Health and Safety Executive

NUCLEAR DIRECTORATE

GENERIC DESIGN ASSESSMENT – NEW CIVIL REACTOR BUILD

STEP 3 INTERNAL HAZARDS ASSESSMENT OF THE EDF and AREVA UK EPR

DIVISION 6 ASSESSMENT REPORT NO. AR 09/026-P

HSE Nuclear Directorate
Redgrave Court
Merton Road
Bootle
Merseyside L20 7HS

EXECUTIVE SUMMARY

This reports presents the findings of the Internal Hazards Assessment of the EDF and AREVA UK EPR Pre-Construction Safety Report (PCSR) (Ref. 1) undertaken as part of Step 3 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process.

This internal hazards assessment report for the UK EPR provides an overview of the safety case in the form of the PCSR as produced by EDF and AREVA, the standards and criteria adopted in the assessment undertaken by the Health and Safety Executive (HSE) Nuclear Directorate (ND) and an assessment of the claims, arguments and evidence provided within the safety case based upon those standards and criteria.

It is important to recognise that ND is currently part way through the GDA process and the intent of this Step 3 assessment is to provide an interim position statement regarding the assessment currently being undertaken.

This report has taken into consideration the findings of the Step 2 Internal Hazards Assessment of the UK EPR (Ref. 2) and has confirmed that the issues contained therein have been addressed within Step 3 and have been satisfactorily resolved with the exception of areas where further assessment work has been specifically identified.

The principal claims and arguments associated with internal hazards are related to redundancy and segregation of plant and equipment important to nuclear safety. The redundancy is achieved through physical segregation of each of the four trains of protection with each train able to provide 100% of the safety duty to enable safe shutdown and post-trip cooling. There are areas where full segregation has not been achieved; in these situations claims and arguments have been presented relating to the application of additional passive protection and the use of geographical distance to separate the trains. The sampling undertaken of the EDF and AREVA UK EPR PCSR relating to internal hazards assessment has been on the examination of the claims and arguments associated with ensuring segregation of plant and equipment important to safety with particular focus on the nuclear fire safety aspects of the PCSR recognising fire as a significant contributor to the design of the facility.

Two Regulatory Observations / Regulatory Observation Actions (ROs / ROAs) have been raised of which ND have received satisfactory responses for one.

To conclude, I am satisfied with the claims and arguments as laid down within the current PCSR and other supporting submission case documents. There are a number of areas of further detailed assessment required to be undertaken during Step 4 to provide ND with confidence that an adequate safety case can be made for the construction and operation of the EDF and AREVA UK EPR within the UK and within the UK Regulatory Regime.

LIST OF ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
BMS	(Nuclear Directorate) Business Management System
C&I	Control & Instrumentation
CRHRS	Containment Residual Heat Removal System
EA	The Environment Agency
EDF and AREVA	Electricité de France SA and AREVA NP SAS
EMI	Electro-Magnetic Interference
EOP	Emergency Operating Procedures
ETC	EPR Technical Code
GDA	Generic Design Assessment
HSE	The Health and Safety Executive
IAEA	The International Atomic Energy Agency
IRWST	In-containment Refuelling Water Storage Tank
LOCA	Loss of Coolant Accident
MSLB	Main Steam Line Break
ND	The (HSE) Nuclear Directorate
NSSS	Nuclear Steam Supply Systems
PCC	Plant Condition Category
PCER	Pre-construction Environment Report
PCSR	Pre-construction Safety Report
PID	Project Initiation Document
RO	Regulatory Observation
ROA	Regulatory Observation Action
RI	Regulatory Issue
RIA	Regulatory Issue Action
RP	Requesting Party
SAP	Safety Assessment Principle
SIS	Safety Injection System
SSC	System, Structure and Component
TAG	(Nuclear Directorate) Technical Assessment Guide
TQ	Technical Query
WENRA	The Western European Nuclear Regulators' Association

TABLE OF CONTENTS

1 INTRODUCTION

1 This report presents the findings of the internal hazards assessment of the EDF and AREVA UK EPR Pre-Construction Safety Report (PCSR) undertaken as part of Step 3 of the Generic Design Assessment (GDA) process. This assessment has been undertaken in line with the requirements of the Business Management System (BMS) document AST/001 (Ref. 3) and its associated guidance document G/AST/001 (Ref. 4). AST/001 sets down the process of assessment within the Health and Safety Executive (HSE) Nuclear Directorate (ND) and explains the process associated with sampling of safety case documentation. The Safety Assessment Principles (SAP) (Ref. 5) have been used as the basis for the assessment of the internal hazards associated with UK EPR design. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

2 The scope of the Internal Hazards Assessment is detailed within the Project Initiation Document (PID), GDA Phase 1 – Steps 3 and 4 Internal Hazards Assessment Strategy (Ref. 5a). The PID states that Step 3 is a review of the safety aspects of the proposed reactor designs by undertaking an assessment primarily at the system level and assessment of the supporting arguments made in the Requesting Party's (RP) PCSR.

3 This Internal Hazards Assessment report for the UK EPR provides an overview of the safety case in the form of the PCSR as produced by EDF and AREVA, the standards and criteria adopted in the assessment undertaken by ND and an assessment of the claims, and arguments provided within the safety case based upon those standards and criteria. The structure of this assessment report is in accordance with the requirements of the BMS standard on assessment reports (Ref. 6) taking due cognisance of the guidance within the BMS relating to assessment report production (Ref. 7).

4 It is important to recognise that ND is currently part way through the GDA process and the intent of this Step 3 assessment is to provide an interim position statement regarding the assessment currently being undertaken.

2 NUCLEAR DIRECTORATE'S ASSESSMENT

2.1 Requesting Party's Case

5 The PCSR for the UK EPR 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.

6 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.

7 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.

8 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.

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

10 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 against 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 an frequency of occurrence within the range of 10^{-6} to 10^{-4} per year.

11 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.

12 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.

13 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 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.

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

2.1.1 Nuclear Fire Safety

15 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.

16 A key reference of the PCSR for the fire safety design is the EPR Technical Code for Fire Protection (ETC-F) (Ref. 29). 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.

17 The safety objective for fire protection is to ensure that the safety functions are performed in the event of a fire inside the installation, where the fire has the same characteristics as the reference fire.

18 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.

19 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.

20 Fires could also occur as a consequence of other internal or external hazards e.g. fire induced Loss of Coolant Accident (LOCA) and severe accidents due to the potential to release hydrogen into the Containment, earthquake induced fires, and the effects of extreme cold on fire protection equipment claimed as part of the safety case.

21 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.

22 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.

23 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.

2.1.1.1 Fire Consequences

24 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.

25 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.

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

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

2.1.1.2 Principles of the Fire Protection Approach

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

29 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.

2.1.1.3 Design Basis for Nuclear Fire Safety

30 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.

31 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.

32 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.

33 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.

34 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.

35 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 1: 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

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

37 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.

38 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.

39 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.

2.1.2 Internal Flooding

40 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.

41 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 and 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.

42 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 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 considered as this originates on site but there is a need to consider the impact of this event with the heat sink water levels and as a result this specific flooding hazard is assessed together with external flooding.

43 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).

44 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.

45 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.

46 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.

47 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.

48 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 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 building drainage system is pessimistically considered to be required for draining water from the respective sump pumps.
- 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.
- In general, the doors are not watertight. Exceptions are specific watertight doors for the Heat Removal System (RIS/ RRA) rooms.
- The flood barriers for safety-classified equipment are taken into consideration.

49 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.

50 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.

51 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.

52 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.

53 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.

2.1.2.1 Design Verification for Internal Flooding

54 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.

55 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.

56 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.

57 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.

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

2.1.3 Dropped Load and Impact

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

60 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.

61 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.

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

63 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).

2.1.3.1 Design Basis for Dropped Loads and Impact

64 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.

65 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.

66 The consequences 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.

67 The associated lifting device is 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.

68 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.

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

70 All other lifting devices are not safety classified.

71 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.

72 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.

73 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.

74 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.

75 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.

76 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.

77 In addition, unintentional travel above critical areas with heavy loads is prevented by means of interlocks.

2.1.3.2 Design Verification for Dropped Loads and Impact

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

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

79 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.

80 Assessments are also made against the most onerous plant conditions. 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.

2.1.4 Missile Generation

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

82 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.

83 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.

84 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.

85 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).

86 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 external locations.

87 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.

88 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

89 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.

90 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.

91 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.

92 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.

93 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.

94 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.

95 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 a turbine disintegration.

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

2.1.5 Internal Explosion

97 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.

98 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.

99 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.

100 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.

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

102 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.

103 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.

104 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.

105 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.

2.1.5.1 Design Basis - Internal Explosion

106 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.

107 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 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.

108 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.

109 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.

2.1.6 Pipework Leaks and Breaks

110 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.

111 For leaks and breaks in 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.

112 For leaks and breaks in 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).

113 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 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.

114 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 against the effects of pipework failure.

115 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.

116 For moderate energy pipework:

- Flooding.
- Radiation.

117 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.

2.1.6.1 Design Verification for Pipework Leaks and Breaks

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

119 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.

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

121 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.

122 Protection requirements must be defined to determine the maximum acceptable effect to 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.

123 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.

124 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 SIS trains, the 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.

125 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, Safeguards Buildings (including the main steam and feedwater valve compartments) and the Fuel Building.

126 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.

127 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.

2.2 Nuclear Directorate Standards and Criteria

128 The SAPs have been used as the basis for the assessment of the internal hazards associated with UK EPR design. The guidance contained within the SAPs considers that internal hazards on a nuclear power plant or nuclear chemical plant site be identified and

addressed in safety assessments. Internal hazards are those hazards to plant and structures such as fire, explosions, release of hazardous material or gas, flooding etc. which originate within the site boundary, but external to the process in the case of nuclear chemical plant or primary circuit in the case of power reactors. The SAPs define internal and external hazards as:

"Internal hazards are those hazards to plant and structures that originate within the site boundary but are, for example, external to the process in the case of nuclear chemical plant, or external to the primary circuit in the case of power reactors. That is, the duty holder has control over the initiating event in some form. Internal hazards include internal flooding, fire, toxic gas release, dropped loads and explosion / missiles."

129 The guidance within the SAPs considers that the risk from hazards be minimised by attention to plant layout, by keeping inventories of flammable materials and toxic substances to a minimum, and through other good safety management practices. In addition adequate provision against the effects of fire, steam release and missiles affecting safety systems both internal and external to the reactor building and turbine hall should be considered. The key SAPs relevant to the assessment of the Westinghouse AP1000 design are contained within Table 1 of this report.

130 There is additional guidance detailed within ND internal guidance for assessment, specifically the Technical Assessment Guide (TAG) T/AST/014 (Ref. 8) on Internal Hazards.

131 In addition to internal guidance there is also relevant good practice contained within nuclear specific international guidance that is used as a means to inform the judgment and as a means to assess adequacy of the design e.g. international guidance produced by the International Atomic Energy Agency (IAEA) and the Western European Nuclear Regulator's Association (WENRA).

2.3 Nuclear Directorate Assessment

132 The approach to the structure of this assessment report for Step 3 was to first confirm, or otherwise, that the observations made during Step 2 of the GDA process had been addressed or adequately captured through further technical queries, regulatory observations or through the continuation of the assessment into Step 4. The outcome of this assessment is contained within Section 2.3.1. Secondly, there was a need to undertake internal hazards assessment on the claims, arguments and evidence contained within the PCSR and other supporting documents that had been produced by EDF and AREVA as part of the safety demonstration for Steps 3 and 4 of the GDA process. This assessment is contained within Section 2.3.2 – 2.3.8 and is concluded within Section 3.

133 It is important to stress that not all areas have been assessed to the same extent due to the sampling nature of the assessment and due to the limited detailed information contained within the PCSR as there are areas where detailed claims and arguments are yet to be presented.

2.3.1 Assessment of Observations made during Step 2

134 Twelve observations were made within the UK EPR Internal Hazards Assessment carried out for Step 2 of the GDA Process. Each of the observations is addressed specifically and details of the further ND assessment is provided against each. At the time these observations were raised a PCSR had not been produced for the UK EPR and as a result the observations were sourced from the fundamental safety overview documentation

provided as part of the Step 2 process, hence some of the RP answers now direct a great deal of the responses to content within the PCSR Revision 1 (Ref. 9).

"O1. Information will be required on the methodology used to identify internal hazards."

135 A Technical Query (TQ) (TQ-EPR-014) (Ref. 10) was raised as part of the assessment specifically requesting EDF and AREVA to provide further information relating to the methodology use to identify internal hazards.

136 Three partial responses have been provided by the RP; the first response detailed a commitment to provide the response in two parts. The RP agreed to provide the following additional information:

- A more detailed description of the UK EPR hazards design principles including:
  - i) A description of the approach to achieve segregation, including use of 3D modelling of plant layout.
  - ii) A description of the design measures to minimise the frequency of occurrence and magnitude of hazards.
  - iii) A statement of the timescale on which a room-by-room hazards assessment would be available for the Flamanville-3 (FA3) EPR.

137 The first partial response (Ref. 11) committed to providing the information within part (a) by November 2008 and stated that the room-by-room hazards assessment as detailed within part (b) would not be available for FA3 until 2010 as it requires the design and layout to be largely complete. The TQ response recognised that this was to be a specific FA3 document and as such not formally submitted to ND for assessment, but be provided for information to aid the internal hazards assessment. I am satisfied with the approach taken to part (b) as there will be undoubtedly subtle changes in the approach taken to the design and installation, however, there is value in understanding the methodology applied to the room-by-room assessment hence why the document is to be provided as a means to further inform my assessment during Step 4.

138 The second partial response (Ref. 12) further addressed at part (a) and provided an overview of many of the aspects of the EPR design relating to the segregated approach to the trains of protection and their resistance to the impact of internal hazards due to the physical segregation and geographic separation applied. There was further information provided relating to the need to avoid installation of any component of a safety train within a foreign division i.e. a different division to the function that the component is serving. In addition, it was stated that each train is designed to be as independent as possible from the other trains and that only inter-divisional connections that are necessary from a safety, reliability or operational point of view are implemented. Whenever such interconnections exist there is a need for them to be passive i.e. closed during normal operation. There is further information contained within the second partial response relating to the UK EPR mechanical, electrical, and instrumentation and control system design as well as details of the specific design requirements and provisions for addressing internal hazards within these system areas.

139 The approach taken to ensuring that the four train design is adequately protected against the effects of internal hazards is through verification that all safety classified functions are correctly protected from internal hazards in the final design. The verification rules are specific to each internal hazard and specified within methodology reports which have been provided for high energy pipe leaks and breaks (Ref. 13), internal flooding – layout analysis methodology (Ref. 14), fire analysis methodology (Ref. 15) and the internal explosion hazard methodology (Ref. 16). References 13 and 14 were provided with the second response and References 15 and 16 were provided with the third partial response

(Ref. 17) along with the a commitment to provide two additional methodology documents, namely, the dropped loads methodology and the internal missiles methodology which are to be provided prior to the end of Step 3.

140 The ND assessment to date has concentrated on hazard identification within the second TQ response together with the four supporting methodology documents that have been provided. The remaining two documents will be assessed when they are issued formally to ND for assessment. I have assessed the information contained within the partial response to TQ-EPR-014 and am satisfied with the methodology and approach that has been taken to identify internal hazards as part of the design for UK EPR for the areas for which information has been provided, however, there will be a need to confirm that the methodology applied to the identification of dropped loads and internal missiles is adequate. 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.

141 The response is currently a partial response due to the need for EDF and AREVA to provide two additional documents relating to the dropped loads methodology and the internal missiles methodology. As a result this observation and subsequent TQ has yet to be fully resolved and therefore, the TQ remains as a 'partial response'.

"O2. Justification will be required for the completeness of the internal hazards listing."

142 A technical query (TQ-EPR-015) (Ref. 18) was raised as part of the assessment specifically requesting EDF and AREVA to provide information justifying the completeness of the internal hazard listing.

143 A full response to this TQ was received on the 27/02/2009 (Ref. 19) which provided evidence of the range of internal hazards covered as part of the EPR design and highlighted Sub-Chapter 3.1 of the PCSR relating to the *"Hazards Identification for the EPR Design"*.

144 The internal hazards listed within Sub-Chapter 3.1 of the PCSR (Ref. 20) are:

- Fire.
- Internal flooding.
- Fractures (of piping, tanks, pumps and valves).
- Internal missiles.
- Internal explosions (including steam explosions).
- Dropped loads and impact.

145 EMI has not been included within the internal hazards listing as this hazard has been included within the PCSR sub-section 7.2 relating to the C&I design of the EPR.

146 Hazardous substances, e.g. toxic and flammable gases, oxidisers etc. are included within sub-chapter 13.2 of the PCSR Issue 2 in relation to explosion risks from the conventional island and from gas storage facilities and noxious substances as a result of fire. The storage of hazardous materials is presented in the Pre-Construction Environment Report (PCER) sub-chapter 3.3 (Ref. 21).

147 This approach is consistent with the HSE SAPs which states within EHA.14 that, *"Sources that could give rise to fire, explosion, missiles, toxic gas, 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."*

148 I have assessed the information relating to the completeness of the internal hazards listing provided within the PCSR and am satisfied that all the potential internal hazards

that could have an impact on nuclear safety have been identified. I am also content that EMI and hazardous substances are to be contained within submissions that have greater relevance to the particular hazard, however, this does not rule out detailed assessment of these two specific areas as part of the assessment within Step 4.

"O3. Information will be required on the most adverse normal operating condition used in the internal hazards analysis."

149 A technical query (TQ-EPR-016) (Ref. 22) was raised as part of the assessment requesting EDF and AREVA to provide information on the most adverse operating condition used in the internal hazards analysis.

150 A full response to this TQ was received on the 31/03/2009 (Ref. 23). This response detailed that the initial conditions for analysis for internal hazards are considered within sub-chapter 13.2 of the PCSR and provided clarification that for hazards not associated with a PCC, initial event conditions considered are normal operating conditions as the initial plant state is not relevant to the modelling of the hazard. Normal operating conditions include the range of operations including normal at-power operation, start-up and shut-down operation, maintenance, testing and refuelling operation. For hazards resulting from a PCC event, the initial condition assumed is the Limiting Condition for Operation (LCO) appropriate to the PCC analysis.

151 In addition, the PCSR recognises that there is the potential for fire to occur during the post accident phase – in the event of a PCC 2-4 event this is after the controlled state has been reached and in the event of an RRC A or B event two weeks later. Fire occurring within this two week period is considered to be a fire which is independent of the RRC, PCC, or seismic event.

152 This approach is consistent with the HSE SAPs which states within EHA.5 that, *"Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition".* I am, therefore, satisfied that the RP has fully addressed the requirements of this TQ.

"O4. Information will be required on specific combinations of internal hazards and faults included in the internal hazards analysis."

153 A technical query (TQ-EPR-017) (Ref. 24) was raised as part of the assessment requesting EDF and AREVA to provide information on the specific combinations of internal hazards and faults included in the internal hazards analysis.

154 A full response to this TQ was received on the 31/03/2009 (Ref. 25). This response states that specific combinations of internal hazards and PCC / RRC faults is provided within sub-chapter 13.2 of the PCSR as well as within an EDF report relating to the inventory of combined events with internal faults and / or other (internal / external) hazards taken into account in the design (Ref. 26). The PCSR addresses internal hazards that could trigger a PCC2 event, the prevention of an internal hazard to trigger a PCC3 / 4 event and the potential consequential internal hazards arising from PCC3 / 4 or RRC events e.g. the consequential effects of a LOCA or Main Steam Line Break (MSLB) associated with steam release, pipe whip, jet impingement etc. Other combinations of internal hazard events with plant generated faults addressed within the PCSR include:

- Internal missiles - Generation of internal missiles resulting from PCC events e.g. control rod ejection or RCP failures. The failure is analysed both from a thermal-hydraulic and / or radiological perspective (PCC accident analysis) as well as from an internal hazard perspective associated with the generation of missiles.
- Dropped loads – The lifting equipment is designed such that on loss of power there is no potential for a dropped load.

- Internal explosion – Hydrogen release in the event of a LOCA or during severe accidents (RRC-B) is considered and design provisions are taken e.g. the installation of passive auto-catalytic re-combiners in containment. This analysis has been done as part of the accident analysis rather than the internal hazards assessment, however, the potential for further detailed assessment of hydrogen explosions within containment will be considered within Step 4.
- Internal fires – As already stated within Section 2.1.1., the PCSR considers fires to occur during a PCC2-4 event after a controlled state has been reached and considers the potential for an independent fire to occur at least two weeks after an RRC event.
- Internal flooding – Internal flooding resulting from PCC or RRC events that result in steam or water release is considered within the PCSR.

155 Ref. 26 considers specific hazard combinations where there have been specific dependencies identified between an internal hazard and a fault or when there is no design provision that allows the hazard combination to be discounted.

156 The HSE SAPs state within EHA.6 that, *"Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects"*. The RP has taken into account simultaneous effects and consequential effects within the TQ response and associated references. Defence in depth and common cause failure had already been considered within the fundamental safety overview document and have subsequently been addressed in detail within the PCSR.

157 I am satisfied that this observation has been satisfactorily addressed, and there is further assessment of the claims made within this report relating to the PCSR.

"O5. Justification will be required for the adequacy of fire barriers. This should include: a justification of the fire severity and the fire barrier resistance, the designation of an appropriate safety categorisation and safety classification which reflects the barriers role with regard to safety and the measures for the control and design of penetrations."

158 A technical query (TQ-EPR-018) (Ref. 27) was raised as part of the assessment identifying the need for a Fire Hazards Analysis (FHA) and to provide information justifying the adequacy of the fire barriers.

159 A full response to this TQ was received on the 11/07/2008 (Ref. 28). This response states that fire barrier resistance requirements are stated within the EDF Technical Code for Fire (ETC-F) (Ref. 29) and refers to the methods by which barriers (including penetrations through the barriers) are controlled through administrative controls associated with combustible inventories and maintenance aspects undertaken. This response did not satisfy the requirements of the TQ and as a result further assessment has been done as part of the Step 3 assessment, the outcome of which is detailed within Section 2.3.2.1 of this report.

"O6. Justification will be required for the adequacy of the fire protection systems that are required to fulfil a safety role. This should include the designation of an appropriate safety categorisation and safety classification which reflects the system's role with regard to safety."

160 A technical query (TQ-EPR-019) (Ref. 30) was raised as part of the assessment requesting EDF and AREVA to provide information to justify the adequacy of the fire protection systems that are required to fulfil a safety role.

161 A full response to this TQ was received on the 20/02/2009 (Ref. 31). This response states that the objectives for fire protection is to ensure that the identified safety functions

can be met in the event of a reference fire within the installation and cites three cases where the fire protection systems installed are required for safety, namely:

- For a safety fire compartment to ensure the integrity of the barriers if the time / severity of the fire exceeds the capability of the compartment.
- At boundaries of the fire cells where the FHA (part of the vulnerability analysis) indicates that fire fighting systems are needed to ensure the integrity of the of safety functions.
- For a fire containment compartment to prevent the release of radioactive or toxic materials.

162 To provide defence in depth, portable fire fighting equipment is installed but no credit is taken for these systems within the UK EPR safety case.

163 The approach taken within point (a) regarding the use of fire protection systems to supplement the fire compartment integrity is not in line with current relevant good practice stated within the IAEA guide for the design of nuclear power plants, NS-G-1.7 (Ref. 32) which states within Section 3.9, *"The fire resistance rating of the barriers should be sufficiently high that total combustion of the fire load in the compartment can occur (i.e. total burnout) without breaching the barriers."*. This shortfall has been raised in the form of a Regulatory Observation (RO) (RO-UKEPR-30) (Ref. 33) and an associated Regulatory Observation Action (ROA) (Ref. 34) which is addressed within the nuclear fire safety assessment contained within this assessment report.

"O7. The use of any fire models should be justified and include appropriate validation and verification studies."

164 A technical query (TQ-EPR-020) (Ref. 35) was raised as part of the assessment requesting EDF and AREVA to provide information to justify the use of any particular fire models, including verification and validation, used as part of the safety case for the UK EPR design.

165 A full response to this TQ was received on the 31/03/2009 (Ref. 36). This response states that modelling of fire propagation and fire loading for FA3 is carried out using the EDF MAGIC code. There is reference to the qualification of the code as well as to the mathematical model within the TQ. No assessment of these reports has been undertaken as MAGIC is a well known fire modelling code that has been used in nuclear facilities since its issue by EDF in November 2005. In addition, ND have been involved in independent verification and validation work that was done on MAGIC through the International Collaborative Fire Modelling Project (ICFMP) which ultimately culminated with the production of NUREG 1824 produced by the Electric Power Research Institute (EPRI) (Ref. 37). I am satisfied therefore, that there is adequate verification and validation of the EDF MAGIC fire modelling code and that the TQ has been adequately addressed by EDF and AREVA.

"O8. Justification will be required for any exceptions to the strategy separating the redundant trains of safety related equipment with fire/hazard barriers."

166 A technical query (TQ-EPR-021) (Ref. 38) was raised as part of the assessment requesting EDF and AREVA to provide information to justifying any exceptions to the strategy of separating redundant trains of safety-related equipment with fire / hazard barriers.

167 A full response to this TQ was received on the 27/02/2009 (Ref. 39). This response states that the general safety approach is to use fire compartments to separate redundant trains of protection (fire containment approach), however, this cannot be achieved in all cases as there are areas where it is not possible to physically segregate the redundant

trains of protection. The two main areas where the fire containment approach cannot be adopted is within the Containment and the Annulus of the Reactor Building. As a result the Reactor Building is split into four cells which are then subjected to a vulnerability analysis. Fire propagation between cells is prevented by utilising a separation distance of 4 metres with no intervening combustibles coupled with the use of physical fire protection (cable wraps) where necessary. In addition the main cable connections in the Annulus are also protected by sprinkler systems. I am satisfied that the response address the observations made within the TQ.

"O9. Information will be required on the application of the defence in depth philosophy (prevention, limiting severity and limiting consequences) to internal hazards."

168 A technical query (TQ-EPR-022) (Ref. 40) was raised as part of the assessment requesting EDF and AREVA to provide information relating to the application of the defence in depth philosophy (prevention, limiting severity and limiting consequences) to internal hazards.

169 A full response to this TQ was received on the 30/04/2009 (Ref. 41). This response states that the approach taken in the general design of the UK EPR comprises of five levels of defence in accordance with the IAEA requirements document, Safety of Nuclear Power Plants: Design (Ref. 42) and the SAPs:

- Prevention of abnormal operation and system failures.
- Detection and control of abnormal operation and system failures and prevent them from escalating to faults.
- Control of faults within design basis.
- Control of severe plan conditions, including prevention of accident progression and mitigation of the consequences of severe accidents.
- Mitigation of radiological consequences of significant releases of radioactive substances.

170 This approach to defence in depth for internal hazards is applied to the design of the UK EPR. The provisions taken for defence in depth for Levels 4 and 5 of internal hazards are the same as that applied for initiating events with Level 4 focussing on the mitigation of core melt and protection of the containment function and Level 5 dealing with the protection of the public against radiological consequences and as a result are therefore addressed within the safety case for UK EPR. The defence in depth approach for internal hazards can, therefore, be summarised as:

- Prevent the hazard.
- Limit the severity of the hazard should it occur e.g. detection and suppression.
- Limit the consequences of the hazard should it occur and be severe, within the design basis.

171 Some of the key measures in place for the UK EPR extracted from the PCSR were included within the response to the TQ. Examples of how the design meets the principle of defence in depth are:

172 **Prevention:** For all safety classified SSCs, stringent and conservative design, manufacturing and installation requirements are applied in order to ensure a very high reliability and prevent failure. This is complimented with a maintenance and in-service inspection and testing program in order to maintain the high level of reliability throughout the life of SSCs.

173 **Prevention:** Sources of initiation of internal hazards are minimised as far as is reasonably practicable and the organisation of plant operations aims to minimise the hazard risks through management of combustible materials, operation of lifting devices, controls on work undertaken associated with the generation of hazards, etc.

174 **Prevention:** In some cases, measures taken to prevent an internal hazard are sufficient and allow the occurrence of the hazard to be discounted (i.e. drop load from lifting devices with 'higher requirements'), and no further measures are taken in next steps of defence in depth.

175 **Limit Severity:** The installation of non-safety classified SSCs in safety classified buildings and in the vicinity of safety equipment is limited to the minimum extent reasonably practicable, so that failure of non-safety SSCs does not result in damage to safety related SSCs. Exceptions are dealt with on a case-by-case basis and additional measures are implemented, if required.

176 **Limit Severity:** Failure detection systems are designed in order to detect early a failure or hazard (fire, flooding etc.), so that automatic actions can mitigate the hazard at an early stage e.g. fire suppression systems and automatic operation of barrier doors and dampers.

177 **Limit Consequence:** Internal hazards are considered in a conservative way in the design process, so that consequences of a hazard remain within plant design basis.

178 **Limit Consequence:** Physical and geographical separation between safety divisions ensures that an internal hazard occurring within one division will not propagate to, or cause damage in, other safety divisions.

179 **Limit Consequence:** Safety systems and emergency operating procedures are used to mitigate the consequences of an internal hazard. These allow the plant to be kept within design basis conditions, and allow a long term safe state to be reached.

180 The approach taken with the UK EPR design is consistent with that contained within principle EKP.3 of the SAPs relating to defence in depth. In addition it addresses aspects of the internal hazards SAPs relating to the analysis of internal and external hazards, EHA.6, as well as the storage and material aspects within EHA.13 and EHA.17. I am content with the response to this technical query.

"O10. Information will be required on the layout provisions required to facilitate access for any necessary recovery actions following an event."

181 A technical query (TQ-EPR-023) (Ref. 43) was raised as part of the assessment requesting EDF and AREVA to provide information relating to layout provisions required to facilitate access for any necessary recovery actions following an event.

182 A full response to this TQ was received on the 30/01/2009 (Ref. 44). This response states that several principles and objectives stated in this SAP cannot be fully addressed during the GDA due to the site specific nature of the layout. There are areas associated with fault recovery within the Safeguard Building and this has been the focus of the response to the TQ.

183 EDF and AREVA state that the 'recovery actions' in the context of the SAPs has been interpreted as operator actions that are necessary to bring the plant to a safe shutdown state or for personnel safety. This means that maintenance and repair actions that are necessary to bring the plant back into normal operation after an event are excluded from the analysis. Fire fighting and extinguishing systems are not required to achieve safe shutdown, however, there are requirements detailed within national standards that require adequate access and provisions are in place to enable fire service operations for conventional fire fighting and casualty recovery; the response addresses these layout requirements.

184 The response details two types of recovery actions required as part of the EPR design, namely:

1 Operational action relating to Nuclear Steam Supply Systems (NSSS) (including spent fuel storage) in order to bring the plant to and maintain the plant in a safe shutdown state.

2 Actions to mitigate the consequences of a hazard on the nuclear facility. These actions are those necessary for the safety demonstration e.g. isolation actions in the event of a pipe break to limit the volume of liquid released following an event that results in an internal flooding hazard or protective actions on safety classified equipment.

185 The actions detailed within point 1, above, are undertaken using Emergency Operating Procedures (EOP). The verification that the initiating event resulting from a hazard is covered by existing emergency operating strategies is to be carried out as part of the functional analysis of internal hazards. If the functional analysis identifies that the existing emergency operating strategies do not address the postulated hazard, then a dedicated strategy would be produced. EDF and AREVA do not anticipate that any further emergency operating strategies would be identified for the internal hazards area.

186 The actions detailed within point 2, above, are undertaken to mitigate the direct consequences of an internal hazard and are integrated into the EOPs or carried out using dedicated operating procedures, according to the result of the hazard functional analysis. The functional analysis assesses the consequences of the hazard in order to determine whether a reactor protection signal is triggered, or if the safe shutdown state cannot be reached using normal operating procedures. In addition, this analysis includes an assessment of the hazard consequences on the availability of support functions and such mitigation, if required, would be included within EOPs.

187 I am satisfied with the response to the TQ as it details the philosophy and principles to be applied in the EPR design, however, as the functional analysis is yet to be produced for FA3, the detailed evidence cannot yet be assessed.

"O11. Justification will be required for the adequacy of the hazard barriers. This should include a justification of the hazard challenge to the barrier, a justification of the hazard barrier resistance, the designation of an appropriate safety categorisation and safety classification which reflects the barriers role with regard to safety and the measures for control and design of penetrations."

188 A technical query (TQ-EPR-024) (Ref. 45) was raised as part of the assessment requesting EDF and AREVA to provide information justifying the adequacy of the hazard barriers. It specifically requested that the information should include:

- A justification of the hazard challenge to the barrier.
- A justification of the hazard barrier resistance.
- The designation of an appropriate safety categorisation and class.
- Measures for the control (i.e. minimisation) and design of penetrations.

189 A full response to this TQ was received on the 27/02/2009 (Ref. 46). The response states that the barriers are used to provide protection against the hazards detailed within Section 13.2 of the PCSR. The approach taken to determining adequacy of the barriers involves assessing the permanent (e.g. deadweight of construction and pressure due to liquids) and variable loads (e.g. those associated with the operation of the station including those resulting from internal hazards studies undertaken.) as part of the design of the UK EPR and then confirming the adequacy through the verification studies contained within the internal hazard methodologies. The methodologies were quoted

within the response to TQ-EPR-014 and assessed in relation to hazard identification. The methodologies have not yet been fully assessed as there are two documents yet to be issued to ND. As a result, the hazard barrier verification through the internal hazards methodology documents are to be subject to further detailed technical assessment within Step 4 of the GDA.

190 The safety classification of the barriers is discussed within the TQ response in which EDF and AREVA state that any functions specifically designed to monitor and control internal hazards are classified as F2. An F2 system is designed with the purpose of maintaining a safe state and is required for functions associated with RRC events and the control of internal and external hazards . The safety classification of barriers and the claims on fire protection systems are discussed further within the report as a result of the responses to TQ-EPR-018, hazard barrier designation and TQ-EPR-019 relating to the claims made on fire protection systems.

191 The TQ response states that the number of penetrations between adjacent safety divisions has to be minimised and based upon the outcome of the verification studies particular penetrations, e.g. ventilation ducts, in some compartments have to be avoided. The response also considers maintenance and modification associated with penetrations and services passing through and concludes that in cases where protection devices could be degraded by maintenance activities are modifications of the plant (e.g. installation of new pipes or cables) such modifications would need to be justified by specific extensions to the safety documentation. I am satisfied with the response to the TQ as it addresses the philosophy and principles associated with control and minimisation of penetrations.

“O12. Claims and supporting arguments will be required for the remaining internal hazard and related SAPs including:

EHA. 3, 4, 7, 10, 13 and 15.
EHF. 7
ESR. 1 and 6”

192 A technical query (TQ-EPR-013) (Ref. 47) was raised as part of the assessment requesting EDF and AREVA to provide information relating to claims and supporting arguments for SAPs detailed within O12.

193 A full response to this TQ was received on the 12/07/2008 (Ref. 48). This response states that the report, Comparison of EPR Design with HSE/ND SAPs (Ref. 49), provides a consolidated compliance analysis for the UK EPR addressing the complete list of SAPs relevant to GDA, including the SAPs detailed specifically within the TQ.

194 I am satisfied with the response as this assessment report considers where the design addresses the SAPs and makes specific comment in a number of the specific internal hazards assessment areas relating to the adequacy of the UK EPR design.

195 To conclude, I am satisfied that the observations made within UK EPR Internal Hazards Assessment carried out for Step 2 of the GDA Process have been either addressed fully or have been captured for assessment during Step 4.

2.3.2 Nuclear Fire Safety Assessment

196 The principle claim associated with the UK EPR is four train redundancy, with each division capable of fulfilling the 3 basic nuclear safety functions: control of reactivity, removal of heat from the core and containment of radioactive substances. The method by which this is achieved is to ensure that fire cannot spread to affect more than one division. This has been the main focus of the claims relating to fire for the UK EPR, as

shortfalls within this area can result in significant changes to layout and design if not adequately conceived and executed.

197 No assessment has yet been undertaken on the Fuel Building, the Waste Building, the Fire Fighting Pumphouse or any of the non safety-classified buildings (Turbine Hall, Nuclear Auxiliary Building, etc.). The focus of the assessment during Step 3 was to identify claims and arguments that, if not adequately conceived, had the potential to result in a significant challenge to nuclear safety as well as result in changes to the design and layout of the UK EPR.

198 It is intended to undertake assessment of the Fuel Building, the Waste Building and the Fire Fighting Pumphouse during Step 4. It is also the intention to undertake a review of the non-classified buildings during Step 4 to determine whether there is the potential for fire to spread and threaten safety-classified buildings. Based upon the outcome of both these areas, there may be further assessment required at the Phase 2 (site licensing) process.

2.3.2.1 Review of ETC-F

199 Given that a number of design provisions within the EPR are based upon an EDF Code for Fire Protection a Technical Service Contractor (TSC) (specialist fire safety consultant) was engaged to undertake a review of ETC-F (Ref. 50) based upon relevant good practice derived from national and international standards and guidance and the practice adopted within the UK nuclear reactor fleet.

200 The review found that in many aspects ETC-F meets the requirements of relevant guidance and accords with relevant good practice and it was recognised that the document is a technical guide and that omissions may be covered by further safety case submissions. In particular a formal fire hazard analysis and demonstration of ALARP will be required – neither is mentioned.

201 It is accepted that ETC-F is a design code rather than a safety case submission, however, there are areas where ND believe that the use of measures such as cable wraps and enclosures do not provide as robust a means of providing segregation of trains of protection for nuclear safety than that afforded by fire protection measures that utilise full structural segregation. The UK EPR design serves to minimise the areas where cable wraps and enclosures are used to those areas where their use cannot be avoided. Although the methodology of achieving segregation of divisions by the use of cable wraps and similar means would not necessarily be in accordance with relevant good practice in the UK for new nuclear build, their use cannot be rejected on this basis alone. Providing all systems used in the UK EPR have been tested to withstand the worst foreseeable credible fire conditions they must be considered as meeting the design objectives for segregation.

202 ETC-F generally sets out an adequate level of fire safety provision, however, there is a need for the detailed safety claims, arguments and evidence to be captured within the safety case documentation specifically relating to the need to demonstrate that the provisions in place to ensure nuclear safety in the event of fire are ALARP.

203 Where there are salient issues raised within the review document they are cited within the detail of the nuclear fire safety assessment and referenced accordingly.

2.3.2.2 ND Assessment of High Level Principles/Claims

204 The deterministic principles identified within PCSR have been assessed with regard to the nuclear safety claims, argument and evidence structure adopted within the UK regulatory system. As previously explained, the intent is to review the claims and

arguments within Step 3, however, where there is limited information relating to arguments, specific comment is made relating to their resolution.

205 The principle associated with the assumption that fire can break out in any room that contains combustible materials and ignition source, is similar with the approach taken within the relevant good practice within NS.G.1.7, paragraph 2.5 (a) which states, *"A fire is postulated wherever fixed or transient combustible material is located"*. However, there is one difference; NS.G.1.7 does not specifically mention the need for an ignition source to be present, it assumes that it is present. Further clarification was sought relating to whether there are any rooms that are claimed to have combustibles and no ignition source. EDF and AREVA have confirmed that wherever there are combustibles, ignition of those combustibles is assumed to occur as part of the deterministic approach to the design of the UK EPR for fire.

206 The PCSR states that there are three key principles in the design for nuclear fire safety; prevention, detection and extinguishing and the measures taken in the design to address these three principles are to prevent fires occurring, and to contain and control any fires that do occur. This approach is consistent with the current UK practice and that stated within the relevant good practice.

207 The principle associated with discounting the potential coincidental occurrence of two or more fires, from independent causes affecting rooms in the same or different plant, is in line with the relevant good practice within NS.G.1.7, paragraph 2.5 (b) which states, *"Only one fire is postulated to occur at any one time; consequential fire spread should be considered part of this single event if necessary"*. This approach is also taken for the assessment of fires within nuclear power and chemical reprocessing plant within the United Kingdom (UK).

208 There is a principle that discounts the potential for ignition associated with low and very low voltage electrical cables and equipment or materials protected by a housing or cabinet. Clarification was sought relating to this claim and EDF and AREVA confirmed that this was entered into the deterministic case in error as the statement forms part of the work undertaken to support the PSA assessment. The deterministic approach that assumes that if there are combustibles within a room, the probability of ignition of those combustibles is taken to be 1.

209 The principle associated with fire compartmentation of buildings into segregated divisions applying the fire containment approach and where this is not achievable application of the fire influence approach to generate fire cells is in line with current UK practice and relevant good practice as stated within Section 3 of NS.G.1.7.

210 The assumption that fire will break out during any normal permissible plant condition (from full power to shutdown condition) is in line with the relevant good practice detailed within NS.G.1.7. and is consistent with the HSE SAPs within the UK.

211 The principle associated with calculation of fireloadings within compartments is consistent to the approach applied within the UK and also consistent with the expectations of both national UK standards as well as NS.G.1.7.

212 The identification and subsequent risk assessment of temporary or permanent storage of fire loads during various plant states is a principle that is, again, in line with current relevant good practice, observed both at nuclear facilities within the UK and within NS.G.1.7.

213 Optimisation of fire protection provisions is also cited as a principle as a means to limit the discharge of toxic or radioactive materials, which again, is in line with current relevant good practice, observed both at nuclear facilities within the UK and within NS.G.1.7.

214 The principle associated with a random failure of an active equipment item of the fire protection systems not leading to a common mode failure on the systems needed to

perform F1 safety functions, is in itself a sound principle, however, a number of areas have been identified associated with this claim, that are to be the subject of further detailed assessment as part the Step 4 assessment. This is due in part to a lack of detailed design information relating to the fire protection systems to be installed and also due to the uncertainty of some of the claims associated with the F2 fire protection system for nuclear safety. A TQ (TQ-EPR-218) (Ref. 51) was raised relating to the claims made on F2 systems to perform a nuclear safety role and further assessment will be undertaken within Step 4.

2.3.2.3 Safety Fire Compartment Assessment

215 The PCSR identifies a number of fire compartments as part of the design for fire safety. Type 1 and 2 fire compartments are considered to have an impact on nuclear safety as Type 1a and 1b compartments are in place to ensure that any direct radiological releases from either within a safety classified building or other non-safety classified building are contained and controlled and Type 2 compartments are those compartments that ensure segregation by passive means of redundant trains of protection. Type 3 and 4 compartments serve to either enable adequate means of escape for occupants and facilitate access for fire fighting teams (Type 3) or to segregate areas of sufficiently high fireload where the potential exists for a flashover, to facilitate intervention by fire crews and to limit the extent of the damage caused by the fire (Type 4).

216 Type 2 - Safety Fire Compartments have been the focus of the ND assessment during Step 3 as these compartments form a fundamental claim in order to demonstrate adequate segregation of each of the four redundant trains of protection. Type 1 – Fire Containment and Fire Environment Compartments have not been assessed in detail as part of Step 3 as these compartments are generally located within buildings that have not yet been subject to detailed design assessment e.g. fuel building and waste building, however, it is important to stress that the comments relating to the Type 2 (SFC) compartments are equally applicable to the Type 1 compartments as they both contribute in varying degrees to the nuclear safety of the facility.

217 In addition to the use of fire compartmentation, there are some areas where fire cells are utilised. Fire cells are areas that cannot be fully compartmented which rely upon claims relating to the application of the fire influence approach. As part of this approach spatial segregation of redundant trains of equipment is employed supplemented in some areas by the use of local fire protection. From the assessment undertaken, it appears that the fire influence approach is limited to only the areas where physical compartmentation cannot be applied e.g. within the containment and within the Main Control Room (MCR). This approach is consistent with the approach taken within the UK and is in line with relevant good practice stated within NS.G.1.7.

218 The PCSR states that should a fire 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 and that fire damage must be limited to one redundant train in a given F1 system. As part of the claim associated with fire affecting only one division, it is stated that should the fireloading within an individual compartment be sufficient to threaten the redundant trains in a separate divisional building, fire protection systems would be sufficient to prevent fire spread to the adjacent division. This is not in line with the statements made within NS.G.1.7 which states, *"The fire resistance rating of the barriers should be sufficiently high that total combustion of the fire load in the compartment can occur (i.e. total burnout) without breaching the fire barriers"*. However, the PCSR does state that priority should be given to physical separation and fire resistance of structures rather than rely on fire protection devices. This issue was initially raised as a TQ (TQ-EPR-019) and was raised as part of the observations. Ultimately, an RO (RO-UKEPR-30) (Ref.33) together with an ROA (RO-UKEPR-30.A1) (Ref.34) which stated, *"The*

design principle for SCO's is inconsistent with UK expectations of relevant good practice and as a result please confirm how EDF and AREVA ensure that these barriers are adequately rated to withstand total burn out without the use of a fire protection system."

219 A partial response has been received relating to the RO (Refs 52, 53) which proposes splitting the ROA into 6 distinct areas:

1 Provide a comparison of the fire drawings from Flamanville 3 (FA3) and Okiluto 3 (OL3) in Safeguard Buildings 2&3.

2 Identify the Safety Fire Compartments in FA3 used to provide protection of redundant F1 safety trains.

3 From the Safety Fire Compartments identified in Step 2, select those compartments with the highest fire loads.

4 Argue why the fire loads in these FA3 compartments do not impair the passive fire barriers in the perspective of Finnish Building Codes.

5 Provide an analysis of corresponding building codes for the UK in terms of the required fire rating of compartments.

6 Perform a MAGIC simulation for one representative safety 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.

220 The first five areas have been included within a technical report (Ref. 53) produced by EDF and AREVA. The specific approach to resolving the RO is a satisfactory approach to addressing the shortfall and I have assessed the technical report relating to the adequacy of the five steps addressed to date.

221 The technical report identified that the design, layout and compartmentation of both FA3 and OL3 facilities was very similar and the overall approach in providing segregated trains of protected by safety fire compartments was identical. As the room structures, configuration, allocation of components, wall dimensions and fire resistance rating being broadly similar, the transfer of the fire load assessment work undertaken for OL3 can be equally applied to FA3. The safety fire compartment with the highest fireloading for OL3 was then selected for assessment to determine the fire resistance requirement for the barriers. This fireload was then subject to analysis using computational fluid dynamics modelling (Fire Dynamics Simulator (FDS)) (Ref. 54) and by application of a German validation procedure (KTA Method) based upon energy balances (Ref. 55). Both the FDS and KTA methods are well known and have been applied within the nuclear industry extensively. The KTA method is one which applied for the determination of fire resistance requirements within the UK nuclear industry. The outcome of the assessment of fireloads revealed that the fire resistance requirements for the compartment of greatest fireloading equated to a fire duration of approximately 90 minutes for both methods, which is within the 120 minute fire rating applied to the safety fire compartment. Both methods showed that any potential fire would be oxygen limiting.

222 The final aspect of the response details that a simulation utilising MAGIC of one representative fire compartment with the highest fireload would be undertaken to compare the results against standard fire curves and would not include modelling of fire protection systems.

223 To conclude, the safety fire compartment rating of 120 minutes has been demonstrated to be adequate to withstand total burnout of all combustibles contained therein and therefore, meets the relevant good practice stated within NS.G.1.7. I am satisfied that the partial response to RO30 is adequate, however, there will be a need to review the full response to the RO within Step 4.

2.3.2.4 Random Failure / Door Control Measures

224 The PCSR does identify that random failure is to be considered for active equipment associated with fire protection provisions e.g. stop check valves, fire dampers and servo controlled doors. Random failure is not considered for items which are claimed to be passive e.g. fire doors within safety fire compartments (SCO) and smoke extraction ducts and floor drains. A TQ was raised (TQ-EPR-029) (Ref. 56) requesting EDF to respond to whether doors in nuclear significant hazard barriers were treated as active or passive safety features. EDF and AREVA responded (Ref. 57) by stating that doors were passive features and this aspect was brought out within the PCSR. This response prompted a further TQ (TQ-EPR-129) (Ref. 58) relating to the provision of door control measures on nuclear significant hazard barrier doors which was discussed within an internal hazards topic meeting (Ref. 59). ND questioned whether it was proposed to install door control measures on nuclear significant hazard barrier doors to which EDF responded that such measures were not adopted within the design for FA3 and not proposed for UK EPR, which was reiterated within the response to the TQ (TQ-EPR-129) (Ref. 60). Within the same meeting AREVA stated that door control measures, in the form of alarms annunciating to a permanently manned security centre were to be installed as part of the design for OL3 in Finland as this was a requirement of the Finnish Regulator, STUK. EDF and AREVA responded to the TQ stating that the approach taken with the FA3 reactor in France and that there was currently no plans to install door control measures as part of the UK EPR design. Given that a number of existing nuclear facilities within the UK have alarms fitted on nuclear significant hazard barriers doors and the fact that overseas regulators would require such provision, I believed that this constituted relevant good practice and as such raised an RO (RO-UKEPR-035) (Ref. 61) together with an associated ROA (ROA-UKEPR-35.A1) (Ref. 62) stating, *"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".* The response to this RO and associated ROA is due to be issued to ND towards the end of Step 3 and as a result will be assessed during Step 4.

2.3.2.5 Cable Routing and Protection within UK EPR

225 There are claims relating to segregation of redundant elements of an F1 system such that failure due to fire is limited to a single train. There are aspects of this claim associated with the aforementioned RO (RO-UKEPR-30) as well as claims associated with providing protection to individual cable trays from foreign divisions passing through cable raceways. The segregation claims associated with cable trays and cable routing have been subject to detailed assessment within Step 3 as there have been specific concerns relating to the approach applied to the design for segregation using cable wraps and the potential for common cable routes within a number of areas requiring the application of retrospective fire protection.

226 As part of the assessment of cable routings, the EDF and AREVA report, 'FIRE (Internal Hazard) – Studies by safeguard buildings 1/2/3/4 justification of fire zoning' (Ref. 63), provided information relating to areas where a number of safety fire compartments where located within a different division's Safeguard Building contains electrical equipment from Division 1 but is within a Division 2 building. This was discussed within the 5th Internal Hazards Topic Meeting (Ref. 64) and further investigation was undertaken using the Plant Design and Modelling System (PDMS), a 3D computer model, of this particular area which identified that this particular safety fire compartment contained cable trays for all four Divisions. The PDMS model showed Divisions 1 and 2 on one side of the

compartment and Divisions 3 and 4 on the other. None of the cable trays were identified as being fire protected / enclosed as had been shown for the supplies from Division 2 passing into the Fuel Building. EDF stated that the FA3 design was still being populated within PDMS and that all the information is not yet present. I stated that this issue relating to segregation of essential trains should be further investigated by EDF and that all exceptions to segregation based on cable tray layouts should be identified. I questioned whether it was possible to route cables from separate divisions within a common area such as this that could result in loss or spurious operation of redundant safety systems. EDF and AREVA stated that the design of the cable routing for FA3 would not be complete until Step 4 and that on completion there is a validation and verification tool by the name of GESTEC utilised to identify potential common cause failures. In addition, from observation of the model it appeared that there was limited space available to provide cable tray fire protection within the specific safety fire compartment that was being discussed.

227 As part of the design for segregation of cables performing a nuclear safety function, it is preferable to provide passive physical segregation in the form of dedicated compartments rather than retrospective application of passive fire protection in the form of cable wrapping or coating. Where this is not achievable, retrospective protection of cable trays is undertaken. In the case of the EPR design, there are areas where I believe that cables could be routed that minimise the need to provide this retrospective cable wrapping, especially since there are areas where cable trays exist for all four divisions that are not either associated with the MCR or within Containment. As part of the review of ETC-F (Ref. 50) which was requested to support my assessment, I tasked the specialists involved to produce a précis of cable wrapping as well as a review of the cable protection calculations. The findings of their assessment has been reviewed and summarised in the following paragraphs.

228 The TAG for Internal Hazards (T/AST/014) states that the preferred approach to segregation of trains of protection is by the use of fire barriers designed to withstand total burnout. Where this is not practical due to conflicts with other plant design requirements, separation of the items important to safety could be achieved using an appropriate combination of limited combustibles, distance, local passive fire barriers, shields, cable wrap and fire suppression systems. Therefore, for a new design it is expected that segregation by use of fire barriers would be used wherever possible and the use of cable wrapping systems be limited to areas only where segregation of the cable routes by means of fire barriers cannot be achieved e.g. beneath the MCR or within Containment.

229 Accepting that there will inevitably be areas where full segregation by means of fire barriers will not be possible, the following design and installation considerations for any proposed cable wrapping would need to substantiated as part of the design:

- The adequacy of the cable wrapping system with regard to cable functionality of the cables (including flame impingement) for the duration of the fire resistance claim made upon the system.
- The adequacy of the cable wrapping system with regard to fire resistance claims and lack of contribution to a fire.
- The adequacy of the installation relating to the design specification.
- The adequacy of the installed system relating to ageing and degradation.
- The control of modifications to the cable wrapping system and / or the installation of any additional cables once the protection has been applied.
- The ability of the installed system to provide the required fire resistance in a fire fighting environment (water, foam) as well as a normal operational one.
- Maintenance and inspection processes associated with the cable wrapping system.

230 This aspect of the assessment is ongoing and will be subject to further assessment during Step 4 when there is more detailed information available relating to the routing and protection of cables installed to ensure segregation of redundant trains of protection .

2.3.3 Internal Flooding Assessment

231 The high level claims and principles contained within the PCSR associated with internal flooding have been assessed and areas for further detailed assessment within Step 4 of the GDA process have been identified.

232 The PCSR considers a number of potential initiators for internal flooding; these are detailed within Section 2.2, and include leaks and cracks in pressurised systems, flooding from neighbouring buildings on site, spurious actuation of fire protection systems, overfilling of tanks, and operator error. Arguments and evidence relating to specific sources of internal flooding, including operator error, are not included within PCSR and further substantiation will, therefore, be required during Step 4.

233 The approach taken to the design for internal flooding is deterministic and the PCSR postulates that only one potential internal flooding initiator occurs at any one time, unless two or more initiators are a direct result of a common cause. The potential for flooding is considered to occur during normal operation (during power operation or shutdown). I am satisfied with this approach as it is consistent the HSE SAPs EHA.5, EHA.6 and EHA.14, as well as the approach adopted currently within nuclear facilities within the UK.

234 The PCSR identifies three types of SSC that are liable to fail during flooding; electrical and C&I equipment, civil structures not qualified against flooding, and non-watertight mechanical equipment. Whilst, the intent of the claim seems reasonable, it is not clear whether there are any SSCs associated with electrical and C&I equipment that are to be specifically rated against the effects of water ingress and what barriers are classified against the effects of internal flooding.

235 The PCSR considers the potential for leaks resulting in internal flooding and discusses a number of aspects and provisions in place to isolate leaks, some automated by C&I systems and some by operator action. There is a clear philosophy applied to manually isolating leaks either from the MCR or locally associated with the time it takes from first identifying the leak to being able to isolate based upon a notional intervention time (30 minutes for operator action within the MCR and 60 minutes from any other location on plant). This approach is consistent with the HSE SAPs which states, *"Where human intervention is necessary following the start of a requirement for protective action, then the time before such intervention is required should be demonstrated to be sufficient."* The supporting text within the SAPs state that current practice within the UK civil nuclear power reactor facilities is that no human intervention should be necessary for approximately 30 minutes. This approach to isolating leaks that could result in an internal flooding event is, therefore, consistent with the approach taken within the UK.

236 It is assumed that any leakage requiring intervention is assumed to continue for the duration of time required to isolate. If there are no means by which to detect or isolate the leak, then release of the full inventory of the failed system is assumed. I am satisfied with this approach to the determination of internal flood volumes.

237 The design of the UK EPR considers the need for collection and discharge of potential flood water through the buildings drainage systems, which is in line with guidance contained within the Internal Hazards Technical Assessment Guide (TAG 014).

238 In addition, the PCSR states that the design of UK EPR is such that the effects from an internal flooding event are minimised and includes high level principles associated with minimising direct effects of internal flooding on SSCs, minimising interactions between a failed SSC and other safety related SSCs, personnel protection and recovery actions,

however, as due to the nature of the high level principles, further substantiation will be required during Step 4.

239 The PCSR cites the main safety objective is to ensure that an internal flood cannot extend to another safety classified building or another safety classified division. As a result there are claims associated with the barriers between the divisions within the Safeguard Building. The principle adopted within the UK EPR design is to prevent flood water passing into adjacent divisions by ensuring that there are no penetrations for doors and ventilation systems beneath 0.0m level within each of the divisional buildings. There may be penetrations associated with cables, however, they have been identified as requiring to be qualified against flood water. This approach is consistent with UK expectations and relevant good practice in relation to the use of fixed passive features to ensure that internal hazards are limited to the division in which they originate.

240 In safety classified buildings other than the Safeguard Buildings, the PCSR states that flooding must be prevented from causing failure in F1 systems and their associated support systems and in the event where such internal flooding threats are identified there is a need to provide protection such as the provision of additional barriers qualified to contain and direct flood water, locating components above the maximum flood height, and the installation of additional drainage. These principles seem reasonable in the event that protection against internal flooding cannot be assured by the provision of physical passive barriers.

241 The PCSR details the principles associated with the detailed design verification and states that the UK EPR analysis takes into account simultaneous effects, common cause failure, defence in depth and consequential effects. A number of factors are taken into account which are detailed within Section 2.1.2.1 of this assessment report. These factors are principle based and are used as part of the verification at the end of the detailed studies. Further assessment associated with the completed verification process is to be undertaken when this process is complete within Step 4 or Phase 2.

2.3.4 Dropped Load and Impact Assessment

242 Dropped loads and impact have been subject to a high level sample of the key claims and arguments detailed within the PCSR. A deep slice sample of those statements and how they impact nuclear safety within specific areas and buildings has not yet been undertaken due to limited amount of detailed information coupled with the focus of the Step 3 assessment being on areas which could ultimately result in significant changes to the design and layout. Dropped load and impact will be assessed in greater detail as part of the Step 4 internal hazards assessment.

243 The case presented within the PCSR considers that protection against dropped loads is deterministic. The PCSR identifies three measures to protect against the potential for a dropped load or impact; the first being the classification of the lifting device, the second, the installation and design rules for potential targets and the third being the operating rules associated with lifting. I consider that this high level approach to determining the level of protection required for dropped loads to be adequate. However, the basis for the determination of the classification of the lifting device appears to be based upon a simplified hazard analysis to which there is no further information relating to what is undertaken within this analysis. This analysis considers consequences to be unacceptable if the dropped load could lead to a criticality accident or a loss of decay heat removal function or a release of radioactivity which exceeds PCC-4 limits. If any of the three potential events could occur the lifting equipment is required to be classified as having 'higher requirements' and as a result these requirements enable the possibility of damage due to the dropped load to be discounted.

244 In addition to the 'higher requirements', there are 'additional requirements', which are required if the consequences of a dropped load are considered to be serious e.g. non-isolatable release of primary coolant into the containment or a failure which leads to consequential failure of an F1 system or a release of radioactivity leading to increased radiation levels inside the area which affects the classification of the radiological zones. 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.

245 The PCSR contains a number of principles associated with the design and layout of site relating to dropped loads such that the potential for dropped loads to impact upon safety significant SSCs is minimised e.g. limiting lift heights and the use of prescribed routes.

246 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 the plant. Further substantiation will, therefore, be required relating to this aspect of dropped load and impact.

247 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.

248 From the limited high level sample that has been undertaken, I can confirm that the principles and methodology applied to the design of the UK EPR appear to be sound, however, there is a lack of detailed information relating to the safety arguments within this area.

2.3.5 Missile Generation Assessment

249 As with other areas of the internal hazards assessment undertaken as part of the Step 3 GDA process, the approach taken to the assessment of potential missile generation has been limited to a high level assessment of the main principles detailed within the PCSR. Further detailed assessment will be undertaken in specific areas identified within this assessment report.

250 The PCSR states that the approach to the UK EPR design associated with missile generation is deterministic and identifies two potential missile sources; the first associated with failure of rotating equipment and the second with failure of pressurised components.

251 Missiles generated as a result of failure of safety classified components and pipework are discounted by virtue of their design. Where there are non-safety classified components within safety classified buildings, the potential for missile generation is considered.

252 The PCSR provides an analysis of the missile threats within the Reactor Building, Safeguard Buildings, Fuel Building and Diesel Generator Buildings. The main claims associated within each building have been assessed in detail within this report:

2.3.5.1 Reactor Building Missile Generation Assessment

253 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.

254 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.

255 The potential for a missile arising from a failure of a Rod Cluster Control Assembly (RCCA) is not considered credible within the PCSR due to the material properties of the housing and quality, construction and pressure testing of the housing. This event is not considered further within this internal hazards assessment. Should the claim that the potential for RCCA ejection change there would be a need to undertake further assessment of the potential impact of a missile arising from such an event.

256 The potential for a disintegration of a Reactor Coolant Pump (RCP) flywheel has been addressed within the PCSR, and due to the design, construction, installation and testing of the RCP is discounted under all operating conditions. In addition to the physical design of the RCP, it is not possible to generate overspeeds of the flywheel due to the potential maximum breach size connected to the reactor coolant system pipework. Should the claim change relating to the potential for disintegration of an RCP flywheel there would be a need to undertake further assessment of the potential impact arising from such an event.

257 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.

258 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.

2.3.5.2 Safeguards Building Missile Generation Assessment

259 The principle claim for protection against missile impact resulting in failure of more than one train of redundant nuclear safety related plant are the hazard segregation barriers installed between the divisions coupled with individual valve compartments. In the majority of areas of the Safeguard Building missiles are not possible; an exception to this is missiles arising from failure of the main steam feedwater valve components, however, these are segregated into four geographically and physically separated compartments. The claim for these such missiles is, given the geographical separation coupled with the

structural protection afforded by the compartments and reactor building concrete shell, that missile affects to all redundant trains are discounted. I am satisfied with this claim as it provides confidence in the deterministic approach to the design against missile impact in this area.

2.3.5.3 Fuel Building Missile Generation Assessment

260 The PCSR claims that for the lower sections of the building (<0.0m) physical segregation forms the basis of the case for protection of the two trained systems in place to ensure adequate pond cooling and Extra Boration System (EBS) function. In the case of the upper levels (≥ 0.0m) the redundant trains are located or protected such that only one redundant train is at risk from missiles. In addition, there is a claim on the building structure to protect the fuel pool from missiles arising from on-site missile hazards. Again, I am satisfied with this claim as it provides confidence in the deterministic approach taken in the design, however, as with the Safeguards Building there is a need to undertake further assessment relating to the specific barriers claimed against missile impact within this area.

2.3.5.4 Diesel Buildings Missile Generation Assessment

261 The claim associated with protection against missiles arising from either the diesel generators or from external sources is based upon physical segregation and geographic separation. The design of the diesels includes provision to prevent overspeed and therefore reduce the potential for missile ejection as a result of failures due to overspeed. In addition, the diesels are not normally operational when the unit is at power. Again, I am satisfied with this claim as it provides confidence in the deterministic approach taken in the design of the essential diesels to ensure that they are not threatened by missiles. Further assessment will be required to determine the adequacy of the segregation and separation principles when more detailed information becomes available during Step 4.

2.3.6 Internal Explosion Assessment

262 The PCSR states that the UK EPR design considers a number of requirements and potential dependencies and combinations of hazards. The principle claim is associated with ensuring that an explosion should not adversely affect more than one element of a redundant F1 system and should not trigger a PCC-3 or PCC-4 event, where possible. In addition an internal explosion should not adversely affect the stability and integrity of safety classified buildings and fire safety barriers and components whose failure is discounted by design.

263 The three potential sources of internal explosions associated with systems, releases of explosive gases, and failure of pressure tanks containing gases or liquefied gases address all potential explosion scenarios for the UK EPR. Explosions arising from mechanical or electrical equipment are not considered due to the design of the specific components. Further assessment of the arguments and evidence associated with the potential for explosions involving electrical or mechanical equipment is to be undertaken when more detailed information related to specific items of plant vulnerable to explosion are known

264 I am satisfied that the claims made relating to the effects of explosions and the method of identifying potential sources of explosion have been identified are consistent with current practice within the UK reactor fleet as well as with the HSE SAPs EHA.13 and EHA.14.

265 The PCSR states that the approach taken to the protection against explosions involves a hierarchical approach associated prevention, detection and limiting consequences. This

is consistent with the HSE SAPs relating to defence in depth stated within EHA.6 and as a result I am satisfied with this principle to the approach to the protection against internal explosions.

266 Included within the PCSR are a number of measures for systems containing explosive gases; these measures are predominantly design principles to ensure that explosive atmospheres do not occur and should they occur the equipment contained within the room at risk of explosion is adequately protected to prevent ignition of any potential flammable vapour or gas. I am satisfied with this approach, however, it relies on detailed information relating to potential rooms at risk early within the design to ensure that adequate protection is designed into the facility. The PCSR states that there is a verification process at the end of the design to ensure that all potential rooms at risk and associated systems containing explosive gases have been identified.

2.3.7 Pipework Leaks and Breaks

267 The PCSR makes a number of claims associated with break (rupture) preclusion and the 2% criterion. These claims are associated with other aspects of the UKEPR design, structural integrity, quality assurance etc., have not been considered within this internal hazards assessment. Should the assessments within these areas identify that the arguments associated with break (rupture) preclusion and the 2% criterion are not valid in the specific areas where they are claimed further assessment would need to be undertaken to determine the nuclear safety significance associated with the potential for leaks and breaks associated with the pipework. The assessment of internal hazards has been limited to those areas where there is the potential for leaks and breaks in pipework.

268 The leaks and breaks considered are, therefore, those that occur in small diameter (≤ 50mm nominal bore) pipework where failure is assumed to occur at any location and for failures of pipework with a diameter >50mm nominal bore, specific locations for failures of the pipework are postulated e.g. pipework terminations and other specific locations depending upon the usage factor and stress rates. The PCSR requires that the leak and break location selected for pipework with a diameter >50 mm nominal bore represent bounding conditions in terms of the nuclear significance for the plant and equipment within the room under analysis. I am satisfied with these principles associated with the approach to the assessment of potential leaks and breaks from pipework that is not claimed under the break preclusion and 2% criterion methodology.

3 CONCLUSIONS

269 It is important to recognise that ND is currently part way through the GDA process and the intent of this Step 3 assessment is to provide an interim position statement regarding the assessment currently being undertaken.

270 This report has taken into consideration the findings of the Step 2 Internal Hazards Assessment of the UK EPR (Ref. 2) and has confirmed that the issues contained therein have been addressed within Step 3 and have been satisfactorily resolved with the exception of areas where further assessment work has been specifically identified.

271 To conclude, I am satisfied with the claims and arguments as laid down within the current PCSR and other supporting safety case documents. There are a number of areas of further detailed assessment identified to be undertaken during Step 4 to provide ND with confidence that an adequate safety case can be made for the construction and operation of the EDF and AREVA UK EPR within the UK and within the UK Regulatory regime.

4 REFERENCES

1 *UK EPR Pre-Construction Safety Report* (PCSR). Sub-Chapter 13.2 – Internal Hazards Protection, UK EPR-0002-132 Issue 02, EDF and AREVA, June 2009.

2 *GDA Phase 1 – Step 2 EDF and AREVA – EPR Internal Hazard Assessment.* ND Assessment Report AR07/013, HSE, December 2007, TRIM File 2007/345678.

3 *ND BMS, Assessment Process.* AST/001, Issue 2, HSE, February 2003.

4 *ND BMS, Guide: Assessment Process.* G/AST/001, Issue 2, HSE, February 2003.

5 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition, Revision 1, HSE, January 2008.

5a *GDA Phase 1 – Steps 3 and 4 Internal Hazards Assessment Strategy.* ND Assessment Report AR08/031, HSE, November 2008, TRIM Record 2008/591915.

6 *ND BMS, Assessment Reports.* AST/003, Issue 2, HSE, October 2003.

7 *ND BMS, Guidance: Assessment Reports.* G/AST/003, Issue 2, HSE, October 2003.

8 *ND BMS, Technical Assessment Guide 014, Internal Hazards.* T/AST/014, Issue 2, HSE, August 2008.

9 *UK EPR Pre-Construction Safety Report (PCSR). Sub-Chapter 13.2 – Internal Hazards Protection*, UK EPR-0002-132 Issue 01, EDF and AREVA, April 2008.

10 *ND GDA UK EPR Technical Query, TQ-EPR-014, Internal Hazards – Identification – Methodology.* HSE, April 2008, TRIM Ref. 2008/133172.

11 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-014, Internal Hazards – Identification – Methodology.* EDF and AREVA, July 2008, TRIM Ref. 2008/267247.

12 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-014, Internal Hazards – Identification – Methodology.* EDF and AREVA, January 2009, TRIM Ref. 2009/74816.

13 *High Energy Pipe Leaks and Breaks Analysis Methodology.* ECEF041142A1, Revision A1, EDF, 2006.

14 *Internal Flooding – Layout Analysis Methodology.* ECEIG040650C1, Revision C1, EDF, 2008.

15 *EPR: FA3 Fire Analysis Methodology.* ECEIG0100581C1, Revision C1, EDF, 2006.

16 *EPR: Internal Explosion Methodology – Safety Requirements.* ECEIG060350A1, Revision A1, EDF, 2006.

17 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-014, Internal Hazards – Identification – Methodology.* EDF and AREVA, March 2009, TRIM Ref. 2009/133509.

18 *ND GDA UK EPR Technical Query, TQ-EPR-015, Internal Hazards – Identification – Completeness of the Internal Hazard Listing.* HSE, April 2008, TRIM Ref. 2008/133228.

19 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-015, Internal Hazards – Identification – Completeness of the Internal Hazard Listing*, EDF and AREVA, February 2009, TRIM Ref. 2009/87326.

20 *UK EPR Pre-Construction Safety Report (PCSR), Sub-Chapter 3.1 – General Safety Principles.* UK EPR-0002-031, Issue 02, EDF and AREVA, June 2009.

21 *UK EPR Pre-Construction Environmental Report* (PCER), Sub-Chapter 3.3 – Aspects having a bearing on the environment during operation phase. UK EPR-0003-030, Issue 01, EDF and AREVA, June 2008.

22 *ND GDA UK EPR Technical Query, TQ-EPR-016, Internal Hazards – Operating Conditions.* HSE, April 2008, TRIM Ref. 2008/133262.

23 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-016, Internal Hazards – Operating Conditions*, EDF and AREVA, 31/03/2009, TRIM Ref. 2009/133263.

24 *ND GDA UK EPR Technical Query, TQ-EPR-017, Internal Hazards – Analysis*, HSE, April 2008, TRIM Ref. 2008/133326.

25 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-017, Internal Hazards – Analysis*, EDF and AREVA, March 2009, TRIM Ref. 2009/133266.

26 *External Hazards – inventory of combined events with internal faults and/or other (internal and external) hazards taken account in design*, ENSNEA080058A, EDF, June 2005.

27 *ND GDA UK EPR Technical Query, TQ-EPR-018, Internal Hazards – Fire Explosion, Missile, Toxic Gas etc. – Fire Detection and Fighting – Fire Barriers*, HSE, April 2008, TRIM Ref. 2008/133362.

28 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-018, Internal Hazards – Fire Explosion, Missile, Toxic Gas etc. – Fire Detection and Fighting – Fire Barriers*, EDF and AREVA, July 2008, TRIM Ref. 2008/267274.

29 *EDF Technical Code for Fire Protection*, ETC-F, ENGSIN050312B, Revision B, EDF, August 2007.

30 *ND GDA UK EPR Technical Query, TQ-EPR-019, Internal Hazards – Fire Explosion, Missile, Toxic Gas etc. – Fire Detection and Fighting – Fire Protection System*, HSE, April 2008, TRIM Ref. 2008/133388.

31 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-019, Internal Hazards – Fire Explosion, Missile, Toxic Gas etc. – Fire Detection and Fighting – Fire Protection System*, EDF and AREVA, February 2009, TRIM Ref. 2009/74833.

32 *IAEA Safety Standard Series, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants*, NS-G-1.7, International Atomic Energy Agency (IAEA), Vienna, 2004.

33 *ND GDA UK EPR Regulatory Observation – RO-UKEPR-030, Internal Hazards – Fire Protection – Safety Fire Compartment*, HSE, March 2009, TRIM Ref. 2009/128305.

34 *ND GDA UK EPR Regulatory Observation Action – RO-UKEPR-030.A1, Internal Hazards – Fire Protection – Safety Fire Compartment*, HSE, March 2009, TRIM Ref. 2009/110923.

35 *ND GDA UK EPR Technical Query, TQ-EPR-020, Internal Hazards – Fire Explosion, Missile, Toxic Gas etc. – Fire Detection and Fighting – Fire Models*, HSE, April 2008, TRIM Ref. 2008/133399.

36 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-018, Internal Hazards – Fire Explosion, Missile, Toxic Gas etc. – Fire Detection and Fighting – Fire Models*, EDF and AREVA, November 2008, TRIM Ref. 2009/158699.

37 *Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications*, Volume 5: MAGIC, NUREG 1824, EPRI 1011999, EPRI, January 2006.

38 *ND GDA UK EPR Technical Query, TQ-EPR-021, Internal Hazards – Fire Explosion, Missile, Toxic Gas etc. – Fire Detection and Fighting – Segregation*, HSE, April 2008, TRIM Ref. 2008/133410.

39 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-021, Internal Hazards – Fire Explosion, Missile, Toxic Gas etc. – Fire Detection and Fighting – Segregation*, EDF and AREVA, February 2009, TRIM Ref. 2009/87322.

40 *ND GDA UK EPR Technical Query, TQ-EPR-022, Internal Hazards – Key Principles – Defence in Depth*, HSE, April 2008, TRIM Ref. 2008/133421.

41 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-022, Internal Hazards – Key Principles – Defence in Depth*, EDF and AREVA, April 2009, TRIM Ref. 2009/173920.

42 *IAEA Safety Requirements*. *Safety of Nuclear Power Plants: Design,* NS-R-1, International Atomic Energy Agency (IAEA), Vienna, 2000.

43 *ND GDA UK EPR Technical Query, TQ-EPR-023, Internal Hazards – Layout – Minimisation of the Effects of Incidents*, HSE, April 2008, TRIM Ref. 2008/133431.

44 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-023, Internal Hazards – Layout – Minimisation of the Effects of Incidents*, EDF and AREVA, January 2009, TRIM Ref. 2009/44208.

45 *ND GDA UK EPR Technical Query, TQ-EPR-024, Internal Hazards – Safety Systems – Failure Independence*, HSE, April 2008, TRIM Ref. 2008/133515.

46 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-024, Internal Hazards – Safety Systems – Failure Independence*, EDF /AREVA, February 2009, TRIM Ref. 2009/87314.

47 *ND GDA UK EPR Technical Query, TQ-EPR-013, Internal Hazards – Remaining Internal Hazards SAPs*, HSE, April 2008, TRIM Ref. 2008/133100.

48 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-013, Internal Hazards – Remaining Internal Hazards SAPs*, EDF /AREVA, July 2008, TRIM Ref. 2008/267244.

49 *UK EPR, Comparison of EPR Design with HSE/ND SAPs*, UK EPR-0005-001, Issue 00, EDF and AREVA, June 2008.

50 *SERCO – Review of EDF Technical Code for Fire (ETC-F)*, SERCO/TAS/REGS/P1969/1/01 Issue 01, SERCO, August 2009.

51 *ND GDA UK EPR Technical Query, TQ-EPR-218, Internal Hazards – Nuclear Safety Claims on F2 Fire Protection Systems*, HSE, June 2009, TRIM Ref. 2009/225710.

52 *Letter from EDF and AREVA to HSE, RO-UKEPR-30 and RO-UKEPR-30.A1 – Internal Hazards – Fire Hazards Analysis – Part Response*, ND(ND)EPR00142N, EDF and AREVA, July 2009.

53 *Technical Report for Steps 1 to 5 of AREVA/EDF Response to RO-UKEPR-030.A1.* NESP/G/2009/en/1322, Rev A, AREVA, July 2009.

54 *Fire Dynamics Simulator.* FDS, Version 5, National Institute of Standards and Testing (NIST), US Department of Commerce, 2007.

55 *Fire Protection in Nuclear Power Plants, Part 1: Basic Principles, Part 2: Structural Components.* KTA2101 Parts 1 and 2, German Nuclear Safety Standards Commission (KTA), December 2000.

56 *ND GDA UK EPR Technical Query, TQ-EPR-029, Internal Hazards – Door Penetrations in Hazard Barriers.* HSE, May 2008, TRIM Ref. 2008/189223.

57 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-029, Internal Hazards – Door Penetrations in Hazard Barriers.* EDF /AREVA, June 2008, TRIM Ref. 2008/232168.

58 *ND GDA UK EPR Technical Query, TQ-EPR-129, Internal Hazards – Door Penetrations in Hazard Barriers.* HSE, February 2009, TRIM Ref. 2009/75176.

59 *ND Contact Report – Internal Hazards Topic Meeting No. 4.* CR09/043, HSE, 23 March 2009, TRIM Ref. 2009/144236.

60 *EDF Response to ND GDA UK EPR Technical Query, TQ-EPR-129, Internal Hazards – Door Penetrations in Hazard Barriers.* EDF /AREVA, May 2009, TRIM Ref. 2009/199645.

61 *ND GDA UK EPR Regulatory Observation, RO-UKEPR-035, Internal Hazards – Nuclear Significant Hazard Segregation – Door Control Measures.* HSE, July 2009, TRIM Ref. 2009/285379.

62 *ND GDA UK EPR Regulatory Observation Action, ROA-UKEPR-035.A1, Internal Hazards – Nuclear Significant Hazard Segregation – Door Control Measures.* HSE, July 2009, TRIM Ref. 2009/285746.

63 *FIRE (Internal Hazard) – Studies by safeguard buildings 1/2/3/4 justification of fire zoning.* EZL/2006/en/0082, Issue 8, EDF and AREVA, December 2008.

64 *ND Contact Report – Internal Hazards Topic Meeting No. 5.* CR09/077, HSE, 29 April 2009, TRIM Ref. 2009/189842.

Table 2

Safety Assessment Principles Relevant to the Internal Hazards Assessment of the UK EPR

SAP No.	Assessment Topic / SAP Title
EHA –	External and Internal Hazards
EHA.1	Identification
EHA.3	Design basis events
EHA.4	Frequency of exceedance
EHA.5	Operating conditions
EHA.6	Analysis
EHA.7	Cliff-edge effects
EHA.10	Electromagnetic interference
EHA.13	Fire, explosion, missiles, toxic gases etc – use and storage of hazardous materials
EHA.14	Fire, explosion, missiles, toxic gases etc – sources of harm
EHA.15	Fire, explosion, missiles, toxic gases etc – effect of water
EHA.16	Fire, explosion, missiles, toxic gases etc – fire detection and fighting
EKP -	Key Principles
EKP.3	Defence in depth
ELO -	Layout
ELO.4	Minimisation of the effects of incidents
ESS -	Safety Systems
ESS.18	Failure independence
EHF -	Human factors
EHF.7	User interfaces
ESR -	Control and Instrumentation of safety-related systems
ESR.1	Provision in control room and other locations
ESR.6	Power supplies

Annex 1 – Internal Hazards – Status of Regulatory Issues and Observations

RI / RO Identifier	Date Raised	Title	Status	Required timescale (GDA Step 4 / Phase 2)
Regulatory Issues				
None.				
Regulatory Observations				
RO-UKEPR-30	30 March 2009	Fire Protection-Fire safety compartments.	Open.	Step 4
RO-UKEPR-35	23 July 2009	Nuclear Significant Hazard Segregation - Door Control Measures	Open.	Step 4