EU Stress Test

Hartlepool

Document Revision Record		
Revision	**Amendment**	**Date**
Rev 000	First Issue	December 2011
Rev 001	Minor editorial changes to Executive Summary	January 2012

Contents

Glossary

AC	Alternating Current
AGR	Advanced Gas-cooled Reactor
ALARP	As Low As Reasonably Practicable
AOD	Above Ordnance Datum
ASME	American Society of Mechanical Engineers
DBE	Design Basis Earthquake
DC	Direct Current
DECC	Department for Energy and Climate Change
DEFRA	Department for Environment, Food and Rural Affairs
g	Acceleration due to gravity
HRA	Hartlepool Power Station
IAEA	International Atomic Energy Agency
INPO	Institute of Nuclear Plant Operators
LC	Licence Condition
NSP	Nuclear Safety Principle
ONR	Office for Nuclear Regulation
pa	per annum
PGA	Peak Ground Acceleration
PWR	Pressurised Water Reactor
SOER	Significant Operating Experience Report
WANO	World Association of Nuclear Operators

Executive Summary

Hartlepool

Executive Summary

Introduction

In response to the 11 March 2011 Great East Japan Earthquake and the subsequent events at Fukushima Dai-ichi Nuclear Power Plant it was immediately clear to EDF Energy[1] that a thorough response was appropriate to assess and take corrective actions to address any identified issues discovered when reviewing the lessons learned from this event.

An internal review of our nuclear facilities and emergency response measures was initiated by the Board; this was then expanded to include the scope of a Significant Operating Experience Report (SOER) issued by WANO, the World Association of Nuclear Operators, an international cross industry organisation which aims to help its members achieve the highest levels of operational safety and reliability.

On 12 March 2011, the Secretary of State for Energy and Climate Change, Chris Huhne, requested Mike Weightman, HM Chief Inspector of Nuclear Installations, to produce a report on the implications for the UK nuclear industry of the accident that took place at the Fukushima Dai-ichi nuclear power station, the interim findings of which were published in May focuses on significant lessons for the safety of nuclear power stations operating in the UK and proposals to build new ones. It looks at the evidence and facts, as far as they were known at that time, to establish technically based issues that relate to possible improvements in safety and regulation in the UK. It also indicates some lessons for international arrangements for such systems.

In addition to this, the Council of the European Union declared that "the safety of all EU nuclear plants should be reviewed, on the basis of a comprehensive and transparent risk assessment ("stress tests")". On 25 May 2011 the European Commission and the European Nuclear Safety Regulators' Group (ENSREG) produced a joint specification for a three stage process covering all 143 nuclear plants in the EU.

The "stress test" is defined as a targeted reassessment of the safety margins of nuclear power plants in the light of the events which occurred at Fukushima: extreme natural events challenging the plant safety functions and leading to a severe accident. The technical scope of the reassessment is concerned with an evaluation of the response of a nuclear power plant when facing a set of specific extreme situations.

An EU Stress Test report has been completed for each station and submitted to the Office for Nuclear Regulation (ONR), the UK independent nuclear industry regulator: This is the EU Stress Test report for Hartlepool.

This report is focused on the adequacy of design basis protection for infrequent external hazards. Infrequent external hazards are assessed as those with a frequency of occurrence of 1 in 10,000 per year. All references to design basis in this report should therefore be interpreted as meaning a hazard with this return frequency unless otherwise stated.

This EU Stress Test Report concludes that there are no significant shortfalls in the safety case for all the UK power stations operated by EDF Energy, and that it is safe to continue their operations.

An overview and summary of each EU Stress Test subject area is provided below.

Earthquakes

In the Office for Nuclear Regulation (ONR) Interim Report into the Japanese Earthquake and Tsunami, it is stated that "The extreme natural events that preceded the accident at Fukushima - the magnitude 9 earthquake and subsequent huge tsunami - are not credible in the UK. We are 1,000 miles from the nearest fault line[2] and we have safeguards in place that protect against even very remote hazards."

With the exception of Heysham 2 (HYB) and Torness (TOR), the Advanced Gas-Cooled Reactors (AGRs) were not originally designed to withstand earthquakes. Sizewell B, a Pressurised Water Reactor, was based on the Standard Nuclear Power Plant (SNUPPS) design and the standard design included qualification against earthquake. However, for the pre-HYB/TOR AGRs, seismic safety cases were developed as part of the first Periodic Safety Review (PSR) in the late 1990s covering both the at-power and shut-down conditions as well as fuel handling operations.

[1] EDF Energy Nuclear Generation Group Ltd (NGGL) is part of EDF Energy. EDF Energy Nuclear Generation Ltd (NGL) is the licensed nuclear entity within NGGL. For the purposes of this document only the term EDF Energy will be used unless otherwise specified.

[2] Assumed to mean tectonic plate boundary

Summary of findings for earthquakes at Hartlepool

Chapter 2 of this report covers the definition of the design basis earthquake and the equipment which is expected to survive an infrequent earthquake, i.e. an event with a return frequency of 1 in 10,000 per year. There are also discussions on the margin to failure of this equipment. It demonstrates that:

- The design basis earthquake was defined as that corresponding to an infrequent event using an extensive study of historical earthquakes and local geology.
- It is not judged credible that a local earthquake would be powerful enough to produce a tsunami. This judgement is supported by a detailed study undertaken by DEFRA in 2005 to evaluate the tsunami risks to the UK.
- The design basis earthquake is reviewed by the periodic safety review process, which concluded that it was still valid in the light of modern standards and data.
- Protection of plant from seismic effects is provided through a qualification process, which ensures the plant needed to safely shut down the reactor and provide post-trip cooling remains available following the infrequent seismic event.
- Suitable processes are in place to ensure that the plant remains compliant with its licensing basis.
- No cliff-edge (i.e. a large change in impact for a small change in hazard) effects are expected for events up to twice as severe as the design basis.

The seismic safety case is based on the provision of a line of protection with redundancy for the infrequent design basis earthquake, and two lines of diverse protection with redundancy, for more frequent earthquakes. These cases are considered to be robust. Emergent issues regarding the validity of these cases are treated using established company processes.

The processes for ensuring robustness of the plant for seismic events are well developed and implemented and give appropriate consideration to the requirement for margins. They make appropriate use of international experience and standards both nuclear specific and discipline specific.

Furthermore they have been reviewed periodically in line with company process and regulatory expectations. The methodologies are internationally recognised and have been constructed with appropriate conservatisms, margins and sensitivity studies employed. Thus:

- The severity of the earthquake chosen for the design basis event is considered conservative.
- There is high confidence that the essential systems structures and components will remain functional in a design basis earthquake.
- The essential systems structures and components are tolerant to more severe earthquakes, with the event needing to be approximately twice as severe in order for significant plant damage to occur.

In considering the robustness to beyond design basis earthquakes, several areas have been identified where enhancement could be considered. These are identified as considerations and will be assessed on an appropriate timescales. The areas for consideration are not considered to undermine the current operating basis of the station.

External Flooding

In the Office for Nuclear Regulation's (ONR) report on the Japanese Earthquake and Tsunami Implications for the UK Nuclear Industry, the following is stated.

"The UK nuclear industry should initiate a review of flooding studies, including from tsunamis, in light of the Japanese experience, to confirm the design basis and margins for flooding at UK nuclear sites, and whether there is a need to improve further site-specific flood risk assessments as part of the periodic safety review programme, and for any new reactors. This should include sea-level protection."

In line with the statement quoted above from the ONR report, the Stress Test focuses on the External Flooding hazard. Within EDF Energy Nuclear Generation, the External Flooding hazard is defined as 'Extreme rainfall, snowmelt, high tide, surge and waves, tsunami, seismic seiches or gross failure of reservoirs external to the licensed site which directly or indirectly could result in the risk of a radiological release'. The Internal Flooding hazard, which considers flooding from sources within the licensed site, such as failed pipework, tanks, etc. is considered by the station safety case but is beyond the scope of this report. Any further references to floods in this report concerns the external flooding hazard.

<u>Summary of findings for external flooding at Hartlepool</u>

Chapter 3 of this report assesses the margins of the existing design basis, as well as the existing flood protection in place at Hartlepool Nuclear Power Plant. It demonstrates that:

- Hartlepool power station occupies an elevated area of land and is protected by its surrounding coast line. As a result the site would not be flooded by an infrequent high tide and storm surge or a tsunami.
- According to the DEFRA report (2005), the probability of a tsunami hitting the UK is extremely low and therefore the risks from tsunami are considered insignificant. This is also concluded within the Weightman report on the response to the Japanese Earthquake and Tsunami.
- An infrequent rainfall event could deposit a significant amount of water on site. However, the natural fall of the land aided by site drainage would prevent a significant amount of water entering the buildings. In addition, all bottom line plant is located on elevated plinths. As a result the loss of safety related plant during an extreme rainfall event would not be expected.
- Hartlepool power station is not vulnerable to flooding as a result of reservoir failure, fluvial flooding or seismic seiches. Flooding caused by rapid melting of snow would be bounded by an extreme rainfall hazard. Accordingly, the loss of safety related plant during an extreme rainfall event would not be expected.
- The information presented shows that the methodology used to calculate the design basis flood for Hartlepool has been constructed using independent expertise based on well regarded sources of information. The methodology has also been constructed with appropriate conservatisms, margins and sensitivity studies employed.
- The methodology for determining external flooding risk has been reviewed periodically in line with company process and regulatory expectations.
- Appropriate consideration has been given to the predicted impact of climate change on the risk of external flooding due to sea level rise and increasing wave heights. It has been demonstrated that appropriate margins will be maintained beyond the operating life of the station.
- Operating procedures and emergency activities identified for the management of actions in response to external flooding have been reviewed and their adequacy confirmed.
- For the purposes of beyond design basis risk management a number of considerations have been identified. These are focused at providing additional plant protection for a beyond design basis flooding event.

The areas for consideration are not judged to undermine the current operating basis of the station.

Extreme Weather

In the Office for Nuclear Regulation Interim Report into the Japanese Earthquake and Tsunami, Recommendation 13 states that "The UK nuclear industry should review the plant and site layouts of existing plants and any proposed new designs to ensure that safety systems and their essential supplies and controls have adequate robustness against severe flooding and other extreme external events." Recommendation 16 states that "When considering the recommendations in this report the UK nuclear industry should consider them in the light of all extreme hazards, particularly for plant layout and design of safety-related plant."

EDF Energy considers a range of hazards, some of which are initiated or come about as a result of events on the site (internal hazards) and others that arise off-site or which relate to conditions which envelop the site (external hazards).

Chapter 4 of this report considers those external hazards that are related to meteorological events other than external flooding. These are:

- Extreme Wind.
- Extreme Ambient Temperatures (Including both seawater and air temperatures).
- Lightning.
- Drought.

In each case consideration is given to the adequacy of the existing design basis event, the inherent margins in the analysis and the potential for improvements in plant robustness. In addition, the tolerance of the plant to combinations of extreme external hazards is also considered.

The findings of this work are summarised below.

Summary of findings for extreme winds at Hartlepool

Extreme winds which directly or indirectly could result in the risk of a radiological release.

This hazard includes consideration of high straight line winds and tornadoes which could rise to wind-induced collapse of structures and wind-borne missiles.

- The design basis for extreme wind is based on adherence to standards and codes. The standards are periodically updated and there is a suitable process within EDF Energy to ensure continuing compliance.
- Equipment required to fulfil the essential safety functions is either located inside buildings which are qualified against infrequent wind, or qualified directly. The safety case has been assessed against the latest codes and is robust.
- There is sufficient equipment qualified against an infrequent extreme straight line wind and tornado to ensure the plant can be shut down and post-trip cooled in all plant states.
- The station operating instructions contain actions to be taken upon receiving warnings of extreme wind, to reduce the impact of the wind on the plant.
- The safety margin against extreme wind has not been quantified in detail. It has been judged that no cliff-edge effects will be seen if extreme winds slightly beyond the design basis are experienced.
- Work is currently underway to produce a formal tornado safety case.

Summary of findings for extreme ambient temperatures at Hartlepool

Extreme Ambient (high or low) Temperatures which directly or indirectly could result in the risk of a radiological release.

The infrequent extreme ambient temperature hazard can be split into four possible events; high temperatures and low temperatures, sea temperature and snow loading. The safety case demonstrates that most equipment is expected to remain functionally available or fail-safe when subjected to the high or low ambient temperatures considered in the design basis. Operator actions play a large part in ensuring that during extreme air temperature events sufficient safety related plant remains available. Changes in sea water temperature will not impact on nuclear safety. Buildings containing essential equipment have been assessed against snow loading and most demonstrate sufficient margin. Where this has not been shown, failure of the building has been shown to be acceptable with no consequences for nuclear safety. A consideration is raised to confirm the adequacy of the existing design basis extreme temperatures, although this is not considered to undermine the current operating basis of the station.

Summary of findings for lightning at Hartlepool

This report considers a lightning strike or strikes which directly or indirectly could result in the risk of a radiological release. Protection against lightning is provided by adherence to relevant codes and standards. It is judged this remains a suitable and appropriate measure. Work is currently being undertaken to produce a formal lightning safety case, although this is not considered to undermine the current operating basis of the station.

Summary of findings for drought at Hartlepool

This report considers a lack of water as a result of prolonged periods of hot or cold weather or as a result of lack of rainfall which directly or indirectly could result in the risk of a radiological release.

This hazard includes consideration of loss of cooling water and water stocks for post-trip cooling, the impact of drought on the foundations of the site and of the civil structures and the effect of the hazard on the main electrical earthing system.

Drought is currently not considered as a formal hazard, as it is difficult to quantify. The primary defence against drought is that it is slow to occur compared with the 24 hour mission time of the station. Work is currently being undertaken to produce a formal drought safety case, although this is not considered to undermine the current operating basis of the station.

Overview of combinations of hazards

A systematic consideration of all the possible combinations of hazards has been undertaken. It has been concluded that combinations of hazards will not impact on nuclear safety.

Loss of Electrical Power and Loss of Ultimate Heat Sink

Severe damage of the reactor is prevented by the essential safety functions of reactor trip, shutdown and hold-down, adequate post-trip cooling monitoring and maintaining the containment for the fuel and fission products. One of the main aspects of the Fukushima incident relates to the provision of adequate post-trip cooling and this is the main essential safety function that is affected by the scenarios in this section.

Chapter 5 of this Stress Test report focuses on prevention of severe damage to the reactor and to the irradiated fuel under various loss of electrical power and loss of ultimate heat-sink scenarios, including an evaluation of times available to prevent severe damage in various circumstances.

The Stress-Test requires a consideration of 'Loss of Electrical Power', including sequential loss of grid supply and on-site AC generation back-up supply leading to a 'Station Black Out' scenario, where all electrical AC supplies are lost.

The Stress Test also requires a consideration of 'Loss of Ultimate Heat Sink'. Within this a number of scenarios are considered, the impact of the loss of the primary ultimate heat sink (seawater) as well as, loss of primary ultimate heat sink combined with loss of alternate heat sinks (i.e. other cooling water supplies and heat-transfer routes to atmosphere). The Stress Test also required the combined consequences of station black out and loss of primary ultimate heat sink.

Chapter 5 considers the impact upon the reactor essential safety functions due to the above scenarios and consider the plant requirements for fulfilling the essential safety function of post-trip cooling for both the pressurised reactor and depressurised reactor state. In addition, it looks at plant requirements for maintaining cooling to fuel route plant areas.

The chapter is based around a number of specified scenarios and the timescales to failure once all lines of protection have been compromised. This chapter therefore considers severe "cliff edge" changes in available reactor cooling.

Summary of risks from loss of electrical power and loss of ultimate heat sink at Hartlepool

This report concluded the following points on consideration of a loss of electrical power and loss of ultimate heat-sink at Hartlepool Power Station.

- Loss of off-site power supplies is covered by the existing safety case and the on-site generators will provide diverse supplies. There are sufficient supplies of stocks available on-site to allow all post-trip essential safety functions to be met for a number of days.
- Loss of off-site power combined with failure of on-site generators is an event considered within the safety case for an operating reactor and adequate provisions already exist to support the essential safety functions.
- There are provisions off-site that could be deployed to station within 10 hours and aid in continued post-trip cooling of the reactor.
- Following a beyond design basis accident, actions required by shift staff could be hindered by conditions on-site. Mitigation of this is provided in the form of the alternative indication centre, the central emergency support centre and procedures for beyond design basis events.
- Modelling of some severe accident scenarios has been carried out. These have been used for the examination carried out in this report. It has been noted that reconfirmation of these analyses and additional sensitivity studies would be beneficial.
- As loss of the primary ultimate heat-sink is covered by the safety case, no external actions beyond those covered by station operating instructions are required to prevent fuel degradation.

- Loss of the primary ultimate heat-sink is within design basis. Alternative provisions already exist to support the essential functions.
- In the event of a loss of the primary ultimate heat-sink, there are sufficient stocks of cooling water for a minimum period of 24 hour.
- In the event of both loss of grid or station black out, sufficient cooling can be maintained to the station fuel route areas for at least 72 hours.
- Whilst there are no vulnerabilities identified in the current design basis for the fuel route against loss of electrical power, further resilience enhancements can be envisaged.

Severe Accident Management

In the ONR Interim Report into the Japanese Earthquake and Tsunami, Mike Weightman states:

"The UK nuclear industry should review the provision on-site of emergency control, instrumentation and communications in light of the circumstances of the Fukushima accident including long timescales, wide spread on and off-site disruption, and the environment on-site associated with a severe accident."

"The UK nuclear industry, in conjunction with other organisations as necessary, should review the robustness of necessary off-site communications for severe accidents involving widespread disruption."

"The UK nuclear industry should review existing severe accident contingency arrangements and training, giving particular consideration to the physical, organisational, behavioural, emotional and cultural aspects for workers having to take actions on-site, especially over long periods. This should take account of the impact of using contractors for some aspects on-site such as maintenance and their possible response."

This EU Stress Test report explores the organisation and management measures which are in place within EDF Energy to deal with severe accidents.

In a number of places, this EU Stress Test report refers to the need for ongoing development work. Some of this work had been previously identified and captured by normal company processes, whilst some is new work highlighted by the post-Fukushima review.

The Japanese event and findings from the stress test has provided EDF Energy with an opportunity to review its accident management capabilities. EDF Energy has concluded that it has robust arrangements for Emergency Response. However there are lessons we have learnt during this process which we will consider in order to improve our response.

These can be broadly categorised into three areas:

- Facilities – this includes site resilience and multi site support.
- Technical – communications and supply chain.
- Procedures – emergency arrangements and procedures taking into account staff welfare.

Training and Exercising encompasses all elements as it is only through these functions EDF Energy can ensure continuous improvement and oversight of our arrangements.

The provision of off-site equipment and support is a maintained and formal process within EDF Energy Nuclear Generation. Following the 2011 emergency in Japan it is recognised that it is possible that the equipment could be enhanced to provide further resilience to the emergency scheme. This is something which is being taken forward within EDF Energy Nuclear Generation.

Conclusion

This EU Stress Test Report concludes that there are no significant shortfalls in the safety case for all the UK power stations operated by EDF Energy, and that it is safe to continue their operations. This conclusion is consistent with conclusion IR-1 from the ONR's Interim Report i.e. "In considering the direct causes of the Fukushima accident we see no reason for curtailing the operation of nuclear power plants or other nuclear facilities in the UK".

Chapter 0 - Introduction

Hartlepool

0 Introduction

0.1 Background

In response to the 11 March 2011 Great East Japan Earthquake and the subsequent events at Fukushima Dai-ichi Nuclear Power Plant it was immediately clear to EDF Energy[3] that a thorough response was appropriate to assess and take corrective actions to address any identified issues discovered when reviewing the lessons learned from this event.

An internal review of our nuclear facilities and emergency response measures was initiated by the Board; this was then expanded to include the scope of a Significant Operating Experience Report (SOER) issued by WANO, the World Association of Nuclear Operators, an international cross industry organisation which aims to help its members achieve the highest levels of operational safety and reliability.

On 12 March 2011, the Secretary of State for Energy and Climate Change, Chris Huhne, requested Mike Weightman, HM Chief Inspector of Nuclear Installations, to produce a report on the implications for the UK nuclear industry of the accident that took place at the Fukushima Dai-ichi nuclear power station, the interim findings of which were published in May focuses on significant lessons for the safety of nuclear power stations operating in the UK and proposals to build new ones. It looks at the evidence and facts, as far as they were known at that time, to establish technically based issues that relate to possible improvements in safety and regulation in the UK. It also indicates some lessons for international arrangements for such systems.

In addition to this, the Council of the European Union declared that "the safety of all EU nuclear plants should be reviewed, on the basis of a comprehensive and transparent risk assessment ("stress tests")". On 25 May 2011 the European Commission and the European Nuclear Safety Regulators' Group (ENSREG) produced a joint specification for a three stage process covering all 143 nuclear plants in the EU.

The "stress test" is defined as a targeted reassessment of the safety margins of nuclear power plants in the light of the events which occurred at Fukushima Dai-ichi: extreme natural events challenging the plant safety functions and leading to a severe accident. The technical scope of the reassessment is concerned with an evaluation of the response of a nuclear power plant when facing a set of specific extreme situations.

A review of safety has been structured to address the needs of an internal EDF Energy review, the Weightman report and the "stress test". An EU Stress Test report has been completed for each station and submitted to the Office for Nuclear Regulation (ONR), the UK independent nuclear industry regulator.

0.2 Scope of Stress Test

This Stress Test comprises an examination safety against the scope of the stress test. This includes a review of the definition and magnitude of the initiating event, the physical safety measures, operator training and the procedural arrangements that are claimed as a barrier to prevent or minimise the release of radioactive material and the arrangements for severe accident management.

The scope of this Stress Test covers the following plant areas, which are described in more detail in chapter 1:

- **the main reactor and associated structure**, which contains the majority of the nuclear material;
- **the fuel route,** where new fuel assemblies are built before they are loaded to the reactor and where used fuel assemblies are removed from the reactor and processed, and;
- **the fuel cooling ponds and buffer stores,** where fuel elements are stored prior to being exported from the site.

As well as the existing safety justifications, this Stress Test considers the response of the plant and the claimed safety measures to challenges of a severity in excess of those already covered in the station Safety Cases. The nature of the challenges has been defined considering the issues that have been highlighted by the events that occurred at Fukushima

[3] EDF Energy Nuclear Generation Group Ltd (NGGL) is part of EDF Energy. EDF Energy Nuclear Generation Ltd (NGL) is the licensed nuclear entity within NGGL. For the purposes of this document only the term EDF Energy will be used unless otherwise specified.

Dai-ichi, including combinations of initiating events and failures. These include the directly relevant hazards such as earthquake and flooding (from tsunamis and other sources) and other extreme weather conditions, potentially more relevant to the UK such as high winds and extreme ambient temperatures.

In these extreme situations, sequential loss of the engineered lines of defence is assumed, in a deterministic approach, irrespective of the probability of this loss. In particular, it has to be kept in mind that loss of safety functions and severe accident situations can occur only when several design provisions have failed.

In addition to the response of the installed lines of defence to a specific initiating event, the Stress Test also considers the effects of:

- Loss of electrical power, including station black out
- Loss of the ultimate heat sink
- Combination of both station black out and loss of ultimate heat sink

In this report the station black out scenario is defined as a loss of **all** station electrical supplies. This includes the loss of the grid electrical supply, the loss of the station on-site normal (ordinary) electrical supplies and on-site diverse (alternative) electrical supplies.

The loss Of the ultimate heat sink scenario is defined as the loss of **all** cooling water supply to the station; including the primary heat sink (sea water) as well as the main and diverse (alternative) heat sink supplies.

These scenarios are conservatively assessed without specifying the likelihood or nature of the initiating event or the probability that loss of all of these safety functions could occur.

The Stress Test also considers the arrangements for managing severe accidents if the engineered safety measures fail to prevent the loss of the essential safety functions.

Throughout the Stress Test considerations are raised. These are defined as 'Opportunities to further examine potential enhancements to plant, process or people for beyond design basis scenarios'.

0.3 EDF Energy's Nuclear Sites

EDF Energy is one of the UK's largest energy companies and the largest producer of low-carbon electricity, producing around one-sixth of the nation's electricity from its nuclear power stations, wind farms, coal and gas power stations and combined heat and power plants. The company supplies gas and electricity to more than 5.5 million business and residential customer accounts and is the biggest supplier of electricity by volume in Great Britain.

In its nuclear activities EDF Energy has partnered with Centrica, which has a 20% stake in the company's eight existing plants and in the project carrying out pre-development work for nuclear new build. EDF Energy has prepared this response to the Japan earthquake on behalf of the joint venture between the two companies.

EDF Energy Nuclear Generation Ltd is the nuclear licensee and operates 15 reactors on 8 sites in the UK: one Pressurised Water Reactor (PWR) at Sizewell in Suffolk and 14 Advanced Gas Cooled Reactors (AGRs) at sites at Hinkley Point in Somerset, Heysham in Lancashire, Torness in Lothian, Hunterston in Ayrshire, Hartlepool on Teesside and at Dungeness in Kent.

Table 0.1: EDF Energy power stations, type, capacity and significant dates.

Power Station	Type	Net MWe	Construction started	Connected to grid	Full operation	Accounting closure date
Dungeness B	AGR	1040	1965	1983	1985	2018
Hinkley Point B	AGR	820	1967	1976	1976	2016
Hunterston B	AGR	820	1967	1976	1976	2016
Hartlepool	AGR	1190	1968	1983	1989	2019
Heysham 1	AGR	1160	1970	1983	1989	2019

Heysham 2	AGR	1235	1980	1988	1989	2023
Torness	AGR	1230	1980	1988	1988	2023
Sizewell B	PWR	1188	1988	1995	1995	2035

Figure 0-1: Map of the UK showing EDF Energy nuclear power stations.

The stations were designed and licensed to operate against standards appropriate at that time. Throughout their respective lives the stations have been subject to regular, formal review of their basis of design in the form of safety case reviews. These reviews form an essential and mandatory part of the UK legislative framework for nuclear facilities (discussed below) and both the reviews and the identified improvement activities are discussed in more detail in chapters 2 to 6.

0.4 Background to UK Nuclear Safety Framework and EDF Energy's Arrangements

The UK Health and Safety at Work Act leads to legislation made under the Act that may be absolute or qualified by expressions such as the need for duty holders to ensure "reasonable practicability". (As Low As is Reasonably Practicable - ALARP). The term reasonably practicable allows for a cost benefit analysis to be used when determining the actions to be taken in response to an identified risk, or for a comparison to be carried out with "good practice" in similar circumstances. The preventative measures taken should however be commensurate with the magnitude of the risk. Both "practicable" and "reasonably practicable" are statutory criminal liabilities in health and safety legislation. HSE guidance has been published on how this should be interpreted and the use of Cost Benefit Analysis. Several important points should be noted:

- There should be a transparent bias on the side of health and safety. For duty holders, the test of 'gross disproportion' requires erring on the side of safety in the computation of health and safety costs and benefits.

- Whenever possible, standards should be improved or at least maintained, thus current good practice is used as a baseline - the working assumption being that the appropriate balance between costs and risks was struck when the good practice was formally adopted.
- Hazards are regulated through a safety case regime requiring an explicit demonstration in the safety case that control measures introduced conform to the ALARP principle.

Nuclear facilities in the UK are required to have a licence to operate issued under the Nuclear Installations Act 1965 as amended (NIA65). The licence is granted to a corporate body by the UK Health and Safety Executive (HSE) and specifies the activities that can be undertaken at the named site. As mentioned previously EDF Energy Nuclear Generation Ltd is the licensed entity for the sites operated in the UK by EDF Energy.

The licence allows for the regulation by the ONR, on behalf of the HSE, of the design, construction, operation and decommissioning of any nuclear installation for which a nuclear site licence is required under NIA65. Attached to each licence is a standard set of 36 conditions developed by the ONR. In the main they require the licensee to make and implement adequate arrangements to address the particular issues identified. The licence conditions are largely non-prescriptive and set goals that the licensee is responsible for achieving. EDF Energy has developed compliance principles for all 36 licence conditions and implements these through identified primary and secondary implementation documents, which include both Company-wide and site-specific documents.

Licence Condition (LC) 14 requires arrangements for the production and assessment of safety cases consisting of documentation to justify safety during the design, construction, manufacture, commissioning, operation and decommissioning phases of the installation. The Safety Case covers all activities undertaken at each site, the hazards associated with these and the safety measures, whether engineered or procedural, necessary to protect against or mitigate these hazards. The Safety Case defines limits and conditions on plant operation within which the safety of the plant is demonstrated. By operating within these limits and conditions it is shown that the risks are adequately controlled and that safety significant issues have been addressed. The limits and conditions arising from the Safety Case form the operating rules for compliance with LC 23, and operating instructions are provided in accordance with LC 24 to ensure these operating rules are implemented, along with any other instructions necessary in the interests of safety.

LC 28 requires regular and systematic examination, inspection, maintenance and testing of the engineered safety systems claimed in the Safety Case to ensure that they remain available and fit for purpose, and a schedule of these requirements is provided for each site. Safety measures and other safety significant actions that require operator action must be carried out by suitably qualified and experienced persons in accordance with LC12 and, in conjunction with arrangements for training in accordance with LC 10, each site maintains records of staff qualification and authorisation.

LC 22 requires arrangements to control any modification carried out on any part of the existing plant or processes which may affect safety. Modifications to implement new plant or processes, or a change to existing plant or processes represent a change that affects the existing safety case. For all modifications, consideration of safety must be full and complete, including any necessary amendment of rules, instructions, plant procedures and training requirements to be undertaken prior to implementing the proposed change. Consideration of such changes is an essential element in the justification of the proposed modification. In accordance with LC 22, EDF Energy has implemented a modifications process; modifications are categorised based on the potential for nuclear safety risk, with additional approvals required as risk increases.

LC15 requires a periodic and systematic review and reassessment of safety cases. Arrangements for periodic review complement the continuous review and maintenance of the Safety Cases under LC22 and ensure that the cumulative effects of plant ageing, operating experience and plant modifications are considered in totality.

Periodic safety reviews discharge the requirements of LC15 and are retrospective (learning from experience) and prospective, in reviewing the impact of changes in safety standards, expected lifetimes, uses, requirements, interaction with other plant and possible contingency measures which may be required. The periodic safety reviews are designed to ensure that a thorough and comprehensive review is made of the safety case at regular intervals throughout a nuclear installation's life. The objectives of the periodic safety reviews are:

- to review the total current safety case for the nuclear installation and confirm that it is robust;

- to compare the safety case with modern standards, evaluate any deficiencies and implement any reasonably practicable improvements to enhance plant safety;
- to identify any ageing process which may limit the life of the installation;
- to revalidate the safety case until the next periodic safety review, subject to the outcome of routine regulation.

The first AGR periodic safety reviews were completed in 1996 for Hinkley Point B and Hunterston B, with other AGR following thereafter. These are referred to as periodic safety review 1 and marked the start of a cycle of periodic safety reviews for all of EDF Energy's nuclear power stations. Periodic safety review 1 for Sizewell B was completed in 2005.

The second wave of periodic safety reviews, referred to as periodic safety review 2, commenced in 2002 with a review process that was broadly similar to periodic safety review1 but included strategic changes to reflect lessons learnt. SZB periodic safety review 2 is underway and is due for completion in 2015.

LC 11 requires the provision of arrangements for dealing with any accident or emergency arising on the site and their effects; arrangements for compliance with LC 11 are described in section 0.9.

0.5 Safety Case Methods and Principles

The AGRs were originally designed using conservative engineering judgement with the application of relevant engineering codes and standards. The safety cases were produced and maintained on the basis of established precedent. In the early 1990s it was recognised that formal guidance on safety standards was required to assist in avoiding inconsistencies and to form the basis for the AGR periodic safety reviews. A set of assessment guidelines, the Nuclear Safety Principles (NSPs), were produced. The NSPs are now the EDF Energy internal standard for AGR safety cases. Equivalent documents were developed for the PWR during the original safety case development phase.

The NSPs were defined taking into account the 'Safety Assessment Principles for Nuclear Plant' issued by ONR, the document issued by the HSE entitled 'The Tolerability of Risk from Nuclear Power Stations (TOR) and the 'Advanced Gas Cooled Reactor Design Safety Guidelines" document, which was employed in the design of the newest AGR at Heysham 2.

The NSPs contain a General Basic Principle, which identifies how safety reviews should be completed, the expectations for which techniques should be used and the application of appropriate quality assurance. This Principle discusses the two complementary techniques of deterministic and probabilistic assessment, which are employed to ensure that the reviews are complete and demonstrate the adequacy of the identified safety measures.

0.5.1 Deterministic Principles (NSP 2)

The Deterministic Principles describe the standard against which EDF Energy complete deterministic assessments. They provide a framework for reaching judgements on the adequacy and acceptability of the safety provisions based on simple qualitative engineering principles, in particular the concept of defence in depth.

Defence in depth is a fundamental principle of nuclear safety and is used throughout the world. The aim of defence in depth is the provision of a series of levels of defence, which can be inherent in the design, specifically engineered safety measures or operational procedures to provide a barrier between radioactive materials and the environment aimed at:

- Prevention of failures of equipment and deviation from normal operation,
- Protection against the release of radioactive material if plant failure or deviation occurs, and,
- Mitigation to minimise the consequence of the fault progression if the protection fails.

The Safety Case considers all potential initiating events induced by both equipment and human faults and the effect of internally and externally generated hazards. Prevention of failures and deviation from normal operation is the first priority as it is generally easier to provide effective preventative measures than to deal with the consequences of failure. Conservative design with large safety margins and operation of the plant within these margins aims to ensure that failure limits are not reached. The plant control systems, operating instructions and maintenance of the plant ensure that this barrier is maintained.

If it is not possible to prevent the fault, to demonstrate that the fault is sufficiently unlikely or that the consequence sufficiently low that it does not need to be considered then protection measures are required. Any initiating event which can affect the reactor or its support systems should be protected by provisions which ensure, as far as is reasonably practicable, the trip, shutdown, post-trip cooling or any other essential function. The purpose of the essential functions is to ensure that the physical barriers to the release of radioactive material are maintained. For an AGR reactor core the physical barriers are the matrix of the fuel, the stainless steel cladding around the fuel pellets and finally the steel lined pre-stressed concrete pressure vessel.

The Deterministic Principles associated with protection ensure that consideration is given to good engineering design and that the protection measures are functionally capable, incorporate redundancy and diversity[4] where required and that at least one line of protection remains available in all permissible plant states. The type of protection required is based on the frequency of the event, with more frequent events requiring protection with a higher level of integrity. These rules have been developed based on sound engineering principles and the likely reliability of the system if the rules are applied.

Hazards, both internal and external, are a particular type of fault and owing to their nature are treated in a slightly different way to the plant based faults. The EDF Energy approach to hazard assessment is described in section 0.6

Unless the likelihood of occurrence is sufficiently small, or the consequences sufficiently limited, any initiating event which can affect the reactor or its support systems, and which potentially could lead to public harm, are protected by provisions which ensure, as far as is reasonably practicable, the trip, shutdown, post-trip cooling or any other essential function.

Initiating events are defined as Frequent if they have an estimated frequency of occurrence greater than 10^{-3}/year. For any frequent initiating event there are at least 2 lines of protection to perform any essential function, with diversity between each line, during any normally permissible state of plant availability, unless it is shown not to be reasonably practicable.

Initiating events are defined as Infrequent if they have an estimated frequency of occurrence less than or equal to 10^{-3}/year. For any Infrequent Initiating Event there is at least 1 line of protection to perform any essential function and that line is provided with redundancy, during any normally permissible state of plant availability, unless it is shown not to be reasonably practicable. As a minimum, during any permissible state of plant or equipment unavailability for testing or maintenance, there should be at least one line of protection to perform any essential function for any initiating event with a frequency of greater than or equal to 10^{-5}/year."

Events whose estimated frequency of occurrence is judged to be less than 10^{-5}/year are not assessed against the Deterministic Principles, however the reasonable practicability of providing protection for such events is considered.

Initiating events which, in the absence of protection, would lead to a dose of less than 1 ERL[5] at the outer edge of the detailed emergency planning zone are not formally assessed against the Deterministic Principles. However, the reasonable practicability of providing protection for such events is considered.

The final Deterministic Principle is concerned with mitigation of the consequences should the initiating event occur (failure of prevention) and the protection measures prove to be inadequate or fail to operate as intended. Arrangements exist in the form of procedures and guidance to provide advice on accident management. These are discussed in section 0.8

4 Redundancy is defined as the provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other. Diversity is defined as the presence of two or more systems or components to perform an identified function, where the systems or components have different attributes e.g. one electrical device and one mechanical device so as to reduce the possibility of common cause failure, including common mode failure.

5 Emergency Reference Levels (ERLs) are used in emergency planning and are specified at a level where the dose saved by countermeasures such as sheltering and evacuation is a greater benefit than the risks and disbenefits associated with implementing them. For example evacuation introduces conventional traffic risks and disruption.

Implicit within the principle is the concept of permissible plant states. Plant can be unavailable for a number of reasons such as breakdown or pre-emptive maintenance and the unavailability of this plant needs to be managed such that the essential safety functions can still be achieved. The allowable plant availability is defined in a series of documents called Technical Specifications (or Tech Specs) which include all of the limits and requirements for normal operation of the plant both at power and shutdown. In addition to the requirements and limits the Tech Specs also include actions to be taken if they are not met.

The Tech Specs use three classes of plant unavailability, which are described below:

(i) The 'normal maintenance' state is one in which the level of essential plant availability is defined in Technical Specifications as being allowed to exist for consecutive period of 31 days.

(ii) The 'urgent maintenance' state, as defined in Technical Specifications, will have an action completion time significantly less than 31 days, typically between 36 and 72 hours. It reflects a lower state of plant availability than the normal maintenance state. Whenever practicable, maintenance and testing shall be planned so as not to introduce an urgent maintenance state.

(iii) If the plant availability falls below the urgent maintenance state, then there is a need for 'immediate remedial action' within short timescales, either to restore essential plant or achieve safe shutdown of the reactor.

0.5.2 Probabilistic Principles (NSP 3)

The second technique used is probabilistic assessment. Probabilistic Safety Analysis (PSA) provides an accompanying role as an aid to judgement, in support of a deterministic approach. PSA provides a comprehensive, systematic and numerical analysis of the plant and the role of its safety provisions, and demonstrates that the risk arising from the plant is acceptable. The PSA can highlight areas where simply following the Deterministic Principles may not lead to adequate reliability of protection or where an excessive claim is being placed on a particular safety system to perform its function.

The Probabilistic Principles provide a framework for assessing whether the risks to the public are both tolerable and as low as reasonably practicable (ALARP). ALARP is a key part of the general duties of the Health and Safety at Work etc. Act 1974 and is a demonstration that the risk is at a level where the time, trouble and cost of further reduction measures become unreasonably disproportionate to the additional risk reduction obtained.

The principles relating to the doses to the public identify two levels of risk; a lower "Broadly Acceptable" level below which the risks are sufficiently low that no detailed review of measures to further reduce risk is required and an upper "Tolerable" level above which, in all but exceptional circumstances, there is a need to identify and implement safety enhancements. Between these two levels is the ALARP or Tolerability region where there is a need to demonstrate that risks are ALARP or to implement safety enhancements to achieve this end.

The Tolerable and Broadly Acceptable levels of risks to the individual and society are discussed in the Tolerability of Risk document by the HSE. In summary these views were that the risk from any large industrial plant should be considered Tolerable provided that the predicted total risk of fatality to any identified individual member of the public lies in the range 10^{-4} to 10^{-6} p.a., and should be considered Broadly Acceptable if the individual risk is $<10^{-6}$ p.a..

The Probabilistic Nuclear Safety Principles used by EDF Energy are based upon two premises. The first premise is that a risk of fatality for any identified individual member of the public of $<10^{-7}$ p.a., from all accidents at a single reactor, is Broadly Acceptable, and that at this level of individual risk it is not necessary to consider the practicability of reducing the risks to society as a whole provided that the frequency of all accidents resulting in a large release (greater than 100 fatalities) is $<10^{-6}$ p.a.. The second premise is that the risk from all accidents for a single reactor is considered to be tolerable provided that the risk to any individual member of the public is $<10^{-5}$ p.a. and the risks to society are demonstrated to be ALARP.

The risk of fatality is calculated as a function of the effective dose received by a member of the public, the frequency that the dose is realised (i.e. the fault frequency) and the probability that the effective dose will lead to a fatality. The Probabilistic Principles are structured in such a way as to introduce surrogates for the levels of risk identified above because, if these surrogates are satisfied, they require less analysis. However if the surrogates are not satisfied, then the analyst has the option of demonstrating compliance with a higher level principle at the expense of further work. These surrogate frequency/effective dose principles are shown graphically below:

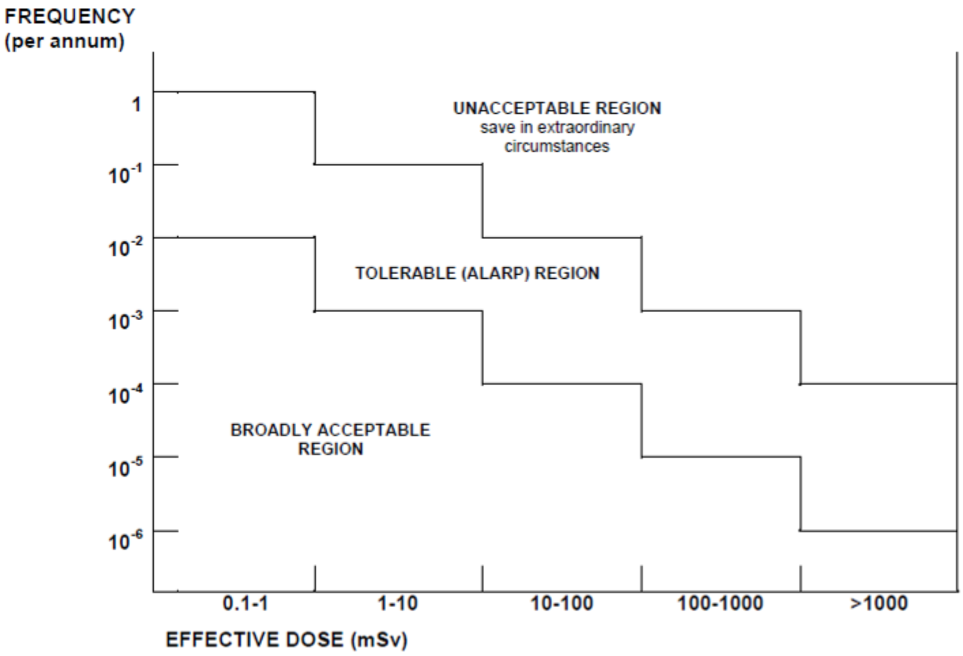

Figure 0-2: Surrogate risk regions as a function of frequency and effective dose.

In addition to the risk criteria for members of the public, the NSPs provide the corresponding safety targets for the risk to workers from accidental exposure to radiation (NSP 4).

0.5.3 Shutdown Cooling Criterion

When a reactor is tripped by the insertion of control rods to halt the nuclear chain reaction, and shutdown commences the cooling plant available will reflect the plant availability prior to the trip. As the decay heat falls, the plant availability and reactor conditions (pressure, atmosphere) can be progressively relaxed. The safety case defines the manner in which this relaxation is performed, defining levels of plant availability and reactor conditions below which the operator should not seek to progress until the decay heat has fallen to an acceptable level.

When a reactor is shutdown, the number of potential configurations of cooling plant is such that a full probabilistic assessment of faults is not practicable. Therefore a set of shutdown fault criteria have been developed to be a surrogate for both the deterministic and probabilistic NSPs. These shutdown fault criteria require levels of diversity and redundancy equivalent to those required by the NSPs, while taking account of the range of plant configurations which need to be implemented for essential maintenance on a shutdown reactor.

The important thing to note on a shutdown reactor is that there may be more demand on operator actions rather than automatic engineered safety systems as the systems may be out for maintenance. This potential increase in risk is offset by the increased timescales available to complete the actions owing to the reduced decay heat.

0.6 Specific Assessment and Design Against Hazards

Hazards are a particular subset of faults within the safety cases that are of particular interest as they have the potential to cause extensive harm in their own right as well as damaging or disabling multiple safety systems across the site. In some cases, such as seen at Fukushima Dai-ichi, not only is the plant affected by the initial event (e.g. seismic acceleration) but there are also consequential effects such as flooding from tsunamis. The NSPs require consideration of internal and external hazards in safety cases. Internal hazards are defined as those which initiate on the nuclear licensed site due to the presence of the power station facility. External hazards are those which initiate external to the nuclear licensed site and would occur even in the absence of the facility.

The main reason for categorising the hazards in this way is that internal hazards are faults for which EDF Energy can have a direct influence in limiting the magnitude and frequency of the hazard by, for example, minimising quantities of flammable materials or ensuring hazardous equipment is suitably segregated. External hazards are those which initiate independently of EDF Energy's operations and to which EDF Energy have limited (such as industrial hazards) or no (such as meteorological hazards) control over the magnitude or frequency of the hazard event.

The nature of the event at Fukushima Dai-Ichi and therefore focus of this Safety Report are the natural external hazards. Unlike other faults they cannot be prevented and so, as far as defence is depth is concerned, one of the barriers is not available. In addition, the external hazards have the potential to affect multiple systems on the site and disrupt large areas in the locality of the site, which could hamper recovery operations, challenging the other levels of defence in depth.

The majority of hazards had limited coverage in the original Station Safety Reports for the early AGRs, although by the time the last of the fleet were built, the concept of hazards and their significance in nuclear safety had been more fully developed, and defence against hazards was built into the design of Heysham 2, Torness and Sizewell B Power Stations.

For the older AGRs the first systematic review of AGR safety cases against a list of potential hazards was completed as part of periodic safety review 1 during the 1990s. Periodic safety review 1 considered a wide range of potential internal and external hazards explicitly and established the basis for a safety case with respect to these. The natural external hazards at the time included seismic, wind loading, external flooding (from rainfall, snowfall, overtopping of sea defences and outflanking of sea defences) and extreme ambient temperatures.

Prior to completion of the first periodic safety review a large capital investment programme, the AGR Safety Review and Enhancement Programme (ASREP) was implemented. The primary objective of this programme was to ensure the safety of the older AGRs to their full design lives. An important component of this was a review of the safety provisions against 'modern standards' and to assess practicability of enhancing safety by the implementation of improved procedures and plant modifications. The ASREP work led to the assessment of the likely hazards and the provision of suitably qualified safety measures to ensure that the essential safety functions could be achieved.

The list of external hazards considered by EDF Energy was further developed as part of the second periodic safety review. The list of hazards was reviewed against international standards and confirmed that the NSPs were consistent with the International Atomic Energy Agency (IAEA) recommendations current at that time. The external hazards specifically considered in the EDF Energy safety case are:

- Seismic
- Extreme Wind
- External Flooding
- Extreme Ambient Temperatures
- Lightning
- Drought
- Biological Fouling

The existing safety case for each of these hazards apart from biological fouling is discussed in chapters 2 to 4 where they exist. It should be noted that the second periodic safety review judged that some of the other hazards listed in the IAEA standards, such as avalanche and mudslide, are not a threat to the EDF Energy sites. Consequently, these are not listed in the NSPs and are not considered in the EDF Energy safety case.

The integrity of protection provided against External Hazards is consistent with the deterministic principles for internal faults described in section 0.5.1, above depending upon whether the event is frequent or infrequent.

External hazard events are defined as Frequent where they have an annual probability of exceedance[6] of greater than or equal to 10^{-3}. For any frequent event there are at least 2 lines of protection to perform any essential function, with

6 The probability of exceedance is the probability that an event will occur that exceeds a specified reference level during a given exposure time.

diversity between each line, during any normally permissible state of plant availability, unless it is shown not to be reasonably practicable, recognising that there should always be at least 1 line of protection.

External hazard events are defined as Infrequent where they have an annual probability of exceedance of between 10^{-3} and 10^{-4}.For any infrequent event there is at least 1 line of protection to perform any essential function and that line is provided with redundancy, during any normally permissible state of plant availability, unless it is shown not to be reasonably practicable.

External hazards events with an annual probability of exceedance of less than 10^{-4} are beyond design basis. This is consistent with the guidance published by the Office for Nuclear Regulation in the UK. The reasonable prediction of these less frequent events is difficult. The approach is therefore to demonstrate that there is no disproportionate increase in radiological consequences given a small change in design basis parameters, i.e. no “cliff-edge” effect where the consequence significantly increases with a slight increase in the challenge.

The magnitude of the hazard for a given probability of exceedance is conservatively derived owing to the uncertainties that exist. For many external hazards the available historic data are sparse and require specialist interpretation to allow a probabilistic treatment and an extrapolation to an annual probability of exceedance of 10^{-3} or 10^{-4} for frequent and infrequent events respectively. The methods used and their adequacy are discussed later in this Stress Test.

The equipment that is claimed to provide the essential safety function during and following the hazard is demonstrated to withstand the event through a process of qualification. This can take many different forms but is essentially a thorough assessment of the ability of the claimed equipment or operator action to perform as required even when the plant has been affected by the external event. Qualification can be through segregation from the challenge e.g. the equipment is located above the maximum flood level or demonstration that it can be exposed to the challenge, and still function, e.g. the maximum peak ground acceleration from the design basis earthquake.

0.7 Mission Time and Offsite Support

The EDF Energy safety cases demonstrate the capability of safety measures claimed to prevent or minimise the releases of radioactive materials. Many of these systems consume stocks such as fuel for diesel generators, water for cooling or liquefied gases to keep the reactor pressurised. It is a normal requirement within EDF Energy to have sufficient stocks of essential consumables on each site for independence from offsite support for at least 24 hours. This is usually referred to as the ‘mission time’. There may be longer mission times, e.g. 48 hours associated with a shutdown reactor, but the cooling requirement during these periods is less onerous and the stocks requirements are considered to be bounded by the at-power requirements.

The 24 hour mission time for essential stocks is well established under the AGR emergency arrangements and the requirement is embodied in NSP 5.1 – Methods for Functional Capability Claims. This principle requires that it is demonstrated that safety systems can operate for a period of 24 hours solely from station resources, and that external replenishment for timescales beyond 24 hours is practicable.

Following an emergency, Station staff will continuously review stocks of essential consumables and make whatever arrangements for their supply/replenishment that are considered appropriate but will, in any event, have the capability to remain independent for at least 24 hours and still safely manage the emergency. The 24 hour mission period is a key assumption incorporated into the corresponding PSA modelling used to aid judgements made and support the risk levels claimed in the safety cases.

Beyond this period it is claimed that adequate arrangements can be established for any required essential supplies to be brought to site. If a significant incident occurs at any site the Central Emergency Support Centre is set up to manage off-site technical resources in conjunction with the on-site Emergency Control Centre and the Emergency Services. If required the Central Emergency Support Centre can contact specific suppliers, with which there are pre-existing arrangements, to deliver additional supplies to the site within the required time period.

It should also be noted that, with the exception of prolonged extreme weather conditions, the external hazards are either of short duration or episodic in nature. They are all expected to have diminished or ceased well within a period of 24 hours. The required stocks to support the 24 hour mission time and the viability of replenishing these stocks have been considered as part of this Stress Test and are discussed in chapter 6.

0.8 Beyond Design Basis Events and Accident Management

The design basis is defined by the requirements of the NSPs and includes all those events identified to occur with a frequency and a consequence within that for which the NSPs require safety measures to address. The safety case demonstrates that the safety measures will perform their function against this defined basis with an appropriate reliability such that the overall risk from the site is acceptably low.

There are events beyond the design basis where the frequency of the events, either a single initiating event or a combination of faults, is such that the NSPs do not require them to be specifically addressed. They are deemed to be sufficiently unlikely that the risk is acceptably low even if the unmitigated consequences were to occur. However, regardless of this, arrangements have been developed to ensure that the fault is managed and consequences are minimised even if these unlikely events occur.

Experience worldwide has shown that the less probable events which have occurred are often a combination of design fault, hardware failure and human error which have not been anticipated. Even if we could anticipate every possible combination of low frequency events, the vast number of these potential events would lead to an unmanageable number of event-based procedures and operating instructions. Such events have to be managed by assessment of the symptoms associated with the potential events.

For the AGRs, guidance to reactor operators on the management of events at the edge of the design basis is provided in a series of documents called symptom based emergency response guidelines. The guidelines are aimed at the prevention of an uncontrolled release and so are concerned with shutting the reactor down and maintaining adequate post-trip cooling. The guidelines are written in such a way that the operators can follow them without needing to know the exact state of the plant. This is useful for low frequency events as there could be unexpected combinations of unavailable plant and plant damage.

If recovery actions within the guidelines are unsuccessful, or irreversible plant/core damage occurs for any other reason, further guidance is given in the AGR severe accident guidelines. These are deliberately non-prescriptive, as prescriptive advice is only appropriate when the fault sequence is reliably predictable, and almost by definition this will not be the case under severe accident conditions. Instead, the severe accident guidelines highlight the physical phenomena likely to be of importance, and focus on measures (an accident management plan) which could be adopted to recover critical safety functions, using non-standard or improvised plant configurations if necessary. This could include equipment available on site or, more likely for a significant event, equipment provided from off-site sources. This approach means that the plan would have to be developed in real time during the course of the accident in response to the specific event. Given the challenges of likely on-site conditions under the circumstances of a severe accident, it is anticipated that much of the technical assessment informing the plan would be carried out in the Central Emergency Support Centre. When operational, the Central Emergency Support Centre can draw upon all of the technical capability within the company.

0.9 Emergency Response Arrangements

The key priority for EDF Energy is the safe, reliable generation of electricity. Generating safely means the prevention of accidents, and recognising the potential hazardous situations that might cause harm to the public, on-site staff, the environment, or the reputation of the company. Despite constant vigilance, and the safeguards incorporated into the design and operation of plant and systems and a positive accident prevention culture, accidents can still happen. Having well rehearsed emergency arrangements in a state of readiness gives another layer of protection by mitigating the effects of unforeseen events.

The Emergency Plan describes the principles of the emergency arrangements and implements the requirements of LC11. The plan also supports compliance with Regulation 7 of Radiation Emergency Preparedness and Public Information Regulations (REPPIR). The Site Emergency Plan together with the Site Emergency Handbook form the 'operators plan' as defined in REPPIR 2001. The plan and handbook are provided to the HSE as the operators plan for REPPIR compliance. REPPIR establishes a framework of emergency preparedness measures to ensure that members of the public are properly informed and prepared, in advance, about what to do in the unlikely event of a radiation emergency occurring, and provided with information if a radiation emergency actually occurs.

If an event should ever occur resulting in a release to the environment of significant quantities of radioactive material then, in addition to the operator, many off-site organisations would be involved and called upon to take actions to protect the public. These organisations include the Police and other Emergency Services, Local Authorities, Government Departments and Agencies, each of which has its own emergency responsibilities and procedures. These procedures are co-ordinated in the Off-Site Emergency Plan by the Local Authority, which fulfils the requirements under REPPIR.

Emergency exercises are used to demonstrate and test the adequacy of the Emergency Plan response for EDF Energy. These exercises demonstrate the on-site arrangements and off-site aspects of an emergency including Central Emergency Support Centre operations and exercising each Strategic Co-ordination Centre, which is activated by the police and co-ordinates the off-site organisations. These exercises are witnessed by the ONR.

0.10 Mandatory Evaluations

As described in section 0.1 an internal review of our nuclear facilities and emergency response measures was initiated by the Board; this was then expanded to include the scope of a Significant Operating Experience Report (SOER) issued by WANO, the World Association of Nuclear Operators, an international cross industry organisation which aims to help its members achieve the highest levels of operational safety and reliability. The primary output of these reviews was two separate Mandatory Evaluations from each of the sites, the scope and results of these initial reviews were used to inform the ‘stress tests’ and are presented below.

All required systems/ equipment for cooling of fuel both within the reactors and the fuel route plant areas were identified and thoroughly tested through visual walk down and audit of compliance to the individual stations normal processes. In all cases the review concluded that the systems meet their safety function.

The next stage was to identify all equipment/systems and processes required to support mitigation of internal and external flooding events required by station design. Then thorough walk downs of all systems, procedures, equipment and materials required to support this situation were completed.

Stations then identified all important equipment required to mitigate fire and flood events which could be impacted by a seismic incident across all reactors within the fleet. Walk downs and comprehensive inspections were completed for all of the identified equipment and all station locations provided significant detailed information on susceptibility of claimed lines of protection in these situations. No shortfalls were identified in the support of current design basis assumptions. Further review beyond the design basis is presented in this report.

A comprehensive review of all equipment required to support the mitigation of severe accident situations was conducted across all 15 reactors within the EDF Energy fleet. Where feasible, testing of this equipment’s readiness to respond in the event of a major incident was completed and all was found to be in a satisfactory state of readiness. Where testing was not possible due to normal plant operating conditions, walk downs and visual inspections of equipment condition were completed and again all was found to be in a satisfactory state.

Procedures required to support mitigation of severe accident situations were identified and thoroughly reviewed across all facilities including central support functions, as appropriate (symptom based emergency response guideline’s and severe accident guideline’s. The findings of this review are detailed in Chapter 6.

All applicable agreements and contracts designed as contingencies to support severe accident mitigation were identified and comprehensively reviewed. Walk downs of the key processes and equipment covered by these arrangements were completed (over and above those routine arrangements already in place for regular inspection/ maintenance of these arrangements). These support arrangements were found to be in line with current expectations and contract agreements.

Chapter 1 – General Data about Hartlepool

Hartlepool

1 General Data about Hartlepool

1.1 Site Characteristics

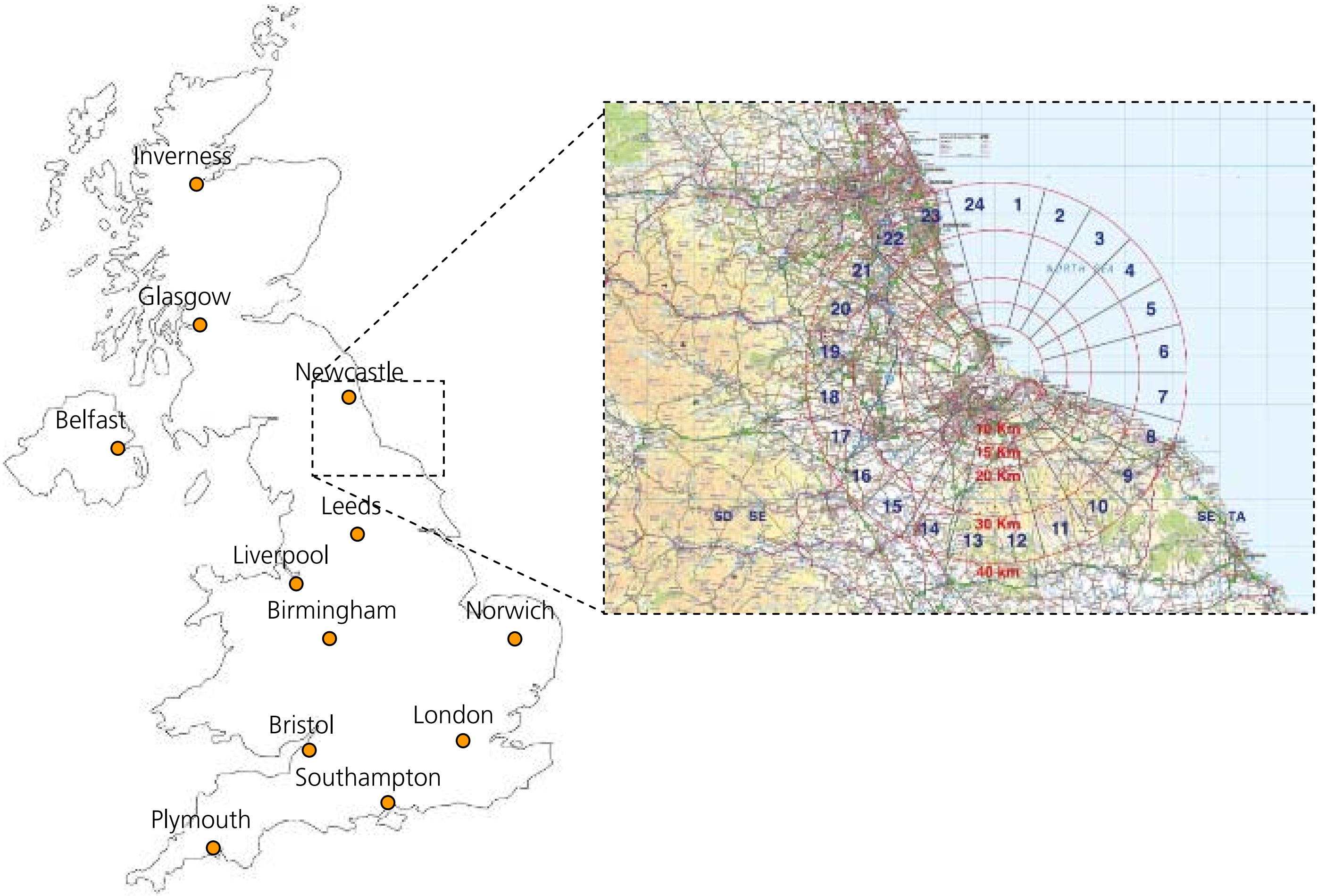

Figure 1-1 Location of Hartlepool Power Station

<u>Site Layout</u>

Hartlepool Power Station (HRA) is a twin reactor Advanced Gas Cooled (AGR) station located on the northern bank of the mouth of the River Tees, approximately 2.5 miles (4 km) south of Hartlepool in County Durham, North East England. Power Generation commenced in August 1983. The station is currently licensed to operate up until 2019. In total the station generates approximately 2% of Britain's energy.

The Teesmouth area is predominantly industrial with an established oil and chemicals industry.

The biodiversity interest around the nominated site at Hartlepool is high and includes a number of internationally and nationally designated sites, which are primarily designated for their valuable coastal habitats and important bird assemblages.

Teesmouth is designated as a Special Protection Area for birds and a Ramsar Wetlands site. (Ramsar sites are wetlands of international importance designated under the Ramsar Convention, first designated in the UK in 1976).

The population in the North East of England has decreased over the past 25 years and now totals approximately 2.6 million.

The site is located approximately 20km to the north of the North York Moors National Park (NP); 16km south of the Durham Heritage Coast and 18km northwest of the North Yorkshire and Cleveland Heritage Coast.

The site is situated within the Tees Lowlands National Character Area (NCA 23) on the north side of the river Tees estuary between the conurbations of Hartlepool, Stockton on Tees, Middlesbrough and Redcar. This landscape is characterised by the broad low lying plain of gently undulating, predominantly arable farmland with wide views to distant hills with the meandering river Tees flowing through the heart of this industrial area. Extensive urban and industrial development is concentrated along the lower reaches of the Tees, the estuary and coast. Large-scale chemical and oil refining works, dock facilities and other heavy plants along the Tees estuary form a distinctive skyline by day and night. Overhead transmission lines and pylons, motorway corridors, railway lines and other infrastructure elements are widespread features. Extensive areas of mud flats, saltmarsh wetlands and dunes at the mouth of the river Tees support valuable wildlife habitats.

Transport: Hartlepool is generally well served by transport links. The A19(T) through the west of the borough provides a major north-south trunk road through the region connecting Hartlepool to Durham and Tyne and Wear to the north and the rest of the Tees Valley and North Yorkshire to the south. The A19(T) is connected to the main urban area of Hartlepool via the A689 and A179 principal roads. These roads also provide the major north-south road link for local trips within the town.

Hartlepool power station is situated on an elevated area of land compared to its surrounds. Along with surrounding dune features this provides protection against seawater flooding.

Hartlepool is operated by the licence holder – EDF Energy Nuclear Generation Ltd, a subsidiary company of EDF Energy plc.

1.2 Main Characteristics of the Hartlepool Reactors

Hartlepool AGR station consists of two reactor units combined in a single complex, linked together with a central block for services, instrumentation and control and an adjacent turbine house. Each reactor drives a single 660 MW turbine generator set. The two reactors are served by one fuelling machine operating within a common charge hall. The primary circuit of each reactor is contained within a pre-stressed concrete pressure vessel.

Table 1.1 - Construction and Operation details for Hartlepool

Start Construction	1 October 1965	1 October 1965
Grid Connection	1983	1984

Table 1.2 - Specific details of Hartlepool reactors

	Reactor 1	Reactor 2
Reactor Type	Commercial Reactor	Commercial Reactor
Model	Advanced Gas-Cooled Reactor (AGR)	Advanced Gas-Cooled Reactor (AGR)
Vendor	British Nuclear Design & Construction (BNDC)	BNDC
Owner	EDF-Energy	EDF-Energy
Operator	EDF-Energy	EDF-Energy
Capacity Net	595 MWe	595 MWe

1.3 Systems for Providing or Supporting Main Safety Functions

Advanced gas-cooled reactor technology differs significantly from that of light water reactors (or the boiling water reactor at Fukushima) and is unique to the UK. The advanced gas cooled reactor core is assembled from high purity graphite bricks. These are keyed together in layers, and are arranged in a polygonal structure with an approximate overall diameter of ten metres and height of eight metres. Circular channels in the bricks allow passage of fuel elements, coolant and control rods. The graphite also acts as a moderator. The fuel in an advanced gas-cooled reactor is slightly enriched uranium dioxide which is contained within stainless steel cans. The fuel is cooled by gaseous carbon dioxide which is chemically stable and does not change phase over the operational temperature and pressure range.

The reactor core is contained within a cylindrical pre-stressed concrete pressure vessel with top and bottom caps. On the inside of the concrete there is a gas tight steel liner. Normal operating pressure is 40bar g.

In an advanced gas-cooled reactor the carbon dioxide heated in the reactor core moves through the primary side of the boilers and is then pumped back into the core with the gas circulators. The boilers are heat exchangers fed by water through their tubes (secondary side) where steam is produced which is directed to the turbine generator to produce electricity.

Compared with light water reactors, the advanced gas-cooled reactor energy power density is low, approximately 2.5MWth/m^3 (million Watts of thermal power per cubic meter of reactor volume) when compared with approximately 100MWth/m^3 in the pressurised water reactor. In addition the thermal capacity of the reactor core is very high, due to the large mass of the graphite moderator (approximately 1000 tons) in the reactor core. This means that if all post-trip cooling was lost following a reactor trip, the temperature increases would be slow allowing ample time for operator intervention.

The advanced gas-cooled reactor has the capacity to tolerate loss of all gas circulators under trip and shutdown conditions with the reactor pressurised. Natural circulation of the gas, using boilers as the heat-sink, provides adequate cooling.

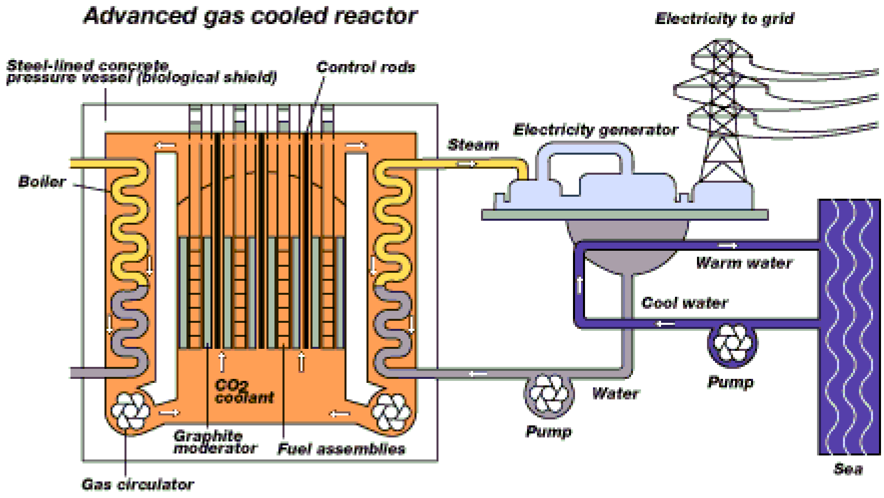

Figure 1-2 AGR showing internal components and the primary ultimate heat-sink

Fuel Handling

Refuelling of the reactor is carried out using a fuelling machine, which is essentially a large travelling crane with the fuel held within a pressure vessel. The fuelling machine is designed to be extremely robust and is fitted with multiple safety systems. Fuel handling may be carried out with the reactor off load and depressurised but always in CO2.

Once removed from the reactor, spent fuel passes through three main stages of the fuel route before being removed off site. First, it is held in a buffer store while the decay heat reduces. Then it is transferred to a dismantling facility where the fuel is separated into individual elements. Finally the elements are transferred to a water filled storage pond prior to shipment off-site in a transport flask.

In each stage of fuel handling, the facilities are designed to remove the decay heat that is produced by the fuel and to protect the fuel from damage.

1.3.1 Reactivity Control

The following sections highlight the safety roles of systems and on-site facilities/operations which are relevant to the control of reactivity at Hartlepool.

1.3.1.1 Reactivity Control - Reactor Core

Reactivity control in Advanced Gas□cooled Reactors is achieved using the following systems:

- The primary means of shutting down the nuclear reaction for all the Advanced Gas- Cooled Reactors is the fall under gravity of control rods into the reactor core. There is a high level of redundancy in the control rod primary shutdown system. The nuclear reaction would be stopped by insertion of a small number of control rods, provided they were fairly uniformly distributed radially about the core.
- All Advanced Gas- Cooled Reactors have an automatically initiated diverse shutdown system, in order to ensure shutdown even if for any reason insufficient rods in the primary shutdown system insert into the core. At some stations the (fully) diverse system is based on rapid injection of nitrogen into the reactor core: nitrogen absorbs neutrons and hence stops the chain reaction. At other stations, the (partially) diverse system is based on an adaptation to the control rod system so that the rods are actively lowered into the core rather than falling under gravity and is then backed up by nitrogen injection manually initiated from the reactor control desk.

- A tertiary shutdown is provided to maintain the reactor in its shutdown state in the longer term if an insufficient number of control rods have dropped into the core and it is not possible to maintain a sufficient pressure of nitrogen. The principle of a hold down system is that neutron absorbing material is injected into the reactor circuit. Such a measure would only be adopted as a last resort and is achieved by injection of boron beads or water.

1.3.1.2 Reactivity Control – Fuel Storage and Transport

All operations involving storage or movement of nuclear fuel on site which could conceivably constitute a criticality hazard (except when resident in the reactors) are assessed to make sure accidental criticality cannot occur. All such operations are therefore controlled by means of criticality safety certificates for each location or operation. These certificates restrict the quantities of fuel accumulated, ^{235}U enrichment, the presence of additional moderators (e.g. graphite or water from fire extinguishers) and flammable materials. They also specify procedures to be followed in the event of fuel damage.

Criticality control is exercised in all locations which receive new or spent fuel and constitutes a combination of design provisions to limit material and operator control. Key aspects are maintaining configuration and limiting the presence of moderator material (in particular water).

Advanced gas-cooled reactor fuel storage and transport throughout the station does not present a credible criticality concern under extreme hazard conditions. In locations where flooding is credible, the criticality assessments demonstrate that criticality will not occur. It should be noted that the criticality assessments include significant conservatisms, e.g. the most reactive fuel is used in the assessments and no credit is taken for burnable poisons which are present in new fuel. Spent fuel storage in the ponds does not require the addition of boron to control criticality. The pond water is nevertheless maintained with a prescribed concentration of soluble boron as a reasonably practicable and prudent safety measure consistent with the application of a 'defence in depth' philosophy.

1.3.2 Heat transfer from reactor to the ultimate heat-sink

1.3.2.1 Means of Heat Transfer from the Shutdown Reactor to the Ultimate Heat Sink

Under normal operation, heat generated in the reactor core is transferred to the primary coolant (CO_2). Gas circulators provide forced circulatory conditions which pass the primary coolant through the boilers, transferring heat to the water in the secondary coolant circuit. Cooling water is continually pumped into the boiler tubes and turned into steam which is passed to the turbines generating electricity. The low pressure steam which remains is passed through seawater cooled condensers where the remaining heat is removed i.e. the sea is used as the primary ultimate heat-sink.

Following a reactor trip, post-trip control systems are provided to initiate post-trip cooling bringing into action various items of plant essential to providing cooling of the shutdown reactor to remove decay heat. The operator is also able to duplicate the actions of the post-trip control system on a slower timescale, thus providing a significant element of defence in depth.

<u>Post- Reactor Trip Control</u>

The process of removing decay heat is known as Post-trip Cooling. The fuel is cooled by the gas circulators pumping the carbon dioxide coolant through the reactor core and boilers. The heat is removed from the boilers by the post-trip feedwater systems which pump water through the boiler tubes.

If the gas circulators fail and the reactor is pressurised, the fuel can be cooled by natural circulation providing the boilers continue to be cooled by the feedwater systems. All advanced gas cooled Reactors have at least two diverse post-trip feedwater systems with redundancy and diversity in their electrical supplies. In addition, some back-up feedwater systems are powered by diesel engines and do not require electrical supplies.

If the reactor pressure vessel is depressurised then the fuel can be cooled by forced gas circulation and feedwater supplied to the boilers. Alternatively, equipment is available to re-seal and repressurise the reactor to establish natural circulation.

The design basis safety cases are supported by the availability of at least 24 hours worth of stocks (e.g. diesel, carbon dioxide, feedwater). This is on the basis that within that timescale it would be possible to obtain the required stocks to go beyond 24 hours. In reality, available stocks are normally provided for longer than 24 hours.

The provision of adequate post-trip cooling requires the capability to stop a number of running systems and start a number of standby systems for all faults and hazards. Such operations carried out automatically via the reactor trip distribution system. The reactor operators are trained to carry out these actions of the reactor trip distribution system fails.

Primary Coolant

The primary coolant, CO_2 gas, flows around the core and transfers heat from the core to the secondary coolant heat-sinks via forced gas circulation. However, providing the primary circuit remains pressurised (and sufficient secondary coolant heat-sinks are in service), the primary coolant will transfer heat from the core via natural circulation.

Forced gas circulation is usually provided by the gas circulators main motors which are supplied at 11kV. Natural circulation does not require gas circulators or electrical suuplies.

The CO_2 primary coolant is topped up using storage tanks. Liquid CO_2 from the tanks passes through steam heated vaporisers and into the CO_2 distribution system, then eventually into the reactor gas circuit. The CO_2 system provides gas not only to the primary circuit but also to some of the facilities involved in fuel handling and its delivery system is designed to include diversity and redundancy.

Secondary Coolant Systems

The main boilers act as the primary to secondary heat transfer surface within the reactor pressure vessel. There is considerable excess capacity in the boiler system: with forced primary coolant circulation, a single fed boiler (there are four boilers in total) is sufficient to adequately cool the core.

The boilers remove heat from the coolant gas through thermal conduction in the boiler tube walls and generate high pressure superheated steam from the boiler feedwater. Steam is used to drive the main turbine and main boiler feed pump.

In normal operation, boiler feedwater is pumped from the condenser to the boilers (via a deaerator) and steam flows from the boilers to the turbine.

Main Feed System

Feed and Condensate System

The feed and condensate systems are defined as all components from the water sources (condensers, deaerators, feedwater storage tanks) through to the point where the feed pipework connects with the boiler closure feed inlet header. The function of the feed and condensate system is to maintain the supply of feedwater, of the specified quality, to the boilers of each reactor/turbine unit.

1.3.2.1.1 Cooling Water Systems

Essential Cooling Water System

The essential cooling water system provides cooling to all the essential systems. It serves both at power and post-trip. It is equipped with a large amount of redundancy, diversity and segregation.

The system is operated as two segregated seawater circuits with one pump running in each circuit with another on standby duty. Each circuit serves both reactors and is capable of providing sufficient post- trip cooling for plant of both reactors in the event of the loss of the other circuit.

Main Cooling Water System

The main cooling water system provides cooling to the Turbine Generator condensers, the dump condenser, the turbine generator auxiliaries and the turbine lube oil coolers. It also provides a source of water to the auxiliary seawater system for cooling of the generator transformers (although the generator transformers are normally cooled by essential cooling water system), and can be set up to supply the essential cooling water system and the fire hydrant system.

Low Pressure Back- Up Cooling Water System

The low pressure back-up cooling water system is an open loop townswater system that provides back-up cooling to essential plant in the event of a number of low probability fault situations, including complete loss of the essential cooling water system. The low pressure back-up cooling pumps are diesel driven and the system is not reliant on electrical supplies.

High Pressure Back- Up Cooling Water System

The high pressure back-up cooling water system is a once through system that provides back-up water to the boilers. The system has its own water tanks and the pumps are diesel driven and the system is not reliant on electrical supplies.

Auxiliary Cooling Systems

Pressure Vessel Cooling System

The pressure vessel cooling system is a closed loop cooling circuit which cools the pressure vessel.

Reactor Auxiliary Cooling System

The reactor auxiliary cooling system is a closed loop cooling circuit containing dosed demineralised water. It has safety significance as it provides cooling to the gas circulators and other items of plant associated with the reactor. Heat removed by the system is transferred to the sea via the essential cooling water system.

Turbine House Ancillaries Cooling Water System

The purpose of the system is to provide cooling to a number of plant items in the Turbine Hall during normal operation and post-trip. The system's main safety role is to provide cooling to the boiler feed pumps following a reactor trip. Heat removed by this system is transferred to the sea via the essential cooling water system.

1.3.2.2 Layout of Heat Transfer Chains

Plant systems which support primary coolant heat transfer are generally located within the reactor building i.e. close to the primary circuit. The plant systems which support secondary cooling comprise water storage tanks and pumps together with the boilers (including boiler depressurisation routes). The latter are located within the reactor building; the boilers are located within the primary circuit pressure vessel.

1.3.2.3 Heat Transfer Time Constraints

The length of time for which heat transfer systems may continue to be supported depends on a number of factors. If grid supplies are available, not only are electrical supplies supported without time constraints - feedwater may also be recirculated. A continued loss of off-site power supplies will require reactor heat transfer to be supported by consumable water supplies and consumable fuel oil supplies. Fuel oil consumables are relevant to direct diesel-driven pumps (as used in the high pressure back-up cooling system) and also to the provision of gas turbine generator supplies. The following tables address consumable feedwater stocks and high pressure back-up cooling system and low pressure back-up cooling system diesel stocks.

Table 1.3 Consumable Feedwater Stocks

Feedwater Source	Timescale
Reserve water feed tanks	The specified reserves are sufficient for 24 hours operation for each reactor under post-trip conditions. However, reserves on site are often greater than specified.
High pressure back-up cooling system tanks	The specified reserves are sufficient for 24 hours operation for each reactor under post-trip conditions. However, reserves on site are often greater than specified.
Low pressure back-up cooling system tanks	> 6 hours townswater supply followed by indefinite operation using seawater. However, reserves on site are often greater than specified.

Table 1.4 Diesel Stocks

Fuel Oil Source	Timescale
High pressure back-up cooling system fuel tank	Each fuel tank contains sufficient fuel for approximately 18 hours continuous running.
Low pressure back-up cooling system fuel tank	Each fuel tank contains sufficient fuel for approximately 24 hours continuous running.
Alternative indication centre fuel tank	Each fuel tank contains sufficient fuel for 24 hours continuous operation.
Gas Turbines	Each fuel tank contains sufficient fuel for approximately 4 hours of continuous running.
Bulk oil storage tanks	2 tanks, each tank contains many days of fuel oil to be used in any of the above systems.

1.3.2.4 AC Power Sources

The provision of ac power sources is addressed in section 1.3.5.

1.3.2.5 Diversity of heat Transfer Chains

Diversity of heat transfer chains is described in the brief system descriptions above.

Probabilistic safety assessments for reactor systems provides an indication of whether the systems deliver diversity and any significant weaknesses in the system relating to diversity would be revealed during the assessment process.

1.3.3 Heat transfer from spent fuel pools to the ultimate heat-sink

None of the operating UK reactors have identical fuel or spent fuel facilities to those at Fukushima. Unlike Sizewell B fuel, which is clad in a zirconium alloy, the advanced gas- cooled reactor fuel is clad in stainless steel. Consequently the chemical reactions of the cladding at raised temperatures and when exposed to steam and / or air are different from those experienced with zirconium alloys.

As discussed in section 1.3, AGR fuel storage and handling comprises three main stages after discharge from the reactor - buffer storage (in CO_2), dismantling (in CO_2) and then storage in water filled cooling ponds followed by shipment off-site in a transport flask.

The heat transfer chains for each stage of fuel storage and handling are summarised in the table below. The primary cooling circuit is the medium that directly cools the fuel, the secondary circuit transfers the heat from the primary circuit to the ultimate heat sink.

Stage of fuel storage and handling	Handling with fuelling machine	Buffer storage	Dismantling	Storage in ponds
Primary cooling circuit	CO_2 by natural circulation to fuelling machine body	CO_2 by natural circulation	CO_2 by forced circulation	Pond water circulated by cooling system
Secondary cooling circuit(s)	None	Recirculating cooling water circuit; and Once-through sea water cooling system	Recirculating cooling water circuit; and Once-through sea water cooling system	Once-through sea water cooling system
Ultimate heat sink	Ambient air	Sea	Sea	Sea

In the event that cooling is lost, then temperatures will increase and there could be a threat to integrity of the fuel. The table below summarises loss of cooling scenarios for each stage of the fuel storage and handling process and the timescales before safety limits are approached:

Stage of fuel storage and handling	Handling with fuelling machine	Buffer storage	Dismantling	Storage in ponds
Potential impact of loss of cooling	Loss of cooling not credible (no active systems required)	Boiling of water in the secondary circuit followed by overheating of fuel	Even with loss of cooling water systems, natural cooling effects mean fuel safety limits will not be breached.	Boiling of water in the ponds followed by overheating of fuel
Assigned safety limit	n/a	Boiling dry of storage tube water jackets	n/a	Cracking of pond concrete at 75C (additional cooling measures to be initiated before water temperature reaches 65°C)
Minimum time to reach safety limit	n/a	Not less than 21 hours for the hottest fuel	n/a	Minimum of 61.6 hours (75°C) Minimum of 41hours (65°C)

It should be noted that the assigned safety limit for storage in the ponds is cracking of the pond concrete once the water temperature reaches 75°C. This leads to a limited leakage of pond water. As the pond continues to heat up it will reach boiling. After boiling commences it will take some time for the water level to reduce by evaporation and leakage through cracking and there is no threat to fuel integrity provided that adequate water cover can be maintained. Potential improvements to mitigate the leakage issue have been implemented including a diverse cooling package system that can be promptly deployed if required. Use of this equipment is limited to a water temperature of 65°C, hence the shorter minimum response time (based on the hottest fuel being present in the pond) for deployment.

For buffer storage the times to reach safety limits are shorter than the ponds because decay heat levels are higher and the relative volume of water to fuel is much smaller. For this reason there are back-up cooling systems available for buffer storage.

1.3.4 Heat transfer from the reactor containment to the ultimate heat-sink

Advanced gas-cooled reactors do not have a containment building. The pre-stressed concrete pressure vessel is a massive, reinforced concrete structure which, due to its construction, provides shielding to the outside environment from the radiation inside the reactor.

None of the design basis loss of coolant accidents for advanced gas-cooled reactors precipitate large scale fuel failure and the plant is designed to be capable of retaining the bulk of any radioactive material that might be released from the fuel.

There are longer timescales available in the event of loss of post-trip cooling and the pressure vessel is a massive reinforced concrete structure. The advanced gas-cooled reactors concrete pressure vessel together with the large mass of graphite in the core provide many hours of heat-sink in case of total loss of cooling.

The pre- stressed concrete pressure vessel contains the reactor and primary coolant gas and its concrete walls act as a biological shield so that the radiation levels out side the vessel are minimal. A steel liner forms a leak-tight membrane on the inside to maintain an integral pressure boundary.

Thermal insulation is provided within the concrete pressure vessel to maintain the temperatures of certain key components at an acceptable level. These insulating components are designed with secondary retention features to ensure that no single failure could lead to detachment.

Under normal operating conditions, the pressure vessel is cooled by a system consisting of two loops. Cooling water flows around the pressure vessel through a network of pipes which are connected to the pressure vessel, vessel liner and the vessel penetrations. The primary ultimate heat-sink for the vessel cooling system is the sea, via the essential cooling water system.

Together with thermal insulation, this cooling system ensures that the pressure vessel components mentioned above are maintained at acceptable temperatures and therefore ensures the integrity of the primary circuit containment by minimising the threat of damage from high temperatures.

1.3.4.1 System descriptions

Pre-stressed concrete pressure vessel

Coolant gas, which transports heat from the reactor core to the boilers, is enclosed within the reactor coolant pressure boundary inside the reactor. The reactor coolant pressure boundary performs an essential safety role by preventing the release of reactor coolant gas (CO_2) to the outside environment. The pre-stressed concrete pressure vessel, its steel liner and penetrations form the primary components of the reactor coolant pressure boundary and together, they provide a barrier against any escape of the reactor gas and thereby maintain gas pressure at a level sufficient to ensure adequate fuel cooling under all normal operating conditions. There are also safety relief valves which can be opened to reduce the pressure if required. The pressure vessel also performs a secondary safety role by providing radiation shielding, thereby minimising radiation doses to station personnel.

Vessel cooling systems

The main safety function of the vessel cooling system is to maintain acceptable temperature conditions in the walls of the pressure vessel, the membrane and the penetrations for a range of coolant gas temperatures, so that the structural integrity of the pressure vessel, liner and penetrations are protected. The system prevents overheating of the concrete pressure vessel and consequent degradation of concrete properties and is required to operate continuously. There are also two diverse pressure vessel cooling systems as redundancy.

1.3.5 AC Power Supply

Electricity produced by Hartlepool power station is exported from the station turbines by a high voltage Alternating Current (AC) transmission system to supply the national grid. This transmission system can act as a two-way system allowing the power station to draw electricity from the grid. Under normal operating conditions the electricity taken from the grid is used to power the various systems around the station, including those essential for safety such as cooling water pumps and motors used for gas circulation. However, there are occasions when the power station is not producing electricity but still requires it in order to support maintenance work, operate other equipment, restart the plant and importantly to operate electrical safety systems.

The grid connection is at a high voltage to minimise transmission losses over the long distances it operates. This high voltage is not suitable for directly running the systems on the site, so transformers are used to reduce the voltage to the various levels required.

Control rods safely shutdown the reactor, but significant heat is still produced from the decay of radioactive fission products. This heat needs to be removed from the reactor core to prevent overheating of the fuel. Reactor cooling systems are powered by an independent source of electricity, either from off-site power (the grid) or on-site emergency back-up power (such as diesel/gas turbine generators).

The reliability of on-site power is assured by providing sufficient independence and redundancy of diesel/gas turbine generators and batteries. The on-site electrical distribution systems are capable of performing essential safety functions even if a single failure occurs.

The grid connection can be lost due to failure of transmission lines which are vulnerable to damage from external hazards. If this happens, the power station is capable of operating independently until grid connections are restored. There are several sets (groups) of generators designed to provide power to safety critical systems, which will automatically start when the grid connection is lost. Generators produce power at different voltages which are all much lower than the voltage supplied from the grid connection but which are suitable for the systems they serve. Switchgear and transformers also allow various combinations of generators to power different systems. Generators are not 'universal' and so it must be noted that only certain generator/plant system combinations work together. However, a very high level of redundancy (whereby more than one generator is available) is intrinsic in the design of the electrical system.

Direct Current (DC) electricity (as opposed to Alternating Current (AC)) is required by some of the station systems, such as control and instrumentation and the station batteries. Therefore, systems are provided to convert ac electricity to dc, and distribute dc around the site. When the station batteries are required to operate ac systems, inverters are available to convert the dc electricity from the battery to ac. Once again, a high degree of redundancy is built in to these systems and connections, so that any single failure will not affect the system.

Table 1.5 Further details on plant required to provide essential safety functions

System	Seismic Qualification	Fuel Provision	Water Provision
11kV Gas Turbines	System designed to function following a seismic event	> 72 hours. See Chapter 5	No water used
Diesel Driven Back up cooling pumps (low pressure)	System designed to function following a seismic event	> 72 hours. See Chapter 5	> 72 hours. See Chapter 5. If power remains available the low pressure back-up cooling system can be sustained by the circulating seawater system
Diesel Driven Back up cooling pumps (high pressure)	System designed to function following a seismic event	> 72 hours. See Chapter 5	> 72 hours. See Chapter 5
DC Battery Support	System designed to function following a seismic event	~ 1 to 2 hours. See Chapter 5	No water used

1.3.5.1 Offsite Power Supply and Station Earthing

<u>275kV Grid Connection</u>

The off-site electrical system consists of a 275kV indoor double busbar substation with interconnections to the National Grid substations.

<u>23kV System</u>

The generators generate at 23kV. The 23 kV system links the generator main connections to the generator circuit breaker, with tee-offs for the unit transformers, and for an earthing transformer. The earthing transformer provides an artificial neutral for the 23kV system when the generator circuit breaker is open. The main electrical distribution system is designed on the generator circuit breaker and unit transformer principle to provide a high integrity supply to all the main auxiliaries. During normal running of the station if a reactor or turbine trips, the generator circuit breaker opens and the grid continues to supply the essential loads.

1.3.5.1.1 Offsite Power Supply reliability

The table below presents loss of off-site power events which have occurred at Hartlepool.

Table 1.6 Hartlepool Loss of Offsite Power Events

Date	Time	Reactor Trip	Weather	Description
6/08/85	15:16	Yes	Storms and lightning	During stormy weather, Hartlepool and its connection with Saltholme (a load of about 48 MW), were disconnected from the rest of the grid, whilst Reactor 2 was generating 300 MW.
27/1/96	10:51	Yes	Adverse	Reactor had been tripped via the Main Turbine Intertrip.

1.3.5.1.2 Connections to the Off-Site Power Supply – Performance in Hazards

No specific provision was made in the original station design for protection against external hazards. Nevertheless, that the underground cable routes are robust against seismic and flooding events. The switch houses are not qualified against seismic events or extreme high winds. This is not a requirement of the safety case since it is assumed that grid supplies would be lost following such initiating events.

1.3.5.2 Power Distribution inside the Plant

The electrical systems are highly redundant. Normally the energisation of a single board is sufficient to maintain an adequate level of post-trip cooling. Furthermore, the technical specifications which control the unavailability of essential electrical plant require compliance against the single failure criterion which is designed to retain a level of redundancy.

Diversity for post-trip cooling is usually a requirement for frequent initiating faults. In the case of Hartlepool the first line of defence is provided by systems deriving motive power from the main electrical systems. Second line protection is usually derived from systems which are diesel driven combined with operator support.

Diversity of plant monitoring is provided using the main central control room or the alternative indication centre. In the latter case the power supplies are obtain from diesel generators independent of the main electrical supply.

1.3.5.3 11kV System

1.3.5.3.1 On-site sources that serve as first back-up if off-site power is lost

The 11kV Electrical System is designed to provide high integrity supplies to all the main auxiliaries, in particular the gas circulator motors, and to ensure that overload and excessive fault levels do not occur.

This is achieved by:

- The use of reliable and well-proven equipment;

- Redundancy of power and control supply sources, supply routes and safety related equipment operated by the system;
- Physical separation and as appropriate segregation of supply sources, cable routes and switchboards; and
- The application to safety related equipment and cabling of protection against potentially damaging credible events (e.g. cable fires and hot gas release).

The main safety related functions of the 11kV electrical system and is to:

- Provide a reliable power supply at the appropriate voltage and frequency for all necessary loads during normal operation (including start-up, operation and shutdown);
- Provide a power supply that is reliable on demand for plant essential for shutdown, post-trip cooling and monitoring for all faults in the fault schedule; and
- Be able to maintain power supplies for an extended period in the event of a complete loss of grid.

11kV Gas Turbines

There are four gas turbine generators connected via circuit breakers to the main electrical system 11kV unit switchboards one per unit board section. The primary purpose of the 11kV gas turbines is to provide an independent electrical supply to ensure the operation of essential post-trip cooling plant in the event of loss of normal grid based electrical supplies.

The main safety related function of the 11kV gas turbines system is:

- Be able to maintain power supplies for an extended period in the event of a complete loss of grid.

The four gas turbines are segregated from each other by a concrete blast wall. Each gas turbine has its own fuel oil tank.

1.3.5.3.2 Redundancy, separation of redundant sources by structures or distance, and their physical protection against internal and external hazards.

Each gas turbine is housed in a walled enclosure. Each turbine and associated generator is segregated by a reinforced concrete blast wall

The bulk fuel oil tanks sit in large bunds and are separated by a concrete wall. Each bulk oil tank is fitted with a fire suppression system.

The day tanks sit in large bunds and are separated by concrete walls. Each tank is fitted with fire suppression.

The building which house the gas turbines has a low level bund dividing the building into two halves, this provides protection against internal flooding.

1.3.5.3.3 Time constraints for availability of these sources and external measures to extend the time of use (e.g. fuel tank capacity)

Each gas turbine has a day tank. This contains sufficient fuel for 4 hours of continuous running. The day tanks are refilled from the bulk fuel oil tanks. The bulk fuel oil tanks contain sufficient oil for many days of running. The bulk fuel oil tanks can also be used to top up the fuel tanks of the back-up diesel driven pumps. See section 5.1.1.2 for further details.

1.3.5.4 3.3 kV Unit Auxiliaries System

The 3.3kV system on each reactor/turbine unit is provided to distribute power for all the unit auxiliary loads required for normal operation and post-trip cooling.

1.3.5.5 Further Available Back-up Power Supplies

There are no neighbouring power plants to Hartlepool. The surrounding area is heavily industrialised. However, in events which might be postulated to result in a loss of off-site power it is unlikely that any neighbouring sites would provide a readily usable source of electrical power.

There is a set of emergency equipment, including electrical generating equipment, that would support essential safety functions (with additional special items) to enable forced cooling to be restored to a reactor. This equipment is located remotely off-site and centrally within the UK on trailers to be transported to the affected site within 10 hours following the declaration of an off-site nuclear emergency. Additional time would then be required to deploy this equipment.

1.3.6 Batteries for DC power supply

<u>415V AC/ 440V DC No Break System</u>

The 415V no-break electrical system provides power for plant essential to reactor safety during reactor operation through start-up, at power, post-trip, and during all emergency, fault and abnormal conditions. Thus, this electrical system has an important safety role at all times.

<u>415V Services System</u>

The 415V services system on each reactor/turbine unit is provided to distribute power to all electrically driven auxiliaries and services which are required for normal operation only. This system is not required to ensure post-trip cooling. All 415V post-trip cooling supplies are provided by the 415V short break boards and the 415V no-break boards.

<u>415V Short Break System</u>

The 415V short break system is provided to distribute power to all electrically driven components which are required for normal operation and post-trip cooling, and which do not require a no-break supply.

<u>110V ac Safety Circuits Supplies</u>

The 110V ac safety circuits supply system provides no break electrical supplies to the reactor guardlines. The reactor guardline equipment is located above ground floor level in the services block building adjacent to the central control room. The reactor guardlines are fail-safe. Loss of electrical power causes the reactors to automatically trip.

<u>*110V dc System*</u>

The 110V dc system provides a high integrity supply to the control circuits of air circuit breakers, contactors and standard motor starters which are dc controlled. The system is required both for normal operation and in the immediate post-trip period and thus has an important safety role.

<u>Post Trip Monitoring</u>

Post trip monitoring represents an important safety function. At Hartlepool the main post-trip monitoring centre is the central control room with an alternative indication centre providing a diverse monitoring location. The alternative indication centre derives its electrical supplies from diesel generators and is hence independent of station supplies.

1.4 Significant differences between units

There are no significant differences between reactor units.

1.5 Scope and main results of Probabilistic Safety Assessments

1.5.1 Probabilistic Safety Assessment – The AGR Approach

The probabilistic safety assessment is used primarily to advise our judgement of risk, while also performing a diverse check on the existing deterministic safety case. Some more recent safety cases have used probabilistic safety assessment extensively for qualitatively demonstrating plant interactions and functions as well as assessing ‘single plant failure’ vulnerabilities as well as quantitatively to assess risk margins & robustness of the reliability of plant - in support of ‘as low as reasonably practicable arguments in particular.

Probabilistic safety assessment is a structured and comprehensive analytical methodology which is used in the assessment of safety critical systems. It allows the evaluations of identified risks to the essential safety systems present within a nuclear reactor. It models identified potential outcomes using a systematic process, including identification of complex interactions between nuclear safety systems, and thus provides a logical, consistent method for evaluating the consequences of failures.

The probabilistic safety assessment does not invent new faults in addition to those identified through deterministic safety cases on the station fault schedule. Instead the probabilistic safety assessment gives further insight to the complex nature of some faults, identification of vulnerabilities to single failures and enables risk estimation that accounts for both the fault frequencies as well as the radiological consequences for those faults (Dose bands).

The probabilistic safety assessment also identifies the most significant faults, and the most important plant, components and operator actions to protect against them. This allows targeted training and plant improvements to be implemented, therefore achieving the greatest risk reduction for effort expended, supporting the as low as reasonably practicable solution.

Chapter 2 - Earthquakes

Hartlepool

2 Earthquakes

In the Office for Nuclear Regulation (ONR) Interim Report into the Japanese Earthquake and Tsunami, it is stated that "The extreme natural events that preceded the accident at Fukushima - the magnitude 9 earthquake and subsequent huge tsunami - are not credible in the UK. We are 1,000 miles from the nearest fault line[7] and we have safeguards in place that protect against even very remote hazards."

With the exception of Heysham 2 and Torness, the Advanced Gas-Cooled Reactors were not originally designed to withstand earthquakes. Sizewell B, the Pressurised Water Reactor was based on the Standard Nuclear Power Plant design and the standard design included qualification against earthquake. However, for the pre Heysham 2/Torness advanced gas-cooled reactors, seismic safety cases were developed with plant modification planned/carried out were necessary as part of the first periodic safety review in the late 1990s, covering both the at-power and shut-down conditions as well as fuel handling operations.

In a number of places, this document refers to the need for ongoing development work. Some of this work had been previously identified and captured by normal company processes, whilst some is new work highlighted by the post-Fukushima review. In the latter group, there are some potential work packages referred to as 'Considerations'. These Considerations will be carefully reviewed following the completion of the Stress Test reports and an appropriate programme of work formulated.

2.1 Design basis

2.1.1 Earthquake against which the plant is designed

2.1.1.1 Characteristics of the design basis earthquake (DBE)

During reactor operation, the integrity of protection against initiating events including external natural hazards is in accordance with the following:

- For any infrequent initiating event, there should be at least 1 line of protection to perform any essential safety function, and that line should be provided with redundancy. The magnitude of an infrequent earthquake corresponds to a severity consistent with a return frequency of 10^{-4} p.a. This is often referred to in the seismic safety cases as the 'bottom line' earthquake.
- For any frequent initiating event, there should normally be at least 2 lines of protection to perform any essential safety function with diversity between each line. Frequent initiating events are defined as more frequent than 10^{-3} p.a.

At Hartlepool, the infrequent earthquake is taken as one which results in a peak ground acceleration (PGA) of 0.17g Uniform Risk Spectrum soft site response spectrum. The Uniform Risk Spectrum was obtained from site-specific evaluation in 1991 using the Seismic Hazard Working Party methodology.

The design basis earthquake at Hartlepool for a frequent event has an assumed PGA of 0.1g Principia Mechanica Limited. spectrum in accordance with IAEA guidelines.

It is important to note that this figure of 0.1g Principia Mechanica Limited was adopted in accordance with IAEA guidelines and is a conservative figure as the actual worst site specific earthquake that could be expected more frequently than 1,000 years (10^{-3}) is 0.07g. Only where as low as reasonably practicable assessments have shown this is not practical have the second line plant items (those items claimed against the frequent event) been qualified against the less onerous 10^{-3} p.a. Uniform Risk Spectrum. It is also worthy of note that parts of the second line plant has been seismically qualified to the more onerous 10^{-4} p.a. Uniform Risk Spectrum where it was reasonably practicable.

According to a Tokyo Electric Power Company report the maximum recorded PGA at Fukushima Daiichi plant was equivalent to 0.561g at Unit 2: this compares with infrequent seismic hazards at UK stations of no more than 0.23g. It should be noted that the same report indicates that the reactors shutdown and post-trip cooling was initiated subsequent to the earthquake. The tsunami was the cause of the majority of the plant failures.

[7] Assumed to mean tectonic plate boundary

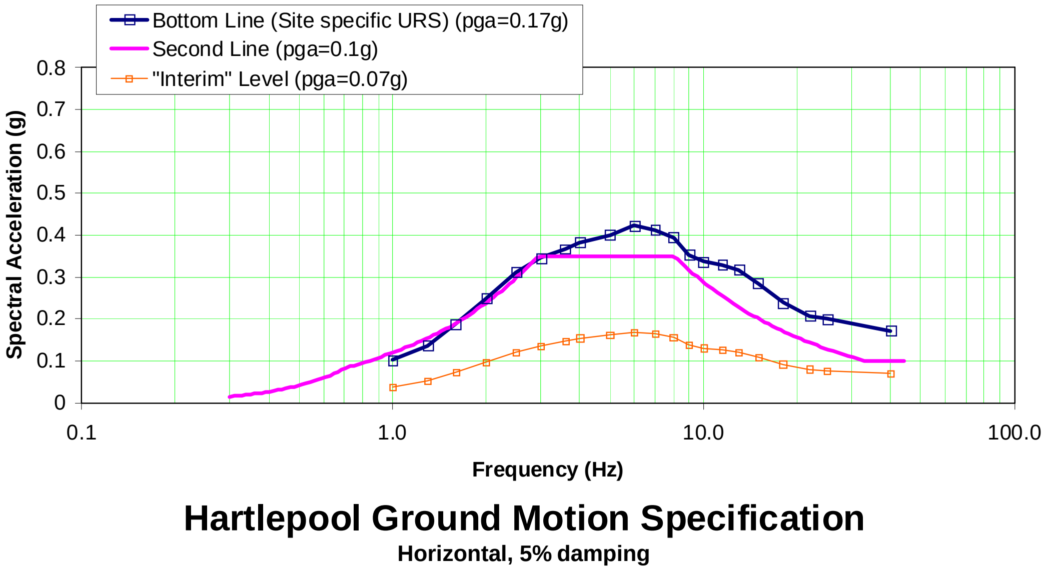

Figure 2-1: Hartlepool Ground Motion Specification

2.1.1.2 Methodology used to evaluate the design basis earthquake

Infrequent Event

The current design basis earthquake for an infrequent event is defined as an earthquake with a return frequency of once in 10,000 years. This is identified as the bottom line event i.e. the most onerous event for which bottom line plant provides protection. Bottom line plant and structures are those plant and structures required to provide a single line of protection during the infrequent, more onerous seismic event. The bottom line plant is required to perform the essential safety functions of trip, shutdown, and post-trip cooling; the bottom line structures are those that must withstand the infrequent earthquake to maintain the reactor in a coolable geometry. Bottom line plant and structures also provide one of two lines of protection against frequent events.

Seismic Hazard Assessment Methodology

The methodology for assessing the seismic hazard at each site was developed in the early 1980s by a group known as the Seismic Hazard Working Party. The seismic hazard working party was chaired and co-ordinated by Central Electricity Generating Board staff, but included individuals drawn from external consulting companies with a specialised knowledge of the relevant disciplines (historians, geologists, seismologists, engineering seismologists etc).

The principle objective was to evaluate the level of ground motion corresponding to various probabilities of exceedance per year. Initially the methodology was only used to calculate peak accelerations with the specified probability of exceedance, but this was soon extended to produce ground response spectra which have a uniform probability of exceedance across the entire frequency range of the spectrum. These spectra are know in the UK as the Uniform Risk Spectra and are used to define the infrequent seismic hazard at the reactor sites.

The methodology is developed in four stages which are as follows:

1) Compilation of a seismic source model in which seismic source zones and specific faults surrounding the sites are represented. The model takes in to account a variety of data sources.

2) Specifying parameters describing factors such as the rates of activity in these zones, source depths and attenuation parameters. These are specified conservatively.

3) Computation of the hazard level at the site. The approach is a probabilistic one and takes full account of uncertainties in the model parameters in order to provide appropriate safety margins.

4) Sensitivity studies to confirm that the results are not unduly sensitive to model or parameter variations, in order to ensure that appropriate margins to safety are present.

The Seismic and Geotechnical Database provides further details of the Seismic Hazard Assessment Methodology, which is applicable to all EDF Energy's Nuclear Generation sites in the UK.

Historical Data

According to the British Geological Survey (Natural Environment Research Council), over 80% of large earthquakes occur around the edges of the Pacific Ocean, known as the 'Ring of Fire', where the Pacific plate is being subducted beneath the surrounding plates.

Significant historical earthquakes in the UK are shown in Table 2.1 below:

Table 2.1: Significant Recent Historical UK Earthquakes

Date	Region	Magnitude	Comment
27 June 1906	Swansea	5.2 ML	
07 June 1931	North Sea (Dogger Bank)	6.1 ML	
10 August 1974	Kintail, Western Scotland	4.4 ML	
26 December 1979	Longtown, Cumbria (Carlisle)	4.7 ML	
19 July 1984	Lleyn Penin, North West Wales	5.4 ML	
2 April 1990	Bishop's Castle, Shropshire	5.1 ML	
26 December 2006	Dumfries	3.6 ML	
28 April 2007	Folkestone, Kent	4.3 ML	Peak ground acceleration of 0.1g at 10 Hz
27 February 2008	Market Rasen, Lincolnshire	5.2 ML	
14 July 2011	English Channel 85km South-East of Portsmouth	3.9 ML	

NB. ML (Local Magnitude): A logarithmic scale, based on the original Richter magnitude scale, used to express the total amount of energy released by an earthquake. This is the magnitude scale used by British Geological Survey (BGS) when describing UK earthquakes. The scale is logarithmic in order to cover a large range of earthquake energies. Due to this, it should be noted that a magnitude 6 ML is around 30 times larger, in terms of energy, than a magnitude 5 ML.

Review of Local Seismic Events

A review of seismic hazards for Hartlepool was carried out during a periodic safety review. This was conducted by comparing the seismic events that have occurred in the locality of Hartlepool with the events that have been considered for the Hunterston B and Dungeness B reviews. These reviews concluded that the events that were considered did not give cause to reconsider the validity of the design basis earthquakes.

The requirements of IAEA NS-G-3.3 stipulate a region of interest of a radius of 150km. The review reported that there had been no events of greater than 3.0ML within the 150km of Hartlepool between 1995 and January 2006 and it is concluded that the recent seismic events will not have a significant effect on the Hartlepool or Heysham 1 hazard assessments. Since 2006 the only event greater than 3.0ML has been the Dumfries event, which occurred at the boundary of the 150km radius for the Hartlepool site.

Since events considered for the recent reviews were less than, or close to, the threshold for the original seismic hazard assessment it was judged that they would not have a significant effect, as the reviews demonstrated. This is judged to remain true when the Dumfries event is also considered.

Events recorded within 15km of the sites have also been considered. On the 8 August 2000 there was a 2.7 ML event 14km from Hartlepool. This event did not lead to any significant seismic motion at Hartlepool and the seismic recording equipment was not triggered. As a seismic recorder activated by a seismometer set at 0.01g was not triggered, this implies PGA of less than 0.01g.

Geological Information on Site

The ground beneath Hartlepool consists of a deep alluvial layer overlying sandstones and deeper limestone strata. The site was levelled prior to the start of construction and parts of it are of made ground. The geological sequence at the site is as follows:

Table 2.2 Hartlepool Geological Sequence

Stratum (m)	Elevation (m, Ordanace Datum)	Depth Below Ground Level (m)
Hydraulic fill	+4.7 to +0.0	0 to 4.7
Alluvial Clay	+0.0 to -3.5	4.7 to 8.2
Upper Glacial Clay	-3.5 to -14.5	8.2 to 19.2
Glacial Sand and Gravel	-14.5 to -23.0	19.2 to 27.7
Lower Glacial Clay	-23.0 to -32.0	27.7 to 36.7
Sherwood Sandstone	Below -32.0	Below 36.7

The thickness of the Sherwood Sandstone is reported to be about 550 feet (167 m).

The simplified sequence above is based on the average thicknesses of strata in the area of the principal power station structures. The depth and level of the sandstone correspond to the top of the zone of weathered rock.

The hydraulic fill was placed on the site in 1967 after the main ground investigations had been largely completed. It was therefore not sampled in the pre-construction ground investigations.

In the simplified sequence of strata presented above, some estuarine sand which was present close to ground level prior to hydraulic filling has been included with the quoted thickness of the fill.

The glacial materials display quite considerable variations in soil type and thickness.

The Sherwood Sandstone consists primarily of sandstone but with a small proportion of siltstone and occasional beds of mudstone. It has a gentle dip towards the north.

In the Principia Mechanica Limited earthquake catalogue, Hartlepool is typical of a seismically soft site and the spectra appropriate to such a site have been selected.

Seismic Source Model and Sensitivity Studies

The derivation of the seismic hazard for Hartlepool was carried out on behalf of Nuclear Electric Ltd by the Seismic Hazard Working Party.

Three alternative source zone geometries were considered; the zones that were furthest from the site were the same in each model, but the models differed in respect to the subdivision of the zones local to the site.

The first zonation (given a weight of 0.4 in the probabilistic treatment) partitioned the north east coast area into two zones with a boundary just to the north of the Hartlepool site. The northerly 'Durham' zone is one of low historical seismicity with no recorded earthquakes of magnitude greater than 4.0. The southerly 'Humber' zone extends seawards to include the 1931 North Sea earthquake. These zones are bordered to the north by a 'Borders' zone, to the west by a 'Pennines' and a 'West Cumbria' zone, to the south west by a zone including the earthquakes of North Wales, Lancashire and Derbyshire and to the north east by an 'Offshore' zone.

The second zonation (also given a weight of 0.4, but preferred to the first zonation) relocates the boundary between the 'Durham' and 'Humber' zones southwards near Flamborough Head, placing the site firmly within the 'Durham' zone. The third zonation (given a weight of 0.2) is a more pessimistic variant of the second zonation in which the 'Durham' zone is extended seawards to include the 1931 North Sea earthquake.

In general, the sensitivity studies tend to reduce the predicted level of ground motion. Even extremely pessimistic scenarios gave only small increases in the predicted motion. For example, assuming a maximum magnitude of 7.0 in every zone gave only a 0.001g increase in predicted pga and only an approximate 5% increase in the 1 Hz spectral acceleration.

The site specific seismic hazard is calculated as 0.17g Uniform Risk Spectrum peak free field horizontal acceleration at 10^{-4} per annum return frequency for the bottom line and 0.1g Principia Mechanica Limited spectrum for the second line. In addition an interim seismic safety case was made utilising 0.07g peak free field horizontal acceleration uniform risk spectra at 10^{-3} per annum return frequency.

The hazard for Hartlepool is relatively low in UK terms and, as a result, the horizontal spectral accelerations below about 2Hz are lower than those associated with the soft site Principia Mechanica Limited spectrum anchored to 0.1g PGA. The effects of soil structure interaction and building dynamic response will be to generally amplify these lower frequency components; the in-structure accelerations associated with the second-line ground motion may therefore be more onerous in some cases than those resulting from the bottom-line ground motion. This is not an anomaly but reflects the comparison between deterministic (fixed) and probabilistic target capabilities.

Safety Margins in the derivation of Design Basis Earthquakes

The methodology used to derive the design basis earthquakes response spectra has made use of expert opinion and uses models that have consensus support from a wide range of external consultants with specialist knowledge of the relevant disciplines. Additionally it has made use of sensitivity studies which demonstrate the absence of cliff edge effects and generally tended to reduce the predicted level of ground motion.

A review of historical events of relevance to Hartlepool and within the IAEA stipulated region of 150km has taken place as part of the periodic review process. It has been concluded that the events considered did not have a significant effect on the assessment of the seismic hazard. The events subsequent to this review have been considered here and it is judged that they do not alter the outcome of the earlier review. It is also noted that the original seismic hazard models only considered events with a surface wave magnitude of greater than 4.0. . When the surface wave magnitude scale was formulated it was intended to give similar values as the local magnitude scale. Further studies have shown that from the experience of the UK catalogue, the surface wave magnitude value is consistently lower than the local magnitude value. This is supported by the estimates of the surface wave magnitude values for the events considered in each of the reviews that found that the surface wave magnitude values were either similar or less than the local magnitude values. Therefore the corresponding threshold would be 4.0 local magnitude or higher. The use of the local magnitude value can be considered conservative in comparison to the surface wave magnitude value.

The frequent event design basis earthquake is 0.1g PGA, in accordance with IAEA guidance and this exceeds that with an annual probability of 10^{-3} which for this site is 0.07g. This shows a clear margin and is therefore a pessimistic representation of a frequent event. Only where as low as reasonably practicable assessments have shown this is not practical have the second line plant items been qualified against the less onerous 10^{-3} pa uniform risk spectra. It is also worthy of note that a significant proportion of the second line plant has been seismically qualified to the more onerous 10^{-4} p.a. uniform risk spectra.

2.1.1.3 Conclusion on the adequacy of the design basis for the earthquake

The methodology used to define the design basis earthquakes for Hartlepool has been constructed using independent expertise based on well regarded sources of information. Furthermore it has been reviewed periodically in line with company processes and regulatory expectations. The methodology has been constructed with appropriate conservatisms, margins and sensitivity studies employed.

Conclusion HRA 2.1: The methodology used for calculating design basis earthquakes is robust, has appropriate conservatisms, margins and sensitivity studies employed and has been periodically reviewed.

2.1.2 Provisions to protect the plant against the design basis earthquake

The safety case addresses the qualification of systems, structures and components whose functionality is important in terms of lines of protection. In addition the safety case addresses interaction threats from plant which is not seismically qualified, consequential hazards and the operator actions required by the safety case. These provisions have all been back fitted to create the current design basis. This is discussed further in the following sections.

2.1.2.1 Identification of systems, structures and components that are required for achieving safe shutdown state and are most endangered during an earthquake. Evaluation of their robustness in connection with DBE and assessment of potential safety margin.

EDF Energy Nuclear Generation now has seismic safety cases for all of its advanced gas-cooled reactors covering both the at-power and shut-down conditions as well as fuel handling operations. The requirement for these cases was identified at the time of the first periodic safety review. These cases were implemented by a programme of seismic walkdowns and analyses together with appropriate plant modifications, which ensured the qualification of the required systems to the appropriate standard for the site.

The qualification of systems, structures and components required by the case took account of the maximum seismic loading they were required to withstand. This loading was specified in terms of floor response spectra at each floor elevation throughout the relevant buildings. The floor response spectra was derived from a finite element analysis of the building, which included the effects of soil structure interaction.

It is important to reflect that with regard to seismic qualification, a key issue is to ensure all plant requiring qualification has been identified. Operational experience is that the failures in an event are typically from plant which has been overlooked as requiring qualification, rather than from plant which has been qualified failing to perform its safety function, even if the event was beyond the design basis.

The following section first describes the current safety case and plant items required for safe shutdown and cooling of all plant states and plant areas on the Hartlepool site. Due to the more extensive nature of the AGR fuel route these plant areas are described individually. The second part of the section is where the evaluation of robustness of the Hartlepool plant is described.

2.1.2.1.1 Operating Reactors

<u>Infrequent Event</u>

The main focus of the seismic safety case is to demonstrate acceptable consequences in the event of the infrequent design basis earthquake described in section 2.1.1 above. This is often referred to as the 'bottom line event', i.e. the most onerous event for which bottom line plant provides protection. Bottom line plant and structures are those plant and structures required to provide a single line of protection during the onerous infrequent event. The bottom line plant is required to perform the essential safety functions of trip, shutdown, post-trip cooling and monitoring. Bottom line plant and structures also provide one of two lines of protection against frequent events as described below.

<u>Frequent Event</u>

As well as the infrequent hazard event, a less onerous but more frequent hazard magnitude is defined against which two lines of protection are demonstrated where this is reasonably practicable. As described in section 2.1.1 above, the response spectra at Hartlepool for a frequent event is taken to be one with has an assumed PGA of 0.1g Principia Mechanica Ltd. Spectrum, this being representative of an earthquake with a return frequency of 10^{-3} per annum, i.e. the lower limit of the frequent band defined in the NSPs.

There is a further level of defence, in that mild ground shaking has never been known to result in damage to industrial plant. The Seismic Qualification Utility Group experience database for example has no recorded instances of damage to industrial plant for peak ground accelerations below 0.12g. This 'second line' plant and the safety case that surrounds it is not discussed further in this report, since the focus of this review is on extreme events.

Essential Safety Functions

Lines of Protection are required for the relevant essential safety functions to prevent an unacceptable radiological release as a consequence of an earthquake. The following main essential functions are relevant:

- Reactor Trip
- Reactor Shutdown
- Post-Trip Cooling
- Post-Trip Monitoring

The case is based on demonstrating that the essential functions of trip, shutdown, post-trip cooling and monitoring can be provided for a infrequent seismic event (corresponding to a peak free field horizontal ground acceleration of 0.17g combined with a pessimistic spectrum).

The safety case was initially based on the assessment in a periodic safety review, but developed in a number of areas as identified in the various safety case documents. The lines of protection identified in the safety case have been confirmed as being appropriate by a subsequent periodic safety review.

Reactor Trip

The requirements for the essential function of reactor trip in a 10^{-4}p.a. seismic event are defined as follows:

- The ability to trip the main shutdown system manually from the central control room following receipt of a seismic alarm.
- The ability for automatic reactor trip in response to a normal trip signal.

The safety case for qualification of essential plant against 10^{-4} p.a. Uniform Risk Spectra seismic event (at-power reactor) outlines the details of the qualified hard-wired alarm in the Hartlepool central control room to alert the operator to the occurrence of a seismic event. The alarm setting associated with the seismic switches has been set at 0.1g, the acceleration associated with the onset of an infrequent seismic event. On receiving the 0.1g alarm signal the operator is instructed to follow seismic operating instructions which requires a prompt trip of both reactors. In addition to the 0.1g alarm that protects against infrequent seismic events, a 0.05g alarm is provided to indicate the occurrence of a frequent seismic event. Also, a seismic recorder is activated by a seismometer set at 0.01g: this activation also generates a hard-wired alarm in the central control room.

The main guardline is fail-safe. Failure of the guardlines in the seismic event will automatically result in the generation of a trip signal to the main shutdown system. It is therefore considered that the functional requirement for automatic trip upon a genuine demand during an infrequent seismic event is met.

Reactor Shutdown

Reactor Shutdown Systems are described in Chapter 1.

Following the infrequent seismic event the control rod mechanisms will continue to operate correctly, the core support structure integrity will be unaffected and the core displacements resulting from the seismic event are sufficiently small such that reactor shutdown via the primary shutdown system is assured.

Post Trip Cooling

When the reactor is at power, post-trip cooling is achieved by either natural circulation for a reactor with an intact pressure boundary or forced circulation capability to protect against the possibility of a minor pressure boundary breach due to the seismic event. Natural circulation is where natural convective flow of reactor coolant achieves adequate cooling of the core. This requires a minimum reactor pressure, boiler feed and reactor pressure vessel cooling. Forced circulation is where coolant needs to be forcibly circulated through the reactor core to achieve adequate core cooling.

This requires gas circulator function and boiler feed. The following sub sections address the functionalities required to support this claimed post-trip cooling.

Pressure Boundary

The safety case demonstrates that all the pressure boundary components, the pressure vessel, safety relief valves and small-bore pipework are capable of withstanding the infrequent seismic loading. The pressure boundary is also maintained during refuelling operations.

Gas Flow Path

A detailed seismic assessment was carried out for the core and associated support and restraint structures to demonstrate the integrity of cooling flow and control rod entry paths. In addition, detailed analysis was carried out to confirm the integrity of the fuel assembly, boiler support and boiler internal components following a bottom-line seismic event.

Forced Gas Circulation

Forced Gas circulation requires gas circulators, gas circulator motors, lubricant oil systems and the electrical supplies associated with these systems. These systems are all qualified against the infrequent seismic event.

Boiler Feed

Natural circulation and forced gas circulation have different boiler feed requirements with forced circulation being the most onerous. The boiler feed system has been qualified against an infrequent seismic event.

Auxiliary Cooling Water System

The gas circulators require cooling to prevent their bearings from overheating. At Hartlepool the integrity of the auxiliary cooling water system has been qualified to enable gas circulator cooling.

Pressure Vessel Cooling

The qualification of the pressure vessel cooling water system head tank and pressure vessel cooling water circuit includes the integrity and functionality of the pressure vessel cooling water pumps, heat exchangers and pipework.

Seismic events whilst the fuelling machine is connected to the reactor

The impact of earthquake on the standpipe connection whilst the fuelling machine is connected to the reactor is covered in section 2.1.2.3 where it is shown that the reactor pressure boundary is not compromised.

Essential Stocks

The safety approach at EDF Energy Nuclear Generation stations requires that sufficient stocks of consumables are held to enable essential functions to operate for at least 24 hours. Replenishment of those stocks to enable the essential plant to continue operating is expected to within the 24 hours period.

Minimum quantities of these essential consumables, to ensure a 24 hour mission time, have been determined and are specified in the relevant Technical Specifications.

Post Trip Monitoring

The requirement for post-trip monitoring in a 10^{-4}p.a. seismic event is defined as qualification of the alternative indication centre. When regarding the events at Fukushima Daiichi the importance of maintaining indications of plant status during extreme events is clear. This issue was highlighted in the Interim Weightman Report by Recommendation 22, specifically the part of that recommendation relating to emergency instrumentation. The functional requirement of the alternative indication centre is stated as post-trip monitoring of essential reactor indications to confirm that the reactor remains shutdown and adequately cooled. Essential indications have been identified and qualification of the alternative indication centre includes these essential indications, alternative indication centre equipment including cabling, and the alternative indication centre uninterrupted power supply system.

Civil Structures

The civil structures house essential equipment that is required to function in a seismic event. Essential buildings have been identified and these civil structures have been qualified against the infrequent seismic event.

Feed & Steam Pipework

The principal reasons for qualifying the feed and steam pipework are:

- To ensure the capability to provide boiler feed to the reactor after the seismic event.
- To ensure that there will not be leakage of steam and water into the reactor and turbine building which could prevent operator access for plant monitoring and recovery operations.

2.1.2.1.2 Shutdown Cooling

The bottom line post-trip cooling described above is also claimed for the scenario where a seismic event occurs when a reactor is shutdown. However, during a reactor outage, decay heat will be much lower than immediately post-trip which means that delays can be accepted in restoring core cooling should faults occur. So providing the decay heat limits are met, it is permitted to depressurise the reactor, open penetrations for inspection and maintenance and admit air to the reactor. In this state adequate cooling is provided by forced gas circulation.

The safety case claims that cooling will be achieved by restoration of gas circulators with main boilers being fed using the back-up cooling system. All the systems, structures and components required for this functionality and restoration times required by the safety case are sufficiently long that such manual actions are acceptable

2.1.2.1.3 Fuel Route

For all stages of fuel handling and storage, the facilities are qualified against the design basis earthquake to ensure that the containment and (where applicable) pressure boundary remain effective, and that mechanical damage to the fuel is prevented.

Of the cooling chains discussed in Chapter 1, the seismic safety case is summarised below:

- Handling with fuelling machine –natural cooling maintains acceptable fuel temperatures;
- Buffer storage - cooling systems are seismically qualified
- Dismantling - loss of cooling is tolerable as natural cooling is adequate
- Storage in ponds – diverse cooling package is seismically qualified.

2.1.2.1.4 Evaluation of their robustness in connection with DBE and assessment of potential safety margin.

The severity of the earthquake used in the safety case to represent the infrequent design basis earthquake with a return frequency of 10^{-4} per annum has been established using a conservative approach, as described in section 2.1.1.

The systems, structures and components claimed to provide protection against this within design basis earthquake have been qualified using conservative methods.

Conclusion HRA 2.2: The methodologies used for ensuring robustness of the plant have appropriate conservatisms and margins, make appropriate use of international experience and standards, and have been periodically reviewed.

2.1.2.2 Main operating contingencies in case of damage that could be caused by an earthquake and could threaten achieving safe shutdown state.

The operators at Fukushima Dai-ichi were hampered in their recovery actions by the situation on and around the site. This was initially as a result of the inundation but also once the waters had receded as a result of debris, radiation levels and conventional hazards as a result of the event.

The EDF Energy Nuclear Safety Principles require that the functional capability claimed of an operator, which constitutes a line of protection, is justified by appropriate means as follows:

- The claims made in the safety case should be supported by appropriate human factors assessments to demonstrate the capability demanded.
- The human factors assessments should include, as appropriate, task analysis, the state of supporting procedures, training, environmental issues (such as the state of emergency lighting), and administrative controls.

This section describes the claims made on operator actions in design basis events and re-assesses these against the events at Fukushima.

2.1.2.2.1 Operating reactor

<u>Trip</u>

If there are no plant faults requiring automatic trip, then the operator will manually trip the reactor.

<u>Shutdown</u>

The main shutdown system is qualified for automatic operation so no operator actions are required.

<u>Post-trip cooling</u>

The manual actions required to establish post-trip cooling are described below:

<u>*Boiler Feed*</u>

The operator is required to start the pumps and initiate feed and ensure that the minimum flow requirements are met.

<u>*Plant Cooling Actions on a Depressurising Reactor*</u>

As the main system for cooling of the gas circulators may be lost, the gas circulators will be shut down while back-up cooling systems are started. Once cooling of the gas circulators has been confirmed, the gas circulators will be restarted.

<u>*Plant Cooling Action under Natural Circulation*</u>

The only operator action associated with plant cooling via natural circulation is to check that back-up feed has automatically been injected into the pressure vessel cooling water system if the normal system is unavailable.

<u>*General Monitoring*</u>

Water and fuel stocks (when the systems are in service) will need to be monitored, and appropriate actions taken to replenish stocks and/or minimise stock usage. At Hartlepool long term water supplies are secured by the seawater make-up system which require deployment of submersible pumps. The operator will need to monitor flow to the pressure vessel cooling water system and concrete and liner temperatures.

Assessments have been carried in developing operator instructions to take account of access to plant. These assessments support the judgement that the actions claimed will be carried out in the required timescales. However in reviewing this area of the safety case in the light of events at Fukushima, it is considered that a review should be carried out of the totality of the required actions and the way these might be influenced by the Emergency Arrangements (e.g. the need for a site muster, and the setting up of the access control point) taking due account of the human factors issues.

2.1.2.2.2 Shutdown Cooling

The approach to ensuring safety for seismic faults on a shutdown reactor is described in section 2.1.2.1.2. The approach is based on claiming operators will restore sufficient plant to provide adequate post-trip cooling in a given timescales (dependent on the plant state) using local to plant actions where appropriate. The claimed ability of the operators to do these actions is on the basis that they are simple and achievable and take due allowance for mustering and deployment via the the access control point and alternative control point. A review of the shutdown actions as part of Consideration 2.1 below is not therefore considered necessary.

Conclusion HRA 2.3: The claims made on the operator make appropriate use of international experience and standards and have been periodically reviewed. The provisions have been reviewed here as part of the response to the Fukushima Dai-ichi event.

Consideration HRA 2.1: Consider the need for a review of the totality of the required actions, and the way these might be influenced by the Emergency Arrangements (e.g. the need for a site muster, and the setting up of the Access Control Points), taking due account of the human factors issues.

2.1.2.3 Protection against indirect effects of the earthquake

2.1.2.3.1 Assessment of potential failures of heavy structures, pressure retaining devices, rotating equipment, or systems containing large amount of liquid that are not designed to withstand DBE and that might threaten heat transfer to ultimate heat-sink by mechanical interaction or through internal flood.

It is necessary to identify plant items and structures which, although not claimed as protection against seismic hazards, could pose a risk to protection systems through physical interaction or in generating a consequential hazard.

Only hazards internal to the power station are considered.

- Fire
- Steam Release
- Hot Gas Release
- Cold Gas Release
- Missile Impact
- Dropped Loads and Lifting Equipment
- Local Flooding
- Toxic gas cloud release
- Vehicular transport

The seismic qualification methods used in EDF Energy include consideration of 'interaction threats'. In other words, when considering the functional capability of systems, structures and components, the potential for the failure of nearby plant, whose functionality may not have been seismically qualified (on the basis that such functionality is non-essential) is considered. In this way, if earthquake induced failure of nearby plant can cause failure of the essential function, then remedial action is taken.

The overall safety case for Hartlepool Station considers a wide range of credible faults and hazards against which adequate measures for prevention, protection and mitigation are demonstrated. The lines of protection for all the significant faults and hazards are common – they are all aimed at achieving adequate cooling of the reactor core. They are based on achieving either natural circulation, forced circulation or both.

A seismic event has the potential to induce other consequential hazards which could indirectly threaten essential safety equipment. Additionally, the plant normally claimed as protection against individual hazards may not remain available after an earthquake.

There are no additional active cooling systems claimed in the fuel route seismic safety case other than those claimed in support of the reactor safety cases. It is demonstrated in the reactor safety cases that these active cooling systems are not vulnerable to the effects of seismically-induced hazards.

The approach taken for consequential internal flooding is typically as follows. The potential sources of internal flooding were identified. For those sources which were not already seismically qualified, the consequences of the flooding were considered and if these had an adverse impact on the protection provided for earthquakes, then appropriate enhancements provided. In most cases, this corresponded to seismic qualification of the pipework, tank, etc. such that consequential failure (which would cause internal flooding) should not occur.

Fire

Fires as a result of earthquakes are associated principally with severance of gas supply mains at domestic and commercial premises. Experience with industrial plant shows that the probability of seismically-induced fires is small, although it cannot be discounted. It is concluded that seismically induced fires will not put at risk the lines of reactor protection claimed against an infrequent event.

Steam Release

The main steam and branch pipework, the dump steam pipework, the start up vessels, the main feed pipework and the high pressure back-up cooling system and associated systems have all been shown to withstand a seismic event. The reheat pipework has been subject to seismic walkdown and all necessary modifications have been implemented to prevent secondary interaction concerns to qualified systems and pipework. A significant risk of steam release to the reactor or fuel route plant is therefore prevented.

Hot Gas Release

It is a requirement of the seismic safety cases for reactor operation that there should be no significant loss of pressure following an earthquake. With the exception of the reactor gas bypass circuits, the pressure boundary has been qualified against the 10^{-4} p.a. seismic events. The gas bypass isolation valves are seismically qualified and will isolate any possible leaks in the bypass plant, thereby preventing depressurisation.

Further work has shown that bottom line plant is unlikely to be affected by seismically induced failure of minor connections to the reactor pressure vessel. The same conclusion can be made for the fuel route plant.

Cold Gas Release

The CO_2 plant is qualified against a infrequent earthquake A smaller cold gas release could however occur for example due to failure of small bore pipework. Areas where smaller cold gas releases could occur from reactor or fuel route systems have been identified and it has been found that the releases will not affect essential plant.

Missile Impact

The only credible sources of missiles that would be capable of causing significant damage are the main turbine low pressure rotors. However, it has been concluded that turbine disintegration as a result of a seismic event is so low that the risk can be discounted. This is supported by world wide experience in seismically active areas.

Dropped Loads and Lifting Equipment

It is shown that lifting equipment that could threaten reactor protection or fuel route essential plant is either seismically qualified, or is only permitted to be used when the consequences of failure would be acceptable.

Local Flooding

The level of water that could accumulate in the reactor or turbine hall basement from the failure of unqualified storage tanks or pipework systems has been assessed and shown not to compromise the lines of reactor protection claimed following a seismic event.

The effects of local flooding on fuel route systems have been analysed and it is judged that the essential safety functions will remain available.

Toxic Gas Cloud Release

There are two possible sources of toxic gas namely ammonia and hydrazine. The ammonia tanks have been seismically qualified to remove the risk to essential personnel in the central control room and alternative indication centre and within the fuel route. At Hartlepool, hydrazine is stored in a location where it will not present a hazard to operators undertaking essential actions following an infrequent seismic event. There is no credible mechanism for toxic gas cloud release to cause a breach of the pressure boundary of any of the fuel route facilities. Fuel assemblies contained within these facilities will be similarly unaffected.

Vehicular Transport

It is considered that there is no risk from vehicular transport incidents during an earthquake, unless it is envisaged that a road tanker carrying ammonia could be damaged by the event and the contents released. The likelihood of this is considered sufficiently low to be discounted since deliveries of ammonia are at a frequency of approximately one per year.

Additionally, the main structures on site are seismically qualified and vehicles are unlikely to be at risk from falling debris.

Conclusion HRA 2.4: Potential interactions of systems, structures and components have been considered as part of the safety case and appropriate qualification has been carried out and reviewed as required.

2.1.2.3.2 Loss of external power supply that could impair the impact of seismically induced internal damage at the plant.

All electrical systems that support reactor and fuel route safety functions are derived from the essential supplies that are backed up with the on-site generators powered from gas turbines at HRA.

The safety case assumes that consequential loss of grid occurs for both frequent and infrequent seismic events. The safety case approach in EDF Energy Nuclear Generation is to ensure that adequate stocks of consumables are held on site to last at least 24 hours. This includes boiler feedwater, CO_2, and generator fuel. The usual approach is for the minimum stock levels quoted in technical specifications to be those that correspond to this 24 hour 'mission period'. It is implicit in the safety case that company emergency arrangements would provide replacement consumables within the 24 hour period to enable the plant to be managed safely. Note that in general, normal stocks levels are higher than the limits specified in tech specifications, therefore the most probable scenario would be that more than 24 hours would be available to replenish consumables.

The events in Fukushima have highlighted that there may be potential benefit in reviewing the evidence that Company Emergency Arrangements would provide replacement consumables within the 24 hour period following a design basis earthquake to identify potential enhancements. This is discussed further in Chapter 6.

Conclusion HRA 2.5: Consequential loss of grid has been considered as part of the safety case. Electrical supplies to essential equipment are provided by the on-site generators which are bottom line seismically qualified.

2.1.2.3.3 Situation outside the plant, including preventing or delaying access of personnel and equipment to the site.

The Local Resilience Forums are the local authority body in the UK with responsibility for providing emergency response in the community. The review of emergency arrangements is detailed in Chapter 6.

A review of site access following external hazards has been carried out. A survey of the approaches to site was completed and the review concluded that there is the possibility of railway bridges collapsing and therefore the potential for the temporary prevention of road access to site following a seismic event. However, it is argued that the extent of the potential blockages would be limited such that arrangements for rapid access to appropriate plant and equipment for temporary repairs and clearing earth, rubble, trees, etc., would allow a route to be re-opened within the 24 hour mission period.

Widespread damage to an extent that cannot be repaired within 24 hours is not expected but cannot be ruled out for more onerous, less frequent events. If such damage did occur, access to site for personnel could be arranged by alternative means. This is discussed further in Chapter 6.

A further review has been carried out to assess the impacts of extreme natural events on access to vital plant around the site and to highlight areas that may be susceptible to the effects of these events. They show that there are no immediate concerns as there are many different contingencies in place to access required parts of the plant.

Conclusion HRA 2.6: Access of personnel and equipment to the site has been considered as part of the Emergency Arrangements, and following a recent review these arrangements are considered to be appropriate in the light of events at Fukushima.

2.1.2.3.4 Other indirect effects (e.g. fire or explosion).

The equipment which is essential for trip, shutdown, post-trip cooling and plant monitoring following a seismic event must also be protected against hazards that are caused by the seismic event. The seismic safety case presents an assessment of seismically induced hazards that could threaten the essential functions in a 10^{-4}p.a. Uniform Risk Spectrum event as discussed. There is a small residual risk from fires. It was demonstrated that this hazard would not affect essential plant or prevent operator actions required following a 10^{-4} p.a. Uniform Risk Spectrum seismic event.

The reactor coolant pressure boundary is expected to remain intact, so there is not expected to be a significant hot gas release hazard. In the unlikely event of small bore branch failure, the resulting hot gas release effects should be small, although this will result in the need for operators to wear breathing apparatus should local to plant actions be necessary in the reactor building

The effects of consequential steam release or cold gas release hazard are discounted on the basis that either the relevant plant has been qualified to the bottom-line level or that there is no significant risk to essential plant from the hazard.

Hartlepool is located in a heavily industrialised area, however all but one of the 39 control of major accidents hazards sites are located more than 2km from the station and would not pose a seismically induced industrial hazard risk to reactor protection or fuel route plant or activities.

Able UK have a dry dock next to the station which is being used for the decommissioning of marine vessels. The site is now registered as top tier control of major accidents hazards site, with the main risk to the station presented by asbestos. The inhalation of asbestos fibres presents a long term risk to personnel health. It is however unlikely that a significant number of fibres would be released as a result of a seismic event and even if this were to occur this would not present a threat to plant operation or inhibit the actions required of the operator. There is a risk of vapour cloud explosions/fires from storage of fuel oil, gas oil and propane but no solid explosives are stored at the site. It has been determined that the risks are low and off-site emergency response planning arrangements are not required for the Able Site although the site is part of the cleveland emergency alarm system.

Worldwide experience is that in urban environments, fires as a consequence of earthquake are not uncommon. This is often as a result of failures in unqualified domestic gas systems and such like. The systems on EDF Energy sites which contain flammable material, like propane tanks, gas turbine or diesel fuel oil systems are generally seismically qualified. Therefore the seismic safety case is based on there being a low probability of consequential fire, and fire protection features have not been formally seismically qualified. Given the small probability of a seismically-induced fire, the extensive use of passive fire barriers, the extensive seismic walkdowns completed to consider the effects of local spatial interactions, and the segregation and redundancy of essential plant, it is judged that the loss of an essential function as a result of seismically induced-fire is acceptably low. Station fire tenders and hose relays (along with the Local Authority Fire Brigade) may be available to assist in extinguishing any seismically induced fires, even though these have not been formally seismically qualified. Nevertheless, given the potential effects of fire and the absence of seismically qualified fire protection, it is appropriate to review the evidence for low probability of consequential fires to establish the ongoing validity of the current approach.

Conclusion HRA 2.7: The potential indirect effects have been considered as part of the safety case and where considered necessary to protect essential plant, interactions have been qualified against the appropriate design basis earthquake.

Consideration HRA 2.2: EDF Energy will consider reviewing the probability of consequential fire as a result of an earthquake.

2.1.3 Compliance of the plant with its current licensing basis

2.1.3.1 Licensee's processes to ensure that plant systems, structures, and components that are needed for achieving safe shutdown after earthquake, or that might cause indirect effects discussed under 2.1.2.3 remain in faultless condition.

All modifications are implemented using the engineering change process which requires that all modification proposals check whether plant affected by the proposal is seismically qualified or whether the modification could have a deleterious effect on seismically qualified equipment. The procedure therefore reduces the risk that the seismic safety case is compromised by changes to the plant and structures.

Inspection and maintenance is important to ensure that the adequacy of the seismic safety case is maintained. The nuclear safety related inspections are listed on the maintenance schedules. The civil structures claimed by the seismic safety case are included on the schedule of Licence Condition 28 (LC28) inspections. Specific entries are included in the maintenance schedule for selected plant items and for a number of the systems, safety system reviews are also specified. The reviews are included on the maintenance schedule and are carried out at frequencies of between three and five years, depending on the system.

Seismic walkdowns have been added to the maintenance schedule at Hartlepool as part of the development of the stage 3 seismic safety case.

As a result of the review carried out following the events at Fukushima, the effectiveness of the processes which manage the ongoing qualification of plant claimed in the seismic safety case will be further reviewed.

Consideration HRA 2.3: EDF Energy will consider conducting a review of the efficiency of the process for maintaining ongoing seismic qualification and consider whether improvements should be implemented.

2.1.3.2 Licencee’s processes to ensure that mobile equipment and supplies that are planned to be available after an earthquake are in continuous preparedness to be used.

The submersible pumps and hose connections that are needed are maintained in a state of readiness. The maintenance schedule requires a regular function and performance check of pumps and inspection of system valves, pipework and fittings. These checks also provide the operators with an opportunity to practice system deployment.

2.1.3.3 Potential deviations from licensing basis and actions to address those deviations

Within the processes outlined above there are mechanisms for identifying any areas of concern or anomalies. These may take the form of a commitment from the productions of a safety case, interim justification for continued operation, periodic safety review commitment, or a justification for continued operation. These are within the processes we use to comply with our licensing and are being addressed on appropriate timescales.

Conclusion HRA 2.8: There are several issues identified with the seismic safety case and appropriate actions are being undertaken on a reasonably practicable timescale to address them.

2.1.3.4 Specific compliance check already initiated by licensee

The checks carried out following the events in Fukushima have confirmed that the safety case is based on the provision of a line of protection with redundancy for the infrequent design basis earthquake, and two lines of diverse protection with redundancy in each line, for the frequent design basis earthquake. These cases are considered robust. Emergent issues regarding the validity of these cases are treated using established company processes.

<u>Reviews</u>

In light of the events at the Fukushima Dai-ichi plant, as responsible operators EDF Energy Nuclear Generation have carried out two separate reviews at each of the sites. The information gathered by these self-assessments was used to provide a formal company response to address the recommendations of INPO IER 11-1 and WANO SOER 2011-2 (which are the same). These are known as the within design basis and beyond design basis evaluations respectively. The scope and findings of the full review are presented in Chapter 0 with the specific seismic aspects as follows.

<u>Scope</u>

The within design basis evaluation was specified to ensure that systems essential to fuel cooling in an emergency situation in a within design basis event including seismic and flooding scenarios were correctly configured, lined up and in a suitable condition to be declared available/operable. Further to this configuration check, a full seismic housekeeping walkdown was carried out. This involved appropriate engineers physically inspecting areas of the plant containing seismically qualified equipment and checking that the plant areas did not contain any items which could cause damage to claimed systems, for example by falling over in an earthquake and striking a system or component.

Stations were asked to capture any issues for further action through condition reports and work requests.

The primary finding was that no major shortfall was identified; however there were a number of minor issues or defects. These are being closed out using the appropriate company processes. There were also a number of conditions highlighted by the walkdowns that whilst being compliant with our existing safety case requirements, did not meet industry best practices. The fleet guidance on housekeeping standards lacks clarity in the seismic area. The associated record keeping requirements also need clarity. A number of commitments were made as a result of the within design basis evaluation. These include the following:-

- Fleet operations manager to update housekeeping standards and associated checksheet to specify fleet standards for seismic housekeeping.
- Fleet operations manager to establish a fleet training request based on the revised housekeeping standards and associated checksheet to lead on the update of op tech training programme

It has been agreed that following the company review of station responses areas for improvement may be identified, and at this stage station will determine if there any additional local areas of improvement

Conclusion HRA 2.9: The reviews undertaken and the actions identified therein, have confirmed that Hartlepool is compliant with the current licensing basis, although a few improvements have been identified.

Conclusion HRA 2.10: The robustness of the plant against design basis earthquakes is considered to be appropriate.

2.2 Evaluation of safety margins

The experiences at Fukushima Dai-ichi outline the significance of the plant experiencing events more severe than were considered within the design basis earthquake. The EDF Energy Nuclear Safety Principles for the advanced gas-cooled reactors require an adequate integrity of protection should be demonstrated against Earthquakes, by considering events with a return frequency of greater than or equal to 1 in 10,000 per year within the design basis safety case.

The nuclear safety principles also state that the integrity of protection against the infrequent external hazard should ideally be demonstrated with a margin that could be argued to accommodate an appropriate more severe level of hazard. This is included to ensure there is no ‘cliff edge’ such that in the event of an earthquake slightly more severe than the design basis earthquake, unacceptable consequences would not occur.

The formal seismic safety cases do not always specifically address this particular aspect of the nuclear safety principles, although it has been considered in the periodic safety reviews.

Section 2.1.1.3 outlined that conservatisms and margins exist in the calculation of the design basis earthquake. Section 2.1.2.1 noted that the methods use to seismically qualify systems, structures and components are also inherently conservative. It is this conservatism which is explored in this section to help illuminate the safety margins.

Technical guidance note for seismic design and assessment for advanced gas-cooled reactor power stations provides detailed guidelines to ensure that the whole process of seismic qualification includes adequate margins. The definition of 'adequate' margins in this context is margins that are sufficient for there to be no disproportionate increase in risk for more severe seismic events, even when all of the uncertainties in the process are taken into account. The preferred methods of assessment have been chosen accordingly. They typically include, for example, the conservatism present in design codes and pessimistic assumptions about natural frequencies. Where different options are available, which are potentially less conservative, these guidelines stress the importance of consulting the seismic design authority to ensure that margins remain adequate, whatever method is adopted. This section explains the mathematical background to how the objective is achieved. The approach that has been adopted is to recommend methods of assessment and acceptance criteria that ensure that, for the specified earthquake excitation, there will generally be a high confidence of low probability of failure. Higher reliability is expected for new plant designed according to code-based methods. In any case, even where 'high confidence of low probability of failure' is not strictly achieved, margins will be sufficiently great that there will be no disproportionate increase in risk for more severe seismic events.

The justification for this assertion lies in the concept of seismic fragility functions. Figure 2-2 is a typical fragility curve for a system, structure or component which has been seismically qualified. It shows the way the probability of failure increases as the severity of the earthquake increases. Curves like this can be used quantitatively in seismic probabilistic safety assessment. In deterministic seismic cases, the curves are used by the concept of the level at which there is a high confidence in the low probability of failure. An high confidence in the low probability of failure acceleration value is set such that there is a high confidence (95%) of a low probability (5%) of failure. In practice this implies an overall probability of failure at the high confidence in the low probability of failure value of 1%. For new plant that is designed to resist earthquakes, the more onerous design code requirements imply a probability of failure of less than 0.1%.

So in Figure 2-2 below, the high confidence in the low probability of failure value is a peak ground acceleration of 0.2g. If plant has been qualified, it is taken that the level to which the plant is qualified is the earthquake at which the plant should not fail, i.e. there is a low probability of failure, and this corresponds to the concept of the high confidence in the low probability of failure value. Thus plant qualified to 0.2g, effectively has a high confidence in the low probability of failure value of 0.2g.

The important point here is that the shape of the curve for systems which have been designed with a seismic capability tends to be similar, although the curve will be shifted to the left or right depending on the level of earthquake for which the plant has been designed. Inspection of Figure 2-2 shows that if the design earthquake is 0.2g, the seismic capacity of the qualified system is well into the tail on the left-hand side of the mean fragility curve.

The curve also shows that in terms of margin to failure, the probability of failure of say, 50% is not reached until the severity of the earthquake has increased to 0.53g, a factor 2-3 higher than the design basis.

Another important point is that for plant which has qualified by design or analysis in which code compliance is achieved, the above approach is conservative, such that the true fragility curve would be expected to be shifted to the right. This means that in these cases, the 50% probability of failure point would require an earthquake whose severity was greater by a factor significantly more than 2-3. For plant that has been qualified by walkdown, or by analysis in which code compliance has not been achieved but in which alternative arguments have had to be utilised, this extra degree of conservatism would not be present, but the factor 2-3 would still be applicable.

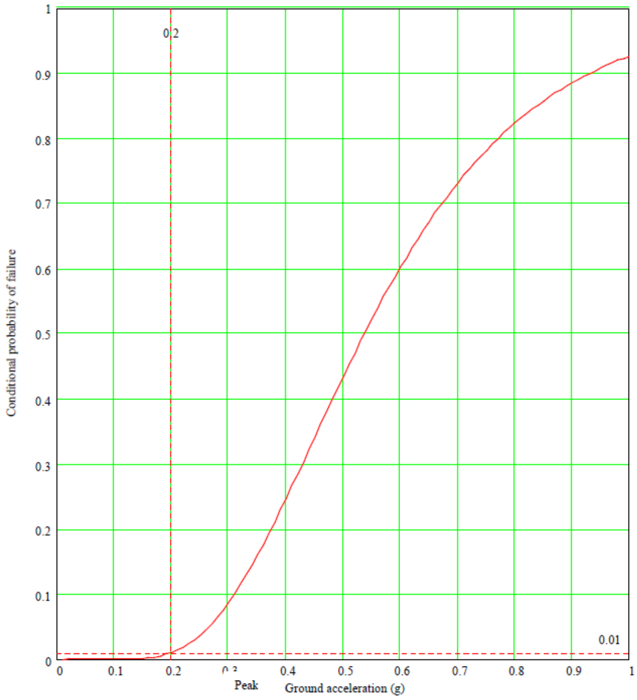

Figure 2-2: Mean Fragility Curve for typical System Qualified to 0.2g peak ground acceleration.

If a structure is brittle (i.e. has limited ductility), then under a statically applied load it will fail at a predictable level of loading, and the corresponding fragility curve would show an abrupt step at the failure load from a probability of zero to a probability of one. This abrupt variation never occurs in seismic fragility curves, which always show a smooth, gradual increase in failure probability because of the random, dynamic nature of seismic loading, even if the structure is brittle.

Conclusion HRA 2.11: When considering beyond design basis earthquakes, the probability of failure of 50% is not reached until the severity of the earthquake has increased to at least a factor 2-3 higher than the design basis.

2.2.1 Range of earthquake leading to severe fuel damage

As noted above, the curve shows that a probability of failure of 50% is not reached until the severity of the earthquake is at least twice that of the design basis earthquake, which for Hartlepool is 0.34g PGA. The seismic hazard assessment reports for the site indicates that this increased level of ground motion has a probability of between 10^{-5} and 10^{-6} per annum.

This needs to be caveated in respect of the human response to the event. The confidence that can be placed on the recovery actions required in earthquakes may not necessarily consistent with the fragility approach. The immediate protective functions (trip and shutdown) do not require any operator action, but manual action is claimed in order to restore feed to the boilers, and then a variety of longer term actions are also required. There is generally no cliff edge in respect of the timescales on which the actions are claimed to be achieved. Therefore, a more severe earthquake which led to additional delays in achieving these actions would not necessarily be a problem. Notwithstanding this, Consideration HRA 6.3 raised in Chapter 6 will lead to further insights into this issue.

Clearly, where there are known issues with the robustness of the plant to withstand the within design basis infrequent earthquake, the margins available for those systems, structures and components may be reduced.

Reactor Core

Some components within the core support and restraint structures have safety factors less than unity under design basis earthquake loading when conservatively assessed against modern design codes. In response, the consequences of failure have been reviewed. These have shown that failure does not present a risk to safe shutdown and maintaining a coolable core geometry. Further work is currently ongoing to establish the capacity of these components to tolerate more onerous seismic events. The analysis undertaken to date shows that the limiting component is able to withstand a loading of up to twice that under design basis earthquake.

2.2.2 Range of earthquake leading to loss of containment integrity

AGRs are not provided with a containment structure. However the reactor pressure boundary does have a containment role, although its main role is to maintain the density of the CO_2 primary coolant. The qualification of the reactor pressure boundary for design basis earthquake is discussed section 2.1.2.1.1. Therefore the comments in section 2.2.1 above relating to margin to failure also apply to here.

2.2.3 Earthquake exceeding the design basis earthquake for the plant and consequent flooding exceeding design basis flood

There are no dams or large water courses within the vicinity of Hartlepool, and although there are large bodies of water surrounding the site (North Sea and the Tees Estuary), these are all below general site level. The safety case does not explicitly cover coincident local earthquakes and tsunami, as it is not judged credible that a local earthquake would be powerful enough to produce a tsunami. This judgement is supported by a detailed study undertaken by the Department for Environment, Food and Rural Affairs (DEFRA) in 2005 to evaluate the tsunami risks to the UK. The potential risk is therefore one of flooding without coincident local seismic effects, which is discussed in Chapter 3.

The other sources of flooding considered at Hartlepool such as extreme rainfall and storm surges are meteorological in origin and are therefore independent of the seismic event. The frequency of a coincident beyond design basis earthquake and beyond design basis flood from these sources is extremely small. Hartlepools main protection against flooding from the sea is that the site is raised up above the maximum credible tide/tsunami height. In addition, the site is provided with sea defences. The sea defences are not seismically qualified, however it is judged unlikely that there would be significant structural failure of the sea defences such as to affect their functionality. The flooding risk Hartlepool is discussed in Chapter 3.

In Chapter 3 it is shown that very high sea levels are required before the site and sea defences would be overtopped. There are therefore large margins between the sea level expected in the design basis earthquake and the level at which significant site flooding could occur. It is therefore considered that there are no cliff edges just beyond the design basis in respect of tsunami as a consequence of seismic events.

Conclusion HRA 2.12: There is not a credible risk posed to UK plant from a beyond design basis earthquake and consequential beyond design basis flood.

2.2.4 Potential need to increase robustness of the plant against earthquakes

EDF Energy undertook mandatory evaluations in light of the events at the Fukushima Dai-ichi plant. The full scope and fleet wide results of these are presented in Chapter 0. The Licensee Board required a number of checks to be carried out in the days immediately following the events and these were reported through the first of these mandatory evaluations.

The information gathered by these self-assessments was also used to provide a formal company response to address the recommendations of INPO IER 11-1 and WANO SOER 2011-2 (which are the same). These are known as the within design basis and beyond design basis evaluations respectively.

Section 2.1.3.4 discusses the scope and findings of the specific seismic aspects for the within design basis. The findings of the seismic aspects for the beyond design basis evaluations are discussed below on a fleet wide basis; this is because the learning from each of the sites is judged to be applicable across the stations.

Scope

The beyond design basis evaluation was specified to ensure that documentation, training and plant associated with response to beyond design basis events were reviewed, along with the adequacy of the emergency response organisation. Due to the nature of the questions asked as part of the beyond design basis evaluation, this was primarily a paper-based exercise with workshops between station and central support engineers where appropriate. Equipment provided specifically for response to beyond design basis events was also physically inspected to ensure that the condition of the plant was as expected.

The fleet wide findings and suggestions for improvements beyond the design basis that may be considered are presented below as part of the 'robustness beyond the design basis'.

Summary of Findings from the beyond design basis evaluation

In general the fire-fighting systems are not claimed for the seismic safety case as there is not considered to be a risk of significant fire in a design basis earthquake. However in line with reviewing the potential for consequential fire, noted in section 2.1.2.3.4, feasibility to enhance the seismic capability of unqualified fire systems could be considered.

It was noted across the fleet that the pond structures are seismically qualified but that the normal pond cooling systems are not necessarily qualified owing to the relatively low decay heat of the fuel ponds. Manually deployed back-up systems are provided in case the normal systems fail which are seismically qualified. This is considered acceptable for the design basis earthquake, however, feasibility to enhance the robustness of pond cooling systems could be considered.

Standard safety case 'mission times' in the UK are 24 hours. With regard to the events in Japan it was noted that site access, although possible in that time frame, remained a significant logistical issue beyond this point. This issue is generic to all situations and is covered in Chapter 5.

Given the extreme nature of the events witnessed in Japan there was a general concern about the pressure and burden that would be placed on the operators during the recovery from an incident of such magnitude. This issue is generic to all situations and is covered in Chapter 6.

A number of potential areas for improvement were identified by the beyond design basis evaluation.

Conclusion HRA 2.13: In considering the robustness of the plant against beyond design basis earthquakes, several areas have been identified where enhancement could be considered.

Consideration HRA 2.4: Consideration should be given to the feasibility of enhancing the seismic capability of appropriate unqualified fire systems.

Consideration HRA 2.5: Consideration should be given to enhancing the robustness of pond cooling systems within the AGR fleet.

2.3 Summary

The seismic safety case is based on the provision of a line of protection with redundancy for the infrequent design basis earthquake, and two lines of diverse protection with redundancy in each line, for the frequent design basis earthquake. These cases are considered robust. Emergent issues regarding the validity of these cases are treated using established company processes and addressed on appropriate timescales.

The processes for ensuring robustness of the plant for seismic events are well developed and implemented and give appropriate consideration to the requirement for margins. They make appropriate use of international experience and standards both nuclear specific and discipline specific.

Furthermore they have been reviewed periodically in line with company process and regulatory expectations. The methodologies are internationally recognised and have been constructed with appropriate conservatisms, margins and sensitivity studies employed. Thus:

- the severity of the earthquake chosen for the design basis event is considered conservative;
- there is high confidence that the essential systems structures and components will remain functional in a design basis earthquake; and
- the essential systems structures and components are tolerant to more severe earthquakes.

In considering the robustness to beyond design basis earthquakes, several areas have been identified where enhancement could be considered. These will be taken forward for detailed review.

Chapter 3 – External Flooding

Hartlepool

3 External Flooding

In the Office for Nuclear Regulation's (ONR) interim report on the Japanese Earthquake and Tsunami Implications for the UK Nuclear Industry, the following is stated.

"The UK nuclear industry should initiate a review of flooding studies, including from tsunamis, in light of the Japanese experience, to confirm the design basis and margins for flooding at UK nuclear sites, and whether there is a need to improve further site-specific flood risk assessments as part of the periodic safety review programme, and for any new reactors. This should include sea-level protection."

In a number of places, this document refers to the need for ongoing development work. Some of this work had been previously identified and captured by normal company processes, whilst some is new work highlighted by the post-Fukushima review. In the latter group, there are some potential work packages referred to as 'Considerations'. These Considerations will be carefully reviewed following the completion of the Stress Test reports and an appropriate programme of work formulated.

Overview

In line with the statement quoted above from the ONR report, the Stress Test focuses on the external flooding hazard. Within EDF Energy Nuclear Generation, the external flooding hazard is defined as 'extreme rainfall, snowmelt, high tides, tsunamis, seismic seiches and gross failure of reservoirs external to the licensed site which directly or indirectly could result in the risk of a radiological release'. The internal flooding hazard, which considers flooding from sources within the licensed site, such as those stemming from failed pipework, tanks, etc. is considered by the station safety case but is beyond the scope of this report. Any further references to floods in this report concerns the external flooding hazard.

This report assesses the margins of the existing design basis, as well as the extant flood protection in place at Hartlepool Nuclear Power Plant. It demonstrates that:

- Sufficient margin exists between the maximum design basis flood (4.24m Above Ordinance Datum - AOD), tsunami (3 m), the general ground level of the site (4.70m AOD) and the physical sea defence barriers in place (>5.08 AOD);
- During extreme rainfall events it is demonstrated that essential function availability is maintained by the natural fall of the land towards the sea aided by site drainage systems;
- The information presented shows that the methodology used to determine the flood risk for Hartlepool has been constructed using independent expertise based on well regarded sources of information. The methodology has also been constructed with appropriate conservatisms, margins and sensitivity studies employed;
- The methodology for determining external flooding risk has been reviewed periodically in line with company process and regulatory expectations;
- Appropriate consideration has been given to the predicted impact of climate change on the risk of external flooding due to sea level rise and increasing wave heights. It has been demonstrated that appropriate margins will be maintained beyond the operating life of the station;
- Operating procedures and emergency activities identified for the management of actions in response to external flooding have been reviewed and their adequacy confirmed;
- For the purposes of beyond design basis risks management a number of physical plant modifications have been considered, primarily affording protection of external plant areas, and will prioritised based on the benefit to robustness of essential plant and the potential risk to plant during implementation/operation.

3.1 Design Basis

The following section identifies the external flooding events that are determined to pose a credible threat to the Hartlepool site, the protection provided against and the compliance route by way of which Hartlepool Power Station complies with the nuclear site licence for the design basis flood.

3.1.1 Flooding against with the plant is designed

International Atomic Energy Agency (IAEA) recommends that the "plant layout should be based on maintaining a 'dry site concept'. Where all items important to safety should be constructed above the level of the design basis flood, with account taken of wind wave effects and effects of the potential accumulation of ice and debris, where practicable, as a defence-in-depth measure against site flooding." (The concept of defence-in-depth is explained in Chapter 1). It is important to note that EDF Energy sites can accept a limited degree of flooding and provide means for draining off the flood water with the intention of providing suitable margins (see section 3.2.1).

An IAEA document on the Flood Hazard for Nuclear Power Plants on Coastal and River Sites has recently been issued. This supersedes safety guides that were issued in the 1980s. The current safety case has been reviewed against the guidance in this IAEA document and no outstanding issues have been identified. The following key points merit comment:

- Section 2.5(2) of the IAEA document requires the maximum probable tsunami hazard to be taken into account.
- Section 15 of the IAEA document recommends monitoring and warning equipment 'when flooding proves to be a significant hazard for a plant site.'

3.1.1.1 Characteristics of the Design Basis Flood

An External Flooding hazard considered by EDF Energy encompasses the following:

- Extreme rainfall and snowmelt.
- Overtopping of sea defences including high tidal conditions, tsunamis and seismic seiches.
- Gross failure of reservoirs and flooding from inland water courses.

The Design Basis Flood is the most severe external flood considered credible that is applicable to the nuclear reactor plant within once in 10,000 years (i.e. 10^{-4} p.a.).

The Design Basis Flood at 10^{-4} per annum is as follows:

- Rainfall for a 1 hour period is predicted to be 105mm;
- Extreme Still-Water Conditions 4.24m AOD (tidal plus surge);
- No significant risk from snowmelt;
- No significant risk from seismic seiches;
- No significant risk from reservoirs;
- No significant risk from flooding from inland water courses; and
- Tsunami and tide 4.7m AOD, frequency $<< 10^{-4}$ p.a.

3.1.1.2 Methodology used to evaluate the design basis flood

<u>Hartlepool geography</u>

Hartlepool is naturally protected from high tide and wave action by sand dunes to the north (Seaton Sands) and east (North Gare Sands) of the site. The dune crest level to the north (Seaton Sands) is typically 7.0m AOD and to the east (North Gare Sands) the dune crest level is typically over 7.4m AOD. The site ground level is 4.7m AOD and the perimeter flood wall is 5.08m AOD. To the south is the Seaton-on-Tees channel and this frontage has a concrete wave wall at a height of 5.69m AOD. Because of the position of this frontage, it is not possible for wave energy to reach it from the open sea. Locally generated waves can, however, be produced at elevated water levels as wind blows across Seal Sands.

See Figure 3-2 in section 3.1.2.2 for a map showing the station and surrounding area.

Rainfall

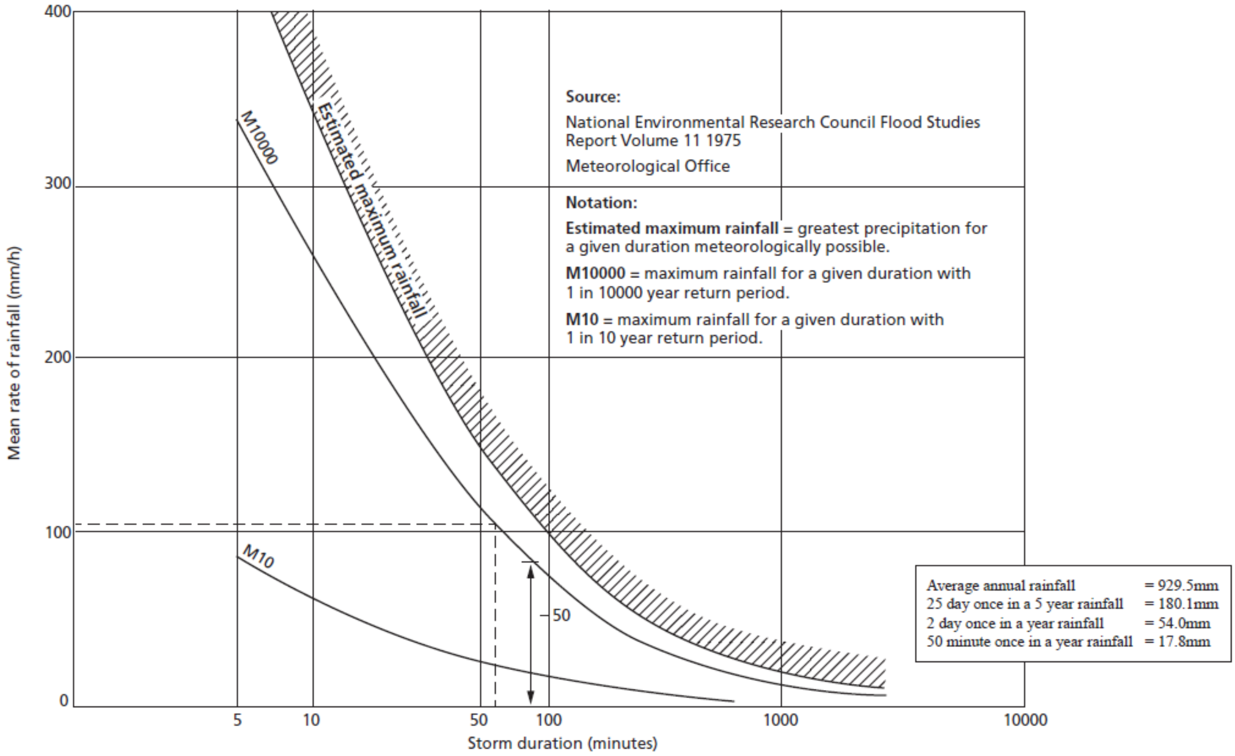

Figure 3-1: Rainfall data at Heysham 1 site.

For Hartlepool station the risk from wave overtopping, outflanking of sea defences and snowmelt is shown to be bounded by that from extreme rainstorms.

A periodic safety review stated that Hartlepool has 60% of the rainfall of Heysham 1. Figure 3-1 displays the estimated mean rate of rainfall for a given duration with a 10^{-4} p.a. return period at Heysham. It can be seen that there can be very large rates of rainfall for short periods, but that such high rates are not sustained. The mean rainfall for a 1-hour, 10,000 year return period rainstorm estimated in a Heysham 1 periodic safety review is 105mm and this estimate was conservatively used for the assessment at Hartlepool also. For any return period less than 10^{-4} p.a., an upper limit will be reached which will be less than the elevated height of sensitive safety related equipment (see section 3.1.2.1).

The site layout at Hartlepool provides a natural escape route for any excess water. Essential plant is protected from any leakage of rainwater into buildings by building thresholds, sump pumps and elevation of the plant above floor level. Any ingress into building basements would be via gaps in cable and pipe access points. This would be well within the capability of the sump pumps and so there is high confidence essential plant would not be affected.

Snowmelt

As Hartlepool is situated on the coast and has prevailing south-westerly winds it is unlikely to be affected by deep, lying snow. It is judged that the conditions of snowmelt combined with a heavy rainfall would be similar to an extreme rainfall event and there would be no threat to safety related equipment at Hartlepool.

Tidal Flooding

Studies commissioned by EDF Energy Nuclear Generation have resulted in the development of a robust methodology for assessing the flooding hazard at UK coastal locations. The methodology used at Hartlepool Power Station was developed by a specialist environmental hydraulics engineering firm for the assessment of the flooding hazard from extreme sea levels. Other standard statistical methods and a joint probability method were then used to produce the extremes of the individual and combined conditions at the station. The effect on the Station was then assessed. The scope of work including the following:

- Derivation of tidal conditions.
- Derivation of wave conditions.
- Derivation of method of transfer of sea conditions inland.
- Identification of protective features.
- A description of sensitivities of the input data.

Three frontage types were identified following visits to the site. These were Seaton Sands, North Gare Sands and Seal Sands. At all three locations overtopping was concluded to be the most likely mode of failure which requires to be tested with overtopping discharge selected as the structural variable. The variables identified as important when overtopping is the mode of failure are as follows:

- Wave height, period and direction
- Still water level (tidal and surge)
- Wind speed and direction

Data describing these variables has been obtained from the following sources:

- Offshore wave and wind conditions – UK Met Office Wave Model
- Measured water level data from North Shields – British Oceanographic Data Centre

Water level would not exceed the height of the site as the site is protected from wave action by Seaton Sand and North Gare Sands. Wave action in Seaton channel is limited and there is a 5.69m wall present. Some water could wash up against the wall of the pumphouse however the building is fitted with dam boards. There is limited potential for ingress however the expected ingress is within the sump pump capacity.

Tsunami

Tsunamis are long period waves that are produced from geological rather than meteorological events, principally submarine earthquakes, but also volcanic activity and submarine or shoreline landslides. A study by DEFRA in 2005 calculated a maximum tsunami generated wave height of up to 2m over a period of 1000 years. However a conservative value of 3m was used in a periodic safety review. The probability at Hartlepool of a 3m tsunami combined with a 1.7m tide (the combination of which is approximately the general level of the site, the critical level for flooding without the sea defences) was estimated to be approximately 10^{-8} per year.

Additionally, the DEFRA report (2005) concluded that the risk of a tsunami affecting the North Easterly coast of the United Kingdom is negligible because the only plausible driving force for such an event would be a Storegga type event which would only occur following an ice age. Comment is also made that local geology precludes the formation of a suitable landslip. The hazard of seiches (an oscillating wave in an enclosed body of water which may have a period from a few minutes to a few hours and is usually a result of seismic or atmospheric disturbances) is considered to be insignificant.

This is also concluded within the ONR report on the response to the Japanese Earthquake and Tsunami.

Climate Change Adaptation

EDF Energy has recently assessed the risks to its generation business posed by climate change and how EDF Energy intends to respond to these challenges, with regard to the Statutory Guidance produced by Government (DEFRA 2009) as required under section 63(3) of the Climate Change Act 2008.

The main flood related adaptation risks for the EDF Energy Nuclear Generation stations were storm surges. It was noted that the current case was secure, although the data needed to be kept under review.

Rainfall increases due to climate change

The most recent report in 2007 predicts that annually there will be a small increase in the mean rainfall in the wintertime (less than 15%) and a decrease in the mean rainfall in the summertime by the 2020s at Hartlepool. The rainfall for a 1-hour, 10,000 year return period rainstorm is predicted to increase by a maximum of 110% by the 2080s. Assuming a linear increase, the maximum increase by 2020 would be approximately 37% (i.e. to approximately 144mm). It is noted that the confidence in the predictions of how climate change will affect rainfall amounts diminishes as the return period increases.

The site layout at Hartlepool provides a natural escape route for any excess water as described above. As a result, climate change will not affect stations tolerance to extreme rainfall events.

Sea-level rise

A report from 2004, discussed the effects of climate change on UK nuclear sites and predictions show a global mean sea-level increase of 4-14cm from 2004 until 2020. This is confirmed in an Intergovernmental Panel on Climate Change study from 2001, which forecasts a mean global sea-level rise of a maximum of approximately 12cm by 2020.

A more recent report gives similar information to that presented in the other reports (but without consideration of the site specific flood defence and coastal geohazard implications) for EDF Energy nuclear power station sites. The predicted maximum global average sea rise by the 2020s, assuming a high emission scenario, is 14cm. A report also estimated local effective mean sea-level rise by the 2080s by combining the predicted isostatic changes (vertical land movements) with the estimates of global mean sea-level and then adding a further error margin due to possible regional effects.

The maximum local sea-level rise at Hartlepool is predicted to be 104cm by the 2080s. Using the high emission scenario and assuming a linear increase in sea-level from 1990, in 2020 the sea-level will have increased by approximately 35cm. It should be noted that the lower estimate of local effective mean sea-level rise by the 2080s is only 5cm. This large range of values is an indication of the uncertainty in prediction of regional sea-level rise.

The estimates made in a periodic safety review of the maximum sea-level rise are 15cm over a 30-year period at Hartlepool. These estimates are clearly below the maximum predictions presented in the latest reports. However, even if these predictions were used, flooding would not exceed the level of the site (i.e. 4.24m+0.35m < 4.70m). Therefore, all essential plant would not be affected.

Wave height increase

A periodic safety review reports for Hartlepool showed that storm surges and wave overtopping of sea defences would not affect essential plant. According to Climate Change 2001, wave height changes at the coast may occur with climate change and in the North Atlantic, a wave height increase has been observed but the cause is poorly understood. The 50-year return period surge height increases at Hartlepool due to climate change to 2080 are zero cm in the low greenhouse gases emission scenario and 60cm in the high emission scenario. Using the high emission scenario and assuming a linear increase in surge height change, in 2020 surge height will have increased by approximately 20cm at Hartlepool. This is lower than the maximum increase expected in sea-level rise due to climate change.

Assuming the maximum local sea-level rise and the maximum 50-year return period surge height increase, the total maximum increase at Hartlepool is 55cm. The perimeter wall is at 5.08m AOD.

Due to the small probability of overtopping at Hartlepool and because the previously calculated overtopping rates are well within the station’s limits, a potential small increase in overtopping from storm surges or wave height increase due to climate change will not affect the safety case.

3.1.1.3 Conclusion on the adequacy of protection against external flooding

The information presented in the preceding sections shows that the methodology used to calculate the design basis flood for Hartlepool has been constructed using independent expertise based on well regarded sources of information. Furthermore, it has been reviewed periodically in line with the company process and regulatory expectations. The methodology has been constructed with appropriate conservatisms, margins and sensitivity studies.

However, as a result of the advancement of scientific understanding of climate change and as a prudent operator, EDF Energy Nuclear Generation has initiated further flooding studies. This is particularly important because the external flooding hazard presents the possibility of 'cliff-edge' effects; for example the overtopping of bunds could lead to significant damage at the point of overtopping with no effect until that point.It should also be noted that as the current methodologies for calculating the design basis flood vary across the fleet, the new flooding studies will allow inter comparison and provide enhanced consistency across the fleet.

Conclusion HRA 3.1: The methodology for calculating the design basis flood is robust, has appropriate conservatisms, margins and has been periodically reviewed.

Conclusion HRA 3.2: In line with Recommendation 10 of the ONR interim report, the design basis flood at Hartlepool has been confirmed, however further studies accounting for climate change have been initiated to reconfirm the design basis flood.

Consideration HRA 3.1: In line with Recommendation 10 of the Weightman report, flooding studies have been initiated for the UK fleet. This study re-evaluates the design basis flooding scenarios using the most recent data and taking account of climate change, until the period of 2035.

3.1.2 Provisions to protect the plant against the design basis flood

3.1.2.1 Identification of systems, structures and components that are required for achieving and maintaining safe shutdown state and are most endangered when flood is increasing.

The systems identified below are those required for achieving and maintaining safe shutdown and cooldown that would be most endangered by flooding were there no flood protection engineered on the site or were there to be a significantly beyond design basis flood at the site. Section 3.1.2.2 outlines the flood defences on the site designed to protect this equipment.

Essential Safety Functions

In order to achieve a safe shutdown state post 10^{-4} per year external flooding event, the following essential functions are required:

- Trip
- Shutdown.
- Post-Trip Cooling.
- Essential Monitoring

Table 3.1: Claimable Lines of Protection for Infrequent External Flood.

Essential Function		Equipment Qualified Against Infrequent Event
Trip		Guardline Equipment
Shutdown		Main Shutdown System
Gas Circulator Run On Protection		Main Motor common breakers
Post Trip Cooling	Gas Circulation	Gas Circulators/Natural Circulation
	Boiler Venting	Boiler Vent Routes
	Boiler Feed	Boiler feed pumps
	Feed Water Source	Feed water tanks
Essential Monitoring		Alternative monitoring location and control room
Heat Sink		Cooling Water
Electrics		On-site Generators

The infrequent rainfall case is the bounding case. As external flooding events are often associated with high winds, grid supply is assumed to be lost as a result of this fault. Table 3.1 shows the claimed Lines of Protection.

Trip

Trip is not required unless there is a threat to safety related plant as a result of flooding. The guardlines are not at risk from external flooding due to their location.

Shutdown System

The main control rod shutdown system is claimed for bottom line events. There is no flooding risk to this system. The protection of the secondary shutdown system is provided by the location of plant on plinths and therefore a second line of shutdown is available.

Post Trip Cooling

The essential cooling water system using seawater is not judged to fail, however a back-up cooling system is available. Should grid supplies fail on-site generators supplies to essential systems would ensure continued availability. The back-up cooling systems are also independent of grid connection due to the supply from separate diesel pumps. Manual action may be taken to initiate these pumps and configure them to provide post-trip cooling in the absences of any electrical supplies.

Gas Circulation

Equipment within the reactor buildings has been shown to be unaffected by an infrequent external flooding event. Gas circulator motors will remain available by virtue of their location. Natural circulation should also be available.

Boiler

The emergency boiler feed pumps are claimed as the post-trip feed system.

The essential safety items that are part of the emergency boiler feed are located well above the turbine hall basement floor and are not at risk from flooding.

Pressure Vessel Integrity

The pressure vessel cooling water system ensures appropriate vessel integrity whilst the reactor is pressurised. Back up cooling is available using diesel driven pumps to ensure continuity.

Electrical Supplies

Normal electrical supplies are derived from grid connection. On loss of grid on-site generator sets are available. Each generator is housed in a walled enclosure within a building, with an air intake shaft at one end of the enclosure and a local control room containing the switchgear and batteries at the other. The building is divided in two by a bund. Sump pumps are installed to prevent water accumulating in ducts and pits.

Essential Monitoring

The central control room would not be susceptible to even very extreme flooding due to its location. The assessment has shown that infrequent rainfall events will not pose a threat to the main buildings. An alternative indication centre is provided and is designed to withstand external flooding. This alternative indication centre is specifically designed to cope with any foreseeable flood as it is built on a plinth greater than 1m, above general site level.

Shutdown Reactors

As outlined in the section above, in the event of an infrequent flood, it is expected that all required systems will remain available other than the grid based supplies. If the reactor is depressurised forced gas circulation will be necessary and remains available using the gas circulator motors.

Fuel Route

There are no direct flooding concerns for fuel route plant as the infrequent external flood does not enter the main nuclear island buildings to a level where the fuel route plant is located. The only exception is the new fuel store, where the flood would not threaten criticality safety.

Conclusion HRA 3.3: The lines of protection required for achieving and maintaining a safe shutdown state and cooling following a design basis flooding event are suitable and sufficient.

3.1.2.2 Main design and construction provisions to prevent flood impact to the plant.

Sea Defence

The site for Hartlepool station is naturally protected from high tide and wave action by dunes to the north and east of the site, at 7m AOD and 7.4m AOD respectively. The frontage with the Seaton on Tees channel to the south of the site has a concrete wave wall of 5.69m AOD but because of its position wave energy cannot reach it from the open sea. Hartlepool also has a secondary inner perimeter wall at 5.08m AOD. The general site finished ground and road level is 4.7m AOD. In the case of an infrequent 10^{-4} p.a. flooding event from the sea, there is demonstrated to be sufficient margin available.

Topography & drainage

The site drainage is shown in Figure 3-2. The surface water drainage system accepts surface water from all buildings, roads and hard standings on the Station, plus discharges from other sources (e.g. generator transformer oil cooler, pumped drainage discharges, discharges from bunded areas). Water from the above sources, flows by gravity to the open drainage channel. Under normal flow conditions this water flows directly through to the tidal reservation and thence to the Seaton-on-Tees Channel. Excess flow can however be pumped from the site drainage pumping station into an outfall in the Seaton-on-Tees Channel. The site drainage system is fitted with a tidal flap where it discharges into the tidal reservation located outside the wave wall. The pumping station is situated inside the wall, but will not operate in the event of an extreme high tide. (It is noted that the pumps are not claimed in the safety case, they are only a mitigating system.).

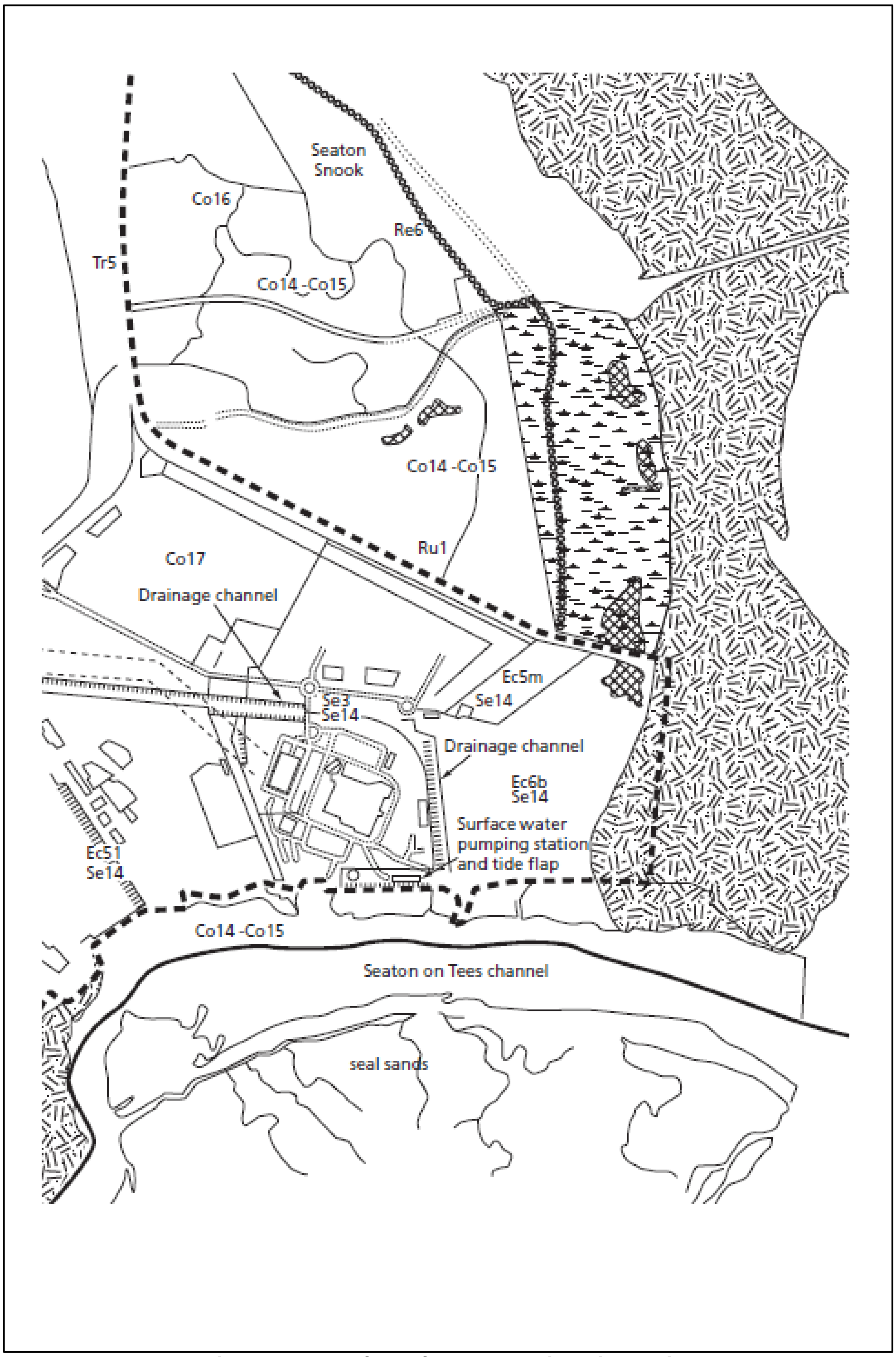

Figure 3-2: Hartlepool Power Station Site Drainage.

Across the site the surface water run-off from buildings and roads is discharged via the drainage channel along the eastern boundary of the site. The surface water is discharged into the Tees channel. This reduces the effects of flooding from storm water and other local flooding hazard sources and is judged to be adequate to protected against infrequent external flooding from the landward side.

Conclusion HRA 3.4: The flood defence provisions for Hartlepool are suitable and robust in the event of a design basis external flood.

3.1.2.3 Main operating provisions to prevent flood impact to the plant.

<u>Operating instructions</u>

The operating instructions specify actions to be taken following warning of external flooding or heavy rainfall.

Following a flooding threat from high tide/wind conditions, building doors and windows are closed and dam boards are deployed. The operator monitors the situation and ensures the operation of essential plant. Flood defences are inspected. Portable pumps are set up if required. Buildings are also checked for water leakage. Similar actions are taken in response to warning of extreme rainfall or rapid snow melt.

<u>Summary</u>

It can be seen from the information presented that the claims made on the operator actions are not onerous in the event of a severe flood. Flood protection is deployed to protect vulnerable equipment. Local operators are expected to inspect the status of the cooling water equipment. If the status of the cooling water plant is such that the operation of the reactor unit is no longer possible then the reactor will be manually shutdown before safety systems are challenged.

Conclusion HRA 3.5: The claims made on the operator for flooding events are not onerous given the level of design basis flood and it is considered that the reliance on these claims continues to be appropriate.

3.1.2.4 Situation outside the plant, including preventing or delaying access of personnel and equipment to the site.

The safety case states that the safety systems are able to operate for a period of 24 hours solely from station resources and therefore does not require access from external personnel to the site. Consideration for the extension of the 24 h mission time is presented within Chapter 5.

A review of site access following external flooding has been carried out. During the infrequent high tide seawater flooding event, large areas surrounding the Hartlepool site could possibly become flooded, including parts of the main site access roads to the extent that the site would be completely surrounded. However, tide related overtopping and out flanking events are episodic in nature and will only be at a significant level for ~2-3 hours around the time of high tide. Following this, flood levels will recede via direct return to the sea and ground seepage. It is most unlikely that by the time of the next high tide, the combination of events that produced the earlier flooding (e.g. high tide levels accentuated by extreme winds) will still be present to cause a repeat event. Certainly after the 24 hour mission period circumstances should be such that access to site will be available for essential supplies.

External to the site, the Local Resilience Forums are the local authority body in the UK with responsibility for providing emergency response in the community. The review of emergency arrangements is in Chapter 6. This assessment aligns with that within EDF Energy and it is expected that there could be difficulty regarding access to and from site for a period of time, although it should be noted that the magnitude of this impact would be very much less than that seen in Japan. Outside the site, there are plans regarding emergencies for the local area. A community risk register has been compiled of potentially disruptive events (including external flooding) that responder agencies (including emergency agencies such as the police, fire services etc.) have considered in order to prepare for the emergencies and return the area to a state of normality.

Work is being undertaken by flood modelling specialists to assess the effect of external flooding on the access to plant in very extreme flooding scenarios and this work will be used to inform the development of any emergency back-up equipment model for mitigation in accident scenarios.

Conclusion HRA 3.6: Access to the site and deployment of personnel has been considered as part of the emergency response and it is considered this continues to be appropriate.

3.1.3 Plant compliance with its current licensing basis

3.1.3.1 Licencee's processes to ensure that plant systems, structures and components that are needed for achieving and maintaining the safe shutdown state, as well as systems and structures designed for flood protection remain in faultless condition.

All modifications are implemented using an engineering change process which requires that all modification proposals check whether plant affected by the proposal is qualified against external flooding or whether the modification could have a deleterious effect on equipment qualified against the flooding hazard. The procedure therefore reduces the risk that the flooding safety case is compromised by changes to the plant and structures.

Inspection and maintenance are important to ensure that the adequacy of the flooding safety case is maintained. The nuclear safety related inspections are listed on the maintenance schedules. The maintenance schedule at Hartlepool covers the maintenance of the sea defences and site flood protection.

A survey of the sea defence wall at Hartlepool is carried out every 60 weeks. Sump pumps are routinely operated and dam boards are fitted and inspected every 60 weeks. In addition, drainage pipework and gullies are routinely inspected every 5 years. Monitoring of the sand dunes is also carried out every 60 weeks.

3.1.3.2 Licencee's processes to ensure that mobile equipment and supplies that are planned for use in connection with flooding are in continuous preparedness to be used.

There is no mobile equipment claimed in the safety case for design basis flooding events.

3.1.3.3 Potential deviations from licensing basis and actions to address those deviations.

There are mechanisms for identifying any areas of concern or anomalies within the safety case. These may take the form of a commitment from the production of a safety case, justifications for continued operation or periodic safety review commitments. Where areas of concern are identified they are captured and tracked using the company's corrective action and work planning processes.

There are currently no outstanding issues relevant to external flooding.

Conclusion HRA 3.7: There are no outstanding issues identified related to the external flooding safety case.

3.1.3.4 Specific compliance checks already initiated by the licensee following the Fukushima-Daiichi Nuclear Power Plant Accident

Review

In light of the events at the Fukushima Dai-ichi plant, as responsible operators EDF Energy have carried out two separate reviews at each of the sites. The information gathered by these self-assessments was used to provide a formal company response to address the recommendations of INPO IER 11-1 and WANO SOER 2011-2 (which are the same). These are known as the within design basis and beyond design basis evaluations respectively. The scope and findings of the evaluations are presented Chapter 0.

Scope

The within design basis evaluation was specified to ensure that systems essential to fuel cooling in an emergency situation in a within design basis event including seismic and flooding scenarios were correctly configured, lined up and in a suitable condition to be declared available/operable.

Stations were asked to capture any issues for further action through condition reports and work requests. A number of commitments were made as a result of the within design basis evaluation.

Summary of site specific findings

All tasks were completed with no specific reference to flooding areas for improvement; however the following general recommendations were made:

- The review has not identified any threats to nuclear safety;
- The review has confirmed that the stations processes are adequate to ensure operability and availability of within design basis cooling plant. This is the fundamental function of the stations management systems.

Conclusion HRA 3.8: The reviews undertaken and the actions identified therein, have confirmed that Hartlepool is compliant with the current licensing basis.

3.2 Evaluation of safety margins

An estimation of the safety margins against flooding is presented below outlining that Hartlepool Power Station has sufficient margin against a design basis flood. The safety case for external flooding is based on demonstrating that the methodology is suitably pessimistic while also demonstrating adequate physical margins between the main safety related plant and the design basis flood. There is also shown to be adequate defence-in-depth.

3.2.1 Estimation of safety margin against flooding.

Physical Margins for the Extreme Rainfall Event

The safety case is predicated on the demonstration that all essential safety plant is located above a pessimistically calculated flood height as determined from the infrequent rainfall event (105mm in 1 hour). The rainfall event is pessimistic as it is based on rainfall data from Heysham 1. Hartlepool receives 60% of the rainfall of Heysham. There is significant margin between assumed level of rainfall and what the plant can withstand. Within design basis, it is not credible that a significant amount of water would enter station buildings during an extreme rainfall event. However if this were to occur in a beyond design basis flood, the essential safety equipment would not be affected as it has been placed on raised plinths.

Loss of grid is assumed during an extreme rainfall event. Therefore on-site generators would be required. The cooling water pumps would be threatened if the turbine hall were to be flooded. This would necessitate the use of the back-up cooling system. The back-up cooling system engines and pumps are on a plinth and would require a flood of greater than 300mm to be threatened. There is therefore significant margin for a beyond design basis event, and there are drainage routes for surface water to be discharge back into the Tees channel. It is also important to state that an extreme rainfall approximately 2-3 times that assumed is highly unlikely.

Physical Margins for the Sea Overtopping

Within design basis, there is judged to be sufficient margin between the maximum sea height and the height of the station and sea defences. In a beyond design basis flood if the sea did overtop, the cooling water pumps and generators would be vulnerable (although this would require a surface flood at around 200mm). If the generators were threatened, then forced gas circulation would not operate requiring the use of natural circulation. The back-up cooling system would be available with their independent diesel pumps to provide water to the boilers and pressure vessel.

Conclusion HRA 3.9: The review has shown that there are suitable and sufficient margins present within the methodology and plant at Hartlepool for compliance with the current safety case.

3.2.2 Potential need to increase robustness of the plant against flooding.

EDF Energy undertook mandatory evaluations in light of the events at the Fukushima Daiichi plant. The full scope and fleet wide results of these are presented in Chapter 0. The Licensee Board required a number of checks to be carried out in the days immediately following the events and these were reported through the first of these mandatory evaluations.

The information gathered by these self-assessments was also used to provide a formal company response to address the recommendations of INPO IER 11-1 and WANO SOER 2011-2 (which are the same). These are known as within design basis and beyond design basis evaluations respectively.

Section 3.1.3.4 discusses the scope and findings of the specific flooding aspects for Hartlepool within the design basis evaluation. The findings of the flooding aspects for the beyond design basis evaluation are discussed below on a fleet wide basis; this is because the learning from each of the sites is judged to be applicable across the stations.

Scope

The beyond design basis evaluation was specified to ensure that documentation, training and plant associated with response to beyond design basis events were reviewed, along with the adequacy of the emergency response organisation. Due to the nature of the questions asked as part of the beyond design basis evaluation, this was primarily a paper-based exercise with workshops between station and central support engineers where appropriate. Equipment provided specifically for response to beyond design basis events was also physically inspected to ensure that the condition of the plant was as expected.

The fleet wide findings and suggestions for improvements beyond the design basis that may be considered are presented below as part of the 'robustness beyond the design basis'.

Summary of Findings

In general all stations have some safety related plant which is either at ground level or in a basement. This plant has adequate flood protection and physical margins for a design basis event.

The sea barriers provide adequate protection from floods expected at site and even in the event of beyond design basis overtopping of the barriers the impact at some sites would be manageable.

There is local to plant protection or margin that would defend against beyond design basis flooding but clearly this could be subject to a cliff-edge effect if for example a local bund overtopped.

Dewatering capability is generally available but is in some cases reliant on electrical supplies, which makes it more vulnerable in an extreme beyond design basis scenario.

Standard safety case 'mission times' in the UK are 24 hours. With regard to the events in Japan it was noted that site access, although possible in that time frame, remained a significant logistical issue beyond this point.

Given the extreme nature of the events witnessed in Japan there was a general concern about the pressure and burden that would be placed on the operators during the recovery from an incident of such magnitude.

Conclusion HRA 3.10: The robustness of the plant against design basis floods is considered to be appropriate; however in considering the robustness to beyond design basis floods, several areas have been identified where enhancement could be considered.

Consideration HRA 3.2: Consideration should be given to the feasibility of additional temporary or permanent flood protection for essential safety functions.

Consideration HRA 3.3: Consideration should be given to enhancing the robustness of dewatering capability, in particular focussing on independence from other systems.

3.3 Summary

- Sufficient margin exists between the maximum design basis flood (4.24m Above Ordinance Datum - AOD), tsunami (3 m), the general ground level of the site (4.70m AOD) and the physical sea defence barriers in place (>5.08 AOD);

- During extreme rainfall events it is demonstrated that essential function availability is maintained by the natural fall of the land towards the sea aided by site drainage systems;
- The information presented shows that the methodology used to determine the flood risk for Hartlepool has been constructed using independent expertise based on well regarded sources of information. The methodology has also been constructed with appropriate conservatisms, margins and sensitivity studies employed;
- The methodology for determining external flooding risk has been reviewed periodically in line with company process and regulatory expectations;
- Appropriate consideration has been given to the predicted impact of climate change on the risk of external flooding due to sea level rise and increasing wave heights. It has been demonstrated that appropriate margins will be maintained beyond the operating life of the station;
- Operating procedures and emergency activities identified for the management of actions in response to external flooding have been reviewed and their adequacy confirmed;
- For the purposes of beyond design basis risks management a number of physical plant modifications have been considered, primarily affording protection of external plant areas, and will prioritised based on the benefit to robustness of essential plant and the potential risk to plant during implementation/operation.

Chapter 4 – Extreme Weather

Hartlepool

4 Extreme Weather

In the Office for Nuclear Regulation Interim Report into the Japanese Earthquake and Tsunami, Recommendation 13 states that "The UK nuclear industry should review the plant and site layouts of existing plants and any proposed new designs to ensure that safety systems and their essential supplies and controls have adequate robustness against severe flooding and other extreme external events." Recommendation 16 states that "When considering the recommendations in this report the UK nuclear industry should consider them in the light of all extreme hazards, particularly for plant layout and design of safety-related plant."

EDF Energy considers a range of hazards, some of which are initiated or come about as a result of events on the site (internal hazards) and others that arise off-site or which relate to conditions which envelop the site (external hazards). This chapter considers those external hazards that are related to meteorological events other than external flooding, which is addressed in Chapter 3.

For each of the hazards addressed by the chapter, consideration has been given to;

- The existing design basis against which the hazard safety case has been made (though it should be noted that formal safety cases do not yet exist for all of these hazards),
- The margins inherent in the cases and,
- The potential for improvements in the robustness of defences against these hazards.

These topics are considered in Sections 4.1, 4.2.1 and 4.2.2 respectively.

The following section identifies the extreme weather events that have been identified as posing a potential threat to the Hartlepool site (including combinations of events), how the challenge has been defined and a review of the continued validity of the challenge definition.

EDF Energy Nuclear Generation has identified the following as external weather hazards for the advanced gas-cooled reactor fleet.

- External Flooding (including rainfall)
- Extreme Wind
- Extreme Ambient Temperatures (Including both seawater and air temperatures)
- Lightning
- Drought

In the EU Stress Test Reports external flooding hazards, as a result of extreme weather conditions, are covered in Chapter 3. This Chapter focuses on the remainder of the identified extreme weather conditions however external flooding is considered in this chapter when combinations of hazards are considered.

In accordance with the Nuclear Safety Principles the magnitude of the External Hazard should correspond to a severity consistent with a return frequency of 1 in 10,000 per year at the site.

As well as looking at individual hazards, it is necessary also to consider hazard combinations. These can arise in different ways, e.g., as independent and coincidental events, events where one hazard arises as a consequence of another, or two or more hazards arising as a result of some underlying cause such as a severe storm. Of these, independently occurring coincidental hazards are normally discounted on low frequency grounds.

The definitions of these external hazards relating to extreme weather conditions are given below.

<u>Overview</u>

<u>Extreme Wind</u>

Extreme winds which directly or indirectly could result in the risk of a radiological release.

This hazard includes consideration of tornadoes, wind-induced collapse of structures and wind-borne missiles, though for some of the stations the main consideration of wind-borne missiles is addressed within the overall assessment of the missiles hazards (which is outside the scope of this review).

- The design basis for extreme wind is based on adherence to standards and codes. The standards are continually being updated and there is a suitable process within EDF Energy to ensure continuing compliance.
- Work is currently being undertaken to produce a tornado safety case.
- There is sufficient equipment qualified against an infrequent extreme wind to ensure the plant can be safely shut down and cooled.
- The station operating instructions contain actions to be taken upon receiving warnings of extreme wind, to reduce the impact of the wind on the plant.
- The safety margin against extreme wind has not been quantified. It has been judged that no cliff edge effects will be seen if extreme winds slightly beyond the design basis are experienced.

Extreme Ambient Temperatures

Extreme Ambient (high or low) Temperatures which directly or indirectly could result in the risk of a radiological release.

As well as the extreme atmospheric temperatures, this also includes snow loading to buildings and structures and snow blockage of air intakes and the effects of ice. In addition, extreme seawater temperatures are considered under this hazard.

- Within the current design basis at least one line of protection is demonstrated to remain available.
- Technical specifications ensure that the plant is shut down and cooled down if temperatures look like they may fall outside the assumed range.
- The current design basis for extreme ambient temperatures has not been robustly defined. A consideration has been raised by this report to redefine the design basis using modern techniques and data.

Lightning

A lightning strike or strikes which directly or indirectly could result in the risk of a radiological release.

As noted above, EDF considers other external and internal hazards that could affect the safety of its stations apart from the meteorologically related external hazards. These include the Electromagnetic Interference hazard and the Lightning Electro-Magnetic Pulse is addressed as part of that Electro-Magnetic Interference / Radio Frequency Interference hazard and are not considered here.

- Protection against lightning is provided by adherence to relevant codes and standards
- Work is currently being undertaken to produce a formal lightning safety case.

Drought

A lack of water as a result of prolonged periods of hot or cold weather or as a result of lack of rainfall which directly or indirectly could result in the risk of a radiological release.

This hazard includes consideration of loss of cooling water and water stocks for post-trip cooling, the impact of drought on the foundations of the site and of the civil structures and the effect of the hazard on the main electrical earthing system.

- Drought is a slow process which would allow plant to be shutdown before safety would be challenged.
- Work is currently being undertaken to produce a formal drought safety case.

Combinations of hazards

- A systematic consideration of all the possible combinations of hazards has been undertaken, and are not expected to impact adversely on nuclear safety.

Section 4.1 considers extreme wind, extreme ambient temperature, lightning and drought. As this section makes clear, discussions on lightning and drought are limited as they do not have a formal design basis. Therefore, Sections 4.2.1 and 4.2.2 are predominantly focused on the extreme wind and extreme ambient temperatures hazards.

4.1 Design Basis

The design basis which has been adopted at Hartlepool for these hazards is discussed in what follows.

Extreme Wind

The hazard presented to the station from normal wind loading was considered and designed for during the design stage of the station. The original building design threshold was a wind loading severity commensurate with a wind with a probability of exceedance of 0.02 per year. The extreme wind safety case required adequate reactor protection against an extreme straight line wind with a probability of exceedance of 10^{-4} p.a. and a less onerous, more frequent second line event. Modifications have been made to plant where necessary to ensure that these requirements are met.

Tornados were not originally considered under the design basis and will be discussed in section 4.1.1 below.

Extreme Ambient Temperatures

Ambient air temperature records were not available for Hartlepool for the original design basis calculations, hence data was used from the weather station at Tynemouth, which is on the coast but is further north. This data has been gathered since 1941. The recorded data for ambient air temperatures has been subjected to an extreme value analysis to obtain the values tabulated.

The design basis for the extreme ambient temperatures event is presented below.

Table 4.1:- Extreme Ambient Temperature Design Basis

Event	Minimum Temperature	Maximum Temperature
Frequent	-13 °C	+30 °C
Infrequent	-18 °C	+34 °C
Extreme Sea Temperature	-2 °C	+25 °C

Lightning

Provisions were made in the original design of the Station to protect against lightning however this was not formally considered within the Hazards Safety Case at that stage. Despite this the lightning protection has been assessed in the Station Stage III Safety Reports to ensure adequacy of the protection.

The original code used had been British Standard Code of Practice 326: 1965. This has subsequently been replaced by British Standard 6651 which was first issued in 1985 and updated in 1990 and 1992. The 1985 version of the British Standard 6651 made it clear that there was no requirement for uprating in existing structures. A zone of protection concept had been used originally and this was retained in these code changes although in the updates this was based on a rolling sphere method of assessment.

The IAEA guidance for evaluation of meteorological events points out that data on parameters relevant to lightning is not routinely recorded and it is therefore not possible to derive any corresponding extreme values. Consequently the approach adopted for this hazard is based mainly on demonstrating the adequacy of the lightning protection system by confirming conformance with appropriate codes and standards.

Lightning has not been formally considered as a hazard and this led to a shortfall being raised in a periodic safety review which required that a formal hazards safety case be produced for lightning.

Conclusion HRA 4.1: The approach adopted for lightning is based mainly on demonstrating the adequacy of the lightning protection system by demonstrating conformance with appropriate codes and standards. A formal safety case is currently being developed.

Conclusion HRA 4.2: The IAEA guidance for evaluation of meteorological events points out that data on parameters relevant to lightning is not routinely recorded and it is therefore not possible to derive any corresponding extreme values. Consequently the approach adopted for this hazard is based mainly on demonstrating the adequacy of the lightning protection system by demonstrating conformance with appropriate codes and standards. This is considered to remain appropriate.

Drought

There was no formal consideration of the effects of drought on Station operation within the original safety case apart from consideration of the effects of settlement on civil structure foundations.

A drought affecting the stations water supplies is very unlikely to happen as the North East is a water rich area able to accommodate extended dry periods without affecting water availability. If the region was going to run out of water the station would be shutdown long before townswater supplies would be lost. In a drought electricity supplies would be important. If the station needed cooling water it would get priority over other users. It can therefore be seen that the complete loss of water to the station due to a drought is extremely unlikely.

More than any other hazard, drought will be characterised as developing over a long period of time. One consequence of this is that mitigation can be put in place prior to the event.

A drought hazard may affect the water levels held within the reservoirs and water main supply. In Station terms drought is the unavailability of water supplies resulting in inability to stock up on water supplies.

It is considered as highly unlikely that extreme drought could prevent the Station from meeting its essential safety functions. However, even if local water authority make-up supplies were lost, seawater could be used to cool the reactors.

Any effects of drought on soil conditions or building foundations are considered to be very gradual, with time being available to allow a safe plant state to be achieved before significant loss of essential systems (including redundant and diverse systems) occurs. Although prolonged drought could potentially cause significant movement in the soil/ subsoil of a site due to drying of soils or reduction in groundwater levels, especially those containing clay, this is not thought to be a significant issue at Hartlepool. At Hartlepool, the ground beneath consists of a deep alluvial layer overlaying sandstone and deeper limestone strata. The site has been levelled and includes made-up ground. These conditions have necessitated piled foundations for the reactor and turbine hall buildings. Based on the foundations of the stations it is judged that prolonged periods of dry weather would not affect the sites or the foundations of any buildings important to nuclear safety. However a number of buried pipework or trenched services are identified as being at risk of ground settlement as a consequence of a period of extended drought. Each of these has a critical interface with a building on the Hartlepool site. A regular survey of various levelling stations positioned at key location associated with the services that have been deemed to be susceptible to drought induced settlement of the ground has been introduced.

A periodic safety review identified that the safety justification for drought should be developed and formally included in the station safety case. This is being progressed as part of normal business.

Owing to the long timescales that will be available to respond to this hazard and its relatively low level of threat to safe operation, this fault is not considered in any further detail in this stress test.

Conclusion HRA 4.3: Advance warning of the discontinuation of off-site water supplies would be available in the event of a prolonged drought. This would provide sufficient time for the operators to take appropriate actions.

4.1.1 Reassessment of weather conditions used as design basis

4.1.1.1 Verification of weather conditions that were used as design basis for various plant systems, structures and components: maximum temperature, minimum temperature, various type of storms, heavy rainfall, high winds etc.

Consideration is given in this section to the continuing validity of the design basis definitions. The hazards are discussed individually in the sections below.

4.1.1.1.1 Extreme Wind

There is an explicit safety case for the extreme winds hazard for Hartlepool. Although the consequences of any hazard, including other consequential hazards, are normally dealt with as part of the case for the initial hazard, the effects of wind blown missiles has been dealt with as part of the overall missiles hazard where it has been shown to be bounded by more severe missiles form other sources.

An assessment of the capability of the structures and exposed plant required to withstand wind loading was undertaken in an early periodic safety review to support the qualification of the identified lines of reactor protection. This assessment used wind loading calculated from British Standard 6399-2: 1995&1997.

Note that British Standard 6399-2:1997 code has been replaced by British Standard 6399-2:1997 (2002). This is presently being addressed as part of company business.

The bottom line of protection was assessed against an infrequent wind with a 10,000 year return period.

A recent periodic safety review assessed the risk from tornadoes and concluded that the risk of tornado damage is adequately covered by the existing extreme wind safety case which is based on 10^{-4} p.a. straight-line wind speeds.

A study of tornadoes in Britain, produced for the Nuclear Installations Inspectorate, divides the UK into two areas to distinguish differing levels of tornado incidence, termed 'Outer Britain' and 'Southern Britain'. In the region of 'Outer Britain' in which Hartlepool is situated, the tornado hazard is less onerous than that associated with the straight-line wind. Therefore, the risk of tornado damage at the Hartlepool site, including the effects of pressure drops and windborne missiles, is considered to be adequately covered by the existing safety case which is based on the infrequent event straight-line wind speed.

However, the findings of more recent studies indicate that the original study may have underestimated the tornado hazard in some regions of the country.

Conclusion HRA 4.4: Tornadoes have been assessed as part of a periodic safety review and no significant shortfalls have arisen.

Consideration HRA: 4.1: Consideration should be given to reassessing the tornado hazard in light of recent studies.

Climate change means that local weather patterns and the average conditions associated with them may change over time. Future prediction of change to wind characteristics is relevant when considering the extreme wind hazard. Further work commissioned by EDF Energy in 2007 predicts a clear increase in the average winter wind speed and a decrease in the average summer wind speed. This pattern is in agreement with the trend for all sites excluding Dungeness B. By 2080, the average winter wind speed and the extreme winter wind speeds for both Hartlepool and Heysham 1 are predicted to have increased by around 4%. These changes are small in the time period under consideration and although changes in wind speed are predicted, the predicted changes are sufficiently small not to have a significant effect on the wind loading hazard and therefore it is judged that nuclear safety is not at any further risk from extreme winds due to climate change.

Conclusion HRA 4.5: For extreme wind loadings there is a current design basis which has been reviewed as part of the periodic review process and found to be adequate.

4.1.1.1.2 Extreme Ambient Temperatures

There is an explicit safety case for extreme ambient temperatures for Hartlepool.

The purpose of previous periodic safety review was to confirm the adequacy of the case up to the next periodic safety review. As part of the scope for the review, the nature of the hazard was not considered to have changed since the initial review however factors like global climate change may have affected the severity of the hazard.

A report commissioned by EDF Energy gives an overview of the climate change including changes in the local weather patterns and the average conditions associated with them for the next 100 years and for different emissions scenarios. It predicted that seasonal average temperatures will increase significantly for all sites with the greatest increase seen in the summer and for sites in the south.

For Hartlepool the model predicted that near-sea surface temperature will increase in range from 2.5 – 3.5 °C by the 2080s (lower winter and upper summer estimates respectively). It should be mentioned here that this range of values predicted are pessimistic as the model used was based on atmospheric conditions only and did not take into account the effect of the ocean. The 10^{-3} p.a. and 10^{-4} p.a. extreme weather temperatures which were reviewed in the recent periodic safety review, have not been formally recalculated to take account of climate change, this is being reviewed under normal company business.

These expected changes were judged to be small for the time period covered by the PSR2 review and did not warrant a revision of the design basis. In light of the recent severe winters (2009/10 and 2011/12) consideration has again been given to the design basis temperatures for all EDF nuclear stations and these have been confirmed as robust. The Climate Change Adaptation Report 2011 has recently reviewed the methodologies for:

- Extreme Ambient (high or low) Temperatures;
- Snow and ice loading to buildings and structures and snow blockage of air intakes and the effects of ice;
- Extreme seawater temperatures.

<u>Extreme Air Temperatures</u>

Bounding temperatures have been derived appropriate to both infrequent, 10^{-4} p.a. return period, ambient temperature extremes, and for the more frequent temperature events. The extreme ambient temperatures that the existing safety case is based on were given in section 4.1.

The work examined and presented the results from a report based on UKCIP02 data and found this to be of greater value than the probabilistic method offered by the UKCIP09 weather generator. With this data it was then able to establish the risk of absolute temperatures on the plant.

Using historic data, a mean of maximum summer temperatures were extrapolated to include the predicted future increase in summer temperature per site. The report also determined absolute maximum and minimum temperatures for a 20 and 70 year return period. This work showed that there was a moderate increase in the predicted temperatures.

Apart from the extreme high temperature hazard, all other extreme ambient temperature related risks were assessed as low or very low by the adaptation report. Where climate change was identified as significantly aggravating hazards, the adaptation report has identified adaptation options to address these issues. These include an option to assess whether the design basis extreme air temperatures are conservative so that this can be reflected in future periodic safety review documents.

<u>Extreme Sea Water Temperatures</u>

It is considered unnecessary to accurately derive the extreme seawater temperatures and confirm the relevant plant against these, particularly since the effect of thermal inertia in seawater is such that the range of upper and lower temperatures is very short and both slow and predictable. The time taken to reach the lower temperatures (several days) means that there would be ample time to seek expert advice and take mitigating actions. Furthermore, a surface water freezing in the vicinity of the cooling water intake is not considered to present a problem, as the intake duct is sufficiently well submerged (c.f. 6.63 meters) and it is noted that although surface ice may begin to form at sea temperatures of -2°C, seawater will not freeze completely until it drops to a temperature of -32°C. It should be noted however that Hartlepool draws its water from the Seaton Channel whose water can be describes as brackish. Therefore it may freeze at a slightly higher temperature, approximately -30°C (still significantly below freezing).

Conclusion HRA 4.6: With regard to extreme ambient temperatures there is a current design basis which has been reviewed as part of the periodic review process. The design basis for seawater temperatures is not a current concern, largely as this would be primarily an environmental and commercial issue rather than a nuclear safety issue. The design basis for air temperatures has recently been further reviewed for all sites as part of Climate Change Adaptation and it was identified that the expected increase in temperature may impact the station within its expected lifetime.

Snowloading

No specific consideration of snow loading was noted in the review of the original design. At present there is no formal safety case for the snow hazard. The original design would have been based upon CP3 Ch. V, Part 1, and this would indicate that an imposed loading of at least 0.75 kN/m² (based on uniform snow loading on the ground), and up to 1.5 N/m² for some structures was used for the snow loading (a load factor of 1.6 would then have been applied). Snow loading is currently specified using British Standard 6399-3:1988, AMD9452 May 1997 with guidance obtained from BRE Digest 439.

The consideration of snow loading from drifting requires a detailed review of the levels of the roofs on the nuclear island and an assessment of the increased snow loads. Wind blown snow can form deep drifts against the vertical faces and can result in significant loadings to the roofs at these points. It was considered by a periodic safety review, that further study is carried out to quantify the full extent of snow loading from drifting and confirm the capability of certain plant areas. Snow loading on these areas was assessed against the current standard British Standard 6399-3:1988 with guidance obtained from BRE Digest 439 and this issue has now been addressed and loads on structures confirmed to be acceptable..

An issue identified by a periodic safety review was to re-assess the hazard posed by snow loading on the roofs of the buildings containing essential nuclear systems at Hartlepool.

Further work commissioned by EDF Energy identified the depth of snow expected from an event with a return frequency of 1 in 50, 100, 1,000 and 10,000 years. It found that the infrequent snow depth assumed at Hartlepool bounded the snow depths calculated in the report.

Studies commissioned by EDF Energy reported that the level of risk from snow loading was low while another report concludes that “significant future reductions in numbers of snow days, mean snowfall rates and the intensity of heavy events are projected for the end of the 21st century, consistent with the projection of warming temperatures”. It also concluded that there will be significant future reductions in numbers of snow days therefore EDF Energy are not concerned that snowfall will pose a more significant threat to the safe and reliable operation of our nuclear power stations than it does today.

Conclusion HRA 4.7: Snowloading has been considered and with only shortfalls of a low safety significance being identified.

Consideration HRA 4.2: Consideration should be given to whether a snow loading hazard case is required and whether all aspects of the snow hazard such snow drifting have been considered.

4.1.1.1.3 Lightning

Provisions were made in the original design of the Station to protect against lightning. In the first periodic safety review, the lightning protection provisions were reviewed and a comparison was made of the codes used during construction against modern versions. Following the subsequent review at a later periodic safety review it was concluded that the design of the earthing and lightning protection systems were adequate for the operation of the station until at least 2019, subject to the resolution of identified issues and the continued maintenance of the protection systems..

Lightning protection was provided by the main civil engineering contractor for the reactor building, control building and main turbine hall. The main buildings are of steel frame construction with aluminium cladding and are considered to be ‘Faraday Cages’. The main structural steelwork is used to provide the downcomers from a grid of lightning conductors positioned on the roofs. Columns, equally spaced around the perimeter of the buildings provide connections, via test clamps, to an earth ring conductor with earth electrodes acting as anchor points at each location. Buildings adjacent to the main building were not separately protected against lightning but deemed covered within the zone of protection afforded by the main buildings.

Tall structures i.e. ventilation discharge stacks, auxiliary boiler chimney, gas turbine exhaust stacks and main reactor buildings are provided with a multiple lightning conductor system.

The Central Electricity Generating Board Standard in place at the time of construction addressed the requirements of the then current British Standard Code of Practice CP 326 and the 45° 'cone of protection' was applied to the lightning protection provisions. The majority of buildings at Hartlepool are plant buildings protected by the 45° 'cone of protection', provided by the reactor, control and turbine hall buildings, or have the normal mode of lightning protection applied to individual buildings.

At Hartlepool, the annual inspection is triggered by the maintenance schedule. It is noted that the lightning protection systems are inspected annually by a competent person(s) in line with BS6651:1999.

The protection system has been designed so that in the event of faults occurring, faulty plant is disconnected, whilst continuity of supply consistent with system stability is maintained

A formal hazard safety case is currently being developed for lightning in response to Consideration 4.1.

4.1.1.1.4 Drought

There is currently no explicit hazard safety case for drought at Hartlepool. This was identified as part of a periodic safety review and a programme of work is in place to produce a formal hazard safety case for drought. Owing to the long timescales that will be available to respond to this hazard and its relatively low level of threat to safe operation (it is considered to be bounded by existing safety cases); further consideration of the hazard in this stress test is restricted.

At Hartlepool, Anglian Water Services Ltd fulfils the role of providing the local water authority make-up supply. In their draft drought plan Anglian Water describes potential drought scenarios, actions and measures that might need to be taken during drought conditions. The Plan confirms that the Magnesian Limestone water resources are resilient to drought, and that the area has not been affected by a significant historical drought. Similarly the company has never applied demand restrictions of any kind. There are no specific measures other than the communication of the prevailing situation and the response to its customers through the media. The Hartlepool zone has significant available headroom between water available for use and current and forecast demand.

In conclusion, it is considered that the water resource plan proposed by the water company provides an adequate level of support to Hartlepool.

4.1.1.2 Postulation of proper specifications for extreme weather conditions if not included in the original design basis.

Section 4.1 and 4.1.1 above have shown that whilst these extreme hazards were not explicitly addressed at the infrequent event level in the original design basis, assessments have been back-fitted as part of an earlier periodic safety review and these have been tested and further developed as part of subsequent a periodic safety review.

For drought and lightning, the interim positions are considered robust and safety cases are in course of development.

4.1.1.3 Assessment of the expected frequency of the originally postulated or the redefined design basis conditions.

The robustness of the existing design bases for the wind and extreme ambient temperature hazards has been addressed in sections 4.1 and 4.1.1.2 above. Suitably conservative safety cases are being developed for the lightning and drought hazards but reviews carried out as part of the second periodic safety review indicated that these were unlikely to present significant threats to the continued safe operation of the plant.

4.1.1.4 Consideration of potential combination of weather conditions.

This section considers the potential for weather events that have been considered to arise individually within this stress test, to combine in such a way as to present simultaneous threats to reactor safety. External flooding, which has been addressed in Chapter 3, has also been included in this consideration. Seismic events (reviewed in Chapter 2) are independent of meteorological events and for this reason have not been considered here. Seismically induced flooding from consequential tsunamis is addressed in Chapter 2.

Hazards may combine together in a number of ways. One potential way involves the random coincident occurrence of hazard events, for example the occurrence of an external flood hazard at the same time as a dropped load incident within the station. In such a case there is no obvious connection between these events, causing one to arise as a result of the other, and their combination is considered as being purely coincidental. Where there is no causal link between the hazards the occurrence of the extreme infrequent event in combination with another event is considered to be of such low probability that the risk is judged to be acceptable. On this basis, unrelated coincident hazards can be discounted.

Another, more significant, way in which hazards can combine involves the occurrence of one hazard that then causes a second or consequential hazard. In general, consequential hazards are dealt with as part of the initial hazard but this way of dealing with the hazards is not followed in every case.

Finally, hazards can combine in situations where each hazard event is the result of, or is caused by, some other underlying condition. Severe weather conditions, for example, may result in both a lightning hazard and an external flooding hazard posing a threat to the station at the same time. It is not that one of these events causes the other but rather that both are caused by the prevailing weather conditions.

Combinations of hazards have been considered. The majority of combinations of weather events lead to consequences no worse than those arising from an individual hazard with respect to the design basis. It is recognised that combined hazards may impact adversely on issues such as site access and the infrastructure and emergency arrangements are considered further in Chapter 6. Additionally, the following combinations of external natural hazards with both internal and other external hazards are considered credible. However, it is judged that these will not affect nuclear essential safety functions.

The Potential for Wind to Cause Internal Hazards:

- Extreme Wind Causing Cold Gas Release;
- Extreme Wind Causing Missiles;
- Extreme Wind Causing Dropped Loads;
- Extreme Wind Causing Vehicular Impact.

Extreme Wind Combining with Other External Hazards:

- Extreme Wind Combining with Extreme Flooding;
- Extreme Wind Combining with Extreme Ambient Temperatures;
- Extreme Wind Combining with Extreme Snow;
- Extreme Wind Combining with Lightning.

The Potential for Extreme Ambient Temperatures to Cause Internal Hazards:

- Extreme Ambient Temperatures Causing Fire;
- Extreme Ambient Temperatures Causing Cold Gas Release;
- Extreme Ambient Temperatures Causing Dropped Loads;
- Extreme Ambient Temperatures Causing Internal Flooding.

Extreme Ambient Temperatures Combining with Other External Hazards:

- Extreme Ambient Temperatures Combining with Lightning;
- Combined Hazards Involving Lightning or Drought.

Although the possibility of combined hazards has been addressed, it is noted that only two hazards combining together have been considered. Other combinations such as external flooding combining with extreme wind and lightning may not have been assessed.

Conclusion HRA 4.8: A recent report considered both consequential hazards and combinations of hazards and they were both judged not to impact adversely on nuclear safety, with those considered credible being bounded by the existing hazards safety cases.

Consideration HRA 4.3: Consideration should be made to confirm that all credible combinations of hazards have been assessed.

Fleet wide Review

During this review, it has been found that the methodology used to calculate the extreme ambient temperature and extreme wind conditions expected during the infrequent event is inconsistent across the fleet. Though this does not invalidate the design bases currently employed, it is considered that the methodologies currently adopted be analysed alongside any modern standards and approach and consideration be given to whether a common fleet wide methodology should be used.

Conclusion HRA 4.9: During this review, it has been found that stations have adopted different methodologies with regards to deriving a design basis for some of the extreme weather hazards

Consideration HRA 4.4: Consideration should be given to evaluating the methodologies used to calculate the infrequent extreme ambient temperature and extreme wind event conditions and whether a fleet wide methodology should be adopted.

4.1.2 Conclusion on the Design Basis

Section 4.1 has confirmed that for the wind and extreme ambient temperatures hazard, appropriate design basis events have been defined. For the lightning and drought hazards, formal hazards safety cases are being developed but the nature of these particular hazards means that it is unlikely that 10^{-4} pa events will be defined. Instead, it is likely that these hazards will be assessed against appropriate standards or for worst envisaged consequences as a surrogate for a design basis derived for a return frequency.

Reviews that have been carried out to date on expected climate change do not invalidate the design bases.

Consideration has been given to combined hazards and it has been judged that these are covered in the existing cases or that the combination is bounded by the existing cases.

4.2 Evaluation of safety margins

4.2.1 Estimation of safety margin against extreme weather conditions

This section considers the degree to which the existing safety cases include margins. It is noted however that the approach that is normally adopted in hazards analysis does not provide any estimation of the difference between the design basis condition and those conditions that would seriously challenge the reliability of the protection plant and equipment. The section highlights what plant items are lost during the hazard, what essential safety functions are claimed to survive the hazard and any actions required to maintain the essential safety functions. The hazards that equipment is qualified against is listed in a database which also states how the equipment has been qualified.

In addition hazard technical specifications are being developed for each of the hazards that will provide instruction to the operator to constrain operations if weather conditions exceed specified values.

Season Preparation

A procedure is in place which is used at Hartlepool Power Station for safe and reliable operation during meteorological and environmental conditions encountered through the year. This Procedure supplies a process for the assessment of Station readiness for seasonal conditions for Summer and Winter Seasons. This Procedure also supplies guidelines that have been developed to assist senior Station staff in making decisions affecting the plant status and the provision of appropriate resources necessary for safe operation or shutdown of reactors during periods of severe weather.

4.2.1.1 Extreme Wind

Reactor

Wind blown missiles that may be generated by this hazard are judged by the safety case not to result in the further loss of essential plant to that already considered as lost due to the immediate effects of the extreme wind.

Lines of Protection

For infrequent hazards (10^{-4} p.a.), the company standards require demonstration of one line of protection. Where reasonably practicable, redundancy and diversity are engineered to provide added robustness (i.e. there is single failure tolerance and in some cases more than one line of protection). The plant listings for the essential functions for the infrequent wind hazard are given in Table 4.2 below.

Table 4.2 : Lines of Protection against Extreme Wind Hazards

<table>
<tr><td colspan="2">Function</td><td>Infrequent (More Onerous) 10^{-4} p.a. event</td></tr>
<tr><td colspan="2">Trip</td><td>Guardline equipment</td></tr>
<tr><td colspan="2">Shut down</td><td>Primary Shutdown System</td></tr>
<tr><td colspan="2">Gas Circulator Run On Protection</td><td>Gas circulator main motors common breakers</td></tr>
<tr><td colspan="2">Vessel Over-pressure</td><td>Safety relief valve not challenged</td></tr>
<tr><td rowspan="4">Post Trip Cooling</td><td>Boiler Venting</td><td>Boiler vent routes</td></tr>
<tr><td>Boiler Feed</td><td>Diverse means of feed remain</td></tr>
<tr><td>Gas Circulation</td><td>Forced gas circulation and Natural Circulation</td></tr>
<tr><td>Feed Water Source</td><td>Several feed sources remain</td></tr>
<tr><td colspan="2">Electrics</td><td>On-site Generators</td></tr>
</table>

Civil Structures

The civil structures claimed for the protection to essential plant and systems against the load effects of the high wind hazard have been reviewed and confirmed to provide adequate sources of structural protection. However it should be noted here that consequential loss of grid supplies is assumed for this hazard.

Reactor Trip

The reactor operators would carry out a controlled reactor shutdown in the events of high winds approaching station design basis. AN automatic trip may occur if plant is affected. For the probabilistic safety analysis assessment, grid is assumed to be lost.

Shutdown

The primary shutdown system (control rods) is housed entirely within the reactor building, which as stated above is qualified to withstand the 10^{-4} p.a. wind loading. Furthermore, the main shutdown system is not directly exposed to high-energy missiles and is considered invulnerable to any fragments or other missiles generated as a consequence of high winds by virtue of the fail-safe principles employed in its design.

Post Trip Cooling

Robust and diverse means of post-trip cooling are expected to remain during an infrequent extreme wind event. Operator actions are in place to conserve provisions if necessary.

Loss of Grid

Loss of grid would cause a double reactor trip however electrical supplies would be automatically reinstated by the gas turbines. In the unlikely event that the gas turbines did not start, diesel driven cooling pumps are available to take over reactor cooling duty.

Monitoring

The essential post-trip monitoring function has been assessed during a periodic safety review, and two lines of protection would remain available in infrequent wind conditions, due to the survival of the central control room, alternative indication centre and local indications in addition to essential instrumentation and cabling.

Operator Action

The only significant operator actions associated with the wind hazard are the closure of doors and the securing of buildings against the formation of dominant openings. No issues were identified in terms of the feasibility to carry out these actions, provided the actions are initiated sufficiently early prior to the onset of high winds. This aspect is covered by station operating procedures.

Shutdown Reactors

As outlined in the section above, in the event of an infrequent wind, it is expected that all required systems will remain available other than the grid based supplies. If the reactor is depressurised forced gas circulation will be necessary and remains available using the Gas circulator main motors.

Fuel route

All fuel route facilities are located within buildings qualified to withstand an infrequent wind loading. Sufficient systems to cool the fuel route facilities are qualified against the infrequent wind event. Back-up generation or manual operation would enable fuel movements to be safely completed in the event of loss of grid. As part of the safety case, the threat of wind-borne missiles (for example, falling glazing panels) has been considered and shown to be acceptable.

If extreme winds are forecast, or the station records extreme winds on site, fuelling operations are suspended and any fuel being handled is moved to a safe position.

Conclusion HRA 4.10: The safety margin of essential safety functions of the plant against extreme winds have not been explicitly defined. It has been judged that no cliff edge effects will be seen if extreme winds beyond the design basis are experienced.

Consideration HRA 4.5: Consideration should be given to defining the safety margin to equipment failure due to extreme wind, either directly or as a result of buildings failing.

4.2.1.2 Extreme Ambient Temperatures

Lines of Protection

Table 4.3: Lines of Protection – Extreme Ambient Temperatures

Function		Infrequent (More Onerous) 10^{-4} p.a. event
Trip		Guardline equipment
Shut down		Primary Shutdown Systems
Gas Circulator Run On Protection		Gas circulator main motors common breakers
Vessel Over-pressure		Safety relief valve not challenged
Post Trip Cooling	Boiler Venting	Boiler vent routes
	Boiler Feed	Diverse means of feed remain
	Gas Circulation	Forced gas circulation and Natural Circulation
	Feed Water Source	Several feed sources remain
Electrics		On-site Generators

A major part of the plant consideration is that the majority of essential plant items operate in a controlled environment (provided by building insulation and operation of the heating and ventilation plant).

Civil Structures

A review of the extreme ambient temperatures hazard on civil structures was presented as part of an early periodic safety review. The temperature of most structural steelwork is expected to drop to a point at which brittle fracture would become a potential problem at the extreme low external air temperature. However, brittle failure would only occur if plant subject to impact loading or significant additional stressing.

Accordingly, any activities which import such loads would be prevented during the period of low ambient temperatures.

Various gas bottles are stored around site; however the ductile/brittle transition temperature for industrial gas bottles is less than –20°C. It is considered that brittle failure would not occur for gas bottles even in extreme low air temperatures.

Heating and Ventilation systems

For the reactor building, taking into account the performance of the heating and ventilation plant and heat generated by the reactors and essential plant, the temperature would be expected to remain above freezing during extreme low external air temperatures and would not exceed 40°C during extreme high external temperatures. There is no heating provision in the turbine hall ventilation system; however plant heat losses with one reactor on load would maintain the temperature in the building above freezing with extreme low external air temperature. The turbine hall has been assessed against a steam release and it has been shown that temperatures up to 82°C can be tolerated without affecting safety.

If both reactors are shutdown and no heating is available from either reactor heating can be provided by the auxiliary boilers. Heating and ventilation systems would be switched to heating. The building would be boxed up and all vent louvers closed.

By considering the design basis of the heating and ventilation systems serving the central control room and safety equipment rooms it was argued that the temperature would fall to no lower 2°C with an extreme low external air temperature. During extreme high external air temperatures the heating and ventilation systems were assessed as capable of limiting the temperature to 26°C.

Trip and Shutdown

The main guardlines and secondary shutdown guardlines provide reactor trip for bottom line and second line protection respectively. Both sets of equipment are located in the rooms where the ambient air temperature lies within the components operating range. Bottom line reactor shutdown is provided by the primary shutdown system where the control rods are within the pressure vessel with their temperature controlled by reactor gas temperature. The control rod clutch contactors are situated in switchrooms within the reactor building. Trip and shutdown functions are not therefore at risk from low ambient temperatures.

Post trip Cooling

Bottom line post-trip cooling utilises the gas circulator pony motors. The pony motors require the services of reactor ancillaries cooling water and essential cooling water. The reactor ancillaries cooling water system is in the reactor basement and is not adversely affected by external air temperatures. The essential cooling water pumps are located in the pumphouse. The depth of the intake duct is well below sea level and is not subject to blockage by ice and passage through the pump would slightly raise the water temperature. New above ground pipework is qualified against extreme ambient temperatures and freezing will be prevented as long as water flow is maintained. Autovent valves are trace heated to ensure their availability in periods of extreme cold. Additionally procedures require the drain down of isolated sections of external essential cooling water pipework to prevent freezing of the seawater when the ambient temperature drop below -2°C.

Bottom line feed is provided by the emergency boiler feed pumps supported by auxiliary cooling water. These are not adversely affected by external air temperature. The water supply to the emergency boiler feed pumps is from the deaerator which is lagged and receives water from internal heaters.

Pressure vessel cooling

Bottom line pressure vessel cooling is provided by a pressure vessel cooling water system located in the reactor basement. Header tanks for the system are located in a temperature controlled area. Second line cooling is provided by the back-up cooling water system and its supply pipeline is lagged and trace heated and the water source is the townswater reservoir that has a high thermal inertia.

Monitoring and Grid Supplies

The central control room is claimed for bottom line post-trip monitoring and the alternative indication centre is claimed for second line monitoring. The alternative indication centre heating and ventilation is designed to maintain a temperature of 22°C and the alternative indication centre equipment is designed with an operating range between –25°C and +55°C. Plant assessments against extreme temperatures are insensitive to the exact temperature extremes and no cliff edge effects exist.

The low temperature assessments assume that grid supplies were not available, as a consequence of the low temperature. A periodic safety review assessment concluded that loss of grid was not more probable in high ambient temperatures than in normal operation. However, for consistency with Hinkley Point B and Hunterston hazards, and based on experience, it is conservatively assumed that gird supplies are lost in high ambient temperature events as well. It should also be noted that the assessments are against extreme temperatures assumed to exist for extended periods of time. In practice, the extreme temperatures will last for only a short period during the day. The assessment is therefore, very pessimistic.

The on-site generator buildings heating and ventilation systems are designed to maintain a temperature up to 10°C above the external air temperature. Essential supplies to the generators have tank heaters and trace heating.

Shutdown Reactors

As outlined in the section above, in the event of an infrequent Extreme Temperature event it is expected that all required systems will remain available other than the grid based supplies. If the reactor is depressurised forced gas circulation will be necessary and remains available using the gas circulators main motors.

Fuel Route

The fuel route facilities are all located deep within the structure of the main buildings, and are qualified against the extreme ambient temperature hazard. Adequate lines of cooling systems and supporting power supplies are qualified against extreme ambient temperatures.

If extreme low ambient temperatures are forecast then fuelling machine operations would be suspended as a precautionary measure.

Extreme Ambient Temperature Safety Margin

A safety margin cannot be defined as essential safety functions are claimed to the design basis temperature range and analysis has not been done to determine at what temperature plant will begin to fail. As the temperature at which plant fails is not known, no explicit understanding of any cliff edges is known however the temperature at which the diesel generators fail would be a possible cliff edge as the cooling of the plant would be compromised. This is discussed in Chapter 5. This is mitigated by operator actions.

Conclusion HRA 4.11: The safety margin of essential safety functions of the plant against extreme ambient temperature have not been defined. Cliff edge effects are also difficult to define for the extreme ambient temperature hazard.

Consideration HRA 4.6: Consideration should be given to defining the safety margin to equipment failure against extreme ambient temperature. This should include consideration of the consequences of loss of grid for an extended period and the ability to prevent freezing. Furthermore, consider the effects of extremely low ambient temperatures on building temperatures when both reactors are shutdown.

4.2.1.3 Lightning and drought

Protection against lightning has been installed on the key buildings in accordance with appropriate standards. The conservatisms inherent in these standards and in the way in which they have been applied should ensure that sufficient margins exist to protect these buildings and the essential plant that they contain. The robustness of the protection afforded against the hazard will be further considered in the safety case that is being developed specifically for this hazard.

A formal hazards safety case is being developed for the drought hazard and this will investigate the robustness of the protection that is available.

Conclusion HRA 4.12: Arrangements are in place to protect against extremes of lightning and drought. To date it has not been relevant to consider margins in the same manner for these hazards. It should be noted that there are no explicit safety cases for these hazards and this has been previously identified through the periodic safety review process and appropriately prioritised work is ongoing.

Consideration HRA 4.7: Consideration should be given to the prioritisation of the ongoing production of the lightning and drought safety case.

4.2.1.4 Human Factors Assessment

The second periodic safety review assessed the operator actions required for the extreme weather hazards discussed in the chapter for advanced gas-cooled reactor stations. The review concluded that these actions were appropriate. However, this review has also highlighted that a comprehensive human factors assessment may not have been carried out to assess whether operator actions can be carried out under the extreme conditions discussed in the chapter.

Conclusion HRA 4.13: Operator actions undertaken during extreme weather events were reviewed and were deemed appropriate.

Consideration HRA 4.8: Consider reviewing whether comprehensive human factors assessments are required for operator actions undertaken during extreme weather conditions.

4.2.1.5 Mitigating Actions

As discussed above, there are operator actions which can help mitigate against the extreme weather hazards due to the predictable nature of the hazards discussed. These include seasonal preparations undertaken prior to winter and summer and undertaking actions when warnings of extreme weather are received.

Conclusion HRA 4.14: The predictable nature of the extreme weather hazards discussed in the chapter allow operator actions to be taken to help mitigate the effect of the hazard.

Consideration HRA 4.9: Consider reviewing the seasonal preparedness measures currently undertaken to identify areas to increase robustness.

4.2.2 Potential need to increase robustness of the plant against extreme weather conditions

Each of the hazards that have been addressed in this chapter have been subject to review as part of the second periodic safety review and will be reviewed again in the third periodic safety review for the station. Whilst the second periodic safety reviews identified some shortfalls with respect to the cases made, very little was found in terms of the need for potential enhancements of the plant robustness. Those shortfalls that have been raised have either been addressed and closed out or are still in process of being addressed.

Climate change has the potential to modify the severity of meteorological hazards and for this reason EDF Energy regularly monitors revisions to predictions. In 2011 EDF Energy undertook a climate change adaptation review. This considered the effects of predicted climate change on meteorological related hazards including those that have been considered in this Chapter. Considering the effect of climate change across EDF Energy's fleet of nuclear stations, a number of generic gaps were identified by the adaptation risk exercise. For each gap identified, a suggested adaptation option was also specified, however these may not apply to every site. Based on these findings, EDF Energy has a number of initiatives that it will be progressing aimed at building on its existing adaptive capability. Over the next year, EDF Energy will be considering in detail its forward strategy with respect to these options. The areas relevant to this chapter are listed below.

Table 4.4 Gaps Identified by Adaptation Report

Gap Identified by Adaptation Report	Suggested Adaption Option
Some chemicals and oils are volatile and/or degrade at extreme air temperatures	Investigate options for cool chemical/oil storage to protect against extreme ambient temperatures

Some stations are more likely to exceed their thermal discharge consents	Liaise with Environment Agency to discuss viability of temperature consent increases on vulnerable sites
Subsidence and landslide: A need for a watching brief	Continue to monitor landslide and subsidence.
Storage of process water from water companies is limited. Thus in the event of a severe drought stations could be left without adequate provision.	Engage with water companies to firm up arrangements for ensuring continued supply of townswater (e.g. Ensure minimum flow rate) during drought conditions
	Engage with Environment Agency on inclusion of sites within drought management plan
	Gauge better understanding as to the likelihood of drought in each catchment and produce a summary report

EDF Energy undertook mandatory evaluations in light of the events at the Fukushima Dai-ichi plant. The full scope and fleet wide results of these are presented in Chapter 0. The Licensee Board required a number of checks to be carried out in the days immediately following the events and these were reported through the first of these mandatory evaluations.

The information gathered by these self-assessments was also used to provide a formal company response to address the recommendations of INPO IER 11-1 and WANO SOER 2011-2 (which are the same). These are known as the within design basis and beyond design basis evaluations respectively.

The findings of the extreme weather aspects for the evaluations are discussed below on a fleet wide basis; this is because the learning from each of the sites is judged to be applicable across the stations.

This assessment was carried out very soon after the event and was primarily focussed on seismic and flooding hazards. Some consideration was given to other extreme events, commensurate with the level of impact of the hazard.

Within design basis evaluation

Scope

The within design basis evaluation was specified to ensure that systems essential to fuel cooling in an emergency situation in a within design basis event including seismic and flooding scenarios are correctly configured, lined up and in a suitable condition to be declared available/operable.

This assessment was carried out very soon after the event and was primarily focussed on seismic and flooding hazards. Some consideration was given to other extreme events, commensurate with the level of impact of the hazard.

Summary of Findings

The within design basis evaluation found that the systems essential to fuel cooling in an emergency situation in a within design basis event are correctly configured, lined up and in a suitable condition to be declared available/operable. No additional concerns were identified at station with regard to all hazards considered in this chapter.

Beyond design basis evaluation

Scope

The beyond design basis evaluation was specified to ensure that documentation, training and plant associated with response to beyond design basis events were reviewed, along with the adequacy of the emergency response organisation. Due to the nature of the questions asked as part of the beyond design basis evaluation, this was primarily a paper-based exercise with workshops between station and central support engineers where appropriate. Equipment provided specifically for response to beyond design basis events was also physically inspected to ensure that the condition of the plant was as expected.

This assessment was carried out very soon after the event and was primarily focussed on seismic and flooding hazards. Some consideration was given to other extreme events, commensurate with the level of impact of the hazard.

Summary of Findings

All stations have procedures for preparation for seasonal readiness and extreme weather events. In general they dictate allowable operations for weather conditions.

Some, but not all, of the stations receive site specific weather forecasts to enable preparation of plant for weather events.

All stations had some experience of within design basis adverse weather conditions such as heavy snow, localised flooding or prolonged heat and in reviewing that experience it was generally noted that some simple actions could provide benefit particularly with regard to station access.

Conclusion HRA 4.15: A fleet wide review has been carried out to identify any fleet wide measures which can be implemented to improve robustness against extreme weather conditions.

Consideration HRA 4.10: Consideration should be given to all stations receiving site specific weather forecasts.

Consideration HRA 4.11: Consideration should be given to the provision of additional station based robust means of personnel transport for extreme weather conditions.

Summary

The design basis for an infrequent extreme wind is based on demonstrating that buildings conform to relevant standards and codes for an event with a probability of 10^{-4} p.a. Equipment required to fulfil the essential safety functions is either located inside buildings which are qualified against an infrequent wind event, or qualified directly. The safety case at Hartlepool has been assessed against the latest codes and is judge to be robust.

The infrequent extreme ambient temperature hazard has been split into four possible events; high temperatures and low temperatures, sea temperature and snow loading. The safety case demonstrates that most equipment is expected to remain functionally available or fail-safe when subjected to the high or low ambient temperatures considered in the design basis. Sea water temperature is primarily a commercial concern and it is not judged to be credible that changes in temperature will impact nuclear safety. The reactor buildings and subsidiary buildings containing essential equipment have been assessed against snow loading and demonstrate sufficient margin.

The Climate Change Adaptation Report predicts by 2030 there will be a rise in the expected maximum air temperature beyond the current design basis. This has been raised as a consideration by this report.

Drought is currently not considered as a formal hazard. The primary defence against drought is that it is slow to occur and it is judged that enough time would be available to put the reactors in a safe state and secure long term cooling provision.

Protection against lightning is provided by adherence to relevant codes and standards. It is judged this remains a suitable and appropriate measure.

Drought and lightning safety cases are currently being produced. The interim position is considered to be robust.

Chapter 5 – Loss of Electrical Power and Loss of Ultimate Heat Sink

Hartlepool

5 Loss of Electrical Power and Loss of Ultimate Heat Sink

Potential damage to the fuel and reactor components is prevented by ensuring that the essential safety functions are always in place and available. These essential safety functions are reactor trip, reactor shutdown and hold-down, provision of adequate post-trip cooling and maintaining containment for the fuel and fission products. One of the main aspects of the Fukushima incident relates to the provision of adequate post-trip cooling and this is the main essential safety function that is affected by the scenarios considered in this chapter.

The focus of this chapter is on prevention of potential damage to the reactor and to the irradiated fuel under various loss of electrical power and loss of primary ultimate heat-sink scenarios. This includes examination of all means available to supply post-trip cooling and an evaluation of timescales available to prevent potential damage in various stress-test imposed conditions.

The stress-test requires a consideration of 'Loss of Electrical Power', including sequential loss of the grid electrical supply, the station on-site normal (ordinary) electrical supplies and on-site diverse (alternative) electrical supplies leading to a 'Station Black-Out' scenario, where all station electrical supplies are lost.

The Stress Test also requires a consideration of 'Loss of Ultimate Heat Sink'. Within this a number of scenarios are considered, the impact of the loss of the primary ultimate heat sink (seawater) as well as, loss of primary ultimate heat sink combined with loss of alternate heat sinks (i.e. other cooling water supplies and heat-transfer routes to atmosphere). The Stress Test also required the combined consequences of station black out and loss of primary ultimate heat sink.

It should be noted that many of the scenarios discussed in this chapter are beyond the design basis. This formally means that they occur with a frequency much less than 1 in 10,000 years. In fact, EDF Energy confidently expect that the scenarios in this chapter, especially those concerning the combination of station black out and loss of heat-sink, are not credible.

The stress-test is applied to both the pressurised and allowable depressurised reactor states. In addition, the stress-test examines the plant requirements for maintaining cooling to station fuel route plant areas.

Figure 5-1 High voltage transmission lines connecting Hartlepool to the electrical grid.

5.1 Nuclear power reactors

The essential safety functions at Hartlepool are briefly described below.

Trip and Shutdown

For a reactor at power, there are diverse trip systems. The main provision for shutdown is the primary shutdown system which comprises control rods which, when power supplies are removed fall under gravity into the core. These systems are designed to fail-safe on loss of power.

Post-Trip Cooling

The first line of post-trip cooling protection for the majority of plant based faults at Hartlepool is based on the provision of forced gas circulation in the primary circuit, with boiler feed to the boilers. Both the gas circulators and the boiler feed pumps are electrically driven by AC power supplies and protect the fuel and essential systems/structures in pressurised and depressurised faults.

A second, diverse line of post-trip cooling against all pressurised faults and hazards is provided by natural circulation cooling of the primary circuit, with diverse boiler feed supplied by the high pressure back-up boiler feed system. At Hartlepool the natural circulation claim is dependent upon pressure vessel cooling in the post-trip period. This cooling is normally provided by the pressure vessel cooling water system, with diverse cooling being provided by automatic initiation of the low pressure back-up cooling system.

Post-trip Monitoring

The central control room is the central control point for the operation of the station under all plant conditions and provides all control, alarm and plant information for both reactor/turbine units and associated common plant. In the event that the central control room becomes untenable, post-trip monitoring capability is provided in the alternative indication centre.

The alternative indication centre is diverse from the central control room and is located away from the reactor/turbine building and designed to withstand extreme events such as flooding and seismic disturbance. The alternative indication centre facility consists of hard-wired indication panels, a data logging system; trend displays and a plant alarm system but has no control or trip functions.

The electrical supplies for the alternative indication centre are derived from dedicated diesel generators. As a result the facility is not dependent on the availability of station electrical supplies.

5.1.1 Loss of electrical power

A summary is given below of the key electrical systems and associated plant that support the essential functions.

The stress-test review of the various scenarios for 'loss of electrical power' at Hartlepool and their impact on the plant that is required to perform the essential safety functions is contained within this section (5.1.1) and its sub-sections. Conclusions and judgements are made throughout the sections below and suggested 'Considerations' for improvement are identified. Further potential improvements to the robustness of plant during a loss of electrical power scenario are considered in section 5.1.2.

5.1.1.1 Loss of off-site power

This stress-test scenario proposes a loss of off-site power supply, which constitutes a loss to the station's reactors of all electrical power supplied by the National Grid system. All off-site electric power supply to the site is lost.

For this stress-test scenario, off-site power is assumed to be lost for several days. The site is isolated from delivery of heavy material for 72 hours by road, rail or waterways. Light, portable equipment can be assumed to arrive to the site from other locations after the first 24 hours.

The off-site power supply, i.e. the Grid network, is described in detail in Chapter 1 (section 1.3.5.1) which also provides an outline of the on-site distribution (section 1.3.5.2). A loss of off-site power event is considered within the safety case and there are installed plant provisions as described below to deliver the essential safety functions.

5.1.1.1.1 Design provisions taking into account this situation: back-up power sources provided, capacity and preparedness to take them into operation

Only one of the four gas turbines is required to satisfy the emergency duty for the minimum pressurised and depressurised post-trip cooling plant in all reactor states.

For a shutdown reactor the design provisions are the same as those discussed above for an operating reactor, although the reactor is already tripped and shutdown.

5.1.1.1.2 Autonomy of the on-site power sources and provisions taken to prolong the time of on-site AC power supply

In general, the Hartlepool Technical Specifications require sufficient stocks of consumables to be available to support operation of the essential systems for at least (but generally much longer than) 24 hours.

The design basis for on-site generators operation was originally set at 12 hours. This was subsequently extended to 24 hours as part of shutdown safety case on the basis that it would allow sufficient time for additional fuel oil to be delivered to site. However, analysis shows that with the current technical specification capacity limits and sensible conservation measures by the operators to reduce the number of generators in operation, supplies will last for considerably longer than 72 hours.

The company's emergency arrangements include provisions for securing replenishment of consumables from off-site suppliers before on-site stocks are exhausted. This is discussed further in Chapter 6.

Conclusion HRA 5.1: Loss of off-site power supplies is covered by the existing safety case and the on-site generators will provide diverse supplies. The on-site generators are started via a battery backed system and continue to run supporting their own auxiliaries. There are sufficient supplies of stocks available on-site to allow all post-trip essential safety functions to be met for a number of days. On a best estimate basis and with sensible fuel conservation measures, a 72 hour mission period could be achieved under the current Technical Specifications.

Consideration HRA 5.1: Consideration should be given to the practicability of further extending the availability of essential stocks for electrical supplies by either providing additional on-site storage facilities or additional means to replenish stocks to allow an extended operating period.

5.1.1.2 Loss of off-site power and loss of the ordinary back-up AC power source

A loss of off-site power combined with gas turbine failure is within the design basis for operating or shutdown reactors provided that the pressure boundaries are sealed, and there are installed provisions to deliver the essential safety functions. If station blackout occurs on a shutdown reactor that is open to air, the safety case is dependent upon the provision of AC supplies to reseal the pressure vessel.

In the event of loss of grid and gas turbine failure on an operating reactor, the essential post-trip cooling functions are met by the back-up systems. These systems are independent of grid and station essential electrical supplies.

5.1.1.2.1 Design provisions taking into account this situation: diverse permanently installed AC power sources and/or means to timely provide other diverse AC power sources, capacity and preparedness to take them into operation

Conclusion HRA 5.2: Loss of off-site power combined with failure of the on-site generators is an event considered within the safety case for an operating reactor and adequate provisions are made to support the essential safety functions.

5.1.1.2.2 Operating Reactor (i.e. pressurised)

In the event of total loss of grid supplies and on-site generators in normal operation, forced gas circulation and boiler feed would be lost and post-trip cooling of the fuel and structures would be reliant on natural circulation in the primary circuit. At Hartlepool, adequate levels of natural circulation can be maintained in this scenario provided that:

- Minimum levels of post-trip boiler feed are provided
- The pressure boundary is cooled

5.1.1.2.3 Shutdown Reactor

Although natural circulation provides adequate post-trip cooling on an operating reactor provided that the reactor is pressurised above ~ 12 bar, the post-trip cooling requirements on a shutdown reactor are more complex, and depend upon the plant state (decay heat, gas density etc) and whether the pressure vessel is sealed or open to air. The timescales extend as decay heat reduces.

There are many hours available to reseal and repressurise the reactor to allow circulation to occur before any fuel damage could occur.

Although a claim on ambient vaporisation of CO_2 to support natural circulation is judged to be possible, the overriding requirement to reseal will require that additional power supplies are made available. However, repressurisation of the reactor could be achieved through ambient vaporisation of carbon dioxide. This does not require the provision of electrical supplies.

5.1.1.2.4 Post Trip Monitoring

In the event of total station blackout, the central control room would remain available for a limited period. Post-trip monitoring would then be carried out from the alternative indication centre. No direct plant control actions can be carried out from the alternative indication centre. Electrical supplies to the alternative indication centre are provided automatically by dedicated uninterruptible power supply batteries for ~ 2 hours and on-site generators can be started to provide power for at least 24 hours**.** Additional fuel oil supplies are available on site to power the alternative indication centre for an extended period.

Conclusion HRA 5.3: With sensible rationing, existing on-site fuel supplies would allow the diverse back-up cooling pumps to operate for 72 hours to support natural circulation following a loss of off-site power and failure of the generators. Similarly, on-site water stocks could be sensibly rationed to allow feed to the boilers for 72 hours. Townswater reservoir stocks would support back-up cooling systems for ~ 8 hours and reliance would then be placed on (gravity fed) make-up from the local water authority.

If station blackout occurs on a shutdown reactor, additional power supplies would be required to reseal the pressure boundary.

Consideration HRA 5.2: Consideration will be given to using diesel generators to power the emergency seawater pumps

Consideration HRA 5.3: Consideration will be given to carrying out a compatibility check to assess whether or not generator supplies can be used for back-up cooling pumps.

It is noted that Consideration 5.3 has now been completed. It has been confirmed that the generator fuel oil can be used to run the back up cooling pumps and all other safety related diesel generator son the Hartlepool site.

5.1.1.2.5 Battery capacity, duration and possibilities to recharge batteries

Battery supplies are not used on the UK AGRs to drive the long-term operation of any cooling / pumping systems.

At Hartlepool batteries are used to provide relatively short term ~ 2 hours electrical supplies - primarily for emergency lighting, control and instrumentation, and engine ignition. As batteries are not required to power prime movers no further consideration is given in this report.

5.1.1.3 Loss of off-site power and loss of the ordinary back-up AC power sources and loss of permanently installed diverse back-up AC power sources

This stress-test scenario proposes a loss of off-site power supply as well as loss of the back-up AC supply as well as any other additional AC generating systems. This is a total loss of all otherwise available AC supply capacity.

As described in the previous section, in the unlikely event of loss of grid and failure of the on-site generators, post-trip cooling is reliant on initiation of the back-up cooling systems. This section considers the failure of on-site generators and back-up cooling systems and is Beyond Design Basis in all reactor states (c.f section 5.1.1.2 which was beyond design basis for shutdown reactors in an air atmosphere).

For an operating reactor, existing beyond design basis accident analysis shows that complete loss of post-trip cooling would result in excessive boiler metal temperatures after many hours.

Consideration HRA 5.4: Consideration should be given to reviewing the status of the arrangements to cover the event of Station blackout for Hartlepool.

5.1.1.3.1 Battery capacity, duration and possibilities to recharge batteries in this situation

Electrical power is not required to circulate the primary coolant in these scenarios. Natural circulation cooling is supported by boiler feed derived from direct diesel driven pumps.

Batteries are not required to support the long term operation of the diesel driven pumps or the alternative indication centre. As a result cooling and monitoring of the reactor should remain available. However, batteries are required to support emergency lighting and some control and instrumentation functions. In the absence of these access to plant and plant operation may be made more difficult.

Conclusion HRA 5.4: During Station blackout, the back-up battery supplies are not required to provide boiler feed in the long term.

Consideration HRA 5.5: Consider providing resilient supplies for essential control and instrumentation and lighting functions.

5.1.1.3.2 Actions foreseen to arrange exceptional AC power supply from transportable or dedicated off-site source

There is a set of emergency equipment that would support essential safety functions with additional special items to enable forced cooling to be restored to a reactor. This equipment is located remotely off-site and centrally within the UK on trailers to be transported to the affected site within ten hours following the declaration of off-site nuclear emergency activation (see section 6.1.2.1). Additional time would then be required to deploy this equipment.

Conclusion HRA 5.5: There are provisions off-site that could be deployed to station within 10 hours and aid in continued post-trip cooling of the reactor.

5.1.1.3.3 Competence of shift staff to make necessary electrical connections and time needed for these actions. Time needed by experts to make the necessary connections.

As it is beyond design basis, there is no formal requirement for the training of shift staff to connect the off-site generators to the station.

However, all shift staff go through a structured training programme for their normal duties and specific additional training for the roles they perform as part of the emergency arrangements. In addition to this the AGR twin reactor design means that there is a relatively large complement of shift staff present, who cover a variety of the plant areas. It is therefore anticipated that the disciplines required for carrying out the necessary work to connect off-site supplies to the plant would be available and with the appropriate equipment would be able to carry out required actions for recovery. (see section 6.1.1.5). In a severe accident situation technical experts at the central emergency support centre would support the technical staff on site by considering the strategies required and formulating a plan to implement those strategies.

Clearly the time then taken on-site to achieve the actions would be dependent on the extent of the work required, which would be a function of the damage to plant by the initiating events.

It is the central emergency support centre organisation which is able to mobilise the beyond design basis trailers, and procure other equipment or consumables. To aid the procurement process there is a standby team of procurement specialists who are part of the central emergency support centre arrangements (see Chapter 6).

Conclusion HRA 5.6: Following a severe accident event, actions required by shift staff could be hindered by conditions on-site. Mitigation of this is provided in the form of the central emergency support centre and procedures for beyond design basis events.

Consideration HRA: 5.6: Consideration should be given to providing emergency plug-in points for portable diesel generators and mobile air compressors.

5.1.1.3.4 Time available to provide AC power and to restore core cooling before fuel damage: consideration of various examples of time delay from reactor shutdown and loss of normal reactor core cooling condition

<u>Reactor: Pressurised</u>

If all AC power is lost when the reactor is pressurised (either at power or shutdown), the gas circulators and pumps for the post-trip systems would be lost and the safety case would rely on natural circulation supported by back-up cooling systems. However, in this scenario we are also assuming that the high pressure back-up cooling system is lost.

- Studies to determine the time available to fuel damage under these circumstances have not been undertaken. However, it is judged that significant fuel damage would not be expected in less than 10 hours.
- It is judged that provision of minimum boiler feed and vessel cooling for the mission time of 24 hours, followed by complete loss of post-trip cooling: temperatures that would cause significant fuel damage would not be reached until something approaching 3 days following station black out.

<u>Shutdown cooling</u>

For a depressurised reactor the minimum cooling requirements require forced circulation unless operator action to reseal and repressurise the pressure circuit is successful. Neither of these is possible under station blackout conditions.

The timescales available to restore shutdown cooling following complete failure of all shutdown cooling are dependant on the particular shutdown state. If the reactor is pressurised and is only recently shutdown, the timescales will be similar to those for the operating reactor given above. When the decay heat has reduced to the point that the reactor can be depressurised and an air atmosphere introduced, many hours are available before any fuel damage would occur.

Conclusion HRA 5.7: Analyses modelling severe accident scenarios have previously been carried out. These have been used for the examination carried out in this report. It has been noted that reconfirmation of these analyses and additional sensitivity studies would be beneficial.

Consideration HRA 5.7: Consider providing transient analysis using the latest route covering the scenario with no available power or cooling to determine the timescales for prevention of fuel and structural damage.

5.1.2 Measures which can be envisaged to increase robustness of the plant in case of loss of electrical power

The preceding sections have shown that there are diverse and redundant provisions for design basis loss of power scenarios. Furthermore, where specific issues have been noted appropriate considerations are raised. These include, across the AGR fleet, consideration of:

- Extended availability of essential stocks
- Improved robustness of re-seal and re-pressurisation arrangements
- Extended control and instrumentation and lighting resilience
- Improved training, planning and pre-engineered provisions in order to improve mitigation measures
- Further transient analysis of severe accident scenarios

Chapter 6 also contains further considerations for additional emergency back-up equipment which would mitigate against the effects of a beyond design basis loss of electrical power.

Conclusion HRA 5.8: The current robustness and maintenance of the plant is compliant with its design basis against loss of electrical power. However, steps to improve the resilience of the plant for a beyond design basis events are being considered.

Consideration HRA 5.8: Consider whether the on-site installation of additional, diverse, permanently installed AC power generators would be appropriate to ensure provision of power to essential systems for an extended mission time, for example 72 hours

Off-site provision of electrical equipment, including AC generators

Chapter 6 (section 6.2.8) contains further considerations for additional emergency back-up equipment to mitigate against beyond design basis loss of electrical power.

5.1.3 Loss of the ultimate heat-sink

A summary is given below of the reactor cooling systems and their associated key plant that support the essential safety function adequate for post-trip cooling.

The stress-test review of the various scenarios proposed for loss of ultimate heat-sink at Hartlepool and their impact on the plant that is required to carry out the essential safety function is contained within this section and its sub-sections.

Conclusions and judgements are made throughout the sections below and suggested 'Considerations' for improvement are identified. Further potential improvements to the robustness of plant during this scenario are also considered.

In many respects, the loss of primary ultimate heat-sink scenario discussed in this section is similar to the station blackout scenario in section 5.1.2. In the loss of primary ultimate heat-sink scenario, normal post-trip plant will function normally for a short period, but the loss of secondary heat rejection from the ancillary plant means that the safety case again relies on the diverse back-up pumps – because they are not reliant on seawater. In short, the two fault scenarios lead to the same situation, and the main difference between the two relates to the mitigating/recovery arguments. In the station blackout for example, any potential claim on forced gas circulation is dependent upon the provision of additional electrical supplies to power the circulators. In the loss of primary ultimate heat-sink scenario, forced gas circulation is potentially available but is dependent upon manual commissioning of back-up cooling systems to cool the circulators. The following discussion describes the loss of primary ultimate heat-sink scenario, and attempts to identify any significant differences between it and the station blackout discussion in section 5.1.2.

At Hartlepool there are two systems designed to serve as the primary ultimate heat-sinks for the station.

Note that central control room functionality would not be affected in the loss of primary ultimate heat-sink scenario, so the normal provisions for monitoring post-trip cooling will remain available.

5.1.3.1 Design provisions to prevent the loss of the primary ultimate heat-sink, such as alternative inlets for seawater or systems to protect main water inlet from blocking

The main defence against total loss of seawater cooling rests on the redundant and segregated design of the essential cooling water system.

A central control room alarm is provided to provide a warning of high water level in the pumphouse sump, indicative of a significant pipe leak and smaller leaks are controlled by sump pumps which start automatically on high water level in the sump.

The essential cooling water pipework is similarly divided into two independent half circuits which serve both reactors. These half circuits are normally segregated so that a single rupture cannot result in total loss of essential cooling water. Circuit interconnection is strictly controlled by the technical specifications and Station operating instructions. An additional essential cooling water supply main is installed to provide maintenance and operational flexibility.

The screening plant for the cooling water systems at Hartlepool consists of four rotating drum screens, each serving one main cooling water pump and a branch of the essential cooling water pump suction main. Seawater flows through the drum screen from inside to outside and debris is carried up to ground level where it removed by washwater jets.

Sodium hypochlorite is added to the seawater in the drum screen chambers, to prevent marine fouling in both the main cooling water and essential cooling water systems. In order prevent corrosion of the condenser tubes, the seawater is also dosed with ferrous sulphate

Gross fouling of the screens could result in the associated essential cooling water pumps becoming unavailable. Protection against this possibility is provided by drum screen differential pressure measurement alarms which provide forewarning of blockage. The operator will become aware of this problem and will trip the main cooling water pumps before the essential cooling water pumps fail due to loss of suction. This action will reduce the demand for screened water by about 90% and consequently essential cooling water will be available post-trip.

Conclusion HRA 5.9: The essential cooling water system is designed to operate as two segregated independent circuits, each capable of meeting post-trip requirements in pressurised faults. Manual intervention to desegregate the diverse cooling water system will extend the capability to depressurisation faults. Several means of preventing the loss of essential cooling water by blockage of the water intakes are employed at Hartlepool, including drum screens and chemical control

5.1.3.2 Loss of the primary ultimate heat-sink (e.g.loss of access to cooling water from the river, lake or sea, or loss of the main cooling tower)

This scenario proposes a loss of all seawater cooling through failure or unavailability, comprising loss of both the main circulating water supply and the essential cooling water supplies. This is a loss only of the seawater heat-sink.

Total loss of seawater cooling from both main cooling water and essential cooling water is covered by the station safety case and is within design basis. The detailed requirements in these scenarios depend upon the reason for the fault. A complete listing of all of the related faults together with the claimed protection is presented in the station safety case documentation.

Conclusion HRA 5.10: As loss of the primary ultimate heat-sink is covered by the safety case, no external actions beyond those covered by Station operating instructions are required to prevent fuel degradation.

5.1.3.2.1 Availability of an alternate heat-sink

At Hartlepool power station there is no readily available alternative heat-sink. The following section describes the current safety case against total loss of seawater cooling.

<u>Operating Reactor</u>

Total loss of essential cooling water due to pump failure or pipework breach is an infrequent event due to the system's segregated design. As described earlier, although drum screen blockage is considered to be a frequent fault, it is considered that the operator would be made aware of the deteriorating situation and would trip the main cooling water pumps. This action would reduce the seawater requirement significantly and allow the essential cooling water functionality to be maintained. As a result, drum screen blockage is not considered further in this chapter.

In the event of complete loss of essential cooling water the reactor will be tripped manually on loss of flow or low pressure alarms or automatically as a result of consequential plant faults. Loss of essential cooling water flow will result in an increase in pressure vessel cooling water temperature and to the automatic injection of the low pressure back-up cooling water system. The safety case claim for this infrequent fault is that post-trip cooling is provided by natural circulation with main boilers fed by a high pressure back-up cooling system and pressure vessel cooling supported by a low pressure back-up cooling system. As described in section 5.1.1.2, both back-up cooling systems operate independently of AC power supplies and seawater cooling systems.

Shutdown Cooling

As in section 5.1.1.2.1, the shutdown cooling requirements depend upon the shutdown state (decay heat, gas density etc) and whether the pressure vessel is open to air. In the context of this chapter, the most significant effect of loss of seawater cooling would be the loss of heat rejection and the consequential affect on the gas circulators. In order to maintain the forced gas circulation capability, the gas circulators would have to be tripped within about 40 minutes and cooling restored using low pressure back-up cooling. Alternatively, natural circulation could be restored by resealing and repressurising the pressure vessel. Neither of these actions is dependent upon the essential cooling water system.

Conclusion HRA 5.11: Loss of the primary ultimate heat-sink is within design basis. The safety case claims are similar to those previously discussed in Section 5.1.1.2 and summarised in Conclusion 5.2. Alternative provisions already exist to support the essential functions.

5.1.3.2.2 Possible Time Constraints for Availability of alternate heat-sink and possibilities to increase the available time

As described above, there is no readily available alternative to seawater as a heat-sink at Hartlepool and the design basis relies on:

- The injection of townswater directly into the primary cooling systems of the essential plant on a once-through basis.
- Manual initiation of demineralised water into the boilers on a once-through basis.

The following discussion considers the time constraints for initiating the back-up systems in the current safety case, and the consequences of failing to meet those timescales.

Operating Reactor

On loss of essential cooling water the reactors would trip due to rising ancillary temperatures. A short time later automatic initiation of the low pressure back up cooling system into the reactor pressure vessel cooling system would then occur. If this failed to operate and the operators were unsuccessful at carrying out this action manually, the operators would depressurise the reactor. The gas circulator main motors would then be restarted once back up cooling water supplies had been established to the motor compartments. This is a straightforward task and the operators are well trained in the procedure. On and off site townswater supplies would allow the reactor to be cooled in this configuration for many days.

The time available to commission the high pressure back up cooling system is reasonably long. During this time fuel and reactor structural temperatures would rise. However, it is judged that many hours would be available to initiate the high pressure back up cooling system before any significant failures would occur.

The initiation of the high pressure back up cooling system is a straightforward task and the operators are well trained in the procedure. The system takes its water supplies from dedicated tanks. These hold sufficient water to cool the reactors for at least 24 hours. After 24 hours water could be readily sourced from off-site supplies.

Shutdown Reactor

For faults on a shutdown reactor, the Technical Specifications arrangements ensure that all permitted states allow sufficient time for the required recovery actions. As in section 5.1.1.3.4, when the decay heat has reduced to the point that the reactor can be depressurised and an air atmosphere introduced, there are many hours available before any fuel damage would occur.

Conclusion HRA 5.12: In the event of a loss of the primary ultimate heat-sink, there are sufficient stocks of cooling water for a minimum period of 24 hours.

Consideration HRA 5.9: Consideration should be given to the practicability of extending the availability of essential stocks of cooling water, by either providing additional on-site storage facilities or additional means to replenish stocks to allow an extended operating period.

5.1.3.3 Loss of the primary ultimate heat-sink and the alternate heat-sink

This event proposes the loss of all seawater, townswater and boiler feed through failure or unavailability.

As described in the previous section, this scenario could lead to damage to some reactor structures. The structures at greatest risk of thermal damage are the boiler spines, the boiler tubes, the boiler closure units and the core support arrangement. Significant fuel damage would not be expected to occur for many hours. Guidance on how to extend this timescale to facilitate plant recovery is available to the operators.

5.1.3.3.1 External actions foreseen to prevent fuel degradation

There is a set of emergency equipment that would support essential safety functions with additional special items to enable cooling to be restored. This equipment is located remotely off-site and centrally within the UK on trailers to be transported to the affected site within ten hours following the declaration of off-site nuclear emergency activation (see section 6.1.2.1). Additional time would then be required to deploy this equipment.

5.1.3.3.2 Time available to recover one of the lost heat-sinks or to initiate external actions and to restore core cooling before fuel damage: consideration of situations with various time delays from reactor shutdown to loss of normal reactor cooling state

If essential cooling water and back-up cooling systems are lost, the natural circulation flows would transfer heat from the core to structures, leading to failure of structural components before the onset of fuel damage. Flows in some circuits should be restricted, if possible, to protect the circulators and boilers in case cooling can be recovered later in the accident.

For this total loss of cooling scenario, many hours are available before the situation is irrecoverable and core damage may occur. This time would be extended if a controlled blow-down of the reactor were to be initiated. This would assist in allowing time to deploy the off-site emergency equipment referred to in the previous section.

It is noted that if the boilers were fed normally for one hour before feed were lost, it is judged that approximately several more hours would be available to restore feed.

In the case of a depressurised reactor, timescales to plant damage are likely to be similar. However, fuel damage is likely to precede the onset of structural failures.

Should fuel damage occur in a depressurised reactor, air ingress into the vessel should be avoided. This will prevent the formation of U_3O_8 which could potentially be distributed around the pressure circuit.

5.1.3.4 Loss of the primary ultimate heat-sink, combined with station black out (i.e. loss of off-site power and ordinary on-site back-up power source)

<u>Operating reactor</u>

This scenario proposes a loss of primary ultimate heat-sink as well as a complete Station blackout comprising loss of off-site power supply as well as loss of all back-up AC supplies.

An additional scenario that this report has decided to cover is for the unlikely event of complete station blackout on a pressurised reactor and a loss of all heat-sinks, including all diesel / petrol driven pump systems.

As described at the beginning of this chapter. The two scenarios discussed in Sections 5.1.2 and 5.1.3 are very similar.

In the unlikely event of complete loss of post-trip cooling on a pressurised reactor, including all back-up systems, it is estimated that damage to some reactor structures may occur after many hours. However, if the boilers are fed for one hour before feed is lost, then the timescale on which feed needs to be restored is increased by several more hours.

Shutdown Reactor

Bounded by Operating Reactor.

5.1.3.4.1 Time of autonomy of the site before start of water loss from the primary circuit starts

Operating Reactor

The loss of the CO_2 gas, which is used as the AGR primary coolant, is covered under the station depressurisation fault safety case. The case takes account of possible loss of off-site power, but does not include coincident loss of primary ultimate heat-sink or failure of other back-up systems as there is no causal link between such failures.

5.1.3.4.2 External actions foreseen to prevent fuel degradation

Actions to prevent fuel degradation will be focused on providing additional means to cool the reactor and the fuel.

This section considers measures that could be attempted to provide the necessary power supply to maintain reactor shutdown (hold-down) and to provide a coolant heat-sink to remove decay heat from the reactor and from the fuel.

As noted earlier in section 5.1.1.3.2, there is a set of emergency equipment that would support essential safety functions with additional special items to enable cooling to be restored. This equipment is located remotely off-site and centrally within the UK on trailers to be transported to the affected site within ten hours following the declaration of an off-site nuclear emergency activation (see section 6.1.2.1). Additional time would then be required to deploy this equipment.

5.1.4 Measures which can be envisaged to increase robustness of the plant in case of loss of ultimate heat-sink

Main Cooling Water / Reactor Sea Water

Loss of seawater supplies through drumscreen blockage is recognised in the existing safety case. The adequacy of protection against drumscreen blockage events was reviewed for Hartlepool a few years ago. In view of the importance of seawater to the station as a heat-sink, it is considered prudent to review the current position to confirm that assumptions remain valid in light of any relevant operating experience.

Consideration HRA 5.10: Any relevant operational experience from a recent drum screen blockage should be considered at Hartlepool once it becomes available.

Consideration HRA 5.11: Consider establishing the amount of additional water stocks that would be required to be held to allow an extended operating period of 72 hours to be claimed for the emergency boiler feed system, and establish whether realistic options for storage of such stocks are available.

See consideration of potential improvements set out above in section 5.1.2.

The preceding sections have shown that there are robust provisions for design basis loss of primary ultimate heat-sink scenarios. The AGR design is generally tolerant to the loss of the primary ultimate heat-sink as a result of the inherent capacity to transfer heat to atmosphere. Hence, fewer specific issues have been identified when compared with the loss of electric supplies scenarios.

It should be noted that a consideration to extend the availability of essential stocks for severe accident scenarios is raised in section 5.1.3.2.2.

Chapter 6 contains further considerations for additional emergency back-up equipment which would mitigate against the effects of a beyond design basis loss of all ultimate heat-sinks.

5.1.5 Licensee Review of Robustness

The Licensee Board required a number of reviews to be carried out in the days immediately following the events.

The findings of the loss of power and primary ultimate heat-sink aspects for Beyond Design Basis are discussed below on a fleet wide basis; this is because the learning from each of the sites is judged to be applicable across the stations.

Scope

The review Beyond the Design Basis was specified to ensure that documentation, training and plant associated with response to beyond design basis events were reviewed, along with the adequacy of the emergency response organisation. Due to the nature of the questions asked, this was primarily a paper-based exercise with workshops between station and central support engineers where appropriate. Equipment provided specifically for response to beyond design basis events was also physically inspected to ensure that the condition of the plant was as expected.

Summary of Findings

All stations noted that there was the potential for improvement to resilience to loss of power and primary ultimate heat-sink scenarios.

In view of Fukushima experience, it was noted that enhancements to the 24 hours mission time for essential stocks could be beneficial.

Disabling reactor cooling while shutdown in air would be a particular challenge for all AGR reactors. This is because there is no identified cooling arrangement for a reactor in air in the event of loss of all electrics. Cooling requires either forced gas circulation, or the reactor to be resealed and repressurised, both of which require electrical supplies.

Loss of non-essential equipment will provide additional challenges for longer term events and various locations have local fire fighting air compressors that will not be resupplied and eventually will lead to deluge valve trips and wetting of equipment and additional demands of water/fuel stocks plus operator action to terminate.

Access issues will be created by loss of supplies at most sites, requiring manual breaching of fences/turnstiles around certain plant areas.

Conclusion HRA 5.13: The current robustness and maintenance of the plant is compliant with its design basis against loss of primary ultimate heat-sink. However, steps can be made to improve the resilience of the plant for a beyond design basis event.

Consideration HRA 5.12: Consideration should be given to increasing the provision of off-site back-up equipment including: equipment to enable boiler feed; a supply of suitable inert gas for primary circuit cooling; electrical supplies for lighting, control and instrumentation.

5.2 Spent Fuel Storage Pools

The AGR spent fuel storage ponds are part of the overall station fuel route. The key components of the fuel route that are also considered here are the buffer stores, fuelling machine, irradiated fuel dismantling facilities and spent fuel cooling ponds.

The following scenarios are considered for each facility:

- Loss of electrical power (grid);
- Loss of on-site back-up generation and grid;
- Loss of primary ultimate heat-sink;
- Loss of on-site back-up generation and grid and primary ultimate heat-sink.

5.2.1 Loss of electrical power

The loss of electrical power is primarily a concern as regards the effect on cooling systems for the various stages of fuel handling and storage. Loss of power to handling systems is generally acceptable as the fuel will be held in a safe state, or manual back-up systems are available to manually operate the relevant drives. The impact of loss of power is summarised in the table below:

Stage of fuel storage and handling	Handling with fuelling machine	Buffer storage	Dismantling	Storage in ponds
Effect of loss of grid	Back-up power available	Back-up power available	Back-up power available	Back-up power available
Effect of loss of grid and on-site generation	Manual operation available for movement of fuel, adequate passive cooling available.	Diesel driven cooling system available	Cooling lost but passive cooling acceptable (see Chapter 1)	Diesel driven cooling package available

Conclusion HRA 5.14: In either the event of both loss of grid or Station blackout, sufficient cooling can be maintained to the station fuel route areas for a 72 hour mission time.

5.2.2 Measures which can be envisaged to increase robustness of the plant in case of loss of electrical power

The preceding sections have shown that there are robust provisions for design basis loss of power scenarios. Furthermore, there are also arrangements for mitigation of the effect of loss of power faults beyond design basis.

Generic measures set out in section 5.1.2 to increase robustness of the plant in case of loss of electrical power would also increase robustness of the fuel route plant areas

The specific issues for the fuel route plant areas are raised below.

Conclusion HRA 5.15: Whilst there are no vulnerabilities identified in the current design basis for the fuel route against loss of electrical power, further resilience enhancements can be envisaged.

Consideration HRA 5.13: To improve resilience of decay store cooling, consider possible enhancement options in respect to guidance to operators, fault recovery techniques, and improved understanding of credible consequences.

Consideration HRA 5.14: To improve resilience of pond cooling and make-up, consider possible enhancement options in respect to guidance to operators, replenishment of lost pond water, and standalone pond cooling facilities having no dependence on any other station supplies or systems.

5.2.3 Loss of the ultimate heat-sink

For the various stages of fuel handling and storage, loss of the primary ultimate heat sink could affect the ability to cool the fuel. Where this is critical, alternative heat sinks are provided. In the effect of loss of all heat sinks, the timescales to restore cooling are as discussed in Chapter 1. The impact of loss of heat sink is summarised in the table below. Note that heat sinks shaded green are not affected by a loss of grid and on-site generation (Station Black Out).

Stage of fuel storage and handling	Handling with fuelling machine	Buffer storage	Dismantling	Storage in ponds
Primary heat sink	Ambient air - loss not credible	Sea	Sea- loss is tolerable as per Chapter 1	Sea
Secondary heat sink	-	Fresh water from on site storage	CO2 stores	Fresh water from on site storage
Tertiary heat sink	-	-	-	-

Conclusion HRA 5.16: In the event of loss of the primary ultimate heat-sink there is adequate alternative heat-sink provision.

5.2.4 Measures which can be envisaged to increase robustness of the plant in case of loss of ultimate heat-sink

The preceding sections have shown that there are robust provisions for design basis loss of the primary ultimate heat-sink. Furthermore, there are also arrangements for mitigation of the effect of loss of the primary ultimate heat-sink beyond design basis.

Generic measures set out in section 5.1.4 to increase robustness of the plant in case of loss of the primary ultimate heat-sink would also increase robustness of the fuel route plant areas

The specific issues for the fuel route plant areas are raised below.

Conclusion HRA 5.17: Whilst there are no vulnerabilities identified in the current design basis for the fuel route against loss of primary ultimate heat-sink, further resilience enhancements can be envisaged.

Consideration HRA 5.15: To improve resilience of decay store cooling against the loss of the primary ultimate heat-sink, consider possible enhancement options in respect to guidance to operators, fault recovery techniques, and improved understanding of credible consequences.

Consideration HRA 5.16: To improve resilience of pond cooling and make-up against the loss of the primary ultimate heat-sink, consider possible enhancement options in respect to guidance to operators, replenishment of lost pond water, and standalone pond cooling facilities having no dependence on any other station supplies or systems.

Chapter 6 – Severe Accident Management

Hartlepool

6 Severe Accident Management

In the ONR Interim Report into the Japanese Earthquake and Tsunami, Mike Weightman states:

"The UK nuclear industry should review the provision on-site of emergency control, instrumentation and communications in light of the circumstances of the Fukushima accident including long timescales, wide spread on and off-site disruption, and the environment on-site associated with a severe accident."

"The UK nuclear industry, in conjunction with other organisations as necessary, should review the robustness of necessary off-site communications for severe accidents involving widespread disruption."

"The UK nuclear industry should review existing severe accident contingency arrangements and training, giving particular consideration to the physical, organisational, behavioural, emotional and cultural aspects for workers having to take actions on-site, especially over long periods. This should take account of the impact of using contractors for some aspects on-site such as maintenance and their possible response."

This chapter will explore the organisation and management measures which are in place within EDF Energy to deal with severe accidents.

In a number of places, this document refers to the need for ongoing development work. Some of this work had been previously identified and captured by normal company processes, whilst some is new work highlighted by the post-Fukushima review. In the latter group, there is some potential work packages referred to as 'Considerations'. These considerations will be carefully reviewed and an appropriate programme of work formulated.

6.1 Organisation and arrangements of the licensee to manage accidents

EDF Energy Nuclear Generation has a robust organisation and has emergency arrangements that have been developed and maintained to respond effectively in the unlikely event of an emergency.

There are three main obligations that underpin EDF Energy Nuclear Generation's approach to an emergency:

Moral – we have a moral duty to protect both personnel and the public. We must have robust emergency plans and their use demonstrated to outside agencies and the public.

Legal - under the Nuclear Installations Act 1965, the Ionising Radiation Regulations 1999 and Radiation Emergency Preparedness & Public Information Regulations 2001 we must ensure safe operations and make arrangements to respond to an off-site nuclear emergency. Our Nuclear Site Licence Condition 11 states: "…the licensee shall make and implement adequate arrangements for dealing with any accident or emergency arising on the site and their effects…"

Commercial – a safe company is also a successful company, so it is in our interests to have robust emergency arrangements.

In addition, EDF Energy Emergency Arrangements are approved by the Office for Nuclear Regulation under a license instrument.

Processes and practices are in place to ensure ongoing development and maintenance of the emergency arrangements.

EDF Energy Nuclear Generation's emergency arrangements form part of a line of defence for the improbable event that robust measures have not been sufficient in preventing. The emergency arrangements are designed to deal with events which, though very unlikely, are reasonably foreseeable. All EDF Energy Nuclear Generation's sites have operator plans as defined by Regulation 7 of Radiation (Emergency Preparedness & Public Information) Regulations. These provide the principles of the site emergency arrangements and the site emergency response guidelines for emergency role holders. These detailed plans are designed to be sufficiently scalable to provide the base from which an extended response to more serious events can be developed.

Regulation 9 of Radiation (Emergency Preparedness & Public Information) Regulations explains the requirement on the Local Authority to prepare an off-site plan for any premises with an operator's emergency plan. The off-site emergency plan is an integrated emergency management document to bring together the emergency arrangements of all the off-site agencies with a role to play in the intervention of an off-site nuclear emergency. EDF Energy supports external stakeholders ensuring an integrated approach to emergency management.

6.1.1 Organisation of the licensee to manage the accident

All of EDF Energy Nuclear Generation power stations' emergency arrangements are developed in line with an EDF Energy Integrated Company Practice; where clear responsibilities and accountabilities are published, highlighting the specific roles assigned within the business to manage the emergency arrangements.

The objectives of the emergency arrangements are:

- To enable the situation and the extent of hazards to people and the environment, on-site and off-site to be determined, in order to provide protection measures and reassurance.
- To enable the event to be managed on-site so as to ensure that a safe and stable plant condition is established.
- To notify those off-site who need to be informed.
- To provide advice to those off-site organisations who have the responsibility for the protection of the public and the need for protective measures to be taken, if any.
- To provide information about the event to the public through the media.
- To enable the business of the company to be secured.

It is an EDF Energy Nuclear Generation policy that the emergency arrangements will be generic and similarly implemented across all nuclear sites and other locations. Locally agreed exceptions to the generic emergency arrangements can occur which take into account geographical or specific local issues. Standards used for managing the emergency arrangements will be traceable back to national and internationally recognised practices or quality standards. The aforementioned process ensures continuously improving arrangements and so optimum intervention at any given time.

Emergency Preparedness Engineers oversee the establishment and maintenance of emergency arrangements at each of EDF Energy's nuclear power station utilising central guidance in the form of company processes and procedures. The emergency arrangements are regularly reviewed, experience is captured, lessons identified and proposed changes are adequately considered and communicated before implementation.

6.1.1.1 Staffing and shift management in normal operation

Maintaining adequate staffing levels is critical to the organisation's ability to maintain its essential functions. Posts and roles essential to the continued safe operation of the nuclear fleet have been identified and, should it become necessary, actions will be taken to implement an 'essential staff only' regime to ensure the continued manning of essential posts and roles by suitably qualified and experienced personnel.

It should be noted that based on learning from other external events, emergency scheme staff with a decision making role will be EDF Energy employees who are suitably qualified and experienced personnel. It is permissible following the completion of the required training for contract staff to fulfil supporting roles within the emergency scheme.

The number of persons on a normal station day shift is approximately 500-600 people, this includes contract staff. During an outage this figure will increase.

6.1.1.2 Plans for strengthening the site organisation for accident management

In line with the company's generic approach to emergency planning, each EDF Energy Nuclear Generation power station adopts the emergency organisation depicted below in Figure 6-1:

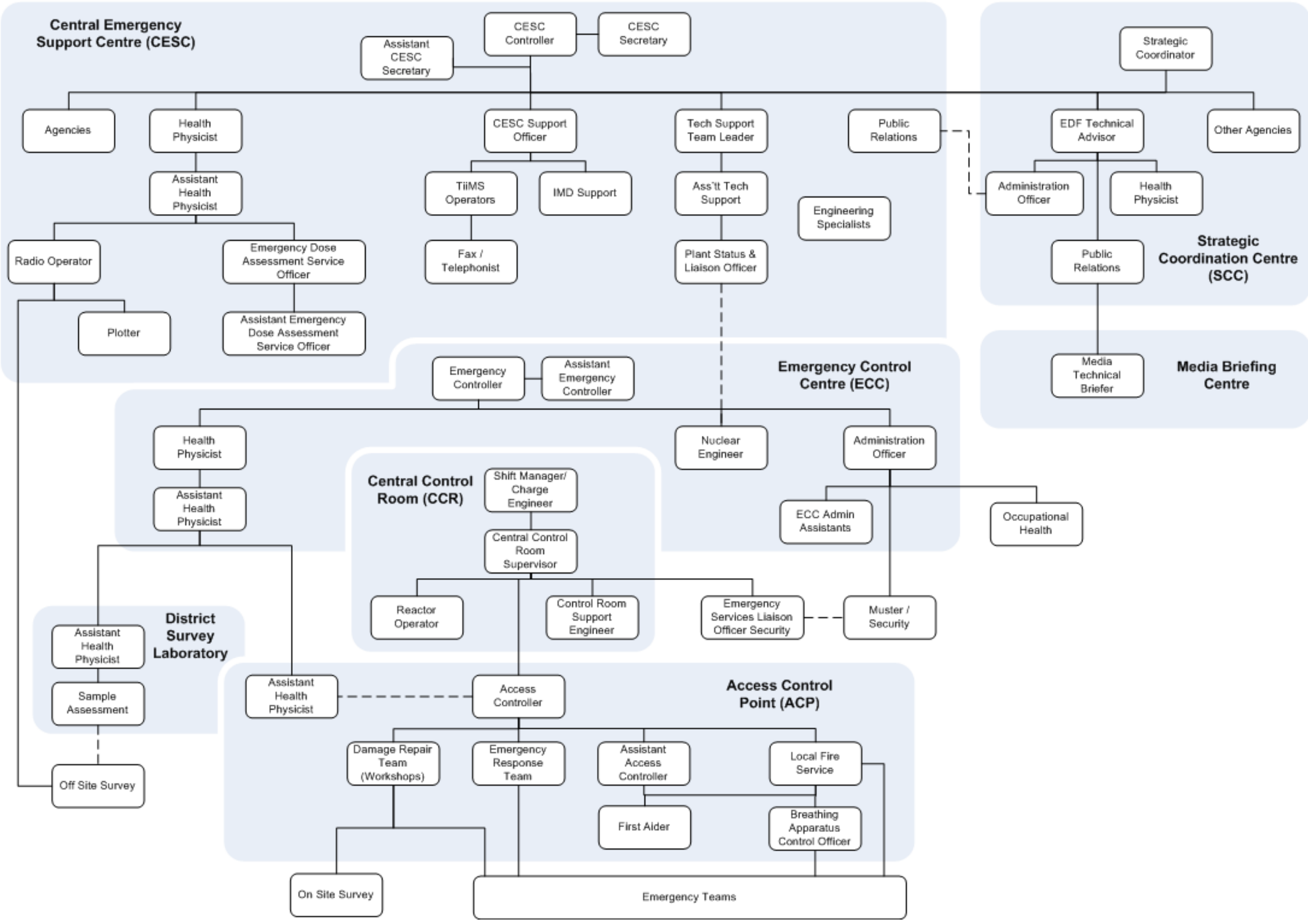

Figure 6-1: EDF Energy Generic Emergency Response Organisation

EDF Energy Nuclear Generation has adopted two declaration states which are as follows:

Site Incident is a hazardous condition which is confined within the boundary of a Nuclear Licensed Site. A site incident could be an accident that is not necessarily nuclear in nature, but possibly a fire or a chemical incident. It may involve the plant becoming hazardous in some way but with no release of radioactivity to an area outside the site boundary.

Off Site Nuclear Emergency is a hazardous condition which results in or is likely to result in the need to consider urgent countermeasures to protect the public outside the site security fence from a radiological hazard. A site incident will usually need a more limited response than an off-site nuclear emergency.

During an emergency of either type, the following centres operate on the station site, working together to provide a co-ordinated and focused response. The centres are detailed below:

<u>Central Control Room</u>

Within the central control room there are dedicated facilities to enable the initial management of the site, take command of the response organisation and interface with external support during an emergency. Once the duty emergency controller takes responsibility, the central control room will be used to manage and co-ordinate the ongoing activities in the damaged area of the site and to make the plant safe. The facilities include maps, station procedures, drawings, communications equipment, tenability monitoring equipment, wind speed and direction indicators, plotting equipment, log sheets and general stationery. The initial location will normally be the central control room, however should the need arise an alternative indication centre is available and is similarly equipped.

Emergency Control Centre

The emergency control centre at Hartlepool is a dedicated facility to enable the site to be managed, take command of the internal response and interface with external support during an emergency. Should the need arise an alternative emergency control centre is available.

The basic equipment provided in the emergency control centre includes maps, station procedures, drawings, communications equipment, tenability monitoring equipment, wind speed and direction indicators, plotting equipment, log sheets and general stationery.

The staff will include the following key personnel available on a 24 hour standby rota to become operational as part of emergency arrangements:

- Emergency Controller.
- Emergency Health Physicist.
- Emergency Reactor Physicist.
- Assistant Emergency Controller.
- Emergency Administrative Officer.
- Emergency Control Centre Communication Co-ordinator.
- Emergency Control Centre Support Staff.
- Security Liaison

Access Control Point

For any event which creates an uncontrolled hazardous area, an entry and egress point will be established to enable command and control activities to be carried out safely in the area. The control point will be located as appropriate for the event, taking into account the prevailing conditions. In its simplest form this may be a single barrier, e.g. in a road for minor fires.

For all events a dedicated access control point facility is available and will be established to provide safe, controlled and rapid access to the affected area. Should the primary access control point be untenable an alternative access control point is available. All access to the affected area will be made through an access control point. Exceptionally other routes may be used but only with the agreement of the access controller.

The access control point and its alternative are equipped with means of communicating directly with emergency teams and the central control room. There is adequate space, equipment and facilities for the contamination, radiation dose and breathing apparatus control necessary for the safe and effective dispatch and reception of emergency teams, including emergency services, and for the initial treatment of casualties.

Site Access and Egress Control

Within the security lodge there are dedicated facilities to enable the site to be secured, initiate the roll call and manage access and egress from the site including the emergency services. The facilities include: maps, emergency procedures, communications equipment and tenability monitoring equipment.

The initial location will normally be the main security gatehouse controlling site access but, depending on the location of the emergency and the prevailing environmental conditions, an alternative site access facility is available and can be similarly equipped.

Declaration of an event

The central control room is manned at all times and has access to detailed information on the state of the plant. In the event of this information indicating abnormal conditions, the shift manager will carry out an immediate investigation and assessment. If the situation demands, the shift manager will initiate actions in accordance with the conditions for declaring a site incident or an off-site nuclear emergency.

Depending upon the nature and duration of an accident the emergency organisation may evolve in three stages:

Stage 1 begins with the declaration of a site incident or off-site nuclear emergency. Trained staff from the nuclear power station forms a site emergency response organisation under the command of the emergency controller. The emergency controller is responsible for initiating the emergency actions to be taken by EDF Energy staff, and for alerting the off-site organisations which have responsibility for countermeasures to protect the public.

Stage 2 occurs when EDF Energy Nuclear Generation establish a Central Emergency Support Centre at the EDF Energy offices located in Barnwood, Gloucestershire. For an off-site nuclear emergency a Strategic Co-ordination Centre and associated Media Briefing Centre will be activated by the Police.

During a Site Incident, the Central Emergency Support Centre will provide technical support to the nuclear power station as necessary and, at the appropriate time agreed with the emergency controller, take over responsibility for off-site monitoring for radioactive release to continuously assess the possibility of the site incident developing into an off-site nuclear emergency.

During an off-site nuclear emergency the Central Emergency Support Centre, staffed by EDF Energy staff, together with other relevant organisations, will at the appropriate time as agreed with the emergency controller, take over control of the deployment of the off-site monitoring resources, assessment of the need for countermeasures and provision of expert advice to the Strategic Co-ordination Centre. The Central Emergency Support Centre will also co-ordinate the technical support to the station.

Stage 3 occurs in an off-site nuclear emergency only, when the Department for Energy and Climate Change appoints a Government Technical Adviser who, after briefing, will assume the responsibility for giving authoritative advice to Police, Local and Health Authorities, and other off-site organisations on any actions necessary to protect the public. The EDF Energy Nuclear Generation Company Technical Adviser and team will support the Government Technical Adviser in this role and continue to liaise with the Central Emergency Support Centre Controller. The Government Technical Adviser will be the principal Government spokesperson for briefing the media.

Emergency Response Staffing

EDF Energy Nuclear Generation emergency arrangements have been developed, embedded and tested against minimum staffing levels for emergency response roles for each nuclear power station in the EDF Energy nuclear generation fleet.

The basis for the current emergency scheme staffing levels was established through systematic analysis. This analysis used an assessment of risks and hazards to identify emergency task requirements. These emergency task requirements were, in turn, used to identify emergency scheme staffing levels and enhancements required for equipment and training.

Emergency plan actions and guidelines have been designed against a minimum staffing resource and with the objective for emergency response to be effective using staff from the power station for the initial 60 minutes of an emergency. The staffing resources are derived for a reasonable foreseeable accident involving a reactor event and release of radioactivity. For other events the resources will be managed to provide additional expertise or staffing levels as required. The emergency roles are staffed from both 'Shift Staff' who would be on-site at the time of an emergency and from 'Standby Staff' who may not be on-site at the time of emergency, but who can attend site within a 60 minute timeframe.

Shift Staff: A record of the current shift staffing is available from the central control room indicating cover for emergency roles which will meet or exceed the minimum manning levels defined. The operations team leader maintains the staffing level for the next 24 hour shift cycle. Any changes in staffing levels during this period will be communicated to the central control room. Part of the shift handover procedure is to ensure that the emergency role responsibility has being passed on effectively.

The site emergency team capability has an incident response team fully staffed on a shift basis and a standby emergency response team staffed by day post holders in an appropriate discipline.

The actions carried out by site emergency team members are predominately those required by their normal post overlaid with skills in fire fighting, search, rescue, first aid and radiation protection monitoring. It is considered within the current emergency plans that the tasks of the site emergency team will be supplemented by specialist resources such as the local Fire and Rescue Service, when the event develops. It is expected that the local emergency services and standby support should be active on site within 60 minutes of a declaration.

The emergency scheme role holders are subject to an ongoing alignment programme to improve scope and depth of competence. In the current phase the programme is reviewing the training and competence levels associated with site emergency team capability.

In addition to Standby Duty Emergency Officers it is recognised by all EDF Energy nuclear sites that additional personnel can be called in when a site incident or an off-site nuclear emergency is declared. The site emergency controller is responsible for anticipating where resources are to be deployed. The supporting staff services may be required immediately or within a few hours of an emergency, depending on the event to provide additional specialist services and supplement the existing emergency teams.

During a protracted emergency, beyond a few days or maybe weeks, it is assumed other role holders from unaffected EDF Energy Nuclear Generation sites would provide support. The benefit of adopting a generic EDF Energy Nuclear Generation approach to the emergency arrangements is that it is possible to call upon emergency scheme responders from other sites. Though it is recognised some roles benefit from a detailed knowledge of their power station when responding to an event, the generic nature of the arrangements makes it possible for people to respond effectively to other affected sites and meet the objectives of the emergency plan.

Although not part of the generic emergency roles, the role of assistant health physicist in the access control point is being staffed on a call in basis in most cases by a member of the duty Health Physics rota. During an prolonged event this could have an impact on health physics resource. As this expertise has been specifically identified it is advisable for the Central Emergency Support Centre to support the site by arranging at an early point in the event for additional resource to be provided by other unaffected sites.

EDF Energy Nuclear Generation have considered the risk of loss of a significant proportion of the duty Incident Response Team staff during an emergency and would additionally utilise the duty standby emergency response team staff to provide the initial response.

EDF Energy Nuclear Generation works on the basis of having trained emergency response staff members available at any given time.

6.1.1.3 Measures taken to enable optimum intervention of personnel

Command and Control

Specific practices and techniques are utilised to ensure efficient decision making during an emergency response. To do this, EDF Energy staff employ a predetermined way of working that is considered and structured. This is known as command and control. The command and control approach means:

- Creating an environment focussed on response and direction.
- Adding detail as the focus and action move down the chain of command.
- There is a faster, more urgent response.
- Staff will be instructed on what to do.
- It is essential that information is communicated and kept up to date.
- Any queries are raised in a timely manner and responded to immediately:

To allow an internal emergency response organisation to function correctly and appropriately it is important to have a command chain structure; so that each part of the organisation understands to whom they are reporting to and from whom they will receive information and tasks. The whole emergency response organisation will be guided by the focus points of the emergency controller. Each layer of the command chain will align their focus to that of the emergency controller. The emergency controller will establish the strategy for the response to the event by use of focus points. The tactics, actions and delivery of operations will be determined by the team leaders and team members of the emergency response organisation. The shift manager will be closely involved in developing the overall strategy for the site with the emergency controller.

All emergency scheme role holders are trained and aware of command and control techniques. This aspect of the emergency response is regularly demonstrated and assessed.

Dose Control

During an off-site nuclear emergency one of the major hazards that has to be managed is radiation. In dealing with radiation our overriding principle is keep exposure as low as reasonably practicable. This principle seeks to ensure that during all emergency activities exposure is kept to a minimum, considering all factors involved. Our priority is to protect everyone involved or affected by an emergency in any way, which includes:

- The public.
- Emergency teams, including the emergency services.
- EDF Energy staff.

ALARP principles are employed throughout the emergency activities lifecycle. ALARP principles influence the design of tasks, the associated preparation and briefing and the approach followed during all tasks

There is legislation covering exposure to radiation in an emergency. The 2001 Radiation Emergency Preparedness and Public Information Regulations impose a duty on nuclear operators to prepare emergency plans and adopt a system of controlled exposures to radiation which would exceed the occupational dose limits. The three fundamental principles of time, distance and shielding are used to minimise exposure:

- Time – the time that people are exposed to radiation should be as short as possible.
- Distance – the distance between people and the radioactive source should be as large as possible.
- Shielding – there should be as much protection between people and the radiation as possible.

Whenever possible the initial control of radiation exposure during an accident or emergency should adhere to the practices adopted during normal operation and the radiation controls within the Ionising Radiation Regulations 1999. In particular whilst dose control is being maintained within these statutory dose limits the following factors must also be taken into account when setting dose control constraints:

- The current year's occupational exposure for each of the intervention personnel.
- The dose limit for women of reproductive capacity where appropriate (13mSv in any consecutive 3 month period).
- Any unmeasured exposures already incurred (e.g. internal exposure from inhalation).

Therefore the maximum whole body dose the access controller can authorise without reference to the Emergency Controller is 10 mSv. The dose constraints selected for each task will be justified, allowing the teams entering the incident area to effectively perform their duties. The teams must perform their duties in a manner that ensures that all doses are kept as low as reasonably practicable.

Doses in excess of 10 mSv and the use of Radiation (Emergency Preparedness & Public Information) Regulations emergency exposures must be authorised by the emergency controller, after seeking advice from the emergency health physicist. All team leaders must report to the access controller whenever they encounter dose rates in excess of 50mSv per hour and also whenever any individual team member is likely to exceed 10mSv whole body dose. As the incident progresses and the radiological conditions are more clearly established, the access controller can adopt more conservative dose limits for the performance of damage repair duties and other less essential operations.

The access controller must be aware, when deploying intervention teams combining EDF Energy staff and emergency services personnel, that there may be different exposure limits allowed by their employers.

The access controller, until advised otherwise by the relevant emergency health physicist, will control exposure on the results of whole body gamma radiation measurements. He will assume that skin and internal doses are less limiting provided that breathing apparatus and protective clothing procedures are properly enforced.

The details of any instances of potential exposure arising from failed procedures or protective clothing will be recorded. When it becomes apparent that the doses to intervention personnel are likely to exceed the access controller's authorisation limit, the access controller must inform the emergency controller, and ask if the team members are to:

- Stand down;
- Have their authorised dose limit increased up to a limit of 100mSv; or

- Should he ask for volunteers willing to exceed their 100mSv limit up to a maximum of 500mSv in order to save life or prevent a major release of radioactivity.

The actions decided and the names of volunteers will be recorded in the access control point, central control room and emergency control centre logs. Volunteers must be made aware of the significance of the risk associated with the doses for which they have volunteered. The access controller will only authorise entry to the incident area to those persons performing essential duties and he will limit the size of entry teams to the number of persons sufficient to perform the assigned duty effectively.

Welfare

As well as managing exposure to the radiation hazard the emergency controller will consider the general welfare of all staff on site and when to replace emergency role and shift personnel on duty. Such a decision will have to be made early to ensure that oncoming staff are informed and provided with access to the site. A comprehensive handover between outgoing and incoming staff is required under the current arrangements. The current arrangements assume ongoing response staff can access site or in extreme cases staff will be available from other sites to support.

Staff involved in serious incidents may require some form of post traumatic stress counselling. EDF Energy has an Employee Support Programme for all staff to use for counselling which would include traumatic events. The Nuclear generation occupational health team are all trained in basic debriefing skills post events. A response to an event would be co-ordinated by the Chief Medical Officer. This aspect of the response would be co-ordinated by the Central Emergency Support Centre.

6.1.1.4 Use of off-site technical support

The nuclear industry continues to learn the lessons from emergencies and accidents all over the world. The events at Three Mile Island in the United States in 1979 conveyed the importance of supporting an affected nuclear site by adopting off-site technical support.

EDF Energy Nuclear Generation utilise this approach and the overarching objective of the Central Emergency Support Centre is to relieve the affected station of the responsibility for liaison with outside bodies on off-site issues in as short a time as possible after an accident, thus allowing them to focus on fixing the issue at hand.

The Central Emergency Support Centre will also acquire and assess all necessary technical data that has a bearing upon the radiological hazard to the public and pass clear advice based upon that technical assessment to the Strategic Co-ordination Centre in such a form that those at the Strategic Co-ordination Centre can make informed and timely decisions on the need to take action to protect the public. The Radiological Assessment Team primarily discharges this function.

The Central Emergency Support Centre includes key roles for central support to any of the nuclear power stations in the EDF Energy fleet, available on a 24hr standby that will become operational within one hour of notification.

For protracted emergencies these roles will be supported by assistants and specialists available on standby within a similar timescale as the aforementioned roles. The Central Emergency Support Centre is under the overall direction of the Central Emergency Support Centre Controller who is responsible for ensuring that this centre operates in such a way as to fulfil its functions of serving and supporting the affected site and Strategic Co-ordination Centre if standing.

The Central Emergency Support Centre also provides a technical support service to the affected station and acts as the focal point for routing advice and material assistance to the affected station. The technical support team primarily discharges this function. The Central Emergency Support Centre will also take responsibility for the onward transmission of monitoring results and the outcome of radiological assessments to external agencies such as Food Standards Agency and to the Strategic Co-ordination Centre, as well as supplying information to the Company's Chief Officers. This function is primarily discharged by the Information Support Team using EDF Energy's Emergency Management Information System.

The EDF Energy emergency organisation adopted within the Central Emergency Support Centre has been demonstrated to be flexible from the differing events that have been supported historically; which include protestor action, on-site issues, fuel shortage response and most recently the company's support to events in Fukushima. In each of these events the internal generic response organisation has been appropriately arranged to suit the specific support required. EDF Energy Nuclear Generation has embedded a culture of support to such incidents and as such has the expertise and resource of all suitable staff in the Barnwood Office to call upon.

Current arrangements show that the minimum staffing levels of trained personnel for standby-roles are met and staffing levels for each role are reviewed quarterly as part of a continual refreshment programme.

The Central Emergency Support Centre facility is also utilised by Magnox Generation Ltd who own a number of nuclear power stations. Some of these stations are located adjacent to EDF Energy Nuclear Generation stations; however these Magnox stations are non-operational. This facilitates effective communications between the companies, but also highlights the potential risk of both organisations requiring the facility to manage their own events at the same time. Contingencies are in place to mitigate this and the following advice is provided: Central Emergency Support Centre and Strategic Co-ordination Centre Handbook

- Primacy should be given to the site which has declared the most severe incident (i.e. an off-site nuclear emergency has primacy over a site incident).
- If all sites have made the same declaration then primacy should go to the company who arrives at the facility first.
- If staff from both companies arrive at the Central Emergency Support Centre then a decision on the manning, based on the types of incident, should be taken by the EDF Energy Central Emergency Support Centre Controller and the Magnox controller or assistant controller

If there is a need for an additional facility due to the situations described above the second party should consider:

- Using the Strategic Co-ordination Centre Gloucestershire Police Headquarters in Quedgeley, Gloucester.
- Not taking over Command and Control.
- Using the Alternative Central Emergency Support Centre which is also located on the Barnwood site.
- Using an alternative facility.

6.1.1.5 Procedures, training and exercises

Procedures

A suite of documents are utilised as part of emergency arrangements to control both preparedness and response activities to comply with applicable legislation.

Preparedness is defined as the organisational structure and associated activities that develop and maintain the emergency response capability.

Response is defined as the organisational structure and activities that are used when an emergency situation occurs. These include compliance documents, e.g. specifications, response guidance handbooks and emergency preparedness procedures.

The standard distribution of emergency planning materials is via electronic medium. Hard copy distribution is kept to a controlled minimum and primarily for storing at response locations. Symptom based emergency response guidelines and severe accident guidelines are available for supporting responders. The symptom based emergency response guidelines provide non-mandatory advice to the emergency controller and his supporting team on the management of beyond design basis faults in order to regain control of safety functions. The severe accident guidelines provide advice on the management of faults escalating towards severe or imminent fuel damage.

Training

The training modules within the EDF Energy Nuclear Generation Generic Emergency Scheme Training Framework are based on the training needs analysis of tasks described in the Emergency Plan and Emergency Handbook. The modules cover a discrete area of procedures, skills and/or knowledge. A module may meet the needs of a number of different role holders who need knowledge or skills in that subject area. Within each module the objective may be differentiated by role. Testing of equipment is carried out by undertaking training modules specified for each emergency scheme role. This is managed and recorded via the standard EDF Energy electronic system.

The EDF Energy Nuclear Generation process for training is outlined in the steps below:

Role Orientation

All role holders will receive orientation for their new role irrespective of whether they are new to EDF Energy, emergency scheme or moving between roles. There are three main elements to this:

- Familiarisation with facilities.
- Provision of practical information, e.g. notification arrangements.
- Analysis and delivery of required training for those moving between or taking on an additional role.

Initial Training and Assessment:

Each emergency role will have a separate route through the training programme for their centre although several elements will be common across roles.

The programme is made up of modules drawn from the matrix of generic Emergency Scheme Training. The programme will involve both national and local provision and include some combination of:

- Role specific mentor guide and job aid.
- Attendance on courses, e.g. breathing apparatus training.
- Use of flexible learning materials, e.g. overview, centre/task specific modules.
- Local mentoring.
- Role observation.
- Role shadowing.
- Assessment.

Most station role holders' initial training will be provided on-site using multiple methods with some provision of courses for station role holders on a national basis, i.e. the Nuclear Power Academy. Training will conform to the standards and expectations set by EDF Energy.

Assessment of initial training will be undertaken module by module, as an integral part of that training. The method of assessment selected will be appropriate to the objectives and the content covered, but may include a combination of the following:

- Paper or computer based tests using appropriate questions.
- Observed practical tasks or procedures in a realistic setting.
- Questioning by a certified instructor, assessor or internal regulator.

As part of qualification for role, all role holders will demonstrate suitability for and competence in role by participating in a shift exercise or equivalent. The prospective role holder will undertake the role in full and be observed by an assessor who will normally be an experienced practitioner in that role.

Continuing Assessment and Training

To maintain competence and compliance, the core competences for each emergency role will be assessed over a three year cycle. All role holders will be assessed on every competence for their role during this period. In addition there may be a small number of fundamental, personnel safety related competences for some roles that need to be assessed annually e.g. use of breathing apparatus.

The role specific mentor guide issued for each role acts as a log book for recording competence. Assessment of core competences will use a number of methods:

- Observation of tasks in exercises and performance assessments events.
- Observation of tasks set in a refresher training session, e.g. simulator.

- Use of computer-based knowledge checks.
- Paper-based tests drawn from initial training.
- Questioning by assessors, i.e. to cover scenarios outside of the scope of a specific exercise/event.

The assessment of core competences will be carried out by:

- Current emergency role holders who have met the requirements of the Umpire/Assessor role. Assessors will have normally completed training specific for umpires & assessors.
- Contracted personnel who provide assessment in specialised key skills or tasks that fall outside of EDF Energy Nuclear Generation core business, e.g. fire fighting, command and control.

Accrediting role holders

Emergency arrangements training, follows the company systematic approach to training. However, as a non accredited programme, a graded approach is adopted with the methodology tailored to the needs of the emergency scheme and role holders.

The above approach to training has recently been introduced and moves the company towards a more focused training programme. Hartlepool is in the process of aligning with the company process associated with emergency scheme training.

Hartlepool has evaluated the exercising and training associated with beyond design basis events and concluded the frequency and content should be altered to reflect the needs of role holders more accurately.

Exercising

To maintain competence and compliance, the core competences for each emergency role will be assessed over a three year cycle. All role holders will be assessed on every competence for their role during this period. In addition there may be a small number of fundamental, safety related competences for some roles that need to be assessed annually e.g. use of Breathing Apparatus.

The following describes the types of exercises, personnel involved and frequency of exercise type:

Table 6.1: Emergency Exercising Arrangements

Exercise Type	Description	Frequency
Assessment and Training Drill	An exercise limited in content to test/demonstrate one or two defined areas of the emergency arrangements, e.g. access control points, off-site survey and District Survey Lab, muster roll-call and site security for training purposes or test/develop skill base of participants.	As required
Shift Exercise	An exercise focused on the activities of the whole shift staff complement to demonstrate their ability to deal with the consequence of a simulated event. Areas of activity are limited to the central control room, access control point and emergency teams. Any support staff from days that could assist in these areas may be included for training purposes.	Annually
Desk Top Exercise	Focused on an emergency facility in operation and driven by simulating realistic inputs to the facility	As required
Full Scope Exercise	An exercise involving the whole of the nuclear power station. It may extend to full station roll-call and may include external agencies such as emergency services for training purposes. These exercises are not witnessed by the Office for Nuclear Regulation. These exercises are used to ensure any training or new procedures associated with the emergency arrangements can be evaluated as part of	Annually

Exercise Type	Description	Frequency
	internal regulation of standards.	
Level 1	An exercise – usually annually- involving all nuclear power station staff, visitors and contractors, to demonstrate the adequacy of the current approved emergency arrangements to the Office for Nuclear Regulation. These exercises may involve emergency services and other external organisations. The extent to which the interface with the Strategic Coordination Centre and Central Emergency Support Centre in dealing with off-site implications is tested will be decided by EDF Energy Nuclear Generation or as required by Office for Nuclear Regulation	Annually
Level 2 (off-site plan)	These exercises are aimed specifically at demonstrating the functions of the Strategic Coordination Centre and Central Emergency Support Centre in dealing with off-site implications of an emergency on the basis of a defined input from the site. The Office for Nuclear Regulation will provide a Government Technical Adviser. EDF Energy Nuclear Generation, the Local Authority and Emergency Services will normally be involved to test the interactions between various parties and the decision making process. The aim will be to demonstrate the function of the Central Emergency Support Centre and Strategic Coordination Centre once every three years.	Every 3 years
Level 2 (support station)	A team from the dedicated support station consisting of emergency controller, health physicist, admin officer and communications co-ordinator will respond to the Strategic Coordination Centre in the event of an off-site nuclear emergency being declared at the affected power station. This is tested on a three yearly basis and involves the aforementioned personnel responding and operating within the designate Strategic Coordination Centre facility.	Every 3 years
Level 3	A Level 2 exercise, nominated by Department for Energy and Climate Change and the Scottish Executive, will be enhanced to become the relevant Level 3 exercise and the aim will be to have one such exercise within the nuclear industry each year. As per a Level 2 exercise, but additionally includes Central Government response and interactions between Government Departments and Ministers.	One such exercise within the nuclear industry each year
Counter Terrorism Exercise	An exercise – usually annually- involving all station staff, visitors and contractors, to test the adequacy of the site and company Counter Terrorism plan arrangements to the Office for Nuclear Regulation. These exercises may involve emergency services and other external organisations.	Annually
RADSAFE Exercise	An exercise, usually conducted annually, involving nuclear power station and other EDF Energy staff, to test the adequacy of the site and company arrangements for accidents involving the transport of radioactive materials, attended by the Department for Transport. These exercises may involve emergency services and other external organisations	Annually

The exercising regime aligns with the requirements of The Radiation Emergency Preparedness and Public Information Regulations.

In order to ensure that the full breadth of the arrangements is adequately exercised, EDF Energy Nuclear Generation manages a rolling programme of exercising to include the alternative response centres and back-up contingencies.

In addition to annual exercise drills, the management team at the nuclear power stations aim to undertake at least 6 full site emergency exercises per year. One of these exercises is formally witnessed by the Office for Nuclear Regulation as the annual Level 1 exercise. In addition to the Level 1 exercise, the station is required to complete a Level 2 demonstration exercise every three years.

For all the witnessed exercises the team of inspectors from the ONR and assessors from EDF Energy will review the adequacy of the emergency arrangements and highlight any identified areas for improvement. A timetable of improvements is established in consultation with the Office for Nuclear Regulation and EDF Energy. This is subject to review at an annual emergency arrangements review meeting between the Office for Nuclear Regulation and Station. This rigorous annual review process ensures the station emergency arrangements satisfy the site licensing requirements.

The emergency exercise planning and administration documentation contains information regarding the processes defining the activities that take place when planning and reviewing emergency exercises and defining the activities for modular exercises. This includes timescales, activities, tasks, responsible personnel and completion dates. Following an exercise thorough debriefs take place to ensure lessons and improvements are identified, captured and any resulting actions recorded.

Conclusion HRA 6.1: EDF Energy has detailed robust arrangements for Emergency Response which are subject to a programme of continuous improvement and exercised as required by standard procedures and regulatory demand. Based on the learning from the Japanese Earthquake, the subsequent EDF Energy Emergency Nuclear Generation review of Station Safety Cases and examination of the associated risks on plant, it is not believed the fundamental risk profile on the nuclear power station has changed. Therefore current arrangements remain fit for purpose. However, as part of EDF Energy standards we ensure any lessons identified by real events and exercises (internal/external) are reviewed and built upon within our arrangements

Consideration HRA 6.1: EDF Energy will consider how lessons identified from Japan and credible beyond design basis events can be reflected in our facilities, procedures, training and exercise programmes. Utilising experience from other emergency response organisations and the military, EDF Energy will consider enhancement of its staff welfare, human factors and emotional aspects associated with emergency response.

Consideration HRA 6.2: Complete Implementation of Emergency Control Centre Communication Co-ordinator role.

6.1.2 Possibility to use existing equipment

6.1.2.1 Provision to use mobile devices (availability of such devices, time to bring them on site and put them into operation)

Each nuclear power station has self sufficient mobile back-up feed pumps. Equipment is inspected and maintained under a maintenance contract to ensure readiness. The contract also includes initial response support arrangements for the deployment of the equipment to the affected site. The equipment has bi-monthly, six monthly and annual inspection programmes to maintain the health and state of readiness of plant. The pumps are serviced annually by swapping out the pump with a spare.

There is a set of emergency equipment replicating the core response equipment used on nuclear power stations with additional special items to enable cooling to be restored to a reactor. A detailed inventory of the equipment is held by the Central Emergency Support Centre. This equipment is located remotely off-site and held centrally within the UK on trailers to be transported to the affected site within a 10 hour timeframe following the declaration of an off-site nuclear emergency. The activation of the trailers is tested weekly. The call to mobilise the trailers by the Central Emergency

Support Centre alerts drivers under contract to be ready to move out from the depot, fully loaded, within an hour of the call. A team is also mobilised which travels directly to the affected site to prepare for the arrival of the trailers. They are then able to execute plans using the equipment available. An additional vehicle is also deployed to provide fuel.

Once a site declares an off-site nuclear emergency the Emergency Plan is initiated and an emergency response organisation within the company and external agencies is mobilised. This includes the Central Emergency Support Centre which brings together a team of experts to deal with the emergency. In a severe accident situation the Technical Team at the Central Emergency Support Centre, supported by the central technical organisation would consider the strategies and formulate an implementation plan. It is the Central Emergency Support Centre organisation which is able to mobilise the trailers, procure other equipment consumables. To aid the procurement process there is a standby team of procurement specialists who are part of the Central Emergency Support Centre arrangements.

Based on the location of the trailers the current deployment time to site would be approximately 4 hours. The lessons identified from the Japanese Earthquake so far highlight the associated issues that degradation of external infrastructure can have on access to and egress from site. The original intent of the off-site equipment focused on specific issues with the plant. The events in Japan have shown that all areas of plant vulnerable to an off-site hazard should be taken into account when designing the off-site equipment requirement.

6.1.2.2 Provisions for and management of supplies (fuel for gas turbines, water, etc)

One of the roles of the Central Emergency Support Centre is to coordinate EDF support cells such as the supply chain to procure essential supplies. The technical support team within the Central Emergency Support Centre is required to acquire materials, equipment and other resources requested by the station this will be done at the earliest opportunity should the need arise. If there are infrastructure issues impacting access to the site this will be recognised as a constraint and an alternative means of delivery will be immediately reviewed.

The judgement is that essential stocks can be procured within the 24hr mission period to replenish the relevant essential systems. However there are uncertainties, for example, the effect of a severe external hazard on transport and communications as noted above, and the detailed arrangements for delivering and offloading the quantities of consumables that may be required.

The essential consumables for the site are identified in station operating instruction and include items such as follows:

- Boiler Feed Systems Stocks
- Plant Cooling Systems Stocks
- Loss of Grid Electrical Supplies Stocks
- Plant for Vessel Gas Cooling System Stocks
- Nitrogen Shutdown System Stocks

There are a minimum of 24 hour of stocks available on the Station for all essential consumables for at power reactors, a single shutdown reactor and a double reactor outage.

Conclusion HRA 6.2: EDF Energy has a range of on and off-site equipment which it can use to respond to emergencies which could affect the site. The provision of this equipment and support is a maintained and formal process within the organisation. This includes arrangements to maintain the essential supply of consumables during and emergency. Based on the lessons from Japan there are areas where EDF Energy could consider further enhancements to equipment and its critical supply.

Consideration HRA 6.3: EDF Energy will consider further resilience enhancements to its equipment and critical supplies which take onboard lessons of extendibility and issues that prolonged events could present. Extensive work has already begun to highlight updates to equipment, its location and deployment.

6.1.2.3 Management of radioactive releases, provisions to limit them

As part of the existing company Emergency Arrangements there are plans in place for the management of radioactive releases and provision to limit the effects of them.

At Hartlepool there is a system that allows the reactor gas coolant to be blown down for operational reasons. All contaminated gases discharged from the reactor, the bypass plant, the circulators, the fuelling machine and other fuel handling facilities, must pass through the blowdown system so that the activity is reduced to a safe level. Blowdown occurs via the various blowdown routes and may pass through particulate filters and the main iodine adsorption plant, before being discharged to atmosphere via the main exhaust.

Following extreme events the blowdown plant could be used in a recirculating mode to reduce the activity in the reactor gas before being discharged to atmosphere.

Management advice to minimise release of activity to the environment can be found in symptom based emergency response guidelines and severe accident guidelines.

A Detailed Emergency Planning Zone is provided around a nuclear installation, where there is the potential for an off-site release of radioactivity that would require implementation of countermeasures.

The Detailed Emergency Planning Zone is defined on the basis of the most significant release of radioactive material from an accident, which can be reasonably foreseen. In the event of an accident being larger than the reasonably foreseeable event, arrangements are in place for extending the Detailed Emergency Planning Zone consistent with the concept of 'extendability'.

A number of emergency preparedness activities take place within the Detailed Emergency Planning Zone around EDF Energy Nuclear Generation sites. As part of the company's responsibility under Radiation (Emergency Preparedness & Public Information) Regulations, prior information in the form of a calendar is produced and distributed to residents within the zone, these contain information about what to do in the event of an emergency event and other factual information regarding the radiation. Potassium iodate tablets are also distributed to residents within the area. Residents are also given the option to be added to a Public Emergency Telephone Information System, which would notify them of what action to take in the event of an emergency at their local power station

6.1.2.4 Communication and information systems (internal and external)

The station has substantial diversity of communications media to ensure requirements are met during a response situation. The on-site links include the use of the station's routine telephone networks - Private Automatic and Branch exchange lines, and a number of BT telephone lines together with dedicated direct wire telephones linking the on site response centres. Across the nuclear power station the ultra high frequency radio system is in constant use by the operations and security staff.

Off-site communication links are established to enable adequate communications from both the main response centres and the back-up facilities.

Nuclear Industry Airwave Service - this is a system which is predominantly used for communications between the Survey Vehicles and the Emergency Control Centre, and then the Central Emergency Support Centre. The Nuclear Industry Airwave Service is part of a national radio system, which has both security and inherent resilience built in to it, and is utilised by emergency response organisations. The system consists of:

- Mobile Terminals in the survey vehicles.
- Airwave radios are currently located in emergency control centre, standby emergency control centre, Central Emergency Support Centre and handheld radios are available in the security lodge.
- Airwave Base Stations transmit and receive information.
- EDF Energy Wide Area Network provides connections to the data servers at Barnwood.
- Dispatcher Terminals located in the emergency control centre, standby emergency control centre and Central Emergency Support Centre which are used to communicate with Survey Vehicles.

Site Siren and Public Announcement – after an emergency is declared the site emergency warning signal will sound for a minimum of 40 seconds and announce a standard message over the Public Announcement system. The announcement will be made by the shift manager or the emergency controller.

Emergency Plume Gamma Monitoring System - provides detection of high and low frequency radiation, by means of monitoring equipment situated around the perimeters of the nuclear power station. The system then alarms in the central control room and Central Emergency Support Centre when high levels are detected.

Rapid Reach Notification System- on the declaration of a site incident or off-site nuclear emergency the affected nuclear power station activates the alert using the Rapid Reach System, which automates the process of calling out duty personnel by paging and phoning staff on various stored numbers simultaneously. Each call requires positive response from the recipient to indicate acceptance or rejection of the call. A display on the computer shows progress of the callout in real time.

Pager System - emergency scheme staff are issued with a pager as the primary form of notifying them to respond to an emergency.

An on-site pager system independent of external service providers also exists though this is not claimed as part of the emergency arrangements equipment.

Public Emergency Telephone Information System - a web based emergency notification service that can dial and transfer messages to landlines, mobiles, faxes, and email recipients and pagers. To activate the system users activate a pre-determined scenario.

Mobile Privileged Access Scheme - mobile telephone networks can become overwhelmed by a high concentration of calls that often occur immediately after an emergency. EDF Energy are currently requesting special mobile telephone SIM cards which allow a higher priority of mobile telephone network access during events where the scheme may be enacted, barring public users. These SIM cards shall be made available to staff who could form part of the emergency response.

Advanced Data Acquisition System muster system – electronic access and egress management system for all EDF Energy sites utilised as part of the electronic muster.

The Incident Information Management System - via a direct link on the EDF Energy IT network. This is a computer-based information system designed for emergency situations. Its purpose is to supply the same information to many users at the same time, so ensuring that everyone uses identical, up-to-date data. The system is able to process large amounts of changing information quickly and accurately. It stores all of the information it transmits providing an auditable trail. Data entry on the system is only carried out within the Central Emergency Support Centre. The information management system is available to external responding organisations as well as internally to EDF Energy.

The systems for communication employed by EDF Energy both internally and externally provide a good level of resilient communications. This is based on the opinion of EDF Technical Teams who maintain the technologies and emergency planning role holders who use the systems, based upon historic use and inherent resilience within the systems design. For Nuclear Industry Airwave service, this is also based upon the use of the emergency services that utilise the Airwave Radio System operationally.

Each of the primary communication vehicles, including telephony, mobile telephony, Nuclear Industry Airwave service and ultra high frequency radio are separate systems and supporting infrastructure, providing a high level of diversity and robust communications. Where there are potential single points of failure or areas identified for further review then considerations have been included within this report.

6.1.3 Evaluation of factors that may impede accident management and respective contingencies

6.1.3.1 Extensive destruction of infrastructure or flooding around the installation that hinders access to the site.

EDF Energy recently conducted a review of access control points and emergency control centres during or after external events, and on operators' actions following the events, to provide confirmation that access routes are viable. The review considered the external hazards:

- Seismic,
- Extreme wind,
- External flooding,
- Industrial hazards,

- Extreme ambient temperatures,
- Electromagnetic Interference / Radio Frequency Interference,
- Lightning,
- Drought, and
- Bio-fouling.

This review was completed by both site-based and centrally based personnel and in conjunction with information gathered from the Local Resilience Forum. It did not identify any specific issues associated with very extreme hazards at this site. Nevertheless, EDF Energy is considering whether there are any resilience enhancements possible to provide self-sufficiency of access and egress to site in very extreme conditions.

Conclusion HRA 6.3: EDF Energy has examined factors that could impede accident management and respective contingencies and accepted that given the range of external hazards (flooding, wind etc) access would not be significantly disrupted. However, the emergency arrangements are scalable to allow for the management of response should access be disrupted. This would be achieved through the use of alternative transportation methods either land, sea or air dependant on the scenario.

6.1.3.2 Loss of communication facilities / systems

Communication is a vital component of emergency response. In the unlikely event of an emergency occurring one of the most important communications to initiate the required response is 'initial notification', both to EDF Energy staff and externally to key stakeholders. There are various communication systems utilised by EDF Energy and key stakeholders both during normal operations and response to emergencies. Robust communication protocols, procedures and systems are imperative for successful emergency management.

As detailed in section 6.1.2.4, EDF Energy Nuclear Generation employs several methods of communication. This section of the document highlights the systems used for effective communication, the current levels of resilience in place and highlights where the stress test has identified points of potential failure against improbable emergency scenarios.

<u>Notifications</u>

Personnel on site: the site emergency warning signal will alert staff on site to muster in the event of an emergency. The emergency warning signal is an important element in alerting staff to muster and to enact the emergency response personnel. In the event that site emergency siren was unavailable for example during loss of power or a fault, then loud hailers would be used. The control room can also initiate a group call on the on-site pager system which will be received by all personnel (who each carry a pager) with a predefined message to either internally or externally muster as necessary (in the event of a site incident or fire respectively).

Emergency responders: the shift manager will instruct a member of the central control room team to notify all off-site emergency responders. Notifications will be made through initiation of the Rapid Reach System, dedicated notification contact numbers and also through the Barnwood Alert Centre.

Off-Site Responders: the alert centre is staffed continually and will receive the notification from the affected power station. They will then cascade the notification to activate the central emergency support centre and inform key off-site agencies. A back-up alert centre also exists.

<u>Rapid Reach (Notification)</u>

When the Rapid Reach system is activated it automatically makes telephone calls to each member of the emergency team, first by use of their pager and, if this fails to gain a response, the system will automatically start a process of trying known phone numbers for that person. Should the system fail to make contact with the first person on the list for that role it will phone, in sequence, other known personnel who are suitably qualified and experienced personnel for that post.

Rapid Reach is a separate system at each site, therefore there is built in resilience, if Rapid Reach fails at one site the support station's Rapid Reach system can fulfil the notification process. If Rapid Reach becomes disabled at further stations then notification will revert back to manual procedures whereby station staff will use the emergency responder contact lists available, contacting staff via telephone / mobile.

Off Site Pager System

Although the system is historically resilient, it is known that there are some areas of the country with poor mobile telephone network coverage could mean that staff are either delayed in being called or will be identified by the system as unavailable, due to coverage of signal in the locality. The resilience for this issue is for emergency responding staff to be contacted by landline telephone.

Telephony

It is recognise that telephony is a primary communication method for EDF Energy internally and for communication with key stakeholders, including emergency response organisations. All of the EDF Energy Nuclear Power Stations and Barnwood Office, which contains the Central Emergency Support Centre, have several levels of redundancy for its telephone communications which reflect its importance in successful response to incidents. Each of the EDF Energy sites involved in emergency response has the following levels of resilience for telephony:

- Two telephone exchanges, of which all emergency facilities have dual connectivity.
- System resilience through multiple external telephony links.
- Connection to the Cable and Wireless Cloud (Multi-Protocol Label Switching network) via IP.
- Connection to the Public Switched Telephone Network, via BT Integrated Services Digital Network lines with physical separation.
- Back up power for exchanges and IP routers for a minimum 7 hours supply to ensure system resilience during loss of AC Power.

Nuclear Industry Airwave Service Radio

When other communication systems have failed the nuclear industry airwave service could also be used as a back-up system to communicate between EDF Energy sites. This service is part of a national radio system, which has both security and inherent resilience built in to it, and is utilised by emergency response organisations.

To avoid a single point of failure within the service there are two routers in separate locations. Should one of the routers fail, the second router would be able to assume responsibility for routing network traffic into the Airwave “cloud”.

Ultra High Frequency Site Radio

A recent report was produced on all EDF Energy existing nuclear stations radio systems.

The primary use of the Hartlepool Power Station’s site radio system is for day-to-day operations. There is not a dedicated emergency channel; however emergency calls have priority. The system comprises of four channels, hence the loss of a channel would reduce the through put of radio traffic (no loss of site coverage). Only if all four channels were lost would radio communication cease on site. Three of the four trunk controllers have telephone cards fitted enabling calls to be made from a radio to a site telephone and vice versa.

Potential enhancements have been identified in the ultra high frequency radio system at each nuclear power station. These are as follows:

- Enhancing security of the radio system.
- Test radio system for performance degradation during radiation exposure.

Conclusion HRA 6.4 EDF Energy Nuclear Generation has a wide range of systems which are used for communication, this diversity in itself provides resilience. It is recognised that individual systems could be enhanced to provide further resilience and improve effects from external hazards. The inherent reliance on telephony means that despite there being numerous back-up systems, a great deal of efficiency would be lost without the telephony network.

Consideration HRA 6.4: EDF Energy to consider enhancing current telephony and communications systems to increase levels of resilience of key technological components based on learning from Japan.

6.1.3.3 Impairment of work performance due to high local dose rates, radioactive contamination and destruction of some facilities on site.

The existing emergency arrangements recognise that there is the potential for radiation levels, in some extreme instances, providing access challenges on site.

If this is ever the case then remote access would be required or the installation of an appropriate level of shielding. If radiation levels are such that some access is possible then this access will be time restricted. This would impair the recovery operation particularly if operations are time consuming and would therefore require staff rotation after a certain time spent exposed to high levels of radiation. Existing plans acknowledge and make provision for these eventualities.

<u>Destruction of Facilities on Site</u>

The destruction of primary facilities on site would result in moving to the appropriate alternative facilities, assuming that they have remained accessible and can be utilised. This movement could restrict work performance since the alternative facilities may have limited capability compared to the primary facility in terms of available specialist systems and equipment.

The dynamics of the event dictates the hazardous environment that operatives and responders will be required to work in. This environment could present numerous issues which EDF Energy needs to manage effectively to ensure staff safety and welfare; this includes the emotional and psycho-social wellbeing of responders. These are covered by our standard procedures. It should be understood that working within these environments impacts response time as responders have limited exposure times due to breathing apparatus, radiation dose or due to the physical nature of work. This may require increased rotation of staff and therefore subsequent increase demand on staff resource overall.

6.1.3.4 Impact on the accessibility and habitability of the main and secondary control rooms, measures to be taken to avoid or manage the situation

At Hartlepool Power Station the central control room is located in an area were habitability would not be directly impacted by an external flooding issue for staff already located in the facility.

In general, the equipment in the control room has not been functionally qualified to withstand a bottom line seismic event, and is not claimed as essential plant, although it is expected to remain habitable. Should for any reason the control room need to be evacuated, an alternative indication centre provides a single area from which the status of the trip, shutdown and post-trip cooling of the two reactors can be monitored.

This alternative indication centre provides the operator with post-trip indications and has been designed to withstand the infrequent level event. The facility has an uninterruptible power supply and is powered by an electrical supply (which is also seismically qualified). Local plant indications may also be available.

6.1.3.5 Impact on the different premises used by the crisis teams or for which access would be necessary for management of the accident.

EDF Energy conducted a recent review of access control points and emergency control centres during or after external events, and on operators' actions following the events. This detailed review outlined the impacts on the existing facilities from a range of external hazards.

These facilities are generally qualified for the full range of external hazards and where they are not alternatives have been identified. The Central Emergency Support Centre which is responsible for management of the accident is remotely located from all nuclear power sites.

Conclusion HRA 6.5 In extreme circumstances some on-site facilities may become unavailable. EDF Energy has arrangements in place through use of mobile facilities to respond to this eventuality; however there are opportunities to enhance communications and equipment contained within.

Consideration HRA 6.5: EDF Energy will consider a review of its mobile facilities and the resilience of equipment contained within.

6.1.3.6 Feasibility and effectiveness of accident management measures under the conditions of external hazards (earthquakes, floods)

There will be a number of issues associated with the effectiveness of accident management measures should they occur under the conditions of external hazards. These include:

Emergency Services Support - the availability of emergency services support is unknown with the potential that services will also be responding to a wider emergency. The tasks of the site Emergency Team at the power station will need to be supplemented by specialists; such as the Fire and Rescue Service when the event develops beyond the limits of capability or require specialist equipment. It is a requirement of the Regulator that emergency services and standby support must be active on site within 60 minutes of a declaration.

Under conditions of external hazard there is an increased risk that attendance of responders external to the site within 60 minutes of emergency declaration will not be met. To improve resilience under such conditions EDF Energy will consider off-site resources in appropriate locations to facilitate the emergency response including provision of equipment and staff.

Access to site - (issues responded to as part of section 6.1.3.1) an associated issue related to access to site is the availability of personnel to resource ongoing shifts particularly in the instance of a prolonged emergency. Under the conditions of an external hazard it is likely trained staff will be unavailable due to their own homes or family members being affected.

Off-site monitoring - there is an established process for providing off-site countermeasures advice to protect the public during a release of radiation from a site involving mobile sampling vehicles. One of the lessons identified from the Japanese Earthquake was the inability of off-site monitoring vehicles to access pre-determined monitoring locations and determine the levels of radiation that were being discharged off-site.

Conclusion HRA 6.6 In light of the events seen at Fukushima it is acknowledged that underpinning assumptions relating to the support of off-site local emergency services and the ability of local staff to attend site is questioned. Following a 'cliff edge' event, the duration of response could extend beyond days or maybe weeks. This could result in issues surrounding prolonged use of staff and resources, which may require calling on staff from other stations.

Consideration HRA 6.6: EDF Energy should consider reviewing existing arrangements to ensure the principles of extendibility are adhered to.

6.1.3.7 Unavailability of power supply

The loss of power supply to nuclear power stations would impinge on the response to accidents and so EDF Energy Nuclear Generation has redundancy in the essential electrical supply system at both nuclear power stations and key sites supporting emergency response, such as the Central Emergency Support Centre.

Following loss of the external power grid, back-up options such as diesel generators and batteries ensure electrical supply to essential plant equipment. This includes the facilities required for emergency arrangements.

6.1.3.8 Potential failure of instrumentation

The primary failure mechanism by which instrumentation would be lost is loss of power. Most indicating instruments/sensors have a designated power supply. This may be a dedicated supply to the instrument or it may be derived from the instrument signal loop. The availability of instrumentation for information on plant status and control of plant systems is crucial to the management of the plant within the design-basis. For this reason station-critical systems have diesel- and battery- backed supplies to provide sufficient indication of the station parameters to monitor shutdown. A detailed review has been undertaken and this did not identify any issues within the design basis.

For managing severe accidents, the company documentation gives a list of plant parameters which aid assessing the Critical Safety Functions. The Emergency Controller, on advice from site experts and the Central Emergency Support Centre, would specify which instruments gave information on these parameters. If all of the instruments giving information on a particular Critical Safety Functions were disabled by plant damage, it is probable that a minimum set could be recovered by improvised connections and dedicated power supplies. Consideration is being given to holding equipment, off-site, to reinstate instruments and remotely telemeter the indications.

6.1.3.9 Potential effects from the other neighbouring installations at the site

At Hartlepool Power Station there are a number of fixed installations within a radius of 2km of the site which handle sufficient quantities of hazardous materials that constitute a possible risk to the station. However, it is demonstrated that the risks are not highly significant and the companies work closely together to ensure an ongoing dialogue.

6.1.4 Measures which can be envisaged to enhance accident management capabilities

The Japanese event and findings from the recent reviews has provided EDF Energy with an opportunity to review its accident management capabilities. EDF Energy has concluded that it has robust arrangements for Emergency Response. However there are lessons we have learnt during this process which we will consider in order to improve our response.

These can be broadly categorised into three areas:

- Facilities – this includes site resilience and multi site support
- Technical – communications and supply chain
- Procedures – emergency arrangements and procedures taking into account staff welfare

Training and Exercising encompasses all elements as it is only through these functions EDF Energy can ensure continuous improvement and oversight of our arrangements.

Conclusion HRA 6.7 The provision of off-site equipment and support is a maintained and formal process within EDF Energy Nuclear Generation. Following the 2011 emergency in Japan it is recognised that it is possible that the equipment could be enhanced to provide further resilience to the emergency scheme.

Consideration HRA 6.7: Further mitigation against the effects of beyond design basis accidents could be provided by additional emergency back-up equipment. This equipment could be located at an appropriate off-site location close to the station to provide a range of capability to be deployed in line with initial post-event assessment. This equipment may include the following capabilities:

- **Electrical supplies for plant facilities.**
- **Emergency command and control facilities including communications equipment.**
- **Emergency response/recovery equipment.**
- **Electrical supplies for lighting, control and instrumentation.**
- **Robust means for transportation of above equipment and personnel to the site post-event.**

- **Equipment to provide temporary shielding and deal with waste arisings from the event**

6.2 Maintaining the containment integrity after occurrence of significant fuel damage (up to core damage) in the reactor core

Reactor shutdown systems, containment integrity and reactor cooling act together in order to ensure, as far as is reasonably practicable, fuel damage and fission product release do not occur.

In advanced gas-cooled reactor designs there are three barriers preventing the release of radioactivity into the atmosphere during steady state and transient operation. These are:

1. The fuel matrix.
2. The fuel clad and
3. The primary circuit (pressure vessel / containment).

The single phase carbon dioxide coolant cannot undergo a sudden phase change as a result of an unexpected rise in temperature or pressure. This means that there can be no sudden discontinuity of cooling under fault conditions, and changes in flows, temperatures and pressures would progress slowly.

The coolant pressure may fall in case of a major leakage to the atmosphere, but the core cannot become uncovered as could occur in a pressurised water reactor.

If an advanced gas-cooled reactor is exposed to a depressurisation accident of the carbon dioxide coolant, forced circulation of the coolant, together with defined boiler feed, continues to provide adequate core cooling. Also, in the event of loss of boiler feed, the large heat-sink represented by the graphite moderator and other reactor internals, provides long timescales before impermissible fuel temperatures are reached.

In the unlikely event that, post-trip, a fault is not controlled by the design basis, engineered protection, either because of multiple plant failures or an initiating event beyond the design basis, the mandatory Station operating instructions would be suspended and the accident managed using advice from either the symptom based emergency response guidelines or the severe accident guidelines. The symptom based emergency response guidelines advise on managing beyond-design-basis accidents when the fuel is still substantially intact and there is a reasonable prospect of re-instating the minimum plant needed to contain fission products. For this reason, the advice is based on best-estimates of timescales for irreversible damage and of the minimum plant requirements, in contrast with design-basis requirements which have substantial margins.

If severe fuel damage has occurred, or is anticipated, or if applying symptom based emergency response guidelines advice has not controlled fission product release, the Emergency Controller would consult the severe accident guidelines for advice on limiting the release. The severe accident guidelines advice is broadly based, to deal with unanticipated situations, and uses existing plant in standard and innovative techniques. In addition, some advice calls for equipment and material not normally held on site.

<u>Symptom Based Emergency Response Guidelines</u>

Symptom based emergency response guidelines are set out in Station Operating Instructions.

The reactor trip station operating instructions and associated check sheets determine if entry to these guidelines is required in a fault that could be a precursor to a beyond design basis condition. The symptom based emergency response guidelines entry checklist provides a sequence of symptom checks to be applied at regular intervals and which guide the user to an actions appropriate to the prevailing conditions to ensure that the plant is brought to a long term safe condition. The advice, based on considered judgements of possible conflicts in requirements, aims to choose actions for best effect and minimum risk.

The symptom based emergency response guidelines must be applied with discretion depending on the prevailing circumstances. The order of actions and the actions themselves are not mandatory. Consequently, it is very important that the user always understands why an action is being suggested. The user must decide whether the advice is relevant to the particular situation. In beyond design basis situations the priorities are:

- To prevent uncontrolled releases of radioactive products.

- To prevent structural damage.
- To prevent economic damage.

The symptom based emergency response guidelines are based on the concept of critical safety functions to provide a systematic way of assessing whether the plant is safe. There is one overriding aim – to confine radioactive products. The principal functions to achieve this aim are:

- To maintain control of reactivity.
- To maintain pressure vessel integrity.
- To provide reactor heat removal.
- To control radioactive releases.

The measurement of plant parameters can indicate whether critical safety functions are being, or are about to be challenged. Parameter measurements become fault symptoms when something is wrong. These symptoms can then be used, with plant status checks, as a basis for selecting an appropriate emergency response guideline to maintain control over the safety functions – hence symptom based emergency response guidelines. This is in contrast with the other post-trip Station Operating Instruction's which are largely event based i.e. the cause of the event is identified and the user then selects and follows the appropriate document for this fault.

The symptom based emergency response guidelines introduction section states that if application of these guidelines is unsuccessful in controlling the sequence then application of the severe accident guidelines would be required. These guidelines are available to provide guidance to Emergency Controllers and technical support staff in these unlikely scenarios. It should be noted that the severe accident guidelines only address reactor scenarios as, on advanced gas-cooled reactors, the potential severity of fuel route scenarios is lower.

EDF Energy considers that its efforts and resources should be focussed primarily on measures and improvements aimed at ensuring successful operation of the required protection for within design basis events and, if necessary on successful recovery by application of the symptom based emergency response guidelines.

Conclusion HRA 6.8: It is acknowledged that it may be beneficial to improve the level of training of EDF Energy personnel in the use of severe accident guidelines, and carry out investigations into the feasibility of implementing the advice in a real scenario.

Consideration HRA 6.8: EDF Energy to review the adequacy of training in the use of the severe accident guidelines and the feasibility of implementing the advice in real scenarios.

6.2.1 Elimination of fuel damage/meltdown in high pressure

6.2.1.1 Design provisions

The power density of the advanced gas-cooled reactor is lower than that in light water reactors. For loss of post-trip cooling, this leads to much longer times before any significant fuel damage, in particular the fuel matrix and clad remain intact for a longer period. This means that high pressure ejection of the corium(fuel containing materials) from the vessel is not possible.

6.2.1.2 Operational provisions

There are no specific operational provisions for this scenario as it is not possible in an advanced gas-cooled reactor.

6.2.2 Management of hydrogen risks inside the containment

The extensive damage to essential plant at Fukushima led to oxidation of the Zircaloy fuel clad and hydrogen formation. When this was vented into upper containment buildings it formed an explosive mixture with oxygen in the ambient air. The resulting explosions destroyed the building causing further damage and challenging the accident management.

In his consideration of the implications for the UK Nuclear Industry, the Chief Nuclear Inspector concluded that hydrogen formation was not a hazard for advanced gas-cooled reactors.

Therefore for the advanced gas-cooled reactor design this section addresses the carbon monoxide risks identified rather than discussing hydrogen.

6.2.2.1 Design provisions, including consideration of adequacy in view of hydrogen production rate and amount

Within the design basis there is no carbon monoxide hazard in an advanced gas-cooled reactor and as such there is no requirement for design provisions to be made.

6.2.2.2 Operational provisions

The severe accident guidelines warn of the gas flammability hazard associated with vessel failure and molten-fuel-concrete interactions. It is considered that the existing advice on containing fission products would minimise the flammable-gas threat to damage control teams and to accident management. Ducting off-gas through a filter, to remove radioactive aerosols, requires that the filter be cooled to remove decay heat. This would also remove any tendency for the gas to auto-ignite. It might, however, be necessary to arrange for the gas to be flared.

6.2.3 Prevention of overpressure of the containment

6.2.3.1 Design provisions, including means to restrict radioactive releases if prevention of overpressure requires steam/gas relief from containment

The final containment barrier on an advanced gas-cooled reactor is the Pre-stressed Concrete Pressure Vessel. The normal operating pressure within this structure is 40 bar, as it is the main pressure retaining part of the reactor.

The design of the advanced gas reactor is such that in order to prevent fuel damage it is generally beneficial to maintain the pressure within the vessel to enable natural circulation of the coolant gas. Depressurising can be carried out for a number of scenarios if required but would not generally be an issue in the way it is for a light water reactor.

The primary design provision to prevent overpressurisation of the pressure vessel is the safety relief valves. In addition there are blowdown routes used in normal operation to provide the route for lowering the vessel pressure and also provide the ability to take the vessel in to air as part of normal maintenance regimes.

All discharge routes are fitted with filters; including particulate filters on the safety relief valves.

6.2.3.2 Operational provisions

The operational provisions supplied in the station documentation give advice on various actions that would be beneficial when dealing with either over or under pressure of the vessel in an advanced gas-cooled reactor beyond design basis scenario. They include advice on innovative or non-standard uses of installed plant. The operators undergo specific training on the symptom based emergency response guidelines and central support staff receive training on the severe accident guidelines.

6.2.4 Prevention of re-criticality

6.2.4.1 Design provisions

All advanced gas-cooled reactors are designed to remain shutdown (with a large shutdown margin) with a group of control rods fully withdrawn from the core. This group of rods, referred to as the 'safety group', is fully withdrawn when the reactor is shutdown and remains available to provide a negative reactivity contribution should there be any indication of an unplanned approach to criticality whilst the reactor remain in this state.

In addition there is provision of plant for the purpose of nitrogen injection. This system can provide additional shutdown margin. In the event that the use of nitrogen injection is no longer possible, a further Boron bead injection system is available. The beads would act as a neutron absorber to prevent re-criticality and ensure long term holddown.

In very severe accident conditions extra absorber may be needed to protect against increasing reactivity. It should be noted that this would not occur until well in to the severe accident sequence.

Any actions to cool the core will be extremely beneficial, as would steps to cool and preserve the core supports or to prevent control rod withdrawal in the extremely unlikely event of the core supports collapsing.

6.2.4.2 Operational provisions

It can be seen from the description of the various plant items available that the primary documents relating to hold-down of the reactor are the normal operating instructions. These are, then supplemented by the symptom based emergency response guidelines and the severe accident guidelines should the plant move in to a beyond design basis scenario.

There is guidance presented in these documents on how to protect against an increase in reactivity that would lead to the potential for re-criticality.

6.2.5 Prevention of basemat melt through

6.2.5.1 Potential design arrangements for retention of the corium in the pressure vessel

This situation is considered to be beyond the design basis for an advanced gas-cooled reactor due to the low power density and other design provisions of the reactor. Nonetheless there are arrangements in place for the severe accident scenario.

The pressure vessel, due to its construction, provides the best means of long term containment of a degraded core. For the prevention of basemat melt through the critical safety function is containment and advice and recommendations are given in severe accident guidelines.

6.2.5.2 Potential arrangements to cool the corium inside the containment after reactor pressure vessel rupture

The possible arrangements to cool the corium inside the containment after reactor pressure vessel rupture would involve the use of the installed pressure vessel cooling water pipework system for the concrete pressure vessel or direct injection of water, as advised in severe accident guidelines.

A potential alternate strategy to cool the vessel is by passing water along the pre stress tendon ducts which pass through the concrete.

Advice and recommendations for alternate cooling strategies are also found in severe accident guidelines.

6.2.5.3 Cliff edge effects related to time delay between reactor shutdown and core meltdown

In an extremely unlikely scenario of inadequate cooling for a prolonged period, it is inevitable that fuel will melt and the core start to fail. The timescales for this to happen in an advanced gas-cooled reactor are considerably larger than for a pressurised water reactor allowing arrangements for the severe accident management plan to be implemented.

This time delay should leave sufficient scope for the adoption of cooling, utilising improvised methods as advised in the severe accident guidelines, to mitigate against any possible cliff edge effects.

6.2.6 for and supply of electrical AC and DC power and compressed air to equipment used for protecting containment integrity

6.2.6.1 Design provisions

The vessel is the third layer of containment after the fuel matrix and clad. The concrete structure and the steel penetrations provide a barrier to fission products. It would, though, be desirable to seal the breach which caused the depressurisation. To meet design basis standards, the vessel is reliant on its own cooling system and other core cooling systems which in themselves may be reliant on AC power supplies when pressurised.

If depressurised and without cooling, the vessel would still function as a passive containment. Studies have shown that, without cooling, the concrete structure would withstand self-weight loads for at least 14 days after excessively internal temperatures.

6.2.6.2 Operational provisions

The severe accident guidelines advise on protecting the containment provided by the vessel after depressurisation and significant fuel damage. Reinstating or preserving that part of the vessel cooling system for the penetrations would protect their containment function. The guidelines advises that in the event of loss of normal pumping systems, improvised use of fire pumps would restore adequate vessel cooling even if dried-out vessel cooling pipework has reached temperatures well above boiling.

Failing this, advice is given for removing outboard insulation from the penetrations and improvising cooling air-blast or water-spray.

6.2.7 Measuring and control instrumentation needed for protecting containment integrity

The central control room provides a single source of alarm and plant information for both reactors and turbine units and associated common plant.

Facilities are provided to monitor and control aspects of plant operation including reactor start-up and operation at power, trip, shutdown and post-trip cooling. The central control room also performs the duty of a communications facility in the event of an emergency.

An alternative indication centre provides a single area from which the status of the trip, shutdown and post-trip cooling of the two reactors can be monitored in the event of hazards that may have rendered the central control room untenable. The alternative indication centre receives a sub-set of the signals provided to the central control room which are buffered to ensure that damage to the central control room does not result in loss of signals to the alternative indication centre. Its uninterruptible power supply makes it independent of station supplies.

Instrumentation for Containment integrity

Instrumentation is required for all critical safety functions for protecting containment integrity. The pressure vessel is fitted with temperature, pressure and flow instrumentation.

Loss of electrical power to this instrumentation will cause the readings to be lost. Consequently, restoring electrical power to this instrumentation is incorporated in considerations detailed below.

6.2.8 Measures which can be envisaged to enhance capabilities to maintain containment integrity after occurrence of severe fuel damage

For the advanced gas-cooled reactor design, the timescales under which severe accident damage occurs is greater than for light water reactor where, in a similar accident, as shown by Fukushima, severe fuel damage occurs very quickly. This significant delay means that for a range of beyond design basis initiating events, either the symptom based emergency response guidelines advice on restoring cooling, or the severe accident guidelines advice on improvising cooling, is likely to be successful. For cases where cooling cannot be restored, they advise on maintaining or improvising containment of fission products released from the degrading fuel. In the guidelines there is also advice on blocking breaches in the vessel and on constructing an ad hoc filter.

In light of the events at the Fukushima Dai-ichi plant, as responsible operators EDF Energy have carried out reviews at each of the sites as a requirement of the Board.

The findings of the severe accident management aspects are discussed below on a fleet wide basis; this is because the learning from each of the sites is judged to be applicable across the stations

Scope

The beyond design basis review ensured that documentation, training and plant associated with response to beyond design basis events were reviewed, along with the adequacy of the emergency response organisation. Due to the nature of the questions asked as part of the reviews, this was primarily a paper-based exercise with workshops between station and central support engineers where appropriate. Equipment provided specifically for response to beyond design basis events was also physically inspected to ensure that the condition of the plant was as expected.

Summary of Findings

All advanced gas-cooled reactors have a suite of symptom based emergency response guidelines designed to manage a beyond design basis fault. The scope of these documents only covers the operating reactors at the site.

In addition, severe accident guidelines have been specifically designed to provide guidance for the management of events beyond the current design basis of the stations when a degraded core is likely or has occurred.

The severe accident guidelines have been developed through incorporating the understanding derived from both real events and dedicated research experimentation into a set of suggested mitigating actions in the event of a severe accident postulated on a generic basis.

There is the opportunity to improve the documentation and training provided for severe accident management using the experiences of the people in the Tokyo Electric Power Company (operators of the Fukushima Dai-ichi plant) as this is one of the very few events where such documentation has been used in a real situation.

Conclusion HRA 6.9: The robustness of the plant against design basis accident is considered to be appropriate; in considering the robustness to beyond design basis accidents, several areas have been identified where enhancement could be considered.

Consideration HRA 6.9: Consideration should be given to providing further mitigation against the effects of beyond design basis accidents. This could be provided by additional emergency back-up equipment. This equipment should provide additional diverse means of ensuring robust, long-term, independent supplies to the sites. This equipment should be located at an appropriate off-site location close to the station to provide a range of capability to be deployed in line with initial post-event assessment. This equipment may include the following capabilities:

- **Equipment to enable pressure vessel cooling.**
- **Supply of suitable inert gas for primary circuit cooling.**
- **Equipment to enable boiler feed.**
- **Compressed air supply for decay tube cooling.**
- **Electrical supplies for primary circuit coolant circulation.**
- **Equipment to enable fuel pond cooling.**
- **Emergency command and control facilities including communications equipment.**
- **Emergency response/recovery equipment.**
- **Electrical supplies for lighting, control and instrumentation.**
- **Water supplies for cooling from non-potable sources.**
- **Robust means for transportation of above equipment and personnel to the site post-event.**

Consideration HRA 6.10: EDF Energy should consider a review, extension and retraining for the symptom based emergency response guidelines.

6.3 Accident management measures to restrict the radioactive release

6.3.1 Radioactive releases after loss of containment integrity

6.3.1.1 Design provisions

Reactor shutdown systems, containment integrity and reactor cooling act together in order to ensure, as far as is reasonably practicable, fuel damage and fission product release do not occur.

In advanced gas-cooled reactor designs there are three barriers preventing the release of radioactivity into the atmosphere during steady state and transient operation; these are the fuel matrix, fuel clad and the pressure vessel.

6.3.1.2 Operational provisions

Emergency planning and actions will be put into effect and will have a major role to mitigate the consequences of a radioactive release.

For a severe accident, to restrict the radioactive release, the severe accident guidelines advise on repairing breaches, strengthening the vessel, and on improvising filters to remove fission products from released gases. Advice on strengthening the pressure vessel is aimed at preventing melt through of the basemat via penetrations, preventing failures of large numbers of penetrations as temperatures increase and blocking paths for activity release through concrete.

Loss of containment integrity would mean that there is a high probability of increased radiation levels off-site. Throughout an off-site nuclear emergency EDF Energy Nuclear Generation and independent experts will be utilising the information they receive to produce advice that will protect the public. The methodology for producing this advice is as follows. Emergency Reference Levels are part of Health Protection Agency – Centre for Radiation Chemical and Environment guidance. This agency provides guidance on introducing countermeasures in the early stages of an emergency and the emergency reference levels show what dose to an individual could be averted if the countermeasure is taken. These levels are based on dose saving and do not take into account the dose already accrued. There are different risks associated with each countermeasure depending on:

- the site location.
- the type of installation.
- conditions at the time of the accident.

For this reason, there are ranges of dose for the introduction of each countermeasure.

<u>The Lower Emergency Reference Level</u>

The Health Protection Agency – Centre for Radiation Chemical and Environment guidance recommends that countermeasures are not justified below this dose level. If the estimated averted dose exceeds the lower emergency reference level, then countermeasures would be justified but are not essential.

<u>The Upper Emergency Reference Level</u>

The upper emergency reference levels are set to avoid the deterministic (non-stochastic) effects of radiation. The Health Protection Agency recommends that, every effort must be made to introduce the countermeasure to avert the doses above the upper emergency reference level.

The most important exposure route after a release of radioactivity from a reactor is inhalation from radionuclide in the plume. It is not possible to measure directly what inhalation dose will result from a particular release in order to make a comparison with the relevant emergency reference level. Consequently, EDF Energy Nuclear Generation has derived simple, initial action levels – Derived Emergency Reference Levels based on the measurement of the concentration of activity in the air. These action levels enable EDF Energy Nuclear Generation to advise on, and implement, countermeasures as the lower emergency reference level of a countermeasure is exceeded. In the early stages of the response to a release, the Emergency Control Centre or Central Emergency Support Centre Health Physicist will use the EDF Energy action levels to advise on countermeasures.

The action levels are based on the total beta/gamma activity of air samples counted by equipment in off-site vehicles. Effective countermeasures are taken to protect the public. The basic principle of countermeasures is that they should be introduced if they are expected to achieve more good than harm in terms of radiation exposure averted the hazards associated with introducing the countermeasure. However EDF Energy Nuclear Generation takes a precautionary approach to protecting the public and agreement has been established with local Health Authorities authorising the Emergency Controller to advise the public to take potassium iodate tablets. The countermeasures of sheltering and taking of potassium iodate tablets will be automatically advised and introduced throughout the Detailed Emergency Planning Zone on the declaration of an off-site nuclear emergency.

The company will provide expert advice to the Strategic Coordination Centre, but the ultimate decision regarding implementation will be made by the Strategic Co-ordinating Group, who will be independently advised by the Government Technical Adviser.

Potassium iodate tablets are an effective countermeasure for releases involving radioiodine and can offer significant benefits even if they are taken after exposure. However, potassium iodate tablets are only relevant to the thyroid radiation exposure, and are only useful if the thyroid is not already saturated with iodine. Stable iodine will not replace radioiodine that is already in the thyroid, but acts to dilute further uptake. Each nuclear power station holds stocks of tablets for staff and contractors. Tablet manufacturers and the National Health Service also carry reserve stocks on behalf of EDF Energy. As well as the pre-distributed tablets to the public living in the Detailed Emergency Planning Zone the local Health Authority holds stocks of tablets for the public and they are responsible for arranging distribution of potassium iodate tablets to the public.

6.3.2 Accident management after uncovering of the top of fuel in the fuel pool

The advanced gas-cooled reactor fuel routes currently have no severe accident guidelines for accidents involving the fuel route. Instead, operator actions required following receipt of alarms or in the event of an emergency are documented in the station administrative controls / linking documents. These actions are implemented using station operating instructions.

The two fuel route facilities of greatest potential fault consequence are the buffer store and the ponds, as these contain the largest quantities of irradiated fuel and require continual provision of active safety functions (principally cooling). Safety cases present evidence demonstrating that the design of plant, and the methods of operation, protect against and mitigate the consequences of faults. These faults can be categorised as either loss of cooling or loss of containment faults. In accordance with the fuel route documentation, the protection and mitigation features allow the buffer stores and ponds to retain the essential functions of cooling and containment of fuel.

Even with a pessimistic decay heat loading, it will take a number of days for the pond water to reach boiling. In reality, timescales will be significantly longer as the actual decay heat loading is lower, and heat losses to the environment will reduce the rate of temperature rise. Once boiling has initiated, it will take several more days before boil-off reduces the cover over the fuel to a level where radiation levels in the pond building have a major impact on operations

6.3.2.1 Hydrogen management

Advanced gas-cooled reactor fuel elements comprise UO_2 fuel pellets clad in stainless steel (not Zircaloy) to form fuel pins, and arrays of these fuel pins are housed with graphite sleeves. There is no threat of hydrogen evolution from advanced gas-cooled reactor fuel housed in the ponds until a temperature threshold is reached. Achieving this limiting temperature for hydrogen evolution is not considered credible.

6.3.2.2 Providing adequate shielding against radiation

6.3.2.2.1 Buffer Stores

<u>Dose rates</u>

The buffer stores are situated within a massive concrete structure, with no reliance placed on the cooling water inventory for shielding. Therefore, even with the tubes boiled dry there is no significant threat from direct radiation shine.

<u>Criticality</u>

The margins to criticality for the buffer store will not be degraded by boiling dry of the water jacket.

6.3.2.2.2 Ponds

<u>Dose rates</u>

The pond civil structure should provide significant shielding in the lateral direction, even with the loss of water. However, in the vertical direction (and with shine at an angle) dose rates around the pond area would become very high once the fuel is uncovered. Installed radiation monitoring would provide warning well in advance of this approaching situation providing it remained functional. Existing analysis suggests that once water levels reach ~1m above fuel, the dose rate adjacent to the pond would start to become hazardous. There are several metres of water above the fuel which would take several days to boil off. This would allow sufficient time for activities to restore cooling or make-up to occur.

Criticality

The vast majority of fuel in the pond would be both highly irradiated and stored in skips designed to prevent criticality excursions. It is not judged credible that fuel in skips in the pond could become critical. If the water remaining in the pond becomes diluted by preceding attempts to maintain water levels (and hence contain little or no boron-10), there is only the potential for a criticality excursion if the fuel is low or un-irradiated. However as almost all fuel in an advanced gas-cooled reactor pond will always be highly irradiated, the criticality risk can essentially be discounted.

If the water were lost completely, there would be no criticality hazard, as there would be insufficient moderation to create a critical assembly in any fuel configuration.

The use of seawater to maintain water levels would have no impact on criticality safety.

Wider impact on dose rates

There is only very limited ranges on-site where there would be an impact on doserates due to uncovering of fuel in the pond due to its situation within a large reinforced concrete structure.

Recovery of shielding

In order to restore effective radiation shielding, particularly local to the pond area, it is necessary to restore the pond water level. There are a number of engineered means of providing make-up water to the ponds. Ad-hoc means of restoring cover to the fuel using the fire hydrant system / flexible hoses might be possible. These methods are likely to be difficult due to the high dose rates, and might require the water to be added indirectly by flooding / spraying into an adjacent (accessible) area that is connected to the ponds.

6.3.2.3 Restricting releases after severe damage of spent fuel in the fuel storage pools

6.3.2.3.1 Buffer Stores

The sub-pile cap contaminated ventilation system would help mitigate any possible release from the buffer store, assuming that the system remains functional or can be put into service.

In the extremely unlikely event of clad melt, the fuel would fall into the buffer store vault. The vault is a massive concrete structure, and it is judged that the fuel should be contained within the vault. The vaults provide containment (are not open to the atmosphere) and in most cases are fitted with contaminated ventilation systems. It may be possible to introduce cooling to the vault, either by forced air cooling or flooding the vault.

6.3.2.3.2 Ponds

In the extremely unlikely event that the pond water level has dropped sufficiently to uncover fuel this could result in elevated fuel temperatures. The primary mitigation for activity release from fuel in the pond is the contaminated heating and ventilation systems. These systems are designed to capture the vast majority of particulate and molecular activity sources. Sealing of leak paths from the building would also be beneficial in reducing releases, as well as restoring water cover to the fuel, as this provides both cooling and some containment. If it is not possible to re-fill the ponds, then even a water spray (deluge) would be beneficial.

6.3.2.4 Instrumentation needed to monitor the spent fuel state and to manage the accident

6.3.2.4.1 Buffer Stores

Primary indications for the buffer stores are temperature and pressure.

For severe faults, it is judged that the most resilient and direct means of monitoring would be to use the coolant gas temperature thermocouples which are fitted to the fuel assemblies, as these provide a direct measure of condition of the fuel via the local gas temperature.

6.3.2.4.2 Ponds

Primary indications for the ponds are of water level and temperature. There are various installed means of indications, which can be manually backed with level markings (visual inspection) and hand held-temperature monitoring.

In very extreme circumstances beyond the design basis there is the potential that installed equipment would not function correctly and portable monitoring equipment would need to be relied upon.

6.3.2.5 Availability and habitability of the control room

6.3.2.5.1 Buffer Stores

Loss of buffer store cooling and fuel damage will not directly affect the Central Control Room.

6.3.2.5.2 Ponds

The pond control room is likely to be uninhabitable if there is a considerable reduction in water level (close to uncovering the fuel) due to high radiation levels. In the event of boiling of the pond, there may also be issues regarding habitability due to ingress of steam. This would present additional challenges to accident management but it should be noted that the requirement for access to the pond control room would be low.

6.3.3 Measures which can be envisaged to enhance capability to restrict radioactive release

Measures which can be envisaged to enhance capability to restrict radioactive release are considered below.

Conclusion HRA 6.10: The robustness of the pond against design basis accidents is considered to be appropriate; in considering the robustness to beyond design basis accidents, several areas have been identified where enhancement could be considered. It should be noted that for the AGR design there are additional fuel route plant areas, measures to enhance robustness in these areas have been considered in Chapter 5.

Consideration HRA 6.11: Consideration should be given to providing further mitigation against the effects of beyond design basis accidents by the provision of additional emergency back-up equipment. This equipment could provide additional diverse means of ensuring robust, long-term, independent supplies to the ponds. This equipment could be located at an appropriate off-site location close to the station to provide a range of capability to be deployed in line with initial post-event assessment. This equipment may include the following capabilities:

- **Equipment to enable fuel pond cooling.**
- **Emergency command and control facilities including communications equipment.**
- **Emergency response/recovery equipment.**
- **Electrical supplies for lighting, control and instrumentation.**
- **Water supplies for cooling from non-potable sources.**
- **Robust means for transportation of above equipment and personnel to the site post-event.**
- **It would be appropriate, if this equipment was developed and in any case to capture learning from events in Japan to review and where necessary revise the documentation and training provided for severe accident management in the fuel route plant areas.**