EU Stress Test

Heysham 2

Save today. Save tomorrow.

edfenergy.com

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	Advance Gas-cooled Reactor
AOD	Above Ordnance Datum
ASME	American Society of Mechanical Engineers
CEGB	Central Electricity Generating Board
DC	Direct Current
DEFRA	Department for Environment, Food and Rural Affairs
ECC	Emergency Control Centre
EDF	Electricity de France
HYB	Heysham 2
IAEA	International Atomic Energy Agency
IPCC	Intergovernmental panel on Climate Change
ONR	Office for Nuclear Regulation
PGA	Peak Ground Acceleration
PML	Principia Mechanica Ltd
PWR	Pressurised Water Reactor
URS	Uniform Risk Spectrum
TOR	Torness
WANO	World Association of Nuclear Operators

Executive Summary

Heysham 2

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 2011 with the final report published in September 2011. The report 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 Heysham 2.

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. 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".

The EU Stress Test Reports also raise 'considerations': these are defined as 'Opportunities to further examine potential enhancements to plant, process or people for beyond design basis scenarios'.

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 line2 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, the Pressurised Water Reactor was based on the Standard

[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

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.

Summary of findings for earthquakes at Heysham 2

Chapter 2 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 years. There are also discussions on the margin to failure of this equipment. It demonstrates that:

- The design basis earthquake was defined using an extensive study of historical earthquakes and local geology. It corresponds to an infrequent event.
- 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, most recently in 2002, 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 an infrequent seismic event.
- Suitable processes are in place to ensure the plant remains compliant with its licensing basis.
- No cliff-edge effects are expected for events only slightly beyond 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 the frequent design basis earthquake. 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 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 out with the scope of this report.

Summary of findings for external flooding at Heysham 2

This Stress Test report assesses the margins of the existing design basis, as well as the flood protection in place at Heysham 2 Nuclear Power Plant. It demonstrates that:

- At Heysham 2, the bounding external flooding case is due to wave overtopping the seawall. The maximum sea level for an infrequent event is 7.63m AOD, and the site threshold level is 8.85m AOD separated from each other by the wave wall at 9.84m AOD.
- Sufficient margin exists between the maximum design basis flood (7.63m Above Ordnance Datum (AOD)) and the physical elevation of the main nuclear island (9m AOD).
- 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
- During extreme rainfall events it is demonstrated that essential function availability is maintained by the site drainage and the natural fall of the land towards the sea.
- The information presented below shows that the methodology used to calculate the design basis flood for Heysham 2 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 focussed at providing additional plant protection for a beyond design basis flooding event.

Extreme Weather

In the Office for Nuclear Regulation's 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 section of the Stress Test 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 1 in 10,000 years 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 Heysham 2

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 hazard (which is outside the scope of this review).

The design basis for an infrequent extreme wind is based on demonstrating that buildings conform to relevant standards and codes for an infrequent event. Equipment required to fulfil the essential safety functions is either located inside buildings which are qualified against infrequent wind, or qualified directly.

Summary of findings for extreme ambient temperatures at Heysham 2

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.

The infrequent extreme ambient temperature hazard can be split into the following events; high and low air and sea temperatures and snow loading. The design basis for the high and low air temperatures has not been verified and a consideration is raised in this Stress Test to do so. 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. Sea water temperature is primarily a commercial concern and changes in temperature will not impact nuclear safety. The reactor buildings and others containing essential equipment have been assessed against snow loading and demonstrate sufficient margin.

Summary of findings for lightning at Heysham 2

This section considers 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. Lightning Electro-Magnetic Pulse (LEMP) affects are addressed as part of that Electro-Magnetic Interference / Radio Frequency Interference hazard and are not considered here.

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.

Summary of findings for drought at Heysham 2

This section considers 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.

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

Combinations of hazards at Heysham 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 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 an infrequent (return frequency of 1 in 10,000 years) 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.

Loss of 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 (leading to a threat to post trip cooling), including an evaluation of times and actions 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 backup supply leading to a 'station black out' scenario, where all 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.

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

Summary of findings for loss of electrical power and loss of ultimate heat-sink at Heysham 2

- Loss of off-site power is an event considered within the Heysham 2 safety case and there are sufficient fuel stocks for the backup onsite AC generation to continue operating under required load for an extended mission time beyond 24 hours supporting the essential safety functions.
- During station black out, the back up battery supplies are not required to provide boiler feed in the long term.
- There are provisions off-site that can be deployed to station in 10 hours that would provide power generation capability and aid 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 accident management.
- 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.
- The current robustness and maintenance of the plant is compliant with its design basis for loss of electrical power. However, steps to improve the resilience of the plant following a beyond design basis event are being considered.

- Several means of preventing the loss of reactor cooling water (by blockage of the water intakes) are employed at Heysham 2 including drum screens.
- Diverse alternative heat sinks for primary circuit cooling (boiler feed) and essential equipment cooling exist in case of loss of the primary ultimate heat sink i.e. the sea – this is covered by the existing safety case. Also there are sufficient stocks of cooling water for a minimum period of 24 hour.
- The current robustness and maintenance of the plant is compliant with its design basis against loss of electrical supplies and ultimate heat sink. However, steps can be made to improve the resilience of the plant for a beyond design basis event.
- In either the event of both loss of grid or station black out, sufficient cooling can be maintained to the station fuel handling 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.
- In the event of loss of the ultimate heat sink there is adequate alternative heat sink provision available to the station fuel route.
- Whilst there are no vulnerabilities identified in the current design basis for the fuel route against loss of ultimate heat sink, further resilience enhancements can be envisaged.

Severe Accident Management

In the ONR Interim Report into the Japanese Earthquake and Tsunami, the report 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.

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

Heysham 2

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 2011. The interim report 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 of 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 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.

[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.

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 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

[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.

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

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 operating rules 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 operating rules also include actions to be taken if they are not met.

The Operating rules 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 the operating rules as being allowed to exist for consecutive period of 31 days.

(ii) The ‘urgent maintenance’ state, as defined in operating rules, 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.

[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.

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:

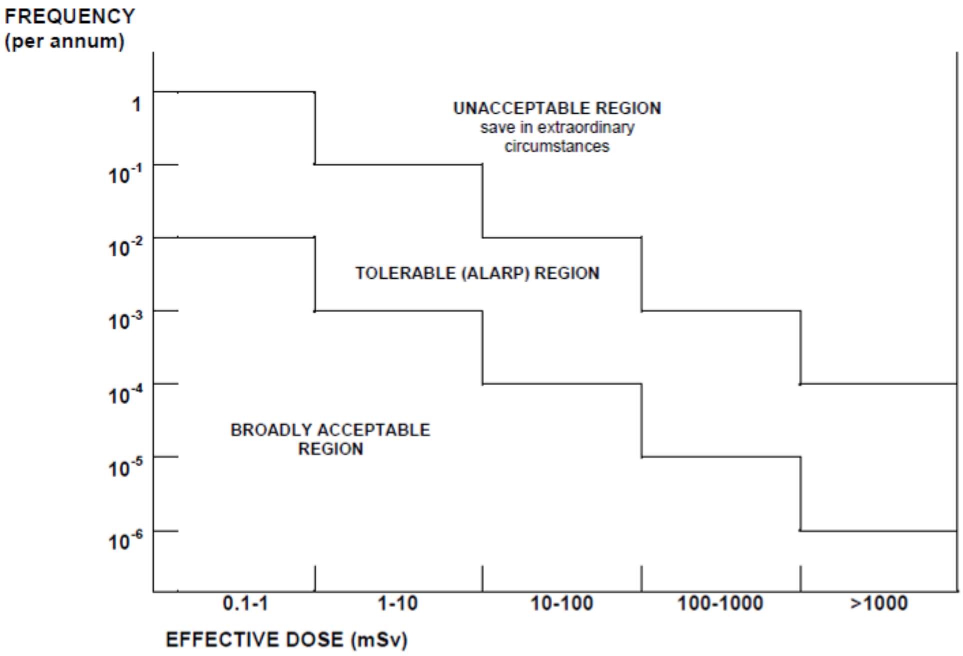

Figure 0.2: Surrogate risk regions as a function of frequency and effective dose.

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 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

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

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 Heysham 2

Heysham 2

1 General Data about Heysham 2

1.1 Brief Description of the site characteristics

Heysham 2 (HYB) is a twin Advanced Gas Cooled Reactor (AGR) located in Heysham, Lancashire. Heysham is a large coastal village near Lancaster in the county of Lancashire, on the North West coast of England. Overlooking Morecambe Bay, it is a ferry port servicing the Isle of Man and Ireland. Heysham is situated within the Morecambe Coast and Lune Estuary National Landscape Character Area No31. Heysham is situated on the eastern side of Morecambe Bay, with the town of Morecambe and the Lake District National Park to the north and the city of Lancaster to the North West. The landscape of this area is characterised by an undulating coastal strip adjoining a flat lowlands before ascending into wooded escarpments to the east. Saltmarshes are a valued landscape character feature on the Morecambe Coast and Lune Estuary and are one of the distinguishing characteristics of the national landscape character area. The Heysham site is located on non agricultural land. The soils and geology comprise Made Ground over tidal flat deposits, underlain by the Sherwood Sandstone Group and Eldroth Grit.

The Heysham site, despite its relatively local isolation, is supported by relatively good transport systems. Strategic transport routes in the North West are dominated by the M6 (north-south) and the M61, which provides links to Manchester and the east. Heysham is served by the A589 and A683, which are identified as routes of regional importance.

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

The Morecambe Bay estuarine system is of particular note. It has numerous international designations associated with it, including the Morecambe Bay Special Area of Conservation (SAC), the Morecambe Bay Special Protection Area (SPA) and the Morecambe Bay Ramsar wetland site.

The main west coast rail line also serves the area, proving recently upgraded services to the south and to Scotland. However the railway to Heysham is a single track and only for transport of passengers and nuclear waste, it may be unsuitable for regular industrial traffic.

Construction commenced on 1 August 1980 and first criticality occurred in July 1988. End of generation is currently scheduled for 2023.

Figure 1.1 Location of Heysham 2 Power Station

Heysham 2 is operated by the licence holder, EDF Energy Nuclear Generation Ltd, a subsidiary company of EDF Energy plc. The Heysham 2 plant with its two reactors adjoins Heysham 1 power station, also a twin unit AGR station operated by EDF Energy Nuclear Generation Ltd.

1.2 Main characteristics of the unit

Heysham 2 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 Prestressed Concrete Pressure Vessel (PCPV).

Table 1.1 Specific details of Heysham 2.

	Reactor 7	Reactor 8
Reactor Type	Commercial Reactor	Commercial Reactor
Model	AGR	AGR
Vendor	National Nuclear Corporation (NNC)	National Nuclear Corporation (NNC)
Owner	EDF Energy	EDF Energy
Operator	EDF Energy	EDF Energy
Capacity Net	605 MW	605 MW

Table 1.2 Construction and Operation details for Heysham 2.

Start Construction	July 1980	July 1980
Criticality	July 1988	November 1988
Grid Connection	September 1988	December 1988

1.3 Systems for providing or supporting main safety functions

Reactor Systems

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 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 pressures are 30bar to 40bar.

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 by 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 1100 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.

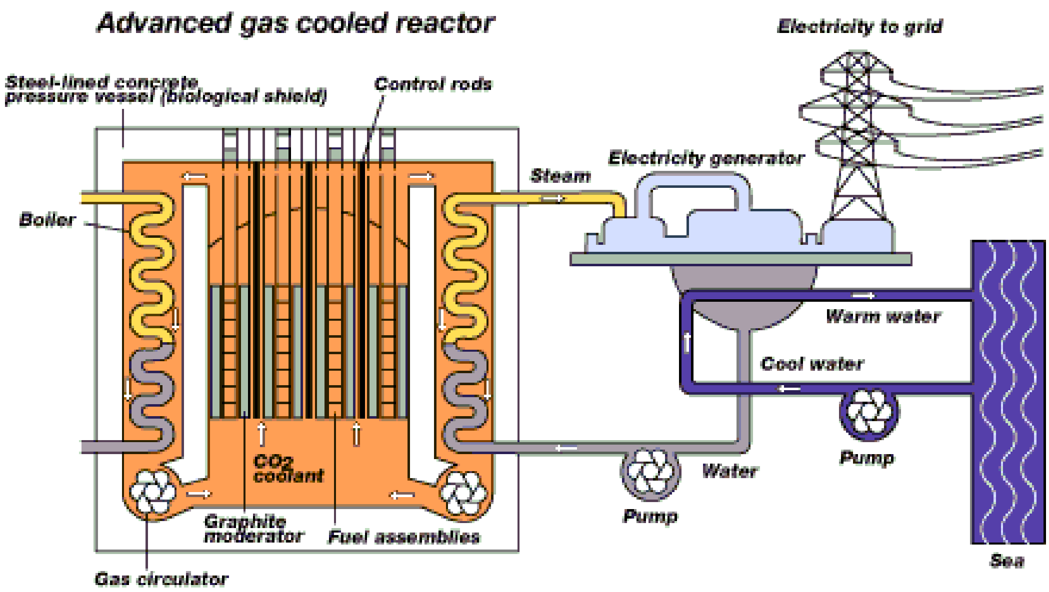

Figure 1.2: Simplified AGR showing internal components and the ultimate heat sink

<u>Fuel Handling</u>

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 at low power, or off load but pressurised in CO_2.

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

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 shut down even if for any reason insufficient rods in the primary shutdown system insert into the core. At Heysham 2 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.
- At Heysham 2, tertiary shutdown is provided to maintain the reactor in its shut down state in the long 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.

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. Compliance with 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 inflammable 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 sea water cooled condensers where the remaining heat is removed i.e. the sea is used as the primary ultimate heat sink.

Following a reactor trip, decay heat removal is via the main boilers, and then decay heat boilers with each being fed with feed water from either the main feed system or the backup feed system respectively. The steam generated in the boilers by decay heat is either returned to the main condenser or the decay heat system condenser vent (whereby the atmosphere is used as an alternative heat sink).

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

The process of removing decay heat is known as Post-trip Cooling. Providing the pressure vessel is intact, 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 feed water 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 feed water systems. All AGRs have at least two diverse post-trip feed water systems with redundancy and diversity in their electrical supplies to carry out this function.

If the reactor pressure vessel is de-pressurised then the fuel can be cooled by forced gas circulation and feed water supplied to the boilers.

The design basis safety cases are supported by the availability of at least 24 hours worth of stocks (e.g. diesel, carbon dioxide, feed water). 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 a number of active systems to be shut-down and standby systems to be started. This process is automatically initiated by a combination of systems. The automatic stopping and starting of the necessary post-trip cooling equipment is designed to be complete in a matter of minutes following a reactor trip. The standby equipment is supported by electrical supplies from either the grid or a number of different diverse, redundant and segregated sources of onsite backup AC electrical power.

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 by the grid. If the grid becomes unavailable, forced circulation is backed up by onsite backup AC electrical supplies.

Natural circulation of the primary coolant does not require gas circulators.

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. The minimum allowable amount of stored CO_2 is sufficient to re-pressurise one reactor while providing pressure support to the other reactor for a 24 hour period. In practice the station usually holds greater than the minimum stock levels.

Secondary Coolant Systems

In normal operation the secondary coolant system comprises main boiler feed water pumped from the condenser through several stages of feed-heating to the deaerator and the boilers, together with steam flows from the boilers to the turbine. Following a reactor trip, the main boiler feed pump is tripped and feed is normally provided by the electric start and standby boiler feed pumps until the decay heat system is operational, note that the decay heat boilers are totally diverse from the main boilers. After each reactor trip, the backup boiler feed pumps (with high redundancy) start automatically and are available to provide feed to the main boilers, should the start and standby boiler feed pumps be unavailable. Note that forced circulation on the start and standby boiler feed pumps, backup boiler feed pumps supplying the main boilers or the decay heat boiler system are all capable for providing sufficient post trip cooling.

A diverse backup boiler feed system is designed to operate whenever a reactor is shutdown to remove and dissipate the decay heat produced. There is one diverse backup boiler feed system per reactor and each is designed to remove and dissipate decay heat from the reactor once it has been tripped. This system consists of a primary heat removal circuit (decay heat boiler feed system), together with a secondary air-cooled heat dissipation circuit (decay heat boiler air cooling system).

Boilers

The boilers are located within the reactor pre-stressed concrete pressure vessel in the annulus between the gas baffle and the liner wall. The boilers are of the once-through sub-critical type, so as to minimise the number of pressure vessel penetrations. The boiler annulus is partitioned into four quadrants, each containing three rectangular boiler units and a pair of gas circulators.

Hot gas from the reactor core is drawn down over the banks of boiler tubing by the gas circulators, which are located underneath the boilers in the bottom of the annulus. The gas is constrained to flow down over the banks of boiler tubing by the casing, which surrounds each boiler unit, and by the gas seals that form a floor across the annulus around the base of the boiler casings, just above the circulators. The feed water tailpipes to the boilers pass through penetrations in the walls of the concrete pressure vessel and enter the unit casing from below, while the superheated steam outlet tailpipes pass out through penetrations level with the top of the casing.

The boilers play a major role in the safety of the reactor in that they are the principal means of removing the heat produced within the reactor while at power and following a reactor trip. At Heysham 2, an additional, much smaller, decay heat boiler is installed beneath the main boiler. This provides a diverse post-trip cooling system and is served by completely independent feed and steam systems.

Auxiliary Cooling Water Systems

The operational duty of the main circulating water system is to remove heat from the turbine condensers whilst at power, and this system has little safety significance.

The pressure vessel cooling system provides cooling to the pressure vessel liner and penetrations to maintain safe temperature levels in the pre-stressed concrete and tendons of the reactor pressure vessel when the reactor is at power. It also provides cooling for the fuel pond, the decay store and the spent fuel disposal cells. Heat removed by the pressure vessel cooling system is rejected to the reactor sea water system.

The circulator auxiliaries cooling system provides cooling to maintain the gas circulator motor winding and bearing temperatures within design limits and rejects heat to the reactor sea water system. Following a reactor trip, heat may be rejected to either the reactor sea water system or the air cooled circulator auxiliaries diverse cooling system.

The diagrid support skirt cooling system provides cooling to the lower section of the core support to reduce fatigue due to reactor temperature cycling.

The pond cooling system removes the decay heat generated by stored fuel elements to maintain acceptable pond water temperatures. The heat is rejected via the pressure vessel cooling system and then the reactor sea water systems.

Cooling Water Systems

Main Cooling water

The purpose of the main cooling water system is to provide adequate, circulating, seawater to various items of plant (including the turbine condensers). The system has no specific safety duty.

Seawater Cooling Water

This system provides cooling water to essential items of plant and maintains this supply post-trip to ensure reactor safety. It also provides the ultimate heat sink for fuel route cooling. The seawater cooling system comprises a recirculating loop which cools the plant coolers and an open loop which removes heat from the recirculating loop.

The system design is to provide a safety related, continuous demand (though with plant status determining heat loading) cooling system with redundant pump capacity and cooling capacity that feeds supported systems which are systematically divided into two half systems. The system must provide cooling to all the essential systems it serves, both at power and post-trip. Sufficient supplies of cooling water to cool the intermediate system for post-trip cooling of both reactors is possible by operation of one half-system of the loop.

Equipment cooled by the seawater cooling system includes: Gas circulators (lubricating oil coolers), vessel cooling systems, feed pumps, and the cooling pond.

Reserve feed water tanks

Feedwater for the backup boiler feed pumps is provided from the three reserve feedwater tanks which are provided for each reactor. Make-up to the reserve feedwater tanks, or the establishment of a recirculatory route for the main boilers, is possible to ensure long-term feed stocks.

Townswater

The purpose of the townswater cooling system is to provide cooling water for that plant for which seawater is unacceptable as a cooling medium. The heat sink is the seawater cooling water system. Systems cooled by the townswater cooling system include:

- Fuel handling facilities (cooling);
- Boiler feed pumps (back-up feed stocks).

The townswater system is required to provide cooling for the essential systems it serves, both at power and post-trip. The system has been designed with a degree of redundancy by the duplication of pumps.

1.3.2.2 Layout of Heat Transfer Chains

Plant systems which support primary coolant heat transfer are generally located close to the primary circuit although there are some systems, for example the seawater cooling water and back-up cooling water which both support forced circulation cooling, which are located outside of the reactor building. Similarly, it may be appreciated that electrical supplies to support forced circulation (power to circulator motors and power to auxiliary cooling systems) will also originate externally to the reactor building. This applies to grid-based and on-site generated AC electrical supplies. 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 buildings; the boilers are located within the primary circuit pressure vessel. The water storage tanks for the various feed systems are outside of the reactor building.

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 off-site power supplies are available, not only are electrical supplies supported without time constraints – main boiler feed water may also be re-circulated. The decay heat boiler system is also recirculatory and requires neither off-site electrical supplies nor the sea as an ultimate heat sink. A continued loss of off-site power supplies and post trip cooling using the main boilers as the secondary heat transfer surface is likely to require reactor heat transfer to be supported by consumable water supplies and consumable fuel supplies.

Table 1.3 Heat Transfer Time Constraints

Feedwater Source	Timescale	Comments
Reserve feedwater tanks	The specified reserves for these systems are sufficient for about 12 hours (these can be topped up to extend this) forced or natural primary coolant circulation post-trip cooling.	If off-site power is available, and recirculatory flow of secondary coolant can be established, there is no time limit associated with feed provision. The decay heat boiler system is recirculatory and can function without off-site power supplies. In terms of providing post trip cooling via the decay heat boiler system, there is no limit associated with feed provision.

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

The design of Heysham 2 addresses diversity within its heat transfer chains via the provision 2 diverse trains of onsite backup AC supply systems, diverse primary coolant circulation (Natural and forced circulation) and ultimate heat sinks (sea water and atmosphere). These systems exhibit diversity, redundancy and segregation as far as is reasonably practicable.

It may also be appreciated that the existence of the petrol driven additional back-up boiler feed system offers a diverse means of providing secondary coolant circulation from the other feed systems at Heysham 2, all of which are reliant on electrical supplies albeit from separate train supplies. Similarly, natural circulation of the primary coolant is a diverse alternative to forced primary coolant circulation using the gas circulators; the latter also having a dependence on electrical supplies.

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 air) 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.

Table 1.4 Heat transfer chains

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	Air flow driven by cooling system (once-through)	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-jacket and once-though seawater circuit	Once-through sea water cooling system
Ultimate heat sink	Ambient air	Sea (also with provision for an air heat sink)	Ambient air / 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:

Table 1.5 Loss of cooling scenarios

Stage of fuel storage and handling	Handling with fuelling machine	Buffer storage	Dismantling	Storage in ponds
Potential impact of loss of cooling	Not credible, entirely passive	Boiling of water in the secondary circuit followed by overheating of fuel	If loss of both forced air flow and water-jacket, an emergency water injection system means 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	Requirement to initiate water injection to submerge fuel (passive gravity feed system)	Boiling of pond water
Minimum time to reach safety limit	n/a	Not less than 24 hours for the hottest fuel	Within 6 hours of loss of both air flow and water jacket cooling.	Not less than 48 hours for the hottest fuel

It should be noted that the assigned safety limit for storage in the ponds is boiling of the pond water. After boiling commences it will take some time for the water level to reduce by evaporation and there is no threat to fuel integrity provided that adequate water cover can be maintained. Potential for deterioration of the pond concrete due to high water temperatures is under review to ensure that system capability for topping up the pond is adequate in extreme circumstances.

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 AGRs 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 AGR concrete pressure vessel together with the large mass of graphite in the core provide 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 the boilers. Its concrete walls act as a biological shield so that the radiation levels outside the pre-stressed concrete pressure vessel are minimal. A steel liner forms a gas-tight membrane on the inside to maintain an integral pressure boundary with the many penetrations.

These penetrations, amongst other things, allow water to enter the boilers and steam to exit as well as provide routes for instrumentation and refuelling operations.

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.

A dedicated cooling system serves the pre-stressed concrete pressure vessel. 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 this cooling system is the sea, via the reactor seawater cooling 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 potential for damage from high temperatures.

1.3.5 AC power supply

Electricity produced by Heysham 2 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 AC electrical power generators.

The reliability of on-site power is assured by providing sufficient independence and redundancy of 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 1.6 Further details on plant required to provide essential safety functions

System	Seismic Qualification	Fuel Provision	Water Provision
3.3kV Generators: X-Train	System designed to function following a seismic event	80 hours (full power, all 4 generator X-trains) *	No water used
3.3kV Generators: Y-Train	System designed to function following a seismic event	60 hours (full power, all 4 generator Y-trains) *	No water used
Petrol-driven Back-up Emergency Feed pumps	System is not qualified to function following a seismic event	At least 12 hours	At least 12 hours (running time)

* Note that these timescales for generators runs are for full power operation of ALL generators at the same time. These timescales are based on the fuel oil supplies normally held on-site (full tanks). However the times do not account for run-down of supplies to match demand, which will result in significantly longer run-times.

1.3.5.1 Off-site power supply

Off-site power supplies connect to the Heysham 2 site via the 400kV and 132kV substations.

The Heysham 400kV substation is an outdoor switching and transforming station that is an important link in the National Grid 400kV supergrid system. It connects the generators at Heysham 1 and 2 to the supergrid system. It comprises a double busbar arrangement with four sections of main busbar and two sections of reserve busbar. The 400kV circuit breakers connect the Grid to Turbine Generators 7 and 8.

The connections between the 400kV substation and the generator transformers are via twin steel cored aluminium overhead lines for about 1.85km and then by single core, paper insulated, oil filled cables for the final 250 to 300 metres to the respective generator transformer.

The Heysham 2 132kV substation is an outdoor switching station situated adjacent to and derived from the 400kV substation and within the same security fence.

The connections between the 132kV substation and the Station Transformers is via 3-core oil filled cables following a diverse underground route on the opposite side of Heysham 2 power station to that followed by the 400kV lines.

1.3.5.1.1 Off-site power supply reliability

Weather effects represent the dominant contribution to the risk of loss of off-site power at Heysham 2, on the basis of evidence of faults that have affected Heysham and all EDF Energy power stations over the years since commissioning.

The table below presents loss of off-site power events which have occurred at Heysham 2.

Table 1.7: Loss of off-site power events at Heysham 2

Date	Time	Duration	Reactor Trip	Description
25/12/97	07:37	3 hrs 30 minutes (total) 07:37 for 18 mins 09:02 for 5 mins 10:36 for 26 mins	Yes	The coast of Lancashire was hit by severe storms on Christmas Day 1997. The strong winds blowing off the sea caused salt deposit on the insulator stacks on the 400kV substation located about 1km from the Heysham Power Stations. The deposit caused many trips of the 400kV transmission lines in the Heysham area. This eventually led to the tripping of both Heysham 2 reactors; reactor 7 at 05:29 hours and reactor 8 at 07:37 hours due to faults on overhead lines connecting generator transformers to the 400kV substation. More importantly, the event at 07:37 hours caused a total loss of grid supplies to the Heysham 2 site. The site was without a reliable grid supply for 3.5 hours. Full restoration of normal supplies was deliberately delayed until the grid was proven to be dependable. As a result the diesel generators supported the station essential systems for the rest of the day. Supplies were restored to normal by the night shift 25/26 December after some 15 to 18 hours.
12/11/10	15:34	2 minutes	Yes	Difficulties were experienced with the grid system external to the station between 15:34 and 15:36, at which time the central control room staff noted that the Unit 7 generator had become isolated from the grid system and indications showed no generated output. Multiple alarms were received and it was agreed that the unit should be manually tripped. This was carried out at 15:37. The reactor was safely shut down, all rods inserted and adequate post trip cooling was provided by the automatic protection systems. Following the rectification of post-trip defects, Unit 7 was resynchronised to the grid at 18:15 on 17 November 2010.

There has only been one loss of offsite power event (i.e. total disconnection) at Heysham 2 over the review period (see above table). This event occurred on 25th December 1997 when gale force winds caused a total of 22 faults around Heysham. At 07:29 on December 25th 1997 there was only a single circuit in service and the Heysham 2 control desk personnel were instructed to manually restore the Heysham-Stanah-Penwortham 2 circuit to service, but were unable to accept the instruction until 07:36. However, before the switching could be undertaken a busbar fault at Heysham severed the direct connection from Unit 8 at Heysham 2 to the remainder of the system. The only connection was via the two grid supply transformers and the 132kV substation, but the excessive power flow through these grid supply transformers resulted in both transformers tripping. As a result all supplies were lost to Heysham 2 unit and station boards, and to Heysham 1 unit 2 unit board.

A partial loss of offsite power occurred on 27th December 1998, again during severe winds. Salt contamination of the transmission system caused a flash over on an overhead line insulator stringer between Unit 8 Generator Transformer and the sub-station, resulting in a loss of the 400 kV grid connection to Generator Transformer 8. The fault was subsequently found to be a displaced arcing horn shorting on an insulator stringer. A number of single and double transmission line faults have occurred, including a double circuit fault caused by a suspected double lightning strike on 29th December 2001, and a double circuit fault caused by pollution on 18th January 2007. The report notes that there have been relatively few single circuit faults between the periods 1999 to 2009 compared to the previous 18 years.

Loss of off-site power is recognised within the station safety case as a frequent initiating event with an overall frequency in the region of 10^{-1} per annum. In the case of reactors operating at power, there are redundant and diverse systems to detect the initiating event and trip the reactor(s). Reactor shutdown is also not reliant on off-site power. Post-trip cooling requires the provision of both primary and secondary coolant flow. Natural primary coolant circulation together with feedwater flow to the boilers (requiring electrical power) is effective although forced primary coolant flow (also requiring electrical power) is the design intent. Following the event of 25th December 1997 shown in Table 1.7, forced primary coolant circulation was established via electrical power derived from on-site diesel generators.

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

Unit and Station Transformer locations are as shown below (see figure in Section 1.3.5.2).

Table 1.8: High voltage transformer locations at Heysham 2

Transformer	Location
Station Transformers	Outdoors in dedicated transformer compounds
Unit Transformers	Outdoors in dedicated transformer compounds

Although it is judged that the underground cable routes are robust against seismic and flooding events, the switching compounds are not qualified against seismic events or extreme high winds. This is not a requirement of the safety case since it is assumed that off-site power supplies would be lost following such initiating events.

1.3.5.2 Power distribution inside the plant

The electrical supplies may be divided broadly into two parts, the main electrical system (i.e. non-essential supplies where supplies are lost when the grid fails), and the essential electrical system where provision is made for continued electrical supplies after loss of grid (either with no break, or after a short interruption for plant that will accept this). Key aspects of the essential electrical system are addressed in Section 1.3.5.3 although it may be appreciated that much of the electrical equipment may be in operation in both a 'non-essential' and 'essential' capacity.

The important items powered by non-essential supplies are the start/standby feed pumps, used as one of the systems for feeding the main boilers post trip, and the main cooling water pumps and condenser extraction pumps which are used when the main condenser is acting as a heat sink during long term operation of the main boilers post trip. The 11 kV switchboards also power the gas circulators during reactor power operation. Thus the grid supply has an important role to play in the safe operation of the reactors, and is the preferred choice of supply to all reactor essential systems.

For all reactor trips and all turbine-generator faults (other than short circuit faults in the generator unit protection zone), the generator load switch is automatically opened, permitting grid supplies to be maintained to the 11 kV unit switchboards (assuming the off-site source supply remains available).

The station transformer-fed switchboards are designated station boards A and B and the unit transformer-fed boards, unit boards C and D. Supply routes to the unit transformers are run separately from those to the station transformers within the station to ensure that the grid, as a source of supply to the essential electrical system, can potentially only be partially affected by internal hazards.

The philosophy behind the design of the electrical supply systems at and below 11kV is to attain a high reliability of supply following fault and hazards by including 4-fold redundancy and 4-way segregation. This is achieved by replicating the required systems in four independent and identical essential supplies buildings.

The 11kV boards within the electrical supply system are 'non essential'. Each reactor has four 11kV switchboards, one associated with each reactor quadrant, designated A, B, C and D to match the designation of the quadrants. Each board supplies the two gas circulators of its associated quadrant and an 11/3.3kV essential auxiliary transformer. The transformer provides the normal supply to the essential electrical supply trained off the quadrant, and the quadrant designation, A, B, C or D is carried to all downstream essential electrical loads and plant. The other electrical loads including the starting/standby boiler feed pumps, main CW pumps and non-essential auxiliary transformers, are divided over the four 11kV boards to balance their loadings and meet the alternative supply requirements for the various loads.

11kV boards A and B are station boards supplied from the 132kV substation via a single station transformer. Each of the unit boards, C and D, is supplied from the turbine generator via a dedicated 23.5/11kV unit transformer. A generator load switch allows isolation of the generator so that post trip, the 11kV unit boards can be supplied from the grid via the 400/23.5kV generator transformer and their associated unit transformers. The electrical auxiliary system thereby provides two independent grid connections for each unit.

Two principal 3.3kV switchboards are provided for each unit. The 3.3kV station and unit auxiliary boards are supplied from the B and D quadrant 11kV boards respectively via their associated 11/3.3kV station and unit auxiliary transformers. 415V non-essential auxiliary loads are supplied from a range of 415V services boards via their associated 3.3kV/415V services transformers. Alternative supplies to the 415V reactor and turbine services boards are derived from the 3.3kV station and unit boards of the associated unit, but for all other 415V services boards, alternative supplies are derived from the non-essential systems of both units.

Boards at other voltage levels (250V DC, 220V DC, 110V AC, 110V DC, 48V DC) are derived from the 415V system via transformers and rectifiers.

1.3.5.2.1 Main Electrical System – Equipment Locations

The primary components of the main electrical system are located as shown in the table below. 415V AC distribution boards for non-essential supplies are not included in the table but are located in the essential supplies buildings and throughout the station, generally in the area of the equipment they support.

Equipment	Location
11kV Station Boards	Essential Supplies Buildings
11kV Unit Boards	Essential Supplies Buildings
11kV/3.3kV station and unit auxiliary transformers	Outside compounds

Table 1.9 - Main Electrical Equipment locations at Heysham 2.

1.3.5.2.2 Main Electrical System – Performance in Hazards

The main (i.e. non-essential) electrical system is designed to support normal operation at power and, following a reactor trip with off-site power supplies remaining available, it will deliver grid-backed power to the essential systems required to support post trip cooling.

Localised internal hazards may result in single failures of main electrical system plant items, but the system is resilient to these due to the 4-way segregation of the system. Should grid supplies be unavailable (this assumption is made in the safety case for most external hazards) power will not be available via the main electrical system as described above but will be provided by back-up diesel generators (see Section 1.3.5.3 below).

1.3.5.3 Primary On-Site Back-up Power Supplies

Section 1.3.5.2 discussed the 'non-essential' aspects of the electrical supply system at Heysham 2. This section (1.3.5.3) addresses the 'essential' parts of the electrical system i.e. those electrical plant items which are required to supply power to enable essential safety functions to be carried out following a reactor trip – including the scenario of loss of off-site power.

The segregation of the electrical supplies system as discussed in Section 1.3.5.2 extends to the essential electrical supplies since the back-up electrical supplies are replicated in the four essential supplies buildings. However, in addition to 4-fold redundancy, the electrical systems at Heysham 2 also include diversity within each essential electrical supplies building. Diverse provision of post-trip cooling is at the heart of the Heysham 2 design: diverse 'lines of protection' are provided by systems forming an 'X-train' and diverse 'Y-train' systems. The separation of 'X' and 'Y' trains is included in the electrical supply systems: each essential supplies building houses both 'X' and 'Y' essential electrical systems.

In respect of the subject headings of the stress test report, it would be reasonable to address 'X' and 'Y' electrical supplies separately as 'Primary' and 'Diverse' on-site back-up power supplies in Sections 1.3.5.3 and 1.3.5.4 respectively. However, it is convenient to address both 'X' and 'Y' trains together in this section since the extent of diversity which can be achieved between separate electrical supply systems is limited and the 'X' and 'Y' electrical supplies share common features.

High voltage back-up 'essential' electrical supplies are provided at the 3.3kV level.

Back-up 3.3kV Supplies

Heysham 2 has two types of diesel generators with one of each type in the four diesel houses adjacent to the four essential supplies buildings.

Separate services are provided for each generator system designed to meet the requirement of high reliability. The eight separate diesel generator systems are provided to meet the essential load and systems reliability requirements. The segregation and redundancy requirements are achieved by an arrangement whereby four generators feed the 'X-trains' and four feed the 'Y-trains', with each generator shared between the same quadrant train on each reactor.

The main X-train loads are the gas circulators (via variable frequency converters), the decay heat boiler feed pumps and the auxiliary systems.

The main Y-train loads are emergency boiler feed (EBF) pumps, the reactor seawater (RSW) pumps and the auxiliary systems. The ratings of the two types of diesel generator have been chosen to provide a margin of spare capacity for the connected loads on the essential system.

Back-up Supplies at Voltages below 3.3kV

Under normal reactor operating conditions, electrical supplies at 3.3kV and lower voltages are derived from the 11kV boards. If grid supplies are lost, with the reactor(s) tripped, automatically started diesel generators are brought into service by action of the PTSE to restore supplies to the essential 3.3kV and 415V AC systems. These constitute the 'short-break' part of the essential electrical system and provide power to those essential loads which can tolerate a short break in supply or are required later in the post-trip sequence of operations. Other essential loads which must remain supplied throughout the period of loss of grid are supplied from the battery backed uninterruptible AC and DC systems, which form the 'no-break' part of the essential electrical supply system.

Short break supplies

As indicated above, short-break supplies are those which cascade from the 3.3kV 'X' and 'Y' diesel backed boards. These typically supply systems which require high operating powers for which battery backed supplies would be impracticable.

No-break supplies

The no-break electrical supplies are designed to provide electrical power to those systems where a short interruption in supplies is either unacceptable or undesirable. The systems are designed to provide this during normal operation, post trip and in the event of loss of off-site power. In the event of loss of off-site power the no-break systems are powered from un-interruptible power supplies until power is restored via the diesel generators.

No-break supplies from UPS are provided at 415V AC (X-train) to support motors essential to circulator lubrication and cooling.

110V DC no-break supplies control supplies to essential switchgear at 11kV, 3.3kV and 415V for the X-train and for tripping specific switchgear on the adjacent train for the purposes of preventing gas circulator run-on.

The 250V DC no-break system supports the Emergency Lighting System for at least 30 minutes during loss of AC supply incidents.

220V DC no-break supplies support the X and Y-trains by providing a secure dc supply for 3.3kV and 415V switchgear closing solenoids for the X and Y-train switchgear of the quadrants of each reactor.

48V DC unit and station no-break supplies support control actions from the Central Control Room.

1.3.5.3.1 Primary On-Site Back-up Power Supplies – Cable and Equipment Locations

Each diesel generator is supplied with diesel fuel from a day tank which is topped up with fuel stored in three bulk tanks located outside each Essential Supplies Building.

Generally, the station cabling is installed in routes passing through cable flats, galleries and tunnels dedicated to the housing of cables and separated from other power station plant except at the approach to the point of connection with the equipment to be served. Within the cable routes through the station, the cables are generally installed in accordance with separation and segregation principles related to their type and function.

Major enclosed cable routes, where cables are installed in cable trays, are provided with fire detection and protection systems dependent upon the number of cables in the particular route. Where systems are served by duplicate cables, then generally these cables are installed in different routes to minimise the risk of total system failure due to faults or hazards.

1.3.5.3.2 Primary On-Site Back-up Power Supplies – Performance in Hazards

The design of the back-up power supplies at Heysham 2 has taken account of credible internal and external hazards. Localised internal hazards (e.g. fire) may adversely affect a single essential supplies building (and the corresponding post trip cooling systems in the affected quadrant of both units) but the remaining three Essential Supplies Buildings are likely to remain unaffected.

Although only the X-train electrical supplies were originally designed to be qualified against a severe seismic event, subsequent qualification of the Y-train has been readily formalised due to the common location in the essential supplies buildings and the similar nature of X and Y-train switchgear.

1.3.5.3.3 Primary On-Site Back-up Power Supplies – Time Constraints

The batteries supporting the essential 'no break' supplies will continue to do so for at least 30 minutes. The requirement to continue supply ceases once the diesels have started and run up to speed.

As indicated above, the diesel supplies are segregated; each one of the 4 X-train and 4 Y-train diesels has its own diesel oil supplies, stored in a small day tank and 3 bulk tanks per generator. The operating rules require stocks in these tanks to support at least 12 hours running of all generators. However, the minimum post trip cooling requirements for most reactor trips could be supported by just one of the eight generators. In extreme conditions there is scope to reduce the number of running diesels and extend the time capacity for cooling.

1.3.5.4 Diverse On-Site Back-up Power Supplies

As discussed in Section 1.3.5.3, diversity in the provision of essential safety functions is a key feature of the Heysham 2 plant design. Diversity in post trip cooling provision is achieved by the 'X-train' and 'Y-train' systems which include the electrical supplies.

It may also be noted that additional diversity in post-trip cooling is available at Heysham 2 through the Back-Up Emergency Feed System (BUEFS). This consists of a separate manually initiated petrol-driven water pump and portable hose connections that are capable of supplying water to the main boilers. (Primary coolant heat transfer is via natural circulation). The BUEFS is completely independent of the electric supply system but provides a diverse means of delivering the required essential safety function.

1.3.5.5 Further Available Back-up Power Supplies

There is a set of emergency equipment, including electrical generating equipment, that would support essential safety functions (with additional special items considered in later chapters) 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 activation (see Section 6.1.2.1). Additional time would then be required to deploy this equipment.

1.3.5.5.1 Potential Connections to Neighbouring Units/Plants

Heysham 2 power station is adjacent to Heysham 1, also a twin unit AGR station. The stations have no shared electrical systems; the only points of commonality are the grid substations. In the event of a loss of off-site power, this effectively electrically isolates the two stations.

1.3.6 Batteries for DC power supply

There are 84 DC systems, of which 61 are safety related, each of which consists of a battery, a charger and a switchboard feeding a number of load circuits. The 61 safety related systems are identified in the following subsections. All the battery/charger systems are connected to supplies derived from the essential, diesel backed electrical supply.

Under normal (station supplies available) conditions each battery and load is supplied at the float charging voltage by its associated mains fed charger. The charger supplies the load and automatically maintains the battery in a fully charged condition.

The chargers incorporate a number of protection features. Each rectifier circuit has fuse protection in each thyristor or diode circuit. Integral voltage sensing monitors are provided across the charger output terminals to initiate an overvoltage trip to protect against voltage surges. Charger fault, battery open circuit, battery on boost charge and earth leakage detection system remote alarms are also provided to continuously monitor each system.

1.4 Significant differences between units

There are no significant differences between the two units at Heysham 2. However, Heysham 2 is located immediately next to Heysham 1 power station. The latter is also a twin unit AGR station but of a significantly different design to Heysham 2. An equivalent and separate stress test report has been produced for Heysham 1 which should be consulted for further information.

1.5 Scope and Main Results of Probabilistic Safety Assessments

1.5.1 PSA: 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 ALARP 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.

For Heysham 2 and Torness, there also exist operator aids that utilise PSA to inform risk-based decision making when making plant available or unavailable (e.g. due to maintenance), helping operators to avoid unnecessary risk increases and manage the risk associated with the plant downwards.

Chapter 2 – Earthquakes

Heysham 2

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 (SNUPPS) design and the standard design included qualification against earthquake. However, for the pre- Heysham 2/ Torness 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.

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

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 1 in 10,000 years. 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 1 in 1000 years.

At Heysham 2, the infrequent earthquake results in a peak ground acceleration (PGA) of 0.23g uniform risk spectrum, however the original design of the plant was to withstand a much more onerous safe shutdown earthquake. The uniform risk spectrum is obtained from site-specific evaluation and always presents a more onerous requirement than the 0.1g Principia Mechanica Limited (PML) spectra, as can be seen in Figure 2.1.

The safe shutdown earthquake was used as the original bounding seismic hazard considered in the Station Safety Reports for both Heysham 2 and Torness. This required a single seismically qualified method of shutdown and post-trip cooling (known as bottom line protection) to be established. A review against the Nuclear Safety Principles (NSPs) was carried out for the first Periodic safety review (PSR) at Heysham 2 and Torness and the provision of two seismically qualified lines of protection (one being the bottom line protection) for frequent seismic events was justified by a comprehensive As Low As Reasonably Practicable (ALARP) assessment. This re-assessment resulted in extending the original safety case to include a second line of protection for frequent seismic events, based on backup shutdown system and natural circulation post trip cooling with backup boiler feed.

The current design basis earthquake at Heysham 2 for a frequent event has an assumed PGA of 0.1g PML spectrum.

It is important to note that this figure of 0.1g was adopted in accordance with International Atomic Energy Agency (IAEA) guidelines and is more onerous than a seismic event that could be expected in 1,000 years at the site.

[7] Assumed to mean tectonic plate boundary

It was recognised that at some level of seismic disturbance, less severe than the frequent design basis earthquake, the station operator would be required to shut the reactor down and subsequently demonstrate that the plant had not been damaged before recommencing power operation. Therefore, following a significant earthquake, the plant should be shut down by the operator and inspected for damage or loss of function before recommencing operation. The level of earthquake above which the operator would consider shutting down the plant is known as the operator shutdown earthquake.

The operator shutdown earthquake was defined as having a peak horizontal free field ground acceleration of 0.05g. Such an earthquake was calculated to have an expected frequency of occurrence at the site of significantly less than one in a hundred years (10^{-2}).

According to a Tokyo Electric Power Company (TEPCO) report the maximum recorded PGA at Fukushima Dai-ichi 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 shut down and post trip cooling was initiated subsequent to the earthquake. The tsunami was the cause of the majority of the plant failures.

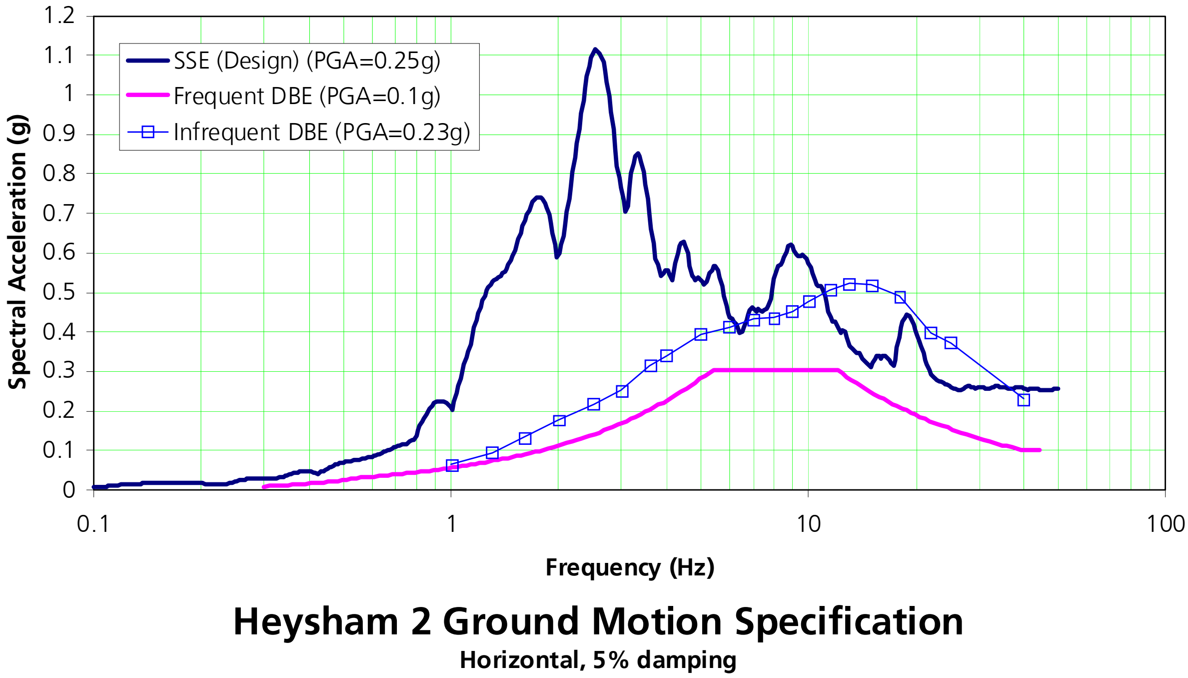

Figure 2.1: Heysham 2 Ground Motion Specification

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 (10^{-4} p.a.). 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 1980's 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 (CEGB) 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 known for Heysham 2 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 Section 1.3 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 recent historical earthquakes in the UK are shown in the 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	PGA 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 Heysham 2 was carried out during the 2008 Torness and Heysham 2 periodic safety review. This was conducted using data from the British Geological Survey (BGS). It was found that all events up to 150km from each station during the review period (Jan 1990 – Aug 2007) were below 4.0ML. This is the threshold value below which the seismic hazard would not be significant. The review also considered smaller magnitude events in close proximity to the power stations and it was concluded that these events would not affect the magnitude or frequency of the seismic hazard.

Within 150km of Heysham 2, there were 14 seismic events in the review period with a magnitude greater than 3.0ML. The largest was of magnitude 3.9 ML and occurred in October 2002, 74km South East of the station.

Within 50km there were six events during the review period with a magnitude greater than 2.0ML. The largest of these was a magnitude 3.0 ML event, in June 1993, 19km North of the station. The closest event with a magnitude of 2.3 ML was 11km East South East of the station, in August 1998.

This review did not identify any significant changes that would affect the severity, frequency or nature of the seismic hazard for Heysham 2.

Geological Information on Site

The natural overburden consists of shore deposits, mostly sandy, and boulder clay. Their thickness is variable, but is usually less than 3 m and sometimes absent over the Permo Triassic bedrock. Most of the site is further overlain by made ground, primarily waste products of the railway company who reclaimed and owned the site from the late 19th century onwards.

The bedrock consists of Permo Triassic sandstone over the western part of the site and shaley mudstones, siltstones and sandstones of the Carboniferous Millstone Grit series in the eastern part of the site. The contact between the Permo Triassic and Carboniferous rocks is faulted with an approximate North-South axis.

A large number of site investigation boreholes, together with trial pits, dilatometer tests and plate loading tests have been carried out in the western part of the site. The upper surface of the sandstone varies in level between about +3 m and 7 m ordnance datum, the higher levels being in the Southern part of the site. The Permo Triassic rocks and the underlying Carboniferous strata have been proved to a level of -100m ordnance datum and their apparent dip is consistently 35-40° to the West.

The Carboniferous formations in the Eastern part of the site have been investigated less thoroughly, due to their general unsuitability as a foundation media for a nuclear power station. The lithology of these strata vary between hard, coarse, gritty sandstones and weak shaley mudstones and display many intermediate graduations. These strata have been proved to a level of about -70m ordnance datum.

The fault has been exposed and examined just below rockhead in an exploration pit and has been investigated also with a number of boreholes. Its dip is between 70 and 80° to the west. The throw is not known. The Permian and Triassic rocks are faulted out at the contact and no correlation has been made between the Carboniferous rocks on each side. In plan the fault is not a single line from North to South across the site, as it appears to step East between Heysham 1 (HYA) and Heysham 2.

Extensive engineering analysis of the Permo Triassic materials took place prior to the construction of the Heysham 2 Power Station. This, together with the back analysis of settlement records etc, was taken into account in the geotechnical design work for Heysham 2. This work was primarily based on an extensive programme of site investigations carried out in 1978.

Safety Margins in the derivation of design basis earthquakes

The methodology used to derive the design basis earthquakes 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.

Heysham 2 and Torness were designed against a safe shutdown earthquake which is more severe than a 1 in 10,000 years design basis earthquake as described below:

The two records (the 'Parkfield 5 N05W' and 'Temblor S25W' records) from which the safe shutdown earthquake was developed were selected from a collection of strong motion acceleration time histories, all from the western United States. These had magnitudes, focal depths and epicentral distances in the range that might be expected in the UK. The two acceleration time histories selected from this set were those whose response spectra largely enveloped all the other response spectra in the collection, so they were a particularly onerous choice.

Seismic hazard calculations carried out between the mid 1970s and early 1980s, based on the overall seismicity of Great Britain, indicated that the peak ground acceleration corresponding to a probability of exceedance of 1 in 10,000 years. was about 0.25g, even for sites of relatively high seismicity. This was in contrast to the selected acceleration time histories which had a peak ground acceleration of around 0.4g. In order not to base the design on an improbable level of ground acceleration, the acceleration time histories were modified to have a peak acceleration of 0.25g horizontally.

The same acceleration time histories were used to assess the response of structures in all three directions, although they were scaled to a peak acceleration of 0.17g (approximately 2/3 of the horizontal value) in the vertical direction.

Further studies, were carried out during construction to show that the stations would also withstand, subject to a few reservations, the effects of a seismic event described by the 0.25g PML design spectra which had been adopted for the design of Sizewell B. Studies for Sizewell B had demonstrated that a peak ground acceleration of 0.25g was indeed a pessimistic representation of the seismic hazard in Great Britain with an annual probability of exceedance of 1 in 10,000 years.

The spectral content of the PML spectra was developed on a pessimistic basis suitable for design for both soft sites (like Sizewell) and harder sites. Notwithstanding this pessimism, it was clear that the spectra of the safe shutdown earthquake used for the design of Torness and Heysham 2 was pessimistic by a factor of typically 2 relative to the Hard Site PML spectra in the frequency range from 1 to 4Hz.

Since the date of those further studies, probabilistic techniques for UK ground spectra have been further developed. It is now standard practice to evaluate, on a site-specific basis, the seismic hazard corresponding to various annual probabilities of exceedance. The results are presented not only as peak ground accelerations, but also as spectral accelerations in the frequency range 1 to 40 Hz. These probabilistic spectral accelerations allow probabilistic spectra to be calculated, the so-called uniform risk spectrum. The uniform risk spectra have been evaluated for both the Torness and Heysham sites. The uniform risk spectrum for the 1 in 10,000 years. probability of exceedance have been used as the basis of seismic assessment of Bottom Line plant in the periodic safety reviews of the earlier AGRs and the corresponding site-specific uniform risk spectrum for the Torness and Heysham 2 sites are considered to represent the current standard for the seismic hazard at these sites.

Comparing the site-specific uniform risk spectrum with the spectra of the modified Parkfield 5 and Temblor records, it is demonstrated that the envelope of the Parkfield 5 and Temblor spectra envelopes the 1 in 10,000 years p.a. site-specific uniform risk spectrum for both stations in both the horizontal and vertical directions.

Furthermore, the envelope of the Parkfield 5 and Temblor spectra is confirmed to be exceptionally onerous in the frequency range from 1 to 4 Hz, by a factor of up to 7 for Torness and up to 5 for Heysham 2. This frequency range dominates the response of the major building structures and so impinges strongly on the overall design of both stations. Viewed another way, the spectral acceleration at 2.5 Hz in the envelope of the Parkfield 5 and Temblor spectra corresponds to an annual probability of exceedance of between 1 in 10,000,000 and 1 in 100,000,000 years for Torness and between 1 in 1,000,000 and 10,000,000 years for Heysham 2. It should be noted that the envelope of the Parkfield 5 and Temblor spectra on its own is equally over-pessimistic over the natural frequency range from 1 to 4 Hz and remains pessimistic over the entire frequency range, except for a band of frequencies above 10 Hz where it fails to envelope the Heysham site-specific uniform risk spectrum.

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 Heysham 2 has been constructed using independent expertise based on well regarded sources of information. Furthermore it has been reviewed periodically in line with company process and regulatory expectations. The methodology has been constructed with appropriate conservatisms, margins and sensitivity studies employed.

As noted above Heysham 2 was originally designed to withstand a spectrum based on the safe shutdown earthquake spectra derived from the earthquake records 'Parkfield 5 N05W' and 'Temblor S25W'. This is more onerous than the infrequent earthquake. Further studies, were carried out during construction that showed that the stations would also withstand, subject to a few reservations, the effects of a seismic event described by the 0.25g PML design spectra. Periodic safety review 1 assessed the seismic safety case against the uniform risk spectrum corresponding to an infrequent probability of exceedance that was considered to represent the current standard for the sites at that the time of the review. It was concluded that the original specification used for the design of both Torness and Heysham 2 is pessimistic with respect to current standards and very pessimistic in the response frequency range from 1 Hz to 4Hz. For Heysham 2, the safe shutdown earthquake is less onerous than the infrequent uniform risk spectrum for frequencies between 10Hz and 35Hz. However, the seismic assessment carried out for Periodic safety review 1 demonstrates that the 0.25g PML spectrum envelopes the part of the spectrum in which the safe shutdown earthquake ground motions were less onerous than the uniform risk spectrum. It is concluded that the seismic assessments carried out to the safe shutdown earthquake and reviewed against the 0.25g PML spectra are conservative in comparison to the infrequent uniform risk spectra. This is consistent with the current requirements and best practice.

Conclusion HYB 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

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 design basis earthquake and assessment of potential safety margin.

EDF Energy Nuclear Generation now has seismic safety cases for all of its AGRs covering both the at-power and shut-down conditions as well as fuel handling operations. At Heysham 2 and Torness, unlike at other AGRs, seismic qualification of the plant was built in to the design of the plant.

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 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.

2.1.2.1.1 Operating Reactors

Seismic classification of the station components was introduced in order to provide a systematic basis for design. The following classification was adopted for Heysham 2 (and Torness) for the seismic qualification of the plant as described in the station safety report.

Class A:

This is the classification for a system or component that must be designed to withstand the safe shutdown earthquake and still perform its required function.

Class B:

This is the classification for a system or component which is not required to function after a seismic event but could fail in a manner which might cause damage to Class A plant.

Class NS (non seismic):

All other components or systems not in categories A or B are non seismic and are permitted to fail during a seismic event.

The following section describes the plant items required for safe shutdown and cooling of all plant areas on the Heysham 2 site. The second part of the section is where the evaluation of robustness of the Heysham 2 plant is described.

Essential safety functions

Essential safety functions are required to prevent or at least minimise potential radiological consequences of an earthquake. In order to achieve a safe shutdown state post an infrequent seismic event, the following Lines of Protection (LOP) are required:

- Reactor Trip
- Reactor Shutdown and Holdown
- Gas Circulator Trip
- Post Trip Cooling
- Primary Circuit Pressure Control

Reactor Trip

A bottom line seismic event would result in an automatic reactor trip (both reactors) as a result of the disruption. A manual trip can be performed via the guardlines which are designed on fail-safe principles; both these systems will remain available (or fail safe) to provide protection for any faults generated by the infrequent (1 in 10,000 years return frequency) seismic event (or for any coincident faults). It should be noted that one of the guardlines is seismically qualified by design.

Reactor Shutdown

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 main shutdown system is assured.

Gas Circulator Trip

In order to protect the boiler and core support structures, the pressure boundary and coolable geometry, the Gas Circulator trip function is qualified against a safe shutdown earthquake. This ensures no mismatch between boiler feed flow and gas mass flow can occur.

Post Trip Cooling

Post-trip cooling following a bottom line (infrequent) seismic event is via forced circulation and decay heat boilers. This equipment and all the necessary supporting systems are qualified against a safe shutdown earthquake.

Essential plant that would comprise a ‘second line’ of protection against a seismic hazard has also been identified in the safety case and appropriately qualified, to provide additional robustness.

Natural Circulation Capability

In order to ensure secondary shutdown capability, and also natural circulation, the primary circuit integrity must be maintained and post-trip cooling provided by an additional boiler feed backup system. The systems which provide this function were included in the seismic assessment and it was confirmed that it was seismically qualified to second line level. It has also been shown that these second line systems are likely to survive a high proportion of infrequent seismic events thus providing back up protection to the bottom line systems.

Forced Circulation Cooling Capability

Cooling can be provided to a depressurised reactor in air using the gas circulators and boilers fed by diverse and robust sources. Onsite backup electrical AC power supplies provide the power required for this capability (since the grid is assumed to be lost following an infrequent seismic event). Both the backup AC power supplies and the boiler feed systems are qualified to function after an infrequent seismic event.

Lines of Protection against Seismic Events

The safe shutdown earthquake was used as the original bounding seismic hazard for both Heysham 2 and Torness. This safety case was updated to the existing safety case to address frequent seismic events, and demonstrate compliance with the NSPs. Appropriate seismic qualification (to second line level) of these systems is justified, to provide a second line of protection for frequent seismic events.

2.1.2.1.2 Shutdown Cooling

The bottom line post trip cooling is also claimed for the scenario where a bottom line 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 in the event of loss of plant due to faults or hazards. Therefore, providing the decay heat limits and moderator temperature 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 shutdown cooling safety case claims that cooling will be achieved by restoration of gas circulators and decay heat boilers being fed using the additional boiler feed system. All the systems, structures and components required for this functionality have been seismically qualified on the basis of manual starting using local to plant actions where appropriate. 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 - seismic event has no effect as cooling is passive
- Buffer storage - cooling systems are seismically qualified
- Dismantling - loss of active air flow and water jacket cooling is tolerable as water injection system is seismically qualified
- Storage in ponds - cooling system is seismically qualified

2.1.2.1.4 Evaluation of their robustness in connection with design basis earthquake 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 1 in 10,000 years 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 HYB 2.2: The methodologies used for ensuring robustness of the plant have appropriate conservatisms, 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

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

The role of the operator in response to a seismic event is to shut down the reactor(s) and initiate plant surveys following a seismic event at operator shutdown earthquake level or above.

The main issues for the operator were identified as recognition of the change in the backup shutdown system seismic inhibit switch setting to second line level, and recognition of the extent and role of plant that has been qualified to second line level. The affected operating instructions at Heysham 2 together with changes required to address these points were identified. The necessary changes have been made at Heysham 2.

A number of human factors assessments have been carried out taking account of access to plant which 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 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 this is based on a degree of judgement.

2.1.2.2.3 Fuel Route

Fuelling machine

If it is desirable to re-start the hoist and move any fuel being handled, this will require manual intervention as the seismic trip should have operated to cut power to the machine.

Decay stores

Manual actions will be required to re-configure the cooling system to the air heat exchangers.

Spent fuel dismantling

Cooling water flow to the dismantling tube can be restored if cooling water is lost by configuring to use the backup water supply as a once-through system. If cooling/extract to the cell is lost, then procedures and equipment are in place to box-up (seal) the cell and to initiate a flood of the dismantling tube. Although backup systems may not be immediately available following a seismic event, time is available before fuel temperatures reach levels of concern.

Spent Fuel Cooling Ponds

Significant timescales are available before additional water make-up needs to be provided to the ponds to compensate for the loss of cooling.

Conclusion HYB 2.3: The claims made on the operator make appropriate use of international experience and standards and have been periodically reviewed. Further review has been undertaken as part of the response to the Fukushima Dai-ichi event.

Consideration HYB 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 design basis earthquake and that might threaten heat transfer to ultimate heat sink by mechanical interaction or through internal flood.

Heysham 2 Class A systems were designed to be seismically qualified as are any potential systems which could interact with the claimed systems during a seismic event i.e. the class B systems. The potential consequential internal hazards were also considered as part of a periodic safety review are as follows:

- Fire - The clarity of the safety case for consequential fires following a seismic event was considered to be poor. Note that this shortfall relates to the clarity of the safety case and was considered to be of low nuclear safety significance.
- Hot Gas Release – No issues were raised.
- Steam Release – The seismic status of certain plant items (primarily the reason why the turbine hall pipework was qualified against the safe shutdown earthquake) is not clear and so, corrective action is in progress as part of normal business. This work is assessed to be of low nuclear safety significance.
- Missiles from rotating objects – The seismic qualification of the steam turbines and the overspeed protection system is not clear.
- Dropped Loads - No issues were raised.
- External Flooding – Flood defences are adequate to ensure that no essential plant will be affected by a tsunami and only minor flooding will occur.
- Nitrogen Release - No issues were raised.

Failure of the LP rotors of the main turbines would pose a risk of consequential missiles to essential plant, however, world experience indicates that direct seismic damage to the turbines is unlikely. Note that this issue was considered as part of the station design and failure in a seismic event was considered to be a low risk.

Indirect failure due to loss of grid and turbine overspeed is protected against by mechanical overspeed bolts that are qualified to the bottom-line seismic level.

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.

Conclusion HYB 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 as a required.

Routine testing of the make-up shield large spherical joint freedom of movement serves to underwrite the seismic protection to the reactor pressure boundary between major make-up shield overhauls.

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

The safety case assumes that consequential loss of grid occurs for both frequent and infrequent seismic events. Power is then provide by an alternate on-site supply. The safety case approach in EDF Energy 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 the operating rules 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 stock levels are higher than the limits specified in the operating rules, therefore the most probably 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.

Conclusion HYB 2.5: Consequential loss of grid has been considered as part of the safety case. Electrical Supplies to essential equipment are provided by essential diesel generators which are qualified to bottom line.

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.

This assessment aligns with our own in that we would expect difficulty with access to and from site for a period, although it should be noted that the magnitude of this impact would be very much less than that seen in Japan.

There is the possibility of the bridges over the River Lune and local 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.

Conclusion HYB 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).

A periodic safety review at Heysham 2 found that the safety case claims that the structures and plant items that could interact and damage the claimed systems in a seismic event are seismically qualified.

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 inflammable material, like propane tanks or 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 HYB 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 HYB 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 (SSRs) 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 some AGRs, including Heysham 2.

As a result of the review carried out following the events at Fukushima it is considered that there is an uncertainty in the efficiency of the processes which manage the ongoing qualification of plant claimed in the seismic safety case.

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

2.1.3.2 Licensee’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.

There is no mobile equipment claimed in the safety case for design basis seismic events for Heysham 2.

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 various forms of commitment. These are within the normal processes used to comply with the licensing basis.

From the periodic safety review process the organisation had already identified areas for enhancements in the interaction aspects of the seismic safety case and a programme of work is underway addressing these issues on a reasonably practicable timescale. It is noteworthy that these were focussed in the area of beyond design basis and in some respects pre-empted the work carried out here.

Conclusion HYB 2.8: There are issues identified with the seismic safety case and appropriate actions are being undertaken on a reasonable timescale as part of a project within the company.

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 generally robust. Emergent issues regarding the validity of these cases are treated using established company processes.

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 as a requirement of the board.

Scope

The review 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 walk downs 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 review. These include the following:-

- Fleet Operations Manager to update station documentation and associated checksheet to specify fleet standards for seismic housekeeping.
- Fleet Operations Manager to establish a fleet training request based on the revised station documentation 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 HYB 2.9: The reviews undertaken as part of MEVL 1, and the actions identified therein, have confirmed that Heysham 2 is compliant with the current licensing basis, although a few improvements have been identified.

Conclusion HYB 2.10: The robustness of Heysham 2 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 DBE. The EDF Energy Nuclear Safety Principles (NSPs) for the AGRs 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 years. within the design basis safety case.

The NSPs also state that the integrity of protection against the 1 in 10,000 years. 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 DBE, 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 periodic safety reviews.

Section 2.1.1.3 outlined that conservatisms and margins exist in the calculation of the DBE. 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.

EDF Energy Civil Engineering guidance 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 PSA. 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 (HCLPF). An HCLPF 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 HCLPF 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 HCLPF value is a PGA 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 HCLPF value. Thus plant qualified to 0.2g, effectively has a HCLPF 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.

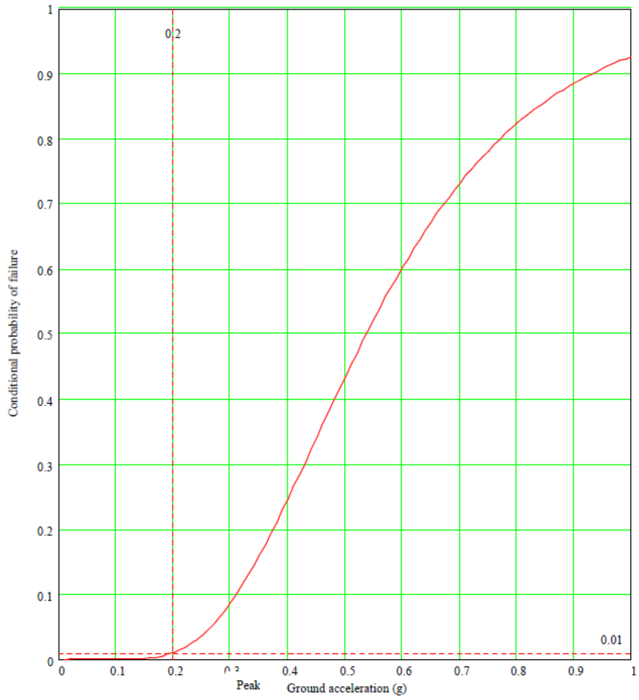

Figure 2.2: Mean Fragility Curve for Typical System Qualified to 0.2g PGA

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 HYB 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% (i.e. a best estimate of the likelihood of severe fuel damage) is not reached until the severity of the earthquake is at least twice that of the safe shutdown earthquake, which for Heysham 2 is 0.23g PGA. The seismic hazard assessment reports for the site indicates that this increased level of ground motion has a probability of between 1 in 100,000 and 1 in 1,000,000 per years.
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 HYB 6.1 raised in Chapter 6 will lead to further insights into this issue.

2.2.2 Range of earthquake leading to loss of containment integrity

As noted in Chapter 1, the AGR design does not feature a containment structure, so this question does not apply.

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 Heysham 2, and although there are large bodies of water surrounding the site (Irish Sea and Lune 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 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 Heysham 2 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. The sea defences are not seismically qualified, but it is judged unlikely that there would be significant structural failure of the sea defences such as to affect their functionality. The potential flooding risk to Heysham 2 is discussed in Chapter 3.

In Chapter 3 it is shown that very high sea levels are required before the sea defences are 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 HYB 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

In light of the events at the Fukushima Daiichi plant, as responsible operators EDF Energy have carried out reviews at each of the sites as a requirement of the Board.

Section 2.1.3.4 discusses the scope and findings of the specific seismic aspects for within the design basis assessments. The findings of the seismic aspects for beyond design basis assessments 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 examined, 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.

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 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.

It was noted across the fleet that the pond structures are seismically qualified but that the pond cooling systems are not necessarily qualified owing to the relatively low decay heat of the AGR fuel ponds.

Standard safety case 'mission times' in the UK are applied. 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 was 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 was generic to all situations and is covered in Chapter 6.

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

Consideration HYB 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 generally 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, and
- 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 fuel damage to be expected

In considering the robustness to beyond design basis earthquakes, several areas have been identified where enhancement could be considered.

Chapter 3 – External Flooding

Heysham 2

3 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 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, overtopping of sea defences 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 outwith the scope of this report. Any further references to floods in this report concerns the external flooding hazard.

This report will assess the margins of the existing design basis, as well as the extant flood protection in place at Heysham 2 Nuclear Power Station. It demonstrates that:

- Sufficient margin exists between the maximum design basis flood (7.63m Above Ordnance Datum (AOD)) and the physical elevation of the main nuclear island (9m AOD).
- During extreme rainfall events it is demonstrated that essential function availability is maintained by the natural fall of the land towards the sea.
- The information presented below shows that the methodology used to calculate the design basis flood for Heysham 2 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 be 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 Heysham 2 site, the protection provided against them and the compliance route by way of which Heysham 2 Power Station complies with the nuclear site licence for the design basis flood.

3.1.1 Flooding against which the plant is designed

International Atomic Energy Agency (IAEA) recommends that the "plant layout should be based on maintaining a 'dry site concept', 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 (DBF)

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

- Extreme rainfall and snowmelt with consideration of the condition of the rooftops and external drainage.
- Overtopping of sea defences including high tidal conditions, tsunamis and seismic seiches.
- Gross failure of reservoirs.

Note: There are no major rivers or reservoirs in the vicinity of the station which could introduce floodwater into the site.

The Design Basis flood is the most severe external flood considered credible for this nuclear power plant. It is considered to be an infrequent event with an initiating frequency of once in 10,000 years. The (infrequent) design basis flood is as follows:

- Extreme Still Water Level 7.63m AOD.
- Mean High Water Spring Tide (MHWS) 4.59m AOD.
- Rainfall for a 1 hour period is predicted to be 100 mm.
- No threat judged from snowmelt.
- Calculated heights of tsunami waves were found to be up to 2m, giving a resultant water height of 9.63m (7.63m AOD (Extreme Still Water Level) + 2m).

3.1.1.2 Methodology used to evaluate the design basis flood

Heysham 2 Geography

The Heysham Power Station complex encompasses both Heysham 1 and Heysham 2 station sites and is located on the west coast of Lancashire on the southern side of Morecambe Bay. Heysham harbour is adjacent to the north and Lancaster is approximately 7 km to the east. The station complex is protected from the sea to the north and west by existing sea defences that provide site wide protection against sea water ingress from tidal surges and wave action.

To the north, the Heysham harbour sea defences provide adequate protection. The structure of the sea defences along the western boundary consists of a lower breakwater sloping embankment constructed out of semi-dressed sandstone blocks with a horizontal reinforced concrete slab from the head of the breakwater to the foot of an upper wave wall. The wave wall extends to a height of 10.66m AOD at the northern most end adjacent to the Heysham 1 site and extends to 9.84m AOD adjacent to the Heysham 2 site. The wave wall is constructed of reinforced concrete and is of the reflecting type. In addition an overtopping drainage system is located behind this wall which discharges all overtopping water at the southern end of the Heysham 2 site.

Original methodology employed at Heysham 2

Flooding methodologies have historically varied across the fleet depending on the requirements for the specific site and as such are not consistent. However, the individual methodologies are considered appropriate.

Wave Overtopping

The external flood hazard from the seaward side arises from the possibility of an adverse combination of:

- The spring tide (the tide generated by the combined gravitational attraction of the moon and the sun)
- Variation in the absolute level of the surface of the sea due to the elastic restoration of relative sea levels following reduction of ice loads and shorter term changes in the predominance of south west winds. Changes in level due to release or capture of water by changes in the volumes of ice also play a part in tidal variations
- High waves and swell, short period storm generated waves sometimes standing. In the northern part of the Irish Sea there is evidence that high surges and waves tend to avoid high tides but as with the rest of United Kingdom waters, there is insufficient data to be able to quantify this.

The methodology employed to evaluate the extent to which waves overtop a seawall depends on the following parameters relating to the state of the sea:

- The height of the waves arriving at the seawall.
- The period (or the wavelength) of the waves.
- The mean water surface level, which is the level of the surface in the presence of the spring tide, and any surge condition, but a complete absence of waves.
- The general direction of arrival of the waves at the seawall.

For calculation of the rate at which water flows over the seawall due to overtopping, the wave height and periods required are given in Table 3.1 having been estimated for combinations of storm and tide conditions having return periods between 50 and 10,000 years.

The original methodology showed that it is not practicable to provide a seawall that will prevent any wave water entering the site. Consequently flood defences have been designed to exclude all seawater up to the extreme still water level (7.63m AOD) but to provide back drainage to the wave reflector wall to intercept the wave water which overtops the wall in windy and storm conditions. In addition to this first line of wave water defence the low catchment areas to the south of the station holds other windblown spray and rainwater at safe levels and drains the water off-site to the south.

A conservatism made in the safety case was that the entire seawall at Heysham 2 is 9.84m AOD. However, the 10.66m AOD seawall adjacent to Heysham 1 extends to the frontage of Heysham 2 before tapering down to 9.84m AOD. This introduces a degree of pessimism within the overtopping calculations and hence the design basis.

To establish the extreme hazard case, the safety case considered that no water would drain off the site via the storm drainage system, the road channels or through ground seepage. To account for possible blockage, drainage is assumed not to be available in the safety case. In practice some drainage capacity will be available, however this has not been quantified. This could be re-evaluated if the design basis is reassessed.

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 commissioned by DEFRA in 2005 reports that within the UK, tsunami waves could possibly hit the south west of England and Wales and the Yorkshire and Humberside area. The assessment was made by collecting past evidence of tsunamis, considering possible source regions, and modelling the propagation of the waves. From the calculated models, heights of tsunami waves were found to be up to 2m. This is comparable to heights of waves from storm surges, however the report does state that that the impact of a tsunami should not be assumed to be the same as that from a storm surge.

Also, Heysham 2 would be sheltered from most (if not all) tsunamis by Ireland and North Wales. At Heysham 2, extreme high tide is 7.63m AOD; this combined with an increase of 2m due to a tsunami would not significantly overtop the seawall that is at a minimum height of 9.84m AOD.

According to the DEFRA report and PSR1, the probability of a tsunami hitting Heysham 2 is extremely low and therefore can be considered as an incredible event. DEFRA considers tsunamis over a 100 year return period, while in comparison those considered within design basis for nuclear plants are within a 10,000 year return period.

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

Self limiting effect of increasing wave height

In a situation where the mean depth of water over the toe of a sloping seawall remains constant, an increase in the height of the waves off-shore would lead to a condition in which they would break at a greater distance from the crest of the wall, since there is a minimum depth of water which is required to support a wave of given height, without breaking. There is the possibility that this increase in distance from the crest would more than offset the greater run up distance, after breaking, of the larger wave. However, the overall effect appears to depend, in a complex fashion, on the slope of the seawall relative to that of the sea-bed at the toe of the wall, and the roughness coefficients of both; it is clear there are self limiting conditions at Heysham but the constant stability of the sand bed cannot be presumed.

Rainfall

The Heysham 2 safety reports state that the mean intensities of the estimated maximum rainfall were used in the safety design of the site. The rainfall for a 1-hour, 10,000 year return period rainstorm was estimated to be approximately 100mm. Calculations show that the road channel system can discharge over $20m^3/s$ without the level rising to 8.85m AOD (-0.15m site datum). This is equivalent to 210mm of rain per hour over the whole catchment area, i.e. approximately twice the rainfall for an infrequent 60 minute storm.

The most recent Met Office report predicts that there will be a small increase in the mean rainfall in the wintertime (less than 10%) and a decrease in the mean rainfall in the summertime by the 2020s at Heysham 2. The rainfall for a one hour, 10,000 year return period rainstorm is predicted to increase by a maximum of 62% by the 2080s. Assuming a linear increase, the maximum increase by 2023 would be approximately 21% (i.e. to approximately 121mm). This is clearly within the drainage capability of the road channel system.

Snowmelt

There is relatively little snowfall at Heysham 2 as it is situated on the coast and is exposed to South Westerly winds, therefore it is unlikely to be affected by deep lying snow. The station has an immediate call out arrangement for road clearance in the event of heavy snowfall, and also has access to a local snow plough. There have been no issues in the past regarding flooding due to snow melt. It is therefore judged that there would be no threat to safety related equipment due to snowmelt. This is confirmed within a recent Met Office report stating that there will be significant future reductions in the number of snow days. There is recent experience of heavy snows over a prolonged period and this issue, with regard to snowloading, is discussed further in Chapter 4.

Climate Change Adaptation

Work has been commissioned by EDF Energy to investigate the effects of climate change. The main flood risks for the EDF Energy Nuclear Generation stations identified within the work were storm surges. It was noted that the current case was secure, although the data needed to be kept under review.

Sea level rise

Reports by the Met Office in 2004 (which did not include Heysham 2) discussed the effect of climate change and show a global mean sea-level increase of between 4 and 14 cm from 2004 until 2020s confirmed by an IPCC (Intergovernmental Panel on Climate Change) study in 2001 predicting a mean global sea-level rise of a maximum approximately 13 cm by 2023. Another recent report produced by the Met Office provided similar information to that presented previously (which included Heysham 2) predicting a maximum global average sea rise of 14 cm by the 2020s with the assumption of a high emission scenario.

The recent Met Office report also estimates the local effective mean sea-level rise by the 2080s through the combination of using predicted isostatic changes (vertical land movements) with the estimates of global mean sea-level. A further margin has been added for specific regional effects. Therefore, the maximum local effective mean sea-level rise at Heysham 2 is predicted to be 101 cm by the 2080s. Using the high emission scenario with the assumption of a linear increase in sea-level from 1990, in 2020 the sea-level will have increased by approximately 33 cm.

Consequently there would be a sufficient margin between the conservatively judged 1 in 10,000 year bounding flooding event including sea level rise and the lowest elevation of the main nuclear island plant.

Wave height increase

A report written by Intergovernmental Panel on Climate Change (IPCC), states that wave height changes may occur at the coast with climate change. It identifies that in the North Atlantic, a wave height increase has been observed, but the cause is poorly understood. The more recent Met Office report states that although climate induced sea-level rise may put some unprotected low-lying coastal regions at risk, it is assumed (given the lack of detailed site level information) that all eight sites included in the report are situated at elevations above even the most extreme estimates of local net sea-level rise. However, it goes on to state that a potential risk of inundation does exist in the form of storm surges. Storm surges are the temporary extremes of sea-level, caused by low atmospheric pressure and strong winds. They occur in regions of shallow water such as on the continental shelf around the UK, including the North Sea. The height of the surge may be increased by the shape of the coastline, particularly in estuaries and river mouths where a funnelling effect can occur. They can reach an extreme level when combined with high tide.

According to the Met Office report "Review of Medium to Long Term Coastal Risks Associated with British Energy Sites: Climate Change Effects", the 50-year return period surge height increases due to climate change in 2080 at Heysham 2 are:

- 0.0 m in the low greenhouse gases emission scenario; and
- 0.6 m in the high emission scenario.

Using the high emission scenario and assuming a linear increase in the 50-year return period surge height change from 1990, in 2023 surge height will have increased by approximately 0.2 m at Heysham 2. This is less than the maximum increase predicted in sea-level rise due to climate change.

There is no new data presented for a 10,000-year return period surge height increase. Table 3.1 presents the original maximum sea-levels (including surge) with a return period ranging from 50 years to 10,000 years. From this table, it can be calculated that the percentage sea-level increase from the 50-year return period to the 10,000-year return period is approximately 19%. Applying this percentage increase to the 20cm surge height increase with a 50-year return period given in the Met Office report would give a 0.24 m surge height increase with a return period of 10,000 years.

Assuming the maximum local sea-level rise and the maximum estimated 10,000-year return period surge height increase, the total maximum increase at Heysham 2 is 0.57m.

Based on the calculations in the Heysham 2 PSR1 which state that the increase in overtopping rate for a 0.10 m increase in sea-level would be 6.6% (assuming a linear relationship), the increase in the rate of seawall overtopping at Heysham 2 for a 0.57 m increase in sea-level would be approximately 38%. The seawater represents only 12% of the calculated total run-off water due to overtopping of the seawall, with the 88% balance coming from failure of the 5000m^3 storage tanks (see Chapter 1 for description of the water storage 'Trimpell' tanks) and rainwater discharge (due to a 1 in 10,000 year 20 minute storm event) via the road channel system. So the overall increase in the calculated run-off water due to a 0.57 m increase in sea-level is only 4.4%.

Hence, flooding from the seaward side, either alone or in conjunction with heavy rainfall and failure of the water storage tanks, does not present a significant hazard to Heysham 2.

Table 3.1 levels, wave heights and wave periods used for calculation of design basis flood

Water level (m)	Water level return period (years)	Wave height (m)	Wave period (m)	Combined wave height/wave period return period (years)
6.4	50	2.1	5.0	1
6.5	100	3.0	6.0	10
6.7	250	3.6	6.5	40
7.0	1000	3.9	6.8	100
7.6	10000	4.2	7.1	200

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 Heysham 2 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 employed.

However, as a result of the advancement of scientific understanding of climate change and as a prudent operator, EDF Energy 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.

This work is currently in progress with two of EDF Energy's contract partners who are specialists in this area and will complete prior to the end of 2011.

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

Conclusion HYB 3.2: In line with Recommendation 10 of the ONR Report, the design basis flood at Heysham 2 has been confirmed, however further studies accounting for climate change have been initiated to reconfirm the design basis flood.

Consideration HYB 3.1: In line with Recommendation 10 of the ONR 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, during the period to 2035.

Conclusion HYB 3.3: There is no credible source of a tsunami that would affect Heysham 2. This is in agreement with the arguments presented in the safety case.

3.1.2 Provisions to protect the plant against the design basis flood

3.1.2.1 Identification of systems, structures and components (SSC) 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 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

Essential safety functions are required to prevent or at least minimise potential radiological consequences of external flooding. In order to achieve a safe shutdown state post infrequent external flooding event, the following essential safety functions are required:

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

A simplified overview of the claimed lines of protection for the infrequent external flooding events is identified within Table 3.2 and covers the following events:

- Infrequent rainfall.
- Infrequent snowmelt.
- Infrequent overtopping of sea defences.

Trip

Trip is not required by the safety case, but the operator may decide to trip the reactor if a threat to safety related plant or personnel is perceived. The main guardline, diverse guardline and the post trip sequencing equipment are not at risk from design basis external flooding due to their location.

Shutdown

As the design basis initiating external flooding is an infrequent fault, only one Line of Protection is required (with redundancy). As an automatic trip is not claimed, the operator may have to manually trip the reactor, leading to shutdown by the main shutdown system, all of this system's equipment is located above any credible flood level. The backup shutdown system – nitrogen injection – (plus born beads for hold-down if insufficient solid absorber can be inserted post trip) is not claimed for an infrequent hazard. Failure of control rods due to a flooding initiating event is not considered to be a credible event within design basis, as it is considered to be fail-safe on loss of supplies.

Table 3.2: Claimable Lines of Protection for an Infrequent External Flood.

Function	Line of Protection claimed for Infrequent Flooding
Trip	Manual Trip using main guardline
Shutdown	Main shutdown system remains available
Post Trip Cooling	Forced circulation of primary coolant gas and back-up boilers
Essential Monitoring	Main control room remains available

Post Trip Cooling

Loss of the seawater cooling is pessimistically assumed to occur during an infrequent flooding event due to flooding of the pumphouse. The loss of seawater cooling requires cooling loads to be met using alternative air-cooled heat sinks.

The minimum post trip cooling essential safety functions claimed for external flooding will not be made unavailable by an infrequent external flooding event.

For the essential safety function of post trip cooling electrical supplies are required for primary coolant circulation and for the pumping of secondary coolant. Post-trip monitoring is generally dependent on electrical instrumentation. The main electrical system comprises transformers, switchgear, generator connections, and cables etc., which are provided to transfer power from the turbine generators.

If Grid connection is lost, the associated reactor and turbine generator will trip and supplies to the loads that must remain available in the immediate post trip period will be sustained by the battery backed systems. Loads that can tolerate a short-break in supply will be supplied automatically from the backup AC power supplies.

Essential Monitoring equipment

The main control room, alternative control room and the 2 back up control centres are not challenged by design basis flooding.

Shutdown reactor

As outlined in the section above, in the event of an infrequent design basis flood it is expected that almost all systems will remain available. If the reactor is depressurised forced circulation is necessary, and it is expected that the gas circulators (supplied by the onsite backup AC electrical generators) will be available for this purpose. In the extremely unlikely event that the gas circulators fail, the reactor will need to be re-pressurised to establish natural circulation.

Conclusion HYB 3.4: Provisions to provide essential safety functions are not compromised by the design basis flood.

Consideration HYB 3.2: The need for a formal reseal/repressurise case is currently being considered in a revision of the shutdown cooling safety case.

Fuel Route

There are no significant flooding concerns for fuel route plant as the infrequent external flood does not enter the main nuclear island buildings where the fuel route plant is located.

As discussed above, infrequent flooding could result in the loss of seawater cooling systems, which support buffer storage, dismantling and ponds cooling. However, alternative fresh water cooling systems are available in this scenario.

Conclusion HYB 3.5: The lines of protection required for achieving and maintaining a safe shutdown state 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

Heysham 2 is protected by a seawall at a minimum height of 9.84m AOD on the west side of the station. The West Catchment area is approximately the area within the security boundary around Heysham 2, Heysham Banks is to the East and the East Catchment area is beyond Heysham Banks. The side view of the seawall at Heysham 2 is shown in Figure 3.1. Due to relative ground levels, the Heysham 1 area will not contribute run-off to that of Heysham 2. However, since Heysham 2 ground levels are generally higher than Heysham 1, a watershed has been formed along the line of the road that divides the two Stations by raising the land level to a height of 8.85m AOD. The east catchment area is largely a grassed golf course. The topography of the site determines that flood waters accumulating in the east catchment area will discharge seaward over the Ocean Edge Caravan Park.

Figure 3.1: Side view of Seawall at Heysham 2

Topography & drainage

The area which lies to the east of Heysham Banks does not contribute to the surface run-off of the west catchment. The topography determines that flood waters accumulating in the east catchment in excess of 7.63m AOD will discharge seaward over the Ocean Edge Caravan Park and the lowest level of the water divide that separates the east and west catchments is 9.65m AOD.

Due to relative ground levels, the Heysham 1 site will not contribute run-off to that of the Heysham 2 site. However, since the Heysham 2 site ground levels are generally higher than those of the Heysham 1 site, a watershed formed to a level of 8.85m AOD is necessary in order to prevent water flowing from the Heysham 2 site into the Heysham 1 site area under extreme conditions. Therefore, only the catchment area contributing to the Heysham 2 site is designed to deal with run-off under extreme conditions.

Under extreme conditions, reliance on the piped drainage system is considered undesirable due to the risk of blockage in the system and no account has been taken of the discharge of flood waters through the piped system. Finished ground levels and falls of the temporary and permanent roads in the west catchment are designed to direct surface run-off away from safety-related buildings and, utilising the roads as a network of drainage channels to discharge the flood waters over the seawall above the maximum tide level of 7.63m AOD. Thus the catchment area under the extreme conditions is determined by topographical considerations alone. The safety case presents a conservatism whereby this drainage is not claimed (see Section 3.1.1.2).

Detail of site levels is given in the Heysham 2 Periodic safety review, Table 3.3 below.

Table 3.3: Summary of site levels

Parameter	Height Above Station Datum (m)	Height Above Ordnance Datum (m)
Height of Heysham 2 seawall	0.84	9.84
Station Datum (SD)	0.0	9.0
Height of safety related building thresholds, all penetrations sealed against flooding below this level	0.0	9.0
Height of watershed between Heysham 1 and Heysham 2 sites	-0.15	8.85
Ground level at SW corner of site (lowest site level)	-1.25	7.75
1 in 10,000 years extreme still water level	-1.37	7.63
1 in 100 years maximum sea water level	-2.44	6.56
Mean High Water Spring (MHWS)	-4.41	4.59
Ordnance Datum (OD)	-9.0	0.0

Conclusion HYB 3.6: The flood defence provisions for Heysham 2 are suitable and are appropriately inspected and maintained.

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

Operating instructions

Station documentation exists for the operator on receipt of notification of potential flood conditions from the National Storm Warning system. Instructions including monitoring, inspections and guidance are in place for the operator who may consider shutting down the reactor.

Summary

Local to plant actions prior to trip are primarily related to the inspection of lower lying areas of the site. If the status of the seawater cooling system is such that the operation of the reactor unit(s) is no longer possible then the reactor(s) will be tripped. The claims made on the operator actions are not onerous in the event of a severe flood before the reactor is shutdown, are specified in station documentation and can be carried out from the central control room.

Conclusion HYB 3.7: 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 hour mission time is presented within Chapter 5.

In the case of infrequent flooding event from the sea, wave over topping is possible but this is demonstrated to be at a minimal level and well within the site drainage capacity. Hence, on-site, the roads are always expected to be available. During the infrequent high tide seawater flooding event, large areas surrounding the Heysham 1/Heysham 2 station complex could possibly become flooded, including parts of the main site access roads. However, tide related overtopping and outflanking 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 a combination of direct return to the sea through drains in the sea defences 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.

Note that the current safety case at Heysham 2 is based on sufficient feed stocks being available for a 12 hour period (these can be topped up). The need to increase fuel stock is currently being reviewed.

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 backup equipment model for mitigation in accident scenarios.

Conclusion HYB 3.8: 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.

Consideration HYB 3.3: The need to increase feed stocks to ensure they are sufficient for a 24 hour period is under review.

3.1.3 Plant compliance with its current licensing basis

3.1.3.1 Licensee'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 the 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 Heysham 2 covers the maintenance of the sea defences and site flood protection.

At Heysham 2, items related to flood protection (the seawall) appear in the station maintenance schedule. This involves an annual check of the condition of both the landward and seaward sides of the seawall, the condition of the drainage trench and outlet grills and the presence of debris, the presence of debris in the surface water drainage outlet grills, and that the surface run-off area at the south end of the seawall is unobstructed. It is carried out by suitably qualified civil engineers.

In addition to the inspection of the sea defences, the barriers and fire seals of the nuclear island buildings are visually inspected every five years to ensure that the potential for flood water to enter the buildings is minimised.

The most recent inspection of the sea defences was completed in 2010.

3.1.3.2 Licensee'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.

Within the processes outlined above there are mechanisms for identifying any areas of concern or anomalies. These may take the form of a commitments from the productions of a safety case, justifications for continued operation or periodic safety review commitments. These are detailed and tracked to completion within the normal company processes that are used to comply with the site licensing basis.

Conclusion HYB 3.9: There are no issues identified with the flooding safety case.

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

In light of the events at the Fukushima Daiichi plant, as responsible operators EDF Energy have carried out reviews at each of the sites as a requirement of the Board.

Scope

The within design basis review was specified to ensure that systems essential to cooling fuel 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 this.

Summary of site specific findings

All tasks were completed. With regard to design basis flooding, a small number of minor improvement actions were identified and are being tracked and progressed within normal company processes.

Conclusion HYB 3.10: The reviews undertaken have confirmed that Heysham 2 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 Heysham 2 Power Station has sufficient margin against a design basis flood. As outlined previously, the bounding case for this site is wave overtopping. The safety case for external flooding is based on demonstrating that the methodology is suitably pessimistic while also demonstrating adequate physical margins for the main safety related plant. There is also shown to be adequate defence-in-depth.

3.2.1 Estimation of safety margin against flooding.

The return period for a beyond design basis event is unknown and sea level would have to rise to the height of the sea wall for this significant overtopping to occur. Physical margins and drainage capacity exist to demonstrate the resilience of the plant.

Physical Margins

It is not considered practicable to provide a seawall that will prevent any wave overtopping entirely. In addition to this first line of wave water defence the low catchment areas to the south of the station will hold other windblown spray and rainwater at safe levels and drain the water off-site to the south. All the safety-related plant and equipment with the exception of the pumps for the reactor seawater system are located in the reactor building or in other buildings at the 9.0m AOD level and there is no route for the ingress of flood water below this level. Thus there would be a margin of safety in the infrequent situation. The margin of safety for the reactor seawater system would be smaller, as the pumps are located in the cooling water pumphouse, on the western arm of the seawall, which is not protected against floods to a level greater than 7.3m AOD. However, the functions of the reactor seawater system can be carried out by alternative means (cooling to air); all the plant and services required for this alternative to the reactor sea water system are located in buildings which have their ground floors at the 9.0m AOD level.

Conservatisms within the Methodology

The seawall height used in the safety case assumed the minimum height of the wall, 9.84m AOD, applies to the entire length of the wall in front of the Heysham site. However, the 10.66m AOD seawall for Heysham 1 extends to the frontage of Heysham 2 before tapering down to 9.84m AOD. This introduces a degree of pessimism within the design basis and presents a margin against any increase in wave and water height leading to seawall overtopping.

Additionally, as stated in Section 3.1.1.2, drainage is not claimed in the safety case. This adds conservatism to the design basis.

Lines of Protection

In extreme external flooding events, essential plant items will not be affected with the possible exception of the seawater cooling system. Therefore in all but a loss of seawater cooling infrequent external flooding event, a second line of protection will remain available in addition to the claimed single line, plus further systems are available to provide mitigation and defence in depth. These are shown in Table 3.4 below. It is concluded that external flooding does not constitute a threat to the trip, shutdown and post trip cooling and monitoring functions for an infrequent hazard.

Loss of grid is assumed in a within Design Basis flood. Therefore, in order to power the main safety related plant, backup AC power supplies and back-up battery systems are used. These systems are segregated and are located at a height above ground level above that of an infrequent flooding event.

Table 3.4: Claimed Lines of Protection for an Infrequent External Flood as well as Defence-in-Depth measures that demonstrate further protection.

Function	Line of Protection claimed for Infrequent Flooding	Defence in Depth
Trip	Main guard line	Diverse guard line
Shutdown	Main shutdown system	Backup shutdown system
Post Trip Cooling	Forced circulation of primary coolant and backup boiler system	Main boiler system fed by alternative backup feed system Natural circulation of primary coolant
Monitoring	Main control room located at such a height above sea level such is not at flood risk	

Conclusion HYB 3.11: The review has shown that there are suitable and sufficient margins present within the methodology and plant for compliance with the current safety case.l.

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

In light of the events at the Fukushima Daiichi plant, as responsible operators EDF Energy have carried out reviews at each of the sites as a requirement of the Board.

Section 2.1.3.4 discusses the scope and findings of the specific seismic aspects for Within the Design Basis assessments. The findings of the seismic aspects for Beyond Design Basis assessments 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 examined, 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.

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.

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 defined. With regard to the events in Japan it was noted that site access, although possible in the necessary time frame, remained a significant logistical issue for longer periods. This issue was 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 was generic to all situations and is covered in Chapter 6

Conclusion HYB 3.12: The robustness of the plant against design basis floods is considered to be appropriate; in considering the robustness to beyond design basis floods, several areas have been identified where enhancement could be considered.

Consideration HYB 3.4: Consideration should be given to the feasibility of additional temporary or permanent flood protection for essential safety functions for example the CW pumphouse.

Consideration HYB 3.5: Consideration should be given to enhancing the robustness of dewatering capability, in particular focussing on independence from other systems.

3.3 Summary

The information presented in the preceding sections shows that the processes for ensuring robustness of the plant for flooding 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.

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

At Heysham 2, the bounding external flooding case is due to wave overtopping the seawall. The maximum sea level for an infrequent event is 7.63m AOD, and the site threshold level is 8.85m AOD separated from each other by the wave wall at 9.84m AOD.

Flooding due to rain is not considered significant because it is judged that seawall overtopping presents the bounding external flooding case.

Chapter 4 – Extreme Weather Conditions

Heysham 2

4 Extreme Weather Conditions

In the ONR 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 Heysham 2 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 AGR 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 1 in 10,000 years 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.

Extreme Wind

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).

Extreme Ambient Temperatures (EATs)

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.

Lightning

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

As noted above, EDF Energy 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 is not considered here.

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.

4.1 Design Basis

The design basis which has been adopted at Heysham 2 for these hazards is discussed in what follows.

Extreme Wind

Heysham 2 was originally designed to the wind loading code CP3: Chapter V: Part 2: 1972 for straight-line wind speeds. A basic wind speed v, was derived from this data for the 3 second gust which occurs once, on average, during a 50 year period. To obtain the design wind speed v_s, the basic wind speed v was multiplied by the design wind speed factors s_1 (topography factor), s_2 (ground roughness, building size and height above ground) and s_3 (statistical factor).

$$\text{i.e. } v_s = v.s_1.s_2.s_3$$

s_1 and s_2 were part of standard structural design procedures, whereas s_3 was used to increase the severity to the infrequent level. Wind pressures were then calculated for the site and building details. Heysham 2 was designed to wind speeds for the site of the sister station at Torness, which has a significantly higher basic wind speed therefore it is conservative. The PSR1 review considered the wind loading changes associated with the introduction of BS 6399-2:1997. This standard provides wind speeds in terms of hourly mean values. This is then subsequently converted into gust speeds by a gust peak factor which is a combination of other factors and takes account of gust duration time, height of the structure being considered above ground and the size of the structure.

Extreme Ambient Temperatures

The occurrence of extreme ambient temperatures is not treated formally as an external hazard against which defined plant items have to be qualified, as is required for earthquake and extreme winds, because the extreme ambient temperatures do not occur as sudden events but are preceded by a lead-in period. During this period the potential hazard becomes known and the station staff are able to take action to reduce some of the consequences.

Hourly temperature readings for Blackpool Airport for the decade 1971 to 1980 have been taken as representative of conditions on the coastline near Heysham. The decade 1971 to 1980 is chosen as being pessimistic relative to the fifty year period up to 1960 over which many of the recordings have been made. This decade includes high and low extremes for the last century. 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	Return Period
Frequent	-11°C	+30.6°C	1 in 50 years
Infrequent	-17°C	+36°C	1 in 10,000 years

Lightning

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 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 effectively 'Faraday Cages' in the context of lightning protection. 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. The effect of lightning current flowing within the structural steelwork is limited as the surge is transient and would only affect plant in the immediate vicinity of the conductor carrying the lightning current. The reactor protection systems comprise redundant, segregated and diverse systems and the earthing and bonding, shielding arrangements and cable installations mitigate the hazard associated with the lightning surge current and the magnetic fields. Buildings adjacent to the main buildings which were not separately protected against lightning were deemed covered within the zone of protection afforded by the main buildings. Surge protection is generally not provided on services to the buildings as the buried cables are provided with a continuous metallic screen of adequate thickness.

The CEGB 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 Heysham 2 are plant buildings which were considered to be protected by the 45° 'cone of protection', provided by the reactor, control and turbine

Lightning has not been formally considered as a hazard and this led to a shortfall being raised in PSR2 which required that a formal hazards safety case be produced for lightning (PICA 5.17.01).

Conclusion HYB 4.1: 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 adequate.

Drought

The Drought hazard was not addressed within a specific hazard topic report in PSR1 and has not yet been formally considered within the current safety case.

The climate at Heysham 2 experiences sufficient precipitation such that drought induced subsidence is not currently an issue. Currently, the Operating rules at Heysham 2 define the level of post-trip cooling stocks that must be available on-site. In addition, current government legislation specifies requirements on, in the case of Heysham 2 United Utilities, responsibilities for the provision of water supplies to the site. This legislation obliges the companies to ensure that essential supplies to the stations are maintained even under the worst drought conditions to ensure the availability of stocks of essential cooling water. There is no specific plant provided for protection against the effects of drought.

One of the effects of long-term climate change is postulated to be the lowering of the ground water table. The site at Heysham 2 is generally built on made ground, shore deposits and boulder clay overlying Bunter sandstone. The made ground consists of clay fill, sand fill and railway ballast. The clay deposits may be susceptible to shrinkage in the event of groundwater lowering, however, in general, it is expected that the granular deposits will not exhibit ground movements.

The major structures at Heysham 2 are founded at a low level on the underlying sandstone, by means of deep basements or by piling. These structures will not be directly affected by any shrinkage of the shallow deposits. However, connections of services and the junctions of adjacent structures to the main structures may be susceptible to ground movements.

It was also considered by PSR2 that joints between buried services and main structures and joints between structures should be monitored for ground movements where they may pose a risk to safety related plant and equipment. This is being addressed under normal company business.

PSR2 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.

In the event of an inability to maintain any of the water stocks at the specified minimum adequate levels within the relevant completion time, then station documentation requires that a controlled unit shutdown of the affected operating reactor(s) is initiated and that an immediate restoration of water stock levels is undertaken.

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 detail in this safety review.

Conclusion HYB 4.2: Drought is difficult to quantify, although advanced warning of the discontinuation of off-site water supplies should ensure that there is sufficient time available to the operators to allow the appropriate actions to be taken. The potential for groundwater changes to affect buried pipework has been identified and is being addressed. The station is founded on appropriate rock foundations such that drought-induced subsidence is not currently considered to be an issue.

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

The philosophy of the UK wind loading codes has changed considerably since the design of the stations. This reflects significant improvements in the understanding of wind loading. There have been amendments to the codes since the review of the hazard for PSR1.

Although the code changes do not affect the actual severity of the wind loading hazard, they are relevant when considering the adequacy of the qualification against wind loading. Heysham 2 and Torness were designed to the wind loading code CP3: Chapter V: Part 2: 1972. The PSR1 reviews considered the wind loading changes associated with the introduction of BS 6399-2: 1997. It was found that the wind loading to BS 6399-2: 1997 was generally less onerous than that to CP3.

A corrected and reprinted version of BS 6399-2 was issued in 2002. This is the current formal standard and will henceforth be referred to as BS 6399-2: 1997 (2002). The changes to BS 6399-2 since PSR1 are considered to be significant and in some respect the wind loading to BS 6399-2:1997 (2002) is more severe than that to CP3.

A normal business process was raised because wind loading to BS 6399-2: 1997 (2002) is more severe in some respects than that to which the safety related buildings were designed.

With regards to wind blown missiles, under commonly occurring wind conditions, the type of material which may become airborne is relatively light and can do little damage to buildings or plant. This is particularly so for the substantial structures of nuclear power stations. The safety case utilised the values calculated for the wind loading codes for the design basis against wind blown missiles. It is therefore claimed that there is inherent protection afforded by the station layout with essential supplies in diverse locations with respect to the main buildings. Very considerable protection derives from the main structures, which are predominately of reinforced concrete construction. Additionally, there is a good standard of 'housekeeping' to ensure the removal of loose objects from roofs, fixing of temporary scaffolding elements, storage of items inside buildings rather than leaving them on verges etc.

Tornado hazard has been assessed and it was found that the infrequent tornado wind speed was bound by the infrequent 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 HYB 4.3: Tornadoes have been assessed in PSR2 and no significant shortfalls have arisen.

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

PSR2 looked into climate change effects to extreme wind. It states that the extreme wind speeds at Heysham 2 and Torness are predicted to increase by around 4% and 2% respectively by 2080. Given the gradual nature of these increases over the next 70 years, any increase in the extreme wind speeds over the PSR2 period would be negligible compared to uncertainties and conservatisms in the design of structures against wind loading. Therefore, it is concluded that any increase in extreme wind speeds over the period covered by PSR2 would not adversely affect the safety case with respect to wind loading and does not present a time-dependent issue.

Conclusion HYB 4.4: 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 (EATs)

A report by the Met Office 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. The Met Office regional Climate Model 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.

These expected changes were judged to be small for the time period covered by the second periodic safety 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 work commissioned by EDF Energy to investigate the effects of climate change has recently reviewed the methodologies for:

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

<u>Extreme Air Temperatures</u>

Climate change prediction data has been obtained from a Met Office climate data report. This report presents an overview of UK climate change and includes a prediction of the change in maximum and minimum temperatures for the next 100 years. The results from the Met Office Regional Climate Model presented therein predict that seasonal average temperatures and daily maximum temperatures will generally increase. Based on high emissions scenario, the predicted temperature data presented in the Met Office climate data report that the summer average daily maximum temperature will rise by approximately 1 to 1.5°C for the Heysham region by 2020. These predicted changes are judged to not be significant in terms of its effect on the assumed return frequencies at Heysham 2. It should be noted, however, that the frequent temperature range maximum temperature has been exceeded recently on a number of occasions. This has been raised and is being addressed under normal company business.

Results from a Met office report based on UKCIP02 data 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 EAT-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 PSR documents.

Extreme Sea Water Temperatures

Sea water temperatures in the Heysham area are expected to be as low as -2°C and as high as 25°C for a return frequency of 1 in 10,000 years. The sea water intake at Heysham 2, however, is positioned at the entrance to a very busy harbour and the movement of ships, in and out of the harbour, will reduce the risk of sea ice. Additionally, local warming of the sea will be produced by the outfall from both Heysham 1 and Heysham 2 Power Stations.

The only essential plant which is claimed against extreme ambient temperatures and has a dependence on seawater cooling, is the circulator auxiliaries cooling system, this system can be cooled by either the reactor sea water system or the circulator auxiliaries diverse cooling system, which is not dependent on seawater cooling. It is concluded that a sea temperature of -2°C, which corresponds to a return frequency of 1 in 10,000 years, will not affect the availability of the RSW for the CACS. This is because the formation of sea ice should not affect the CW intake, which is at sufficient depth below the surface.

The normal at-power and post trip duty maximum temperature for cooling water intake safety case as 30°C, hence, it is concluded that a sea temperature of 25°C, which corresponds to a return frequency of 1 in 10,000 years, will not affect the availability of the plant. During normal operation, the sea water heat removal route is the ultimate heat sink for both essential and non essential plant with the reactor at full power. The initial effects of high sea temperature would be to reduce the output of the turbo-alternators as the increase in temperature resulted in higher pressures in the low pressure end of the turbine. Adequate post trip cooling would always be ensured, as all systems are designed to remove the heat generated when the reactors are on load. If necessary, non essential heat loads can be shut down to ensure post-trip cooling to essential plant. It is considered that appropriate operator intervention will prevent unacceptable damage or significant loss of performance to safety related plant.

Conclusion HYB 4.5: 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 sea water temperatures is not a current concern, largely as this would be primarily an environmental and commercial issue rather than a nuclear safety impact. 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 be beyond the design basis temperature.

Snowloading

PSR2 found that the original design loading of the metal decking to the Turbine Hall is in excess of the uniform snow loading derived using the current standard and there is substantial margin. However, the consideration of snow loading from drifting requires a detailed review as to quantify the full extent of snow loading from drifting and confirm the capability of the Turbine Hall building roofs. This has been raised as part of normal company business.

This assessment is currently ongoing (all nuclear safety related structures will be reviewed, not just the Turbine Hall).

A 2010 Met Office report on snow loading 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 showed that for Heysham 2 the expected snow loading from an infrequent event is 0.67 kN/m^2. This snowloading value is bounded by the design basis.

The work commissioned by EDF Energy to investigate the effects of climate change used a UKCIP09 met office report specifically written for EDF Energy sites and consultation with in-house specialist civil engineers and reported that the level of risk from snow loading was low.

EDF Energy has reviewed the information contained within the UKCP09's 'Interpretation and use of future snow projections from the 11-member Met Office Regional Climate Model ensemble' and also commissioned the Met Office to undertake a 'Study of snow loading for UK nuclear power stations: final report'.

The UKCP09 snow note discusses the number of snow days associated with different snow scenarios. The 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".

At present snowfall has not affected the safe and reliable operation of EDF Energy's nuclear power stations. As the UKCIP09 snow note states 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 does it does today.

Conclusion HYB 4.6: Snowloading has been considered in PSR2 and with only shortfalls of a low safety significance being identified.

Consideration HYB 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.

4.1.1.2 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 these extreme hazards were explicitly addressed at the infrequent event level in the original design basis.

For those hazards where an infrequent design basis event cannot be easily derived, (i.e., drought and lightning) this has been recognised and suitably pessimistic 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 PSR2 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 safety review, 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 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 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 not been considered in the safety case. However, the Hunterston B and Hinkley Point B safety cases do consider combinations of hazards and the findings therein are broadly applicable across the AGR fleet. They found that 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, although it is recognised that combined hazards may impact adversely on issues such as site access. The infrastructure and emergency arrangements are considered in Chapter 6. The following combinations 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

Though some stations have addressed the possibility of combinational hazards, it seems 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 HYB 4.7 Combinations of hazards have been considered in the HNB and HPB safety cases (Combined Hazards Review, August 2006), where they were judged not to impact adversely on nuclear safety. These findings are broadly applicable across the AGR fleet.

Consideration HYB 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 HYB 4.8: 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 HYB 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

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 infrequent 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.

Season Preparation

The station carries out winter readiness checks during the Autumn to assess plant and equipment for duty during the winter. For example, the procedure includes checking the Heating & Ventilation systems and intakes.

There are also station operating procedures that supply guidelines when a forecast of adverse weather has been received. These 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 the periods of severe weather.

In addition Hazard operating rules exist for each of the hazards that provide instruction to the operator to constrain operations if weather conditions exceed specified values.

4.2.1.1 Extreme Wind

Wind blown missiles that may be generated by this hazard are judged in 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.

Reactor at Power

Lines of Protection (LoP)

Table 4.2: Claimable Lines of Protection for Essential Safety Functions - Extreme Wind Hazards

Fault Title	Fault detection /trip initiation	Shutdown	GC trip	Post-trip cooling	Primary circuit pressure
High winds and wind blown missiles	Main guardlines	Main shutdown system	Gas circulation run-on protection remain available	Main boilers fed by backup feed system, primary coolant natural circulation	Not required

Note that the safety case places no reliance on automatic trip in response to high wind events. However, it is conservatively assumed that an infrequent high wind event will result in loss of grid, leading to an automatic trip. Although loss of grid would be likely in infrequent high winds, there is a reasonable chance that the grid supplies will remain operational. The issue of reliance on loss of grid to initiate a trip is not considered to affect the safety case as there is no requirement for trip initiation given that the plant forming the line of protection for shutdown and post-trip cooling is protected against infrequent (1 in 10,000 year) winds.

Trip

Trip is not required by the safety case, but the operator may decide to trip the reactor if a threat to safety related plant or personnel is perceived. The main guard lines, alternative diverse guard lines and the sequencing equipment are not at risk from design basis infrequent wind due to their location.

Shutdown

As the design basis initiating wind is an infrequent fault, only one Line of Protection is required (with redundancy). As an automatic trip is not claimed, the operator may manually trip the reactor, leading to shutdown by the main shutdown system. The secondary back up shutdown system is not claimed for an infrequent hazard. Failure of control rods due to a wind initiating event is not considered to be a credible event within design basis, as it is considered to be fail-safe on loss of supplies.

Post Trip Cooling

It is conservatively assumed that in the event of an infrequent design basis wind event, that the air-cooled boiler system is unavailable. It is also assumed that the seawater cooling system and the grid are lost.

It is considered that the pressure boundary could only be threatened if collapse or partial collapse of the charge hall were to occur. The main structural steelwork frame of the Charge Hall is designed to withstand the infrequent wind. This avoids risk of damage to the charge face or fuelling machine caused by falling structural members or the main charge hall crane. It is therefore considered that the integrity of the primary circuit is adequately protected.

The primary cooling of the reactor claimed for the infrequent event is by natural circulation. The various systems required to maintain this function are supplied by an onsite AC electrical supply system which is diverse, redundant and segregated. The building structures which house these systems are designed to withstand infrequent wind loadings.

The back up alternative boiler feed system and associated tanks are claimed as part of the line of protection for the secondary cooling function for infrequent events. All plant necessary for the function of these systems are located within buildings which are designed to withstand an infrequent wind.

Essential Monitoring

The control room and the alternative monitoring location, together with their associated instrumentation and cabling, are located in buildings that would remain available during infrequent wind conditions.

Electrical Supplies

As mentioned above, reserve sources of on-site AC power have been qualified against the infrequent wind hazard.

Shutdown Cooling

It is judged that the extreme wind hazard does not present a more onerous challenge to a shutdown reactor than one at power. Forced gas circulation will remain available, powered by onsite backup AC power systems if the grid is lost.

The safety cases for Heysham 2 and Torness do not require a re-seal/re-pressurise capability. An ongoing revision to the Torness safety case will review this justification and the relevance of any outcomes will be considered for Heysham 2.

Operator Actions

The operator has a role in monitoring conditions that lead up to the extreme event and in taking mitigating actions where appropriate. The operator is required to secure all doors and loose materials and equipment. The operator also takes specific actions as the forecast or actual wind speed reaches pre-defined levels. These actions include the restriction of roof working, non-essential movements around the site and the monitoring of essential plant states.

Operator responsibilities and actions to be taken in the event of extreme weather have been specified. The actions to be taken include:

- Confirm fuel handling operations are curtailed as specified in the relevant Operating Instructions.
- When the wind has abated it is recommended that a survey of essential post trip cooling plant is conducted to determine if any external equipment has been damaged by the wind or wind blown missiles.

Precautions and Limitations:

- Consider limiting fuel and component handling operations due to high wind speeds on receipt of high wind speed warnings or recordings.

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, and their power supplies, are qualified against the infrequent wind event. Back-up generation 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.

Wind Safety Margin

A safety margin for wind is difficult to define as an increase in the design basis wind will lead to different effects on different plant buildings as when failure will occur depends on the material and geometry of the building. However, it should be noted that assessment of buildings against the design basis wind involves calculating whether the wind will be strong enough to cause the building to yield. If the building does begin to yield, it will first start to experience plastic deformation before the structural integrity of the building is compromised. Plastic deformation will not lead to an immediate concern to nuclear safety therefore no cliff edge effect will be experienced if extremes winds greater than the design basis wind are experienced.

Conclusion HYB 4.9: 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 HYB 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: Claimable Lines of Protection for Essential Safety Functions – Extreme Ambient Temperatures

Fault Title	Fault detection /trip initiation	Shutdown	GC trip	Post-trip cooling	Primary circuit pressure
Extreme Ambient Conditions	Not required (option – operator)	Main shutdown system	Gas circulation run-on protection remain available	Main boilers fed by backup feed system, primary coolant natural circulation	Not required

It is assumed that Loss of Offsite Power occurs at Extreme Low Ambient Temperature events and not during Extreme High Ambient Temperatures.

Extreme Low Ambient Temperature

Trip

Reactor trip to ensure reactor safety is not required in the event of design basis extreme ambient temperatures, however the operator may decide to initiate manual shutdown as a precaution. The main guard lines are located in safety rooms. The safety rooms are within an area which receives H&V supply, which meets the condition requirements for a minimum external air temperature of -13°C. For the -17°C winter extreme, the temperature in the safety rooms could fall below the design minimum by a few degrees, but would remain within plant limits. In addition, the trip systems are inherently fail-safe.

Shutdown

The control rod clutches are within the pressure circuit and their temperature is controlled by the pile cap concrete, which is not sensitive to external temperatures. Low external ambient temperatures will not, therefore, have any significant effect on the Primary Shutdown system.

Post Trip Cooling

Extreme high or low ambient temperatures are not expected to lead to a depressurisation fault. For pressurised reactor trips, adequate post-trip cooling can be achieved either by forced circulation, or by natural circulation providing the pressure boundary is maintained.

Three lines of post-trip feed are qualified to withstand an infrequent low extreme ambient temperature event (-17°C). It can therefore be concluded that adequate post-trip cooling protection, with redundancy and diversity, is qualified to withstand the low ambient temperature infrequent event.

Essential Monitoring

The temperatures in the central control room would not be expected to fall below +16°C during prolonged periods with external temperatures at -17°C due to the H&V system and secondary heaters which would be available.

Electrical Supplies

All back up electrical AC supplies and associated systems are qualified for -25°C and utilise electrical heating and trace heating for maintaining acceptable temperature levels during periods of extreme low temperature conditions. Heaters and trace heating associated with essential plant are checked during periods of extreme cold weather to confirm functionality.

Shutdown Cooling

As outlined in the section above, in the event of an infrequent ambient temperature event, it is conservatively assumed that the grid is lost.

If an infrequent extreme low ambient temperature event occurs during a period whereby the reactor is shutdown depressurised, then forced circulation is maintained by the gas circulators powered by the onsite backup electrical AC supplies, using diverse means in order to maintain reactor cooling

Note the alternative boiler feed system supplied by the alternative water supply tanks will also remain available.

The existing safety cases for Heysham 2 and Torness do not require a re-seal/re-pressurise capability. An ongoing revision to the Heysham 2 safety case will review this justification.

Operator Actions

Various operator actions are laid out in station documentation in order to safeguard the plant from extreme low temperatures. When very low air temperatures or any prolonged period of low temperature are predicted the operator actions include:

- Reduce ventilation airflow in essential supplies buildings and cable tunnels to conserve heat, protect against freezing conditions and guarantee battery performance.
- Secure fire fighting systems against freezing condition.
- Confirm operation of backup feed systems and AC supplies.
- Consider the shutdown of operating reactors if the ambient temperature is predicted to fall below -17 °C.
- Provide additional temporary heating as appropriate to support essential systems.
- Suspend use of charge hall crane at temperature below +5°C.
- Fire auxiliary boilers.
- Confirm air supply grills are not blocked by snow / ice.

Extreme High Ambient Temperature

Trip

The main guardlines are located in the safety rooms. The safety rooms are within the area controlled by the H&V supply, which meets the condition requirements for +29.5°C maximum external temperature. For the +36°C summer extreme, the temperature in the safety rooms could rise above the design maximum by a few degrees, but would remain within plant limits. Very high temperatures, sufficient to threaten equipment, would require widespread H&V plant failures to occur, and such temperatures are separately detected and would result in an automatic reactor trip at 40°C. In addition, the trip systems are inherently fail-safe.

Shutdown

The control rod clutches are within the pressure circuit and their temperature is controlled by the pile cap concrete, which is not sensitive to external temperatures. High external ambient temperatures will not therefore have any significant effect on the Primary Shutdown System.

Post Trip Cooling

Extreme high or low ambient temperatures are not expected to lead to a depressurisation fault. For pressurised reactor trips, adequate post-trip cooling can be achieved either by forced circulation, or by natural circulation providing the pressure boundary is maintained.

Three lines of post-trip feed are qualified to withstand the infrequent high extreme ambient temperature event (+36°C). It can therefore be concluded that adequate post-trip cooling protection, with redundancy and diversity, is qualified to withstand the high ambient temperature infrequent event.

Essential Monitoring

The H&V system ensures that the temperatures in the main control room will be maintained within the condition requirements for a temperature of +29.5°C. At the high temperature extreme, the main control room temperature could exceed the design maximum by a few degrees. Although the station computers could be affected, safety of the reactors remains with the reactor protection systems, post-trip autosequence and post trip cooling systems, all of which are independent of the station computers. Operations which utilise the computer could be safely suspended.

Electrical Supplies

All onsite back up electrical AC supply equipment is qualified to +40°C.

Shutdown Cooling

As outlined in the section above, in the event of an infrequent ambient temperature event, it is conservatively assumed that the grid is lost.

If an infrequent extreme high ambient temperature event occurs during a period whereby the reactor is shutdown depressurised, then forced circulation is maintained by the gas circulators powered by the onsite backup electrical AC supplies, using diverse means in order to maintain reactor cooling.

Note the alternative boiler feed system supplied by the alternative water supply tanks will also remain available.

The existing safety cases for Heysham 2 and Torness do not require a re-seal/re-pressurise capability. An ongoing revision to the Heysham 2 safety case will review this justification.

Operator Actions

Various operator actions are laid out in station documentation in order to safeguard the plant from extreme high temperatures. When very high air temperatures or any prolonged period of high temperature are predicted the operator actions include:

- Improve cooling air flow to quadrant areas by operation of upper and lower hot gas vents.
- Provide additional cooling for computer and instrument rooms as appropriate.
- Restrict use of high voltage connectors at outside air temperature approaching 36°C.
- Seek specialist advice if the outside air temperature is predicted to reach 36°C and consider the shutdown of operating reactors (Decay heat air cooled system design temperature 34°C. Above this level additional flash steam produced).

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 (High and Low) Ambient Temperature Safety Margin

A safety margin can not 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 backup

AC electrical power supplies fail would be a possible cliff edge as the cooling of the plant would be compromised. This is mitigated by operator actions.

Conclusion HYB 4.10: 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 though a possible cliff edge has been identified.

Consideration HYB 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 HYB 4.11: Arrangements are in place to protect against extremes of lightning and drought. It is not 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 HYB 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

A periodic safety review reviewed the operator actions required for the extreme weather hazards discussed in the chapter for AGR stations. The safety 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 HYB 4.12: Operator actions undertaken during extreme weather events were reviewed in PSR2 and were deemed appropriate.

Consideration HYB 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 actions undertaking when warnings of extreme weather are received.

Conclusion HYB 4.13: 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 HYB 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 PSR and will be reviewed again in the third PSR for the station. Whilst those PSR2 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 on climate change across EDF Energy's fleet of nuclear stations, a number of gaps were identified by the adaptation risk exercise. For each gap identified, a suggested adaptation option was also specified. 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 climate adaptation review work

Gap identified	Suggested adaptation 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 EA 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 town's water (e.g. Ensure minimum flow rate) during drought conditions
	Engage with EA 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

It is considered that by regular monitoring of meteorological trends and assessment of the plants response to these, the robustness of the protection against extreme weather conditions will be maintained.

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, justification for continued operation periodic safety review commitment, and justification for continued operation. Whilst these are within the processes we use to comply with our licensing basis we have listed below all of the significant relevant issues in these categories along with the outline of the work we are undertaking to address them.

EDF Energy undertook reviews in light of the events at the Fukushima Dai-ichi plant. 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 reviews.

The findings of the extreme weather aspects for within design basis review and the beyond design basis review 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 review

Scope

Within design basis review 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 review found that that 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 review

Scope

Beyond design basis review 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 review, 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 HYB 4.14: 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 HYB 4.10: Consideration should be given to all stations receiving site specific weather forecasts.

Consideration HYB 4.11: Consideration should be given to the provision of additional station based robust means of personnel transport for extreme weather conditions.

4.3 Summary

The design basis for an infrequent extreme wind is based on demonstrating that buildings conform to relevant standards and codes for an infrequent wind event. 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 at Heysham 2 has been assessed against the latest codes and is robust.

The infrequent extreme ambient temperature hazard can be split into four possible events; high temperatures and low temperatures, sea temperature and snow loading. The design basis for the high and low air temperatures has not been verified and a consideration is raised in this report to do so. 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. Sea water temperature is primarily a commercial concern and it is judged incredible that changes in temperature will impact nuclear safety. The reactor island buildings and others containing essential equipment have been assessed against snow loading and demonstrate sufficient margin.

Work commissioned by EDF Energy to investigate the effects of climate change predicts that 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, as it is difficult to quantify. The primary defence against drought is that it is slow to occur compared with the station mission time.

Protection against lightning is provided by adherence to relevant codes and standards. It is judged this remains a suitable and appropriate measure.

Chapter 5 – Loss of Electrical Power and Loss of Ultimate Heat Sink

Heysham 2

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 ultimate heat sink scenarios. This includes examination of all means available to supply post-trip cooling and an evaluation of time scales 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 de-pressurised 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 Heysham 2 to the electrical grid.

5.1 Nuclear power reactors

The essential safety functions described above are briefly described in some more detail below.

Trip, Shutdown and Hold-down

Reactor trip is provided via two diverse trip systems or by manual trip by the operators. Reactor shut-down is enforced by introduction into the reactor of any one of three systems that absorb the neutrons; the main shutdown system does this with control rods, the backup shutdown system consists of Nitrogen gas injection system or finally by the manual injection of Boron beads. The main shutdown system comprises control rods, whose power supplies are removed from their clutches on a reactor trip signal causing them to fall into the core under gravity. These systems are designed to be fail-safe on loss of power.

Post-trip Cooling and Containment

Post-trip cooling is usually provided by forced CO_2 gas circulation. Forced gas circulation requires a supply of power from either the main grid or on-site back-up generators.

Natural circulation of the CO_2 will provide adequate gas circulation and heat transfer from the fuel to the boilers when the reactor is pressurised and without the need for electrical supplies. In an unpressurised reactor natural circulation can not provide a sufficient amount of post-trip cooling.

Post-trip feed water is normally provided to the boilers from on-site tanks by electrically powered pumps. Various other feed systems are also available.

The concrete pressure vessel provides a robust containment for the reactor primary coolant (CO_2). Cooling of the concrete pressure vessel requires both electrical supplies and a heat sink. The nuclear fuel's irradiated 'fission products' are primarily constrained by the fuel material itself and by the fuel assembly's steel cladding.

5.1.1 Loss of electrical power

The stress-test review of the various scenarios for 'loss of electrical power' at Heysham 2 and their impact on the plant that is required to carry out the essential safety functions 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 a loss of electrical power scenario are considered later.

Under normal operating conditions, supplies to the station essential electrical system loads are provided by the National Grid via the main electrical system and transformed and/or converted to produce alternating current (AC) or direct current (DC) supplies at the various required voltage levels. However, if supplies from the grid are lost or vary outside of defined tolerances, the station essential electrical systems are automatically isolated from the source of the disturbance by the Grid Disturbance Protection which trips the relevant station incoming circuit breakers. The associated reactor and turbine generator will trip, and supplies to the loads that must remain available in the immediate post trip period will be provided by the battery backed systems. Loads that can tolerate a short-break in supply will be supplied from the diesel generator backed essential systems following automatic starting of the diesel generators.

Heysham 2 has two types of diesel generators with one of each type in four diesel houses and associated essential supplies buildings. This provides diversity, segregation and redundancy to meet the essential load and systems reliability requirements. The segregation and redundancy requirements are achieved by an arrangement whereby four generators feed one train of equipment and four feed a diverse second train.

For the purposes of the stress-test, one train has been allocated as the 'ordinary AC back-up' and the other train as the 'diverse AC back-up'.

Normal Power Operation

Following a reactor trip due to loss of availability of the grid-derived supplies, all eight essential diesel generators are automatically started up simultaneously. There are battery backed electrical systems to support the operation of the loads that must remain available in the immediate post trip period until diesel generators have been fully started. After a time delay of about thirty seconds that allows for the start and run-up of the diesel generators, all loads required post trip are sequenced onto the diesel generator supply.

Reactors Shutdown and Depressurised

The essential diesel generators are only started automatically following a reactor trip.

If a loss of grid event occurred when the reactor was shutdown and depressurised, for example during an outage, the diesel generators would be started manually. The diesel generators can be started manually from any of three places:

- Diesel generator control room
- Diesel generator local control panel
- Central control room

5.1.1.1 Loss of off-site power

This stress-test scenario proposes a loss of off-site AC power supply, which constitutes a loss to the station's reactors of all of the electrical power supplied by the National Grid network. For this stress-test scenario, off-site power is assumed to be lost for several days and the site is isolated from delivery of heavy material for three days. This 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

Ordinary on-site AC back-up power system

The most significant loads on the ordinary essential system are those required to support forced circulation of gas in the primary circuit after a reactor trip. These loads are the circulator variable-frequency converters, the decay heat boiler system and other circulator auxiliaries post-trip. This load is provided by the 'ordinary AC back-up' system.

The generators have the capacity to supply their loads for a number of days of operation (operator can manage the supply from the generators in order to meet load requirements). Only one of the four diesel generators is required to operate throughout the mission time to provide AC supplies for the essential plant. In order to ensure the 'preparedness' to deploy this system a formal maintenance regime is in place.

Guaranteed Supplies System: "Uninterruptible Power Supply" Battery Banks

Battery supplies are not used on the UK AGRs to drive the long-term operation of any cooling / pumping systems.

The need for battery capacity is therefore limited to ensuring that the batteries are capable of providing supplies to support the essential system functions on loss of the ordinary grid supply.

Batteries are also needed to feed essential lighting invertors, many instruments and post-trip control panels and the diesel generator starting controls.

Three starting air receivers are provided per diesel generator, two of which are used for automatic starting of the diesel engine and one for manual starting. A minimum of six starts of the diesel engine can be achieved without recharging the receivers.

Black Start-up

The essential diesel generators require that battery backed supplies are available in order to start. In the loss of off-site power fault the generators would be able to start. However, if in addition these battery supplies were not available, due to some unknown reason, then a number of solenoid-operated air-start valves would not be able to operate and the generators would not start.

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

Fuel Oil & Mission Run-times

A fuel oil day tank is provided at high level to feed each diesel engine and this has the capacity to meet the full load running requirement for approximately 8 hours. Gravity feed allows start up under loss of grid conditions. Three bulk tanks designated to each diesel generator are all inter-connected in order that transfers of fuel inventory can be made between them.

It is judged that each ordinary AC backup generator and each diverse AC backup generator could support an extended run time of up to three days based on fuel stocks held on-site, although some prioritisation of key loads to support would need to be made. The run times given are for each separate train in service. Clearly as only one train out of eight is needed, if all eight were available, there would be potential for an extension to the run time if each train is used in turn.

5.1.1.2 Loss of off-site power and loss of the ordinary back-up AC power source

This stress-test scenario proposes a loss of off-site power supply as well as loss of the AC supply from the ordinary diesel generator systems through failure or unavailability. This is considered within the station safety case.

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

Diverse on-site AC back-up power system

The most significant loads on the diverse essential electrical trains are those required to support the post-reactor-trip natural circulation cooling of the reactor core. These loads are basically the emergency boiler feed pumps, the valve actuators and pressure control systems enabling these pumps to feed the main boilers, and the post-trip systems required to co-ordinate them.

The diverse generators have the capacity to supply their loads for up to several days (or more depending on fuel stocks) of operation. Only one of the four diesel generators is required to operate throughout the mission time to provide AC supplies for the plant (operator can manage the supply from the generators in order to meet load requirements).. Although they can be interconnected, these diesels would not normally be used to supply normal system loads. In order to ensure the 'preparedness' to deploy this system a formal maintenance regime is in place.

Conclusion HYB 5.1: In the event of loss of grid, there are sufficient supplies of fuel oil for the ordinary backup generators to continue operating under operator controlled load for several days mission time.

Conclusion HYB 5.2: In the event of loss of grid, there are sufficient supplies of fuel oil for the diverse backup generators to continue operating under operator controlled load for several days mission time.

Consideration HYB 5.1: Consideration should be given to the practicability of 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.

Conclusion HYB 5.3: Loss of off-site power combined with loss of the ordinary back-up AC power supply is an event considered within the safety case and adequate provisions are made to support the essential safety functions.

5.1.1.2.2 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.

The need for battery capacity, duration and recharge at Heysham 2 is limited to ensuring that the batteries are capable of providing supplies to support control and instrumentation and lighting requirements and to ensure the no-break systems function while the ordinary or diverse AC power supplies start up. The batteries are normally recharged from essential services supplies that are supported by diesel generators. Batteries are also provided to start the diesels, but once started, the batteries have no further role in supporting post trip cooling, so do not need to be recharged as part of the scenario.

There are also three different telecoms systems provided with separate battery supplies and systems to provide the power supply for control action from the CCR.

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.

For Heysham 2 this scenario proposes a loss of off-site power supply as well as loss of the back-up AC supply from both the normal and diverse essential diesel generator systems. This comprises the 'Station Blackout Scenario' for Heysham 2 as the station does not have further, alternative AC generating capability.

This scenario is not considered within the safety case since significant diversity, redundancy and segregation is provided such that complete loss of power is not considered credible within the design basis.

On loss of all on-site AC power, trip and shutdown are fail safe however all of the installed equipment providing forced circulation will be lost, as will all auxiliary cooling including the pressure vessel cooling system.

There are no provisions for any further, diverse permanently installed AC power source at Heysham 2. The safety case relies solely on the availability of the installed normal and diverse generators for AC power.

<u>Reactor: Pressurised – Natural Circulation</u>

In a station blackout situation an emergency feed system is available that can be manually connected to main boilers in order to provide post-trip cooling for a number of hours. Natural circulation of coolant gas within the reactor pressure vessel would be promoted by the temperature difference induced by the cooling water feed to the boilers. Water feed from tanks is provided to the boilers for one quadrant on each reactor.

To implement this feed system an isolating valve in the emergency boiler feed line would require stripping out and the internals of the valve would be removed and a special fire hose connection assembly fitted. The boilers would be vented and gas circulator flow vanes opened (if they were not already open) to allow natural gas circulation to be established.

As both reactors could be tripped at the same time, equipment capacity is sufficient to feed one main boiler on each reactor. It should be noted that this feed system is not currently formally claimed as a line of protection for the plant and is currently provided as a risk mitigation measure.

The emergency feed system would need to be fully implemented within a number of hours post-trip, in order to provide effective cooling to establish natural circulation. If the emergency feed system was ever to be claimed as an additional line of protection, the simplicity of the means of connecting it to the main boiler via the existing pipework would need to be ensured.

Conclusion HYB 5.4: Although there are no diverse permanently installed AC power sources, there exists a Backup Emergency Feed System (BUEFS) on-site that can be used for post trip cooling but does not generate any electrical power. The existing BUEFS has a number of potential areas for improvement.

Consideration HYB 5.2: The potential for improving redundancy, reliability and ease of installation of the BUEFS should be considered.

Primary Circuit Integrity

A no-break electrical system supplied by 415V batteries is provided as a means to close the primary gas treatment plant isolation valves. This ensures that the reactor circuit is isolated post-trip to those parts of the gas treatment plant that are not seismically qualified.

Reactor: Shut down & De-pressurised

If the reactor has been depressurised, then forced circulation is necessary to provide adequate post-trip cooling, and it is expected that the gas circulators (supplied by the ordinary AC back-up generators) would normally be available for this purpose.

However, as this stress test assumes the loss of all generator supply and hence all gas circulators; then natural circulation post-trip cooling would need to be established by re-sealing and re-pressurising the reactor. The provision of boiler feed would need to be made to the main boilers in order to remove the decay heat. This would normally be done via one of two boiler feed systems but in this loss of all generator supply scenario this would be provided by the back-up emergency feed system discussed above.

Conclusion HYB 5.5: There is currently no safety case explicitly covering Station Black Out (SBO) for Heysham 2.

Consideration HYB 5.3: Consideration should be given to reviewing the status of the arrangements to cover the event of Station Black Out (SBO) for Heysham 2.

5.1.1.3.1 Battery capacity, duration and possibilities to recharge batteries in this situation

Battery supplies are not used on the UK AGRs to drive the long-term operation of any cooling / pumping systems.

The need for battery capacity, duration and recharge at Heysham 2 is therefore limited to ensuring that the batteries are capable of providing supplies to support the no-break system functions and those described in Section 5.1.1.2.2.

There are no provisions to recharge the batteries during a station black-out once they have been depleted. The batteries are normally recharged from the essential services supplies that are fed by diesel generators. Most batteries are only claimed for 30 minutes operation. There is currently no safety case to support a 72 hour mission time for battery supply, as there is an expectation that essential diesel generators will be made operational within 30 minutes.

Conclusion HYB 5.6: A no-break DC battery back-up system is provided to supply plant that cannot tolerate the short breaks in power on loss of grid supplies during the Essential Diesel Generator start, run-up and loading time. During Station Black Out (SBO), the back up battery DC supplies are claimed for 30 minutes in the current safety case. The primary concern here is about control and instrumentation.

Consideration HYB 5.4: Consider whether additional means could usefully be installed in order to extend the formally claimed battery mission time by some margin.

Consideration HYB 5.5: Consider providing resilient supplies for essential control and instrumentation and lighting functions (fixed and portable) for all relevant areas of plant on-site.

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 an appropriate time frame following the declaration of an off-site nuclear emergency.

Conclusion HYB 5.7: There are provisions off-site that could be deployed to station within a number hours that could provide power generation capability and aid 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 advanced gas-cooled reactor 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 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. 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 HYB 5.8: 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 CESC and procedures for beyond design basis events.

Consideration HYB 5.6: Consideration should be given to provision of training, planning or pre-engineering in order to improve mitigation measures.

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

Reactor: Pressurised

If all AC power is lost when the reactor is pressurised (either at power or shut down), the gas circulators and pumps for the post trip heat removal systems could not be operated. In this situation, cooling by natural circulation would be limited as without the provision of cooling to the main boilers, to create a temperature difference in the reactor, unforced flow of the coolant is not promoted.

Only the back-up emergency feed system remains available to supply main boiler feed.

- Studies to determine the time available to fuel damage under these circumstances have not been undertaken.
- It is judged that provision of minimum boiler feed for the mission time of 24 hours, followed by complete loss of post trip cooling: temperatures that would cause significant fuel damage would be reached after something approaching 3 days.

Reactors: Shut down & De-pressurised

For a de-pressurised reactor the minimum cooling requirements require forced circulation unless operator action is taken to re-seal the pressure vessel and then re-pressurise the primary coolant to enable natural circulation. Neither of these is possible under station black-out conditions.

A reactor which is in a depressurised state will have been shut down for the minimum post trip cooling period of several days before depressurisation is permitted. As the number of days since shutdown increases and the reactor decay heat decreases, the operators are permitted to start more complicated tasks and open up penetrations which will take longer to re-seal. The shutdown safety case provides guidance on timescales to ensure that the re-seal operation can be readily achieved by ensuring all resources are in place at a given time into the reactor outage.

EDF Energy is currently undertaking new thermal-hydraulic transient analysis work using the latest analysis techniques to determine more accurate timescales available to provide electrical power for re-seal and re-pressurisation in order to restore cooling before the onset of any potential fuel or structural damage.

Conclusion HYB 5.9: 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 HYB 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 reseal 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 contains further considerations for additional emergency backup equipment which would mitigate against the effects of a beyond design basis loss of electrical power.

Conclusion HYB 5.10: The current robustness and maintenance of the plant is compliant with its design basis for loss of electrical power. However, steps to improve the resilience of the plant following a beyond design basis event are being considered.

Conclusion HYB 5.11: There are not sufficient electrical supplies to provide 72 hours of post trip cooling in the event of a station black out (loss of on-site power & Loss of both emergency diesel generator trains). The current assumption is that the EDGs could be made functional within this time.

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 of provision of adequate post-trip cooling.

The stress-test review of the various scenarios for 'loss of ultimate heat sink' at Heysham 2 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.

The water for the two main cooling water systems is obtained from the Irish Sea via intakes in Heysham Harbour to the forebay and screening plant. Coarse screens are located in the water intakes to the individual screen chambers to remove fine debris from the seawater and prevent the passage of seaweed, fish and other debris into the cooling water systems. The drum screens are continuously backwashed to remove screened material.

The various cooling water systems provided at Heysham 2 are described in detail in Chapter 1.

In summary these are as follows:

- During normal at power operation, boiler feed is normally supplied by the main boiler feed system; this comprises re-circulating boiler feed water which has been cooled by sea water-fed condensers. Reserve feed water tanks provide makeup water to the boiler feed when required.
- The main cooling water system provides a heat sink for the condensate system by supplying seawater to the main condenser and returning this warmed water to the sea. This system does not perform a safety function and its functional failure is not of direct nuclear safety significance.
- The second main seawater cooling water system provides essential cooling water to items of plant and maintains this supply post-trip to ensure reactor safety. It also provides the heat sink for the gas circulator cooling system as well as for aspects of fuel route cooling and the pressure vessel cooling system.
- During shutdown, boiler feed is normally supplied by a closed loop decay heat boiler feed system. This re-circulating cooling water system is used to transfer heat to atmosphere via air coolers.
- Two diverse heat sinks exist for cooling the gas circulators; one with a seawater heat-sink and the other with an atmospheric heat-sink.
- A pressure vessel cooling system provides cooling to the pressure vessel liner and penetrations, to maintain safe levels of temperatures in the pre-stressed concrete and tendons of the reactor pressure vessel when the reactor is at power.

5.1.3.1 Design provisions to prevent the loss of the primary ultimate heat sink, such as alternative inlets for sea water or systems to protect main water inlet from blocking

The screening plant for the cooling water systems at Heysham 2 consists of self-cleaning rotating drum screens, each one serving a main cooling water pump and also a pair of pumps serving the essential (safety related) cooling water system. The screens prevent fish, seaweed and marine debris from entering the system.

The safety related essential main cooling water pumps draw significantly less water than the other main cooling water system. The station operators are also required to trip the main pumps on receipt of low suction alarms in order to safeguard the supply to the safety related essential cooling water system.

A company specification defines the best practice for chemical control of marine fouling. At Heysham 2, the cooing water intake is dosed continuously, all year round. Full or partial blockage of the cooling water drum screens will initiate an alarm at the central control room. This enables operators to take preventative action in the case of gradual build up of biological fouling.

Conclusion HYB 5.12: Several means of preventing the loss of main cooling water supply by blockage of the water intakes are employed at Heysham 2 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 river, lake, sea or main cooling tower)

This scenario proposes a loss of all seawater cooling through failure or unavailability, comprising loss of both the main cooling water supply and the essential cooling water supplies. This is a loss only of the seawater heat-sink. Alternative heat sinks are available at Heysham 2 and these are described in Section 5.1.3.2.1 below.

The loss of both main cooling water system feed is allowed for within the station safety case.

During normal reactor operation, the circulator cooling system rejects heat to the sea via the essential cooling water system. Following a reactor trip, gas circulator system heat may be rejected to that system or via a diverse system to the atmosphere. The essential main cooling water system for each reactor is configured to operate as two separate circuits, such that in the event of loss of one circuit the remaining circuit would provide cooling to two circulator cooling loops.

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 alternative heat sink

Alternative heat sinks remain available at Heysham 2, comprising:

Towns-water

The station reservoir, located within the site boundary, has two storage compartments supplied by two underground local water board pipelines. The two storage compartments each provide an alternative supply to the station, should one compartment ever become empty.

Raw water from the reservoir is pumped by one of three booster pumps to two storage tanks. From here the water is distributed (gravity-fed) to services throughout the station and nuclear island including the water treatment plant which in turn supplies the 3 reserve feed tanks. Two of the booster pumps are required to be in service, operated automatically via a level control system. The third pump is on standby and is started manually when required.

Emergency boiler feed system (reactor & fuel) cooling

This system can be used for long term cooling of the main boilers with water supplied from the reserve feed tanks. The water is transferred using pumps driven by power from the diverse AC back-up diesels and is then vented off as steam.

Back-up emergency feed system (reactor & fuel) cooling

This system can be employed when the emergency boiler feed pumps are unavailable to carry out the same function; drawing water directly from the towns-water supplied ring-main through the main boiler to be vented as steam. Water is transferred from the ring-main using a petrol-driven pump.

Pressure vessel cooling system

In the event of loss of either one or both pressure vessel cooling circuits for a period of 30 minutes there is a requirement for the reactor to be tripped. If both cooling circuits have been lost, then the reactor should be cooled at the maximum rate possible. Fire hose connections have been provided to allow an alternative supply of cooling water from the fire hydrant system to be used for the pond cooling heat exchanger, pressure vessel heat exchanger, decay store heat exchanger and the irradiated fuel dismantling cell.

Decay heat boiler system (reactor & fuel) cooling

This system circulates water through the decay heat boilers and eventually transfers the heat to atmosphere through an air-cooled system. The water is circulated using pumps driven by power from the ordinary AC back-up diesels. There are four separate cooling loops; one per reactor quadrant. Only one single loop is required to carry out the satisfactory post trip cooling function.

Reactors: shut down

The only significant impact that complete loss of essential cooling water would have on the plant claimed for cooling on a shut down reactor would be to affect the heat sink which provides cooling to the gas circulators. However, an alternative heat sink is available.

Diagrid support cooling system

This system provides cooling to the lower section of the Diagrid support skirt to reduce fatigue due to reactor temperature cycling. The cooling reduces the magnitude of bending stresses that arise from differential thermal expansion between the skirt and the bottom slab of the pressure vessel. The system is required to operate both during reactor operation and following a reactor trip. The heat absorbed by the cooling system is normally rejected to the sea, via the essential cooling water system. The occasional total loss of this cooling function can be tolerated and there is a requirement for the reactor to be tripped if all cooling is lost for a period longer than 30 minutes.

Conclusion HYB 5.13: Diverse alternative heat sinks for primary circuit cooling (boiler feed) and essential equipment cooling exist in case of loss of the primary ultimate heat sink i.e. the sea – this is covered by the existing safety case.

5.1.3.2.2 Possible time constraints for availability of alternate heat sink and possibilities to increase the available time

Towns-water

The towns-water for the emergency boiler feed system is held in permanently installed and connected reserve feed tanks and therefore there would be no delay in making this available. If towns-water make-up supply is available, this heat sink will remain available indefinitely, as long as there is electrical power being supplied to the pumps.

The pressure vessel cooling system head tank has a capacity which is sufficient for 24 hours normal operation without make-up. Make-up is provided by the reserve feed water system booster pumps, and is controlled by a ball float valve. The fire hose reels for the pressure vessel cooling system alternate heat sink would require a manual connection to be made in order to re-establish cooling. This would only be carried out if both circuits are lost. If towns-water supply is available, this heat sink will remain available indefinitely, as long as there is electrical power being supplied to the pumps.

Atmosphere

The decay heat boiler and circulator cooling systems are permanently installed and connected to their respective air cooler fans. Therefore there would be no delay associated with using this heat sink. This heat sink would remain available indefinitely, as long as there is electrical power being supplied to the pumps and the air coolers.

Conclusion HYB 5.14: In the event of a loss of the heat sink, there are sufficient stocks of cooling water for a minimum period of 24 hour.

Consideration HYB 5.8: 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, towns-water and any air based cooling systems through failure or unavailability. This is a total loss of all otherwise available cooling via any systems available.

Note that this pessimistic scenario assumes, in addition to the loss of normal seawater cooling, loss of the two separately claimed alternative heat sinks, as well as the further mitigating heat sink that could be provided by the back-up emergency feed system. This scenario is considered to be beyond the design basis.

5.1.3.3.1 External actions foreseen to prevent fuel degradation

In this total loss of cooling scenario, the key action required would be to restore feed-water to at least one boiler or decay heat boiler on each reactor. Note that whilst pressure vessel cooling is desirable, in these very low frequency scenarios, it is not essential.

However, the need for pressure vessel cooling is dictated by the requirements to maintain vessel integrity, particularly if there is a need to maintain pressurisation and the potential for natural circulation.

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 an appropriate timescale following the declaration of an off-site nuclear emergency (Chapter 6).

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

Reactor: Pressurised

If the ultimate and alternative heat sinks are lost, natural circulation flows would transfer heat from the core to structures, leading to failures of key components before the onset of severe 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.

Depending on the station design and on the fault conditions, either boiler supports or core supports will fail first, although the relevant timescales are many hours even under the most pessimistic scenarios.

For this total loss of cooling scenario if a viable boiler feed can be restored within several hours, the situation is recoverable and severe core degradation is not expected to 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.

A sensitivity study has been carried out which indicates that if the boilers are fed for a time before being lost, then the timescale on which feed needs to be restored is increased accordingly. Each additional period of initial boiler cooling gives further extension to the time available to restore longer term cooling.

Reactor: Shut-down & De-pressurised

If the reactor is depressurised, then forced circulation is necessary to provide adequate post-trip cooling, and it is expected that the gas circulators (supplied by the diesel generators) would normally be available for this purpose. In the extremely unlikely event that the gas circulators fail, the reactor will need to be re-pressurised to establish natural circulation.

Adequate post-trip cooling would need to be established by the provision of boiler feed water within many hours post-trip.

This scenario pessimistically assumes the loss of all heat sinks as well as the petrol-driven back-up emergency feed system. These transfer systems do however retain their electrical supplies. Therefore, an alternative measure would need to obtain further water to use as a heat-sink to feed either the decay heat boilers or the main boilers. However, it should be noted that the decay heat boiler system is a closed system and if appropriate AC power supplies are available, the system can be operated with minimal losses of inventory.

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)

This scenario proposes a loss of primary ultimate heat sink (sea water cooling) as well as a complete station blackout comprising loss of off-site power supply as well as loss of all back-up power supplies.

This is a total loss of all otherwise available AC supply capacity combined with loss of seawater cooling; not just the ‘ordinary’ supply but also any ‘diverse’ supplies are lost. This scenario is thus a combination of the scenarios considered in Sections 5.1.1.3 and 5.1.3.2.

If loss of ultimate heat sink coincided with station blackout, the power to drive the decay heat boiler cooling system would be lost leaving the petrol-driven back-up emergency feed system pump as the only alternative heat sink still available. The system could provide minimal cooling to the reactor using towns-water passed through the main boiler and vented as steam. The potential issue in this scenario would be loss of post-trip monitoring provisions.

In itself this would not lead to severe core damage but would impede management of the recovery.

An additional scenario that this report has decided to cover is for the unlikely event of complete station black out on a pressurised reactor and a loss of all heat sinks, including all diesel / petrol driven pump systems. In that case, the estimate is that important structural failures would occur after several hours, implying that if boiler feed can be restored before then, the situation is recoverable and severe core degradation is not expected not occur.

5.1.3.4.1 Time of autonomy of the site before start of water loss from the primary circuit starts

Advanced Gas-Cooled Reactors do not use water in the primary cooling circuits of the reactors. The cooling medium is pressurised CO_2 gas.

The loss of the CO_2 gas, which is used as the 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 heat sink or failure of other back up systems as there is no causal link between such failures and the systems have been demonstrated to survive the effects of hot CO_2 gas release.

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. Consideration is given to measures that could be attempted to provide the necessary power supply to maintain reactor shut down (hold-down) and to provide a coolant heat sink to remove decay heat from the reactor and from the irradiated fuel.

- In the sole event of a total loss of ultimate heat sink there are still three alternative heat-sinks (decay heat boiler system, emergency boiler feed system and back-up emergency feed system).
- In the sole event of a station blackout the back-up emergency feed system would remain available.

From the two scenarios it can be seen that the station blackout is the most detrimental to the ability to cool the reactor and fuel. Therefore, it is likely that safety margins could be improved by providing alternative means for electrical AC supplies to provide power to the already installed cooling systems.

For the scenario of a total loss of ultimate heat coinciding with a station blackout, the only remaining on-site alternative heat-sink that does not depend upon station AC supplies is the petrol-driven back-up emergency feed system. This could provide adequate cooling to the reactor using towns-water passed through the main boiler and vented as steam. There is also a potential to use gravity feed from the reserve feed tanks to the boilers along with a potential to use the heat removal capabilities of the pressure vessel cooling system.

As noted earlier there is a set of emergency equipment that would support essential safety functions with additional special items to enable cooling to be restored.

5.1.4 Measures which can be envisaged to increase robustness of the plant in case of loss of the ultimate heat sink

The preceding sections have shown that there are robust provisions for design basis loss of 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 has been raised.

Conclusion HYB 5.15: The current robustness and maintenance of the plant is compliant with its design basis for loss of the ultimate heat sink. However, steps to improve the resilience of the plant following a beyond design basis event should be considered.

5.1.5 Licencesee 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 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 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 at the advanced gas-cooled reactors would be a particular challenge: 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 re-pressurised, 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 HYB 5.16: The current robustness and maintenance of the plant is compliant with its design basis for loss of the electrical supplies and heat sink. However, steps can be made to improve the resilience of the plant for a beyond design basis event.

Consideration HYB 5.9: 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 advanced gas-cooled reactor spent fuel storage ponds are part of the overall station fuel route. The four key components of the fuel route that are also considered here are the decay stores, fuelling machine, irradiated fuel dismantling facilities and spent fuel cooling ponds. The essential safety functions for the fuel route are:

- to provide cooling to remove the decay heat
- to prevent mechanical damage to the fuel and maintain containment of fission products
- to avoid criticality.

These safety functions are provided by the design of the plant and control of operations.

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:

Table 5.1 Impact of loss of power to fuel handling

Stage of fuel storage and handling	Handling with fuelling machine	Buffer storage	Dismantling	Storage in ponds
Effect of loss of	Back-up power	Back-up power	Back-up power	Back-up power

grid	available	available	available	available
Effect of loss of grid and on-site generation	Manual operation available for movement of fuel, cooling is passive	Cooling can be provided by diesel driven pumping systems	Cooling lost but water injection can be manually initiated (see Chapter 1)	Cooling lost, timescales to recover as per Chapter 1. Note that diesel driven pumps can top up water level.

Conclusion HYB 5.17: In either the event of both loss of grid or Station Black Out (SBO), 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 HYB 5.18: 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 HYB 5.10: To improve resilience of decay store cooling against loss of electrical power, consider possible enhancement options in respect to guidance to operators, fault recovery techniques, and improved understanding of credible consequences.

Consideration HYB 5.11: To improve resilience of pond cooling and make up against loss of electrical power, 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).

Table 5.2 3 Impact of loss of heat sink to fuel handling

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	Ambient air - loss not credible / Sea (loss tolerable)	Sea

Secondary heat sink	-	Fresh water from mains	Fresh water from mains (loss tolerable)	Fresh water from mains
Tertiary heat sink	-	Air	Water injection and maintained submersion	-

5.2.3.1 Station Black Out combined with Loss of Ultimate Heat Sink

Conclusion HYB 5.19: In the event of loss of the 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 ultimate heat sink. Furthermore, there are also arrangements for mitigation of the effect of loss of the 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 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 HYB 5.20: Whilst there are no vulnerabilities identified in the current design basis for the fuel route against loss of ultimate heat sink, further resilience enhancements can be envisaged.

Consideration HYB 5.12: To improve resilience of decay store cooling against the loss of the ultimate heat sink, consider possible enhancement options in respect to guidance to operators, fault recovery techniques, and improved understanding of credible consequences.

Consideration HYB 5.13: To improve resilience of pond cooling and make up against the loss of the 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

Heysham 2

6 Severe Accident Management

In the ONR Interim Report into the Japanese Earthquake and Tsunami, it 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:

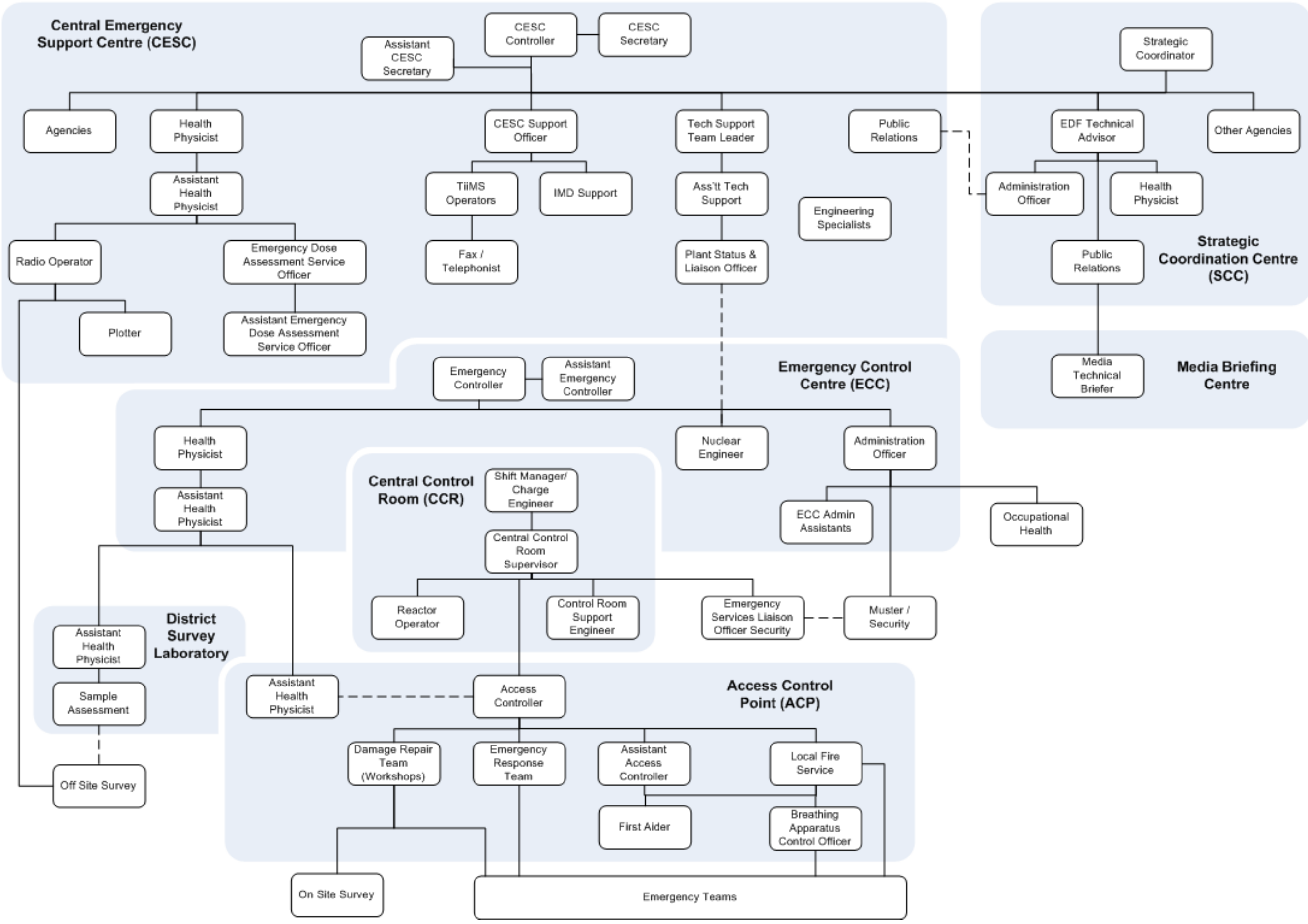

Figure 6.1: EDF Energy Generic Emergency Response Organisation

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:

Central Control Room

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 Heysham 2 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 HQ 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

<u>Procedures</u>

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.

<u>Training</u>

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:

<u>*Role Orientation*</u>

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. Heysham 2 is in the process of aligning with the company process associated with emergency scheme training.

Heysham 2 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 internal regulation of standards.	Annually
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

Exercise Type	Description	Frequency
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 (CT) 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 HYB 6.1: EDF 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 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 HYB 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 will consider enhancement of its staff welfare, human factors and emotional aspects associated with emergency response.

Consideration HYB 6.2: Review in detail the benefits of having a co-located ECC particularly focusing on the benefits that could be gained during Heysham 1 and 2 response to a multi unit event.

Consideration HYB 6.3: Complete Implementation of ECC 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 timeframe of several hours 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 many 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 diesel generators, water, etc)

One of the roles of the Central emergency support centre is to coordinate EDF Energy 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 24 hour stocks available on the Station for all essential consumables for at power reactors, a single shutdown reactor and a double reactor outage.

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 Heysham 2 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 blow-down 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 re-circulating 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

Conclusion HYB 6.2: EDF 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 could consider further enhancements to equipment and its critical supply.

Consideration HYB 6.4: 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.

6.1.2.4 Communication and information systems

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 UHF 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 PA 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 Energy 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 UHF 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 HYB 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.

Notifications

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.

Rapid Reach (Notification)

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”.

UHF Site Radio

A report was produced in 2009 on all EDF Energy existing nuclear stations radio systems. The primary use of the Power Station site’s radio system is for day-to-day operations. Heysham 2 Power Station has a UHF Radio System with 5 Channels.

Potential enhancements have been identified in the UHF 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 of HYB 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 HYB 6.5: 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 does 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.

Destruction of Facilities on Site

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 Heysham 2 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 of HYB 6.5: In extreme circumstances some on-site facilities may become unavailable. EDF has arrangements in place through use of alternative/mobile facilities to respond to this eventuality; however there are opportunities to enhance communications and equipment contained within.

Consideration HYB 6.6: EDF Energy will consider a review of its mobile facilities and the resilience of equipment contained within.

Consideration HYB 6.7: Due to Heysham 1 and 2 utilising the adjacent sites ECC as a back up facility this could potentially result in vulnerabilities in the station response to a multi unit event. Establishment of an independent back up ECC should be considered.

Consideration HYB 6.8: Heysham 1 and 2 should consider carrying out a review of equipment and where possible align to allow for ease of use during an emergency. Equipment logs and location could be kept in both stations ECC to allow emergency responders to quickly identify and access equipment as needed.

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 HYB 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 HYB 6.9: 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, onsite back-up onsite AC electrical power generation 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 backup AC electrical power generation - 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

AGR power stations are twin reactor design. This means that each site has two reactors of the same design within the same facility. This is taken into account as part of the design of the safety systems.

Heysham 2 Power Station is located next to Heysham 1 Power Station both of which operate two advanced gas cooled reactors.

On declaration of an event at either site, both sites activate their emergency sirens to muster all staff. Both sites will set up their emergency control centres to ensure ongoing communications. The central emergency support centre will also be manned by representatives from the unaffected sites company to ensure support is provided where required.

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 HYB 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 HYB 6.10: Further mitigation against beyond design basis accidents could be provided by additional emergency backup 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.

Symptom Based Emergency Response Guidelines

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 HYB 6.8 It is acknowledged that it may be beneficial to improve the level of training of EDF Energy personnel in their use, and carry out investigations into the feasibility of implementing the advice in a real scenario.

Consideration HYB 6.11: 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 hold-down.

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 Need 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 high internal temperatures.

6.2.6.2 Operational provisions

The severe accident guidelines advise on protecting the containment provided by the vessel after de-pressurisation and significant fuel damage. Re-instating 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.

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.

Consideration HYB 6.12: EDF Energy should consider a review, extension and retraining for the symptom based emergency response guidelines

Conclusion HYB 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 HYB 6.13. Further mitigation against the effects of beyond design basis accidents should be provided by additional emergency backup 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 (AGR only).

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.

Equipment to provide temporary shielding and deal with waste arisings from the event

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 base mat 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

Dose rates

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.

Criticality

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

Dose rates

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 sea water 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 dose rates 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 and failure of the steel pressure tube, 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 HYB 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 HYB 6.14: Consideration should be given to providing further mitigation against beyond design basis accidents by the provision of additional emergency backup 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.