 *Filtration Test studies – Resolution of NRC – GSI191.* Letter from UK EPR Project Front Office, EPR00896N. 27 July 2011. TRIM Ref. 2011/39680064

*64* *Step 4 Fault Studies, Containment and Severe Accidents Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-020 Revision 0. TRIM Ref. 2010/581403.

65 *Step 4 Mechanical Engineering Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-026 Revision 0. TRIM Ref. 2010/581505.

**Table 6**

**Relevant Safety Assessment Principles for Internal Hazards Considered During Step 4**

| SAP No. | SAP Title | Description |
|---|---|---|
| SC.4 | Safety case characteristics | A safety case should be accurate, objective and demonstrably complete for its intended purpose. |
| EKP.3 | Defence in depth | A nuclear facility should be so designed and operated that defence in depth against potentially significant faults or failures is achieved by the provision of several levels of protection. |
| EKP.4 | Safety function | The safety function(s) to be delivered within the facility should be identified by a structured analysis. |
| EKP.5 | Safety Measure | Safety measures should be identified to deliver the required safety function(s). |
| ECS.1 | Safety Categorisation | The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be categorised based on their significance with regard to safety. |
| ECS.2 | Safety classification of structures, systems and components | Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance with regard to safety. |
| EDR.2 | Redundancy, diversity and segregation | Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety. |
| EDR.4 | Single failure criterion | During any normally permissible state of plant availability no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function. |
| ELO.4 | Minimisation of the effects of incidents | The design and layout of the site and its facilities, the plant within a facility and support facilities and services should be such that the effects of incidents are minimised. |

**Table 6**

**Relevant Safety Assessment Principles for Internal Hazards Considered During Step 4**

| SAP No. | SAP Title | Description |
|---|---|---|
| EHA.1 | Identification | External and internal hazards that could affect the safety of the facility should be identified and treated as events that can give rise to possible initiating faults. |
| EHA.3 | Design basis events | For each internal or external hazard, which cannot be excluded on the basis of either low frequency or insignificant consequence, a design basis event should be derived. |
| EHA.4 | Frequency of exceedance | The design basis event for an internal and external hazard should conservatively have a predicted frequency of exceedance in accordance with the fault analysis requirements (FA.5). |
| EHA.5 | Operating conditions | Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition. |
| EHA.6 | Analysis | Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects. |
| EHA.7 | ‘Cliff-edge’ effects | A small change in DBA parameters should not lead to a disproportionate increase in radiological consequences. |
| EHA.10 | Electromagnetic interference | The design of facility should include protective measures against the effects of electromagnetic interference. |
| EHA.13 | Fire, explosion, missiles, toxic gases etc – use and storage of hazardous materials | The on-site use, storage or generation of hazardous materials should be minimised, and controlled and located so that any accident to, or release of, the materials will not jeopardise the establishing of safe conditions on the facility. |
| EHA.14 | Fire, explosion, missiles, toxic gases etc – sources of harm | Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed. |

**Table 6**

**Relevant Safety Assessment Principles for Internal Hazards Considered During Step 4**

| SAP No. | SAP Title | Description |
|---|---|---|
| EHA.15 | Fire, explosion, missiles, toxic gases etc – effects of water | The design of the facility should prevent water from adversely affecting structures, systems and components important to safety. |
| EHA.16 | Fire, explosion, missiles, toxic gases etc – fire detection and fighting | Fire detection and fire-fighting systems of a capacity and capability commensurate with the credible worst-case scenarios should be provided. |
| FA.6 | Fault sequences | For each initiating fault in the design basis, the relevant design basis fault sequences should be identified. |

## Annex 1

## Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

## Internal Hazards – UK EPR

| Finding No. | Assessment Finding | MILESTONE (by which this item should be addressed) |
|---|---|---|
| AF-UKEPR-IH-01 | The Licensee shall provide evidence to support the design change associated with the configuration of the valves, EVU1111VP within Division 1 SAB and EVU4111VP within Division 4 SAB including a demonstration that closure of the valves during normal operations does not have a detrimental effect on the design basis analysis undertaken in support of the safety case. | Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning. |
| AF-UKEPR-IH-02 | The Licensee shall provide evidence to demonstrate how the requirements from analyses associated with common mode failure in the event of fire are captured within future revisions of the safety case given the impact changes may have on the overall safety case. | Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning. |
| AF-UKEPR-IH-03 | The Licensee shall provide evidence to demonstrate that the design of the doors required to open in the event of increased pressure (due to a steam release) will do so at the requisite pressure and thus allow the steam release path to be realised in accordance with the requirements of the safety case. | Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning. |
| AF-UKEPR-IH-04 | The Licensee is required to provide evidence relating to the specification of cables including wrapping and layout to demonstrate that the cables within the cable raceways (HLK/N3403ZL) are able to withstand temperatures of 300$^{o}$C and pressures of up to 2 bar. | Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning. |
| AF-UKEPR-IH-05 | The Licensee shall provide evidence to demonstrate that the design of the doors required to remain intact in the event of increased pressure (due to a steam release) will withstand requisite pressure and ensure that the engineered discharge routes for the steam release to be realised in accordance with the requirements of the safety case. | Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning. |

## Annex 1

## Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

## Internal Hazards – UK EPR

| Finding No. | Assessment Finding | MILESTONE (by which this item should be addressed) |
|---|---|---|
| AF-UKEPR-IH-06 | The Licensee shall provide evidence to demonstrate that the potential for a hydrogen explosion within the Battery Rooms during the most onerous operating conditions has been considered within the UK EPR design. | Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning. |
| AF-UKEPR-IH-07 | The Licensee shall provide evidence to demonstrate that the specification, design and implementation of the door control measures are included within the UK EPR design. | Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning. |

Note: It is the responsibility of the Licensees / Operators to have adequate arrangements to address the Assessment Findings. Future Licensees / Operators can adopt alternative means to those indicated in the findings which give an equivalent level of safety.

For Assessment Findings relevant to the operational phase of the reactor, the Licensees / Operators must adequately address the findings during the operational phase. For other Assessment Findings, it is the regulators' expectation that the findings are adequately addressed no later than the milestones indicated above.

## Annex 2

## GDA Issues – Internal Hazards – UK EPR

### EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

### GDA ISSUE

### SUBSTANTIATION AND ANALYSIS OF THE CONSEQUENCES OF DROPPED LOADS AND IMPACT FROM LIFTING EQUIPMENT INCLUDED WITHIN THE EPR DESIGN

### GI-UKEPR-IH-01 REVISION 2

| | | | |
|---|---|---|---|
| **Technical Area** | **INTERNAL HAZARDS** | | |
| **Related Technical Areas** | Mechanical Engineering<br>Civil Engineering | | |
| **GDA Issue Reference** | **GI-UKEPR-IH-01** | **GDA Issue Action Reference** | **GI-UKEPR-IH-01.A1** |
| **GDA Issue** | Substantiation and analysis of the consequences of dropped loads and impact from lifting equipment included within the EPR design. | | |
| **GDA Issue Action** | Provide substantiation of the nuclear safety significant structures, systems and components vulnerable to dropped load and impact from RS1 and RS2 lifting equipment.<br>It is the expectation of ONR that dropped loads be considered for lifts that may result in nuclear significant consequences. The response should include detailed assessment of potential loads that could be dropped under such conditions and demonstrate that the provisions in place to ensure that the risk to nuclear safety of a load drop or impact is ALARP. Such assessment may include multi-legged arguments which consider the following:<br>• Claims on civil structures.<br>• Additional physical protection.<br>• Limits and conditions on the use of the RS1 and RS2 lifting equipment.<br>• Provision of detailed load path routes avoiding areas of highest nuclear significance.<br>• Measures (both system based and administratively controlled) in place to ensure the potential for impact of the load is minimised.<br>• Any further defence in depth and ALARP measures that could be implemented into the design.<br>• The impact of the changes made to the PCSR relating to the outcome of this substantiation on other safety case submissions submissions.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my expectations.<br>With agreement from the Regulator this action may be completed by alternative means. | | |

## Annex 2

### EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

### GDA ISSUE

### SUBSTANTIATION AND ANALYSIS OF THE CONSEQUENCES OF DROPPED LOADS AND IMPACT FROM LIFTING EQUIPMENT INCLUDED WITHIN THE EPR DESIGN

### GI-UKEPR-IH-01 REVISION 2

| | | | |
|---|---|---|---|
| **Technical Area** | | **INTERNAL HAZARDS** | |
| **Related Technical Areas** | | Mechanical Engineering<br>Civil Engineering | |
| **GDA Issue Reference** | **GI-UKEPR-IH-01** | **GDA Issue Action Reference** | **GI-UKEPR-IH-01.A2** |
| **GDA Issue Action** | Provide a description of the approach taken to treat dropped loads on civil structures, including consideration of the following:<br>• Derivation of design loads.<br>• Analysis methods.<br>• Design rules.<br>• Reliability expectations.<br>• Consistency between ECEIG070272 REV A1 “EPR- Load Drops - Methodology for risk analysis in civil engineering and building installations - Design review preparation conditions” and ETC-C in relation to consideration of Global stability.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my expectations.<br>With agreement from the Regulator this action may be completed by alternative means. | | |

## Annex 2

## EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
## GDA ISSUE
## VERIFICATION AND VALIDATION
## GI-UKEPR-IH-02 REVISION 2

| | | | |
|---|---|---|---|
| **Technical Area** | **INTERNAL HAZARDS** | | |
| **Related Technical Areas** | Structural Integrity<br>Civil Engineering<br>Fault Studies<br>PSA | | |
| **GDA Issue Reference** | **GI-UKEPR-IH-02** | **GDA Issue Action Reference** | **GI-UKEPR-IH-02.A1** |
| **GDA Issue** | Outstanding Verification and Validation for internal flooding, cable routing, high energy line break and missiles forms part of the requisite evidence and will be required in order to demonstrate an adequate internal hazards safety case. | | |
| **GDA Issue Action** | Provide the requisite evidence in the form of the detailed Flamanville 3 verification and validation analysis and/or other supporting documentation in support of the claims and arguments presented within Chapter 13.2 of the PCSR associatedwith internal flooding. The response should include analysis that supports the claims and arguments relating to:<br>• Civil structures (including surface coatings) claimed as flood barriers.<br>• Watertight doors and penetrations including qualification data.<br>• Drains and sumps claimed to prevent damage to nuclear significant SSCs.<br>• Calculations in place to support any claims made on potential water volumes.<br>• Any further defence in depth and ALARP measures that could be implemented into the design.<br>• Any identified design changes and their implementation within the PCSR.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my expectations.<br>With agreement from the Regulator this action may be completed by alternative means. | | |

## Annex 2

## EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
## GDA ISSUE
## VERIFICATION AND VALIDATION
## GI-UKEPR-IH-02 REVISION 2

| | | | |
|---|---|---|---|
| **Technical Area** | **INTERNAL HAZARDS** | | |
| **Related Technical Areas** | Structural Integrity<br>Civil Engineering<br>Fault Studies<br>PSA | | |
| **GDA Issue Reference** | **GI-UKEPR-IH-02** | **GDA Issue Action Reference** | **GI-UKEPR-IH-02.A2** |
| **GDA Issue Action** | Provide the requisite evidence in the form of the detailed Flamanville 3 verification and validation analysis and/or other supporting documentation in support of the claims and arguments presented within Chapter 13.2 of the PCSR associated with the routing of electrical cables within the EPR design in order to prevent a single fire resulting in loss of more than one divisional separation group.<br>The response should include analysis that supports the claims and arguments relating to:<br>• The routing and identification of protected cable trays.<br>• Justification of claims and arguments made relating to geographical separation.<br>• The provision of passive protection applied to cables and cable trays specifically.<br>• Any further defence in depth and ALARP measures that could be implemented into the design.<br>• Any identified design changes and their implementation within the PCSR.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my expectations.<br>With agreement from the Regulator this action may be completed by alternative means. | | |

## Annex 2

## EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
## GDA ISSUE
## VERIFICATION AND VALIDATION
## GI-UKEPR-IH-02 REVISION 2

| | | | |
|---|---|---|---|
| **Technical Area** | **INTERNAL HAZARDS** | | |
| **Related Technical Areas** | Structural Integrity<br>Civil Engineering<br>Fault Studies<br>PSA | | |
| **GDA Issue Reference** | **GI-UKEPR-IH-02** | **GDA Issue Action Reference** | **GI-UKEPR-IH-02.A3** |
| **GDA Issue Action** | Provide the requisite evidence in the form of the detailed Flamanville 3 verification and validation analysis, specifically, the FA3 1st Stage Pipe Break Analysis and/or other supporting documentation in support of the claims and arguments presented within Chapter 13.2 of the PCSR associated with high energy line break (HELB) within the EPR design. The response should include analysis that supports the claims and arguments relating to:<br>• Consequence analysis, where applicable.<br>• Break preclusion.<br>• Identification and qualification of physical restraints, barriers and doors.<br>• Identification and qualification of pressure relief panels/routes.<br>• Any further defence in depth and ALARP measures that could be implemented into the design.<br>• Any identified design changes and their implementation within the PCSR.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my expectations.<br>With agreement from the Regulator this action may be completed by alternative means. | | |

## Annex 2

## EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
## GDA ISSUE
## VERIFICATION AND VALIDATION
## GI-UKEPR-IH-02 REVISION 2

| | | | |
|---|---|---|---|
| **Technical Area** | **INTERNAL HAZARDS** | | |
| **Related Technical Areas** | Structural Integrity<br>Civil Engineering<br>Fault Studies<br>PSA | | |
| **GDA Issue Reference** | **GI-UKEPR-IH-02** | **GDA Issue Action Reference** | **GI-UKEPR-IH-02.A4** |
| **GDA Issue Action** | Provide the requisite evidence in the form of the detailed Flamanville 3 verification and validation analysis and/or other supporting documentation in support of the claims and arguments presented within Chapter 13.2 of the PCSR associated with internal missiles. The response should include analysis that supports the claims and arguments relating to:<br>• Identification of all potential sources of internal missile which could result in a threat to nuclear safety significant SSCs.<br>• Consequence analysis, where applicable.<br>• Break preclusion.<br>• Identification and qualification of physical restraints, barriers and doors.<br>• Any further defence in depth and ALARP measures that could be implemented into the design.<br>• Any identified design changes and their implementation within the PCSR.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my expectations.<br>With agreement from the Regulator this action may be completed by alternative means. | | |

## Annex 2

## EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
## GDA ISSUE
## INTERNAL FLOODING SAFETY CASE
## GI-UKEPR-IH-03 REVISION 2

| | | | |
|---|---|---|---|
| **Technical Area** | **INTERNAL HAZARDS** | | |
| **Related Technical Areas** | Human Factors<br>Civil Engineering<br>Environment Agency | | |
| **GDA Issue Reference** | **GI-UKEPR-IH-03** | **GDA Issue Action Reference** | **GI-UKEPR-IH-03.A1** |
| **GDA Issue** | The internal flooding claims stated within the PCSR appear inconsistent with the deterministic approach to the analysis of potential sources of internal flooding. | | |
| **GDA Issue Action** | Please provide adequate substantiation of the internal flooding safety case through a deterministic analysis that initally assumes an unmitigated flood source and applies a multi-legged argument that may include consideration of the following:<br>• Potential failure mechanisms of water based systems.<br>• Civil engineering aspects including barriers and drainage.<br>• Systems (both engineered and administrative) to ensure that the effects of an internal flooding event are limited to loss of one division.<br>• Any further defence in depth and ALARP measures that could be implemented into the design.<br>• The impact of the changes made to the PCSR relating to the outcome of this substantiation on other safety case submissions such as civil engineering and human factors.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my expectations.<br>With agreement from the Regulator this action may be completed by alternative means. | | |

## Annex 2

## EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

## GDA ISSUE

## CONSEQUENCES OF MISSILE GENERATION ARISING FROM FAILURE OF RCC-M COMPONENTS

## GI-UKEPR-IH-04 REVISION 2

| | | | |
|---|---|---|---|
| **Technical Area** | | **INTERNAL HAZARDS** | |
| **Related Technical Areas** | | Structural Integrity<br>Civil Engineering<br>Fault Studies | |
| **GDA Issue Reference** | **GI-UKEPR-IH-04** | **GDA Issue Action Reference** | **GI-UKEPR-IH-04.A1** |
| **GDA Issue** | Consequences of missile generation arising from failure of RCC-M Components. | | |
| **GDA Issue Action** | Provide substantiation of the claims made within the PCSR associated with the preclusion of missile generation from failure of RCC-M components which are not designated as High Integrity Components (HIC) as defined in the consolidated PCSR. This could be undertaken through detailed analysis of the consequences of failure. The detailed analysis should include consideration of:<br>• Identification of those potential sources of internal missile which could result in a threat to nuclear safety significant SSCs.<br>• Analysis of the consequences of failure.<br>• Passive features such as barriers and restraints.<br>• Examination, maintenance, inspection, and testing as a potential part of a multi-legged safety justification for missiles.<br>• Any further defence in depth and ALARP measures that could be implemented into the design.<br>• Any identified design changes and their implementation within the PCSR.<br>• The impact of the changes made to the PCSR relating to the outcome of this substantiation on other safety case submissions such as civil engineering and mechanical engineering.<br>The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of ONR expectations.<br>With agreement from the Regulator this action may be completed by alternative means. | | |