



EU Stress Test

Hunterston B

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

© 2011 Published in the United Kingdom by EDF Energy Nuclear Generation Ltd.
All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, without the written permission of the copyright holder, EDF Energy Nuclear Generation Ltd, application for which should be addressed to the publisher. Such written permission must also be obtained before any part of this publication is stored in a retrieval system of any nature. Requests for copies of this document should be referred to Barnwood Document Centre, Location 12, EDF Energy Nuclear Generation Ltd, Barnett Way, Barnwood, Gloucester GL4 3RS (Tel: 01452-652791). The electronic copy is the current issue and printing renders this document uncontrolled. Controlled copy-holders will continue to receive updates as usual.

LIMITATION OF LIABILITY – Whilst EDF Energy Nuclear Generation Ltd believes that the information given in this document is correct at the date of publication it does not guarantee that this is so, nor that the information is suitable for any particular purpose. Users must therefore satisfy themselves as to the suitability of the information for the purpose for which they require it and must make all checks they deem necessary to verify the accuracy thereof. EDF Energy Nuclear Generation Ltd shall not be liable for any loss or damage (except for death or personal injury caused by negligence) arising from any use to which the information is put.

Contents

Executive Summary	7
0 Introduction	15
0.1 Background	15
0.2 Scope of Stress Test	15
0.3 EDF Energy's Nuclear Sites	16
0.4 Background to UK Nuclear Safety Framework and EDF Energy's Arrangements	18
0.5 Safety Case Methods and Principles	19
0.5.1 Deterministic Principles (NSP 2)	19
0.5.2 Probabilistic Principles (NSP 3)	21
0.5.3 Shutdown Cooling Criterion	22
0.6 Specific Assessment and Design Against Hazards	23
0.7 Mission Time and Off-site Support	24
0.8 Beyond Design Basis Events and Accident Management	25
0.9 Emergency Response Arrangements	25
0.10 Mandatory Evaluations	26
1 General Data about Hunterston B	28
1.1 Site characteristics	28
1.2 Main characteristics of the unit	29
1.3 Systems for providing or supporting main safety functions	29
1.3.1 Reactivity Control	30
1.3.2 Heat Transfer from Reactor to ultimate heat sink	31
1.3.3 Heat transfer from spent fuel pools to the ultimate heat sink	35
1.3.4 Heat transfer from the reactor containment to the ultimate heat sink	37
1.3.5 AC power supply	37
1.3.6 Batteries for DC Power Supply	45
1.4 Significant differences between units	45
1.5 Scope and Main Results of Probabilistic Safety Assessments	45
1.5.1 PSA: The AGR Approach	45
2 Earthquakes	47
2.1 Design basis	47
2.1.1 Earthquake against which the plant is designed	47
2.1.2 Provisions to protect the plant against the design basis earthquake	52
2.1.3 Compliance of the plant with its current licensing basis	59
2.2 Evaluation of safety margins	61
2.2.1 Range of earthquake leading to severe fuel damage	63
2.2.2 Range of earthquake leading to loss of containment integrity	63
2.2.3 Earthquake exceeding the design basis earthquake for the plant and consequent flooding exceeding design basis flood	63
2.2.4 Potential need to increase robustness of the plant against earthquakes	64
2.3 Summary	64
3 External Flooding	67
3.1 Design Basis	67
3.1.1 Flooding against which the plant is designed	68
3.1.2 Provisions to protect the plant against the design basis flood	73
3.1.3 Plant compliance with its current licensing basis	77
3.2 Evaluation of safety margins	78
3.2.1 Estimation of safety margin against flooding	78
3.2.2 Potential need to increase robustness of the plant against flooding	80

3.3	Summary	81
4	Extreme Weather	83
4.1	Design Basis	84
4.1.1	Reassessment of weather conditions used as design basis	86
4.1.2	Conclusion on the Design Basis	92
4.2	Evaluation of safety margins	92
4.2.1	Estimation of safety margin against extreme weather conditions	92
4.2.2	Potential need to increase robustness of the plant against extreme weather conditions	101
4.3	Summary	103
5	Loss of Electrical Power and Loss of Ultimate Heat Sink	106
5.1	Nuclear power reactors	107
5.1.1	Loss of electrical power	107
5.1.2	Measures which can be envisaged to increase robustness of the plant in case of loss of electrical power	112
5.1.3	Loss of the ultimate heat sink	112
5.1.4	Measures which can be envisaged to increase robustness of the plant in case of loss of ultimate heat sink	116
5.1.5	Licensee Review of Robustness	116
5.2	Spent fuel storage pools	117
5.2.1	Loss of electrical power	117
5.2.2	Measures which can be envisaged to increase robustness of the plant in case of loss of electrical power	118
5.2.3	Loss of the ultimate heat sink	118
5.2.4	Measures which can be envisaged to increase robustness of the plant in case of loss of ultimate heat sink	118
6	Severe Accident Management	121
6.1	Organisation and arrangements of the licensee to manage accidents	121
6.1.1	Organisation of the licensee to manage the accident	122
6.1.2	Possibility to use existing equipment	134
6.1.3	Evaluation of factors that may impede accident management and respective contingencies	137
6.1.4	Measures which can be envisaged to enhance accident management capabilities	142
6.2	Maintaining the containment integrity after occurrence of significant fuel damage (up to core damage) in the reactor core	142
6.2.1	Elimination of fuel damage/meltdown in high pressure	144
6.2.2	Management of hydrogen risks inside the containment	144
6.2.3	Prevention of overpressure of the containment	145
6.2.4	Prevention of re-criticality	145
6.2.5	Prevention of basemat melt through	146
6.2.6	Need for and supply of electrical AC and DC power and compressed air to equipment used for protecting containment integrity	146
6.2.7	Measuring and control instrumentation needed for protecting containment integrity	147
6.2.8	Measures which can be envisaged to enhance capabilities to maintain containment integrity after occurrence of severe fuel damage	147
6.3	Accident management measures to restrict the radioactive release	148
6.3.1	Radioactive releases after loss of containment integrity	148
6.3.2	Accident management after uncovering of the top of fuel in the fuel pool	150
6.3.3	Measures which can be envisaged to enhance capability to restrict radioactive release	152

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
EDF	Electricity de France
HNB	Hunterston B Power Station
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
WANO	World Association of Nuclear Operators

Executive Summary

Hunterston B

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 Energy¹ 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 Hunterston B.

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

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.

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, a Pressurised Water Reactor, was based on the Standard Nuclear Power Plant (SNUPPS) design and the standard design included qualification against earthquake. However, for the pre-HYB/TOR AGRs, seismic safety cases were developed as part of the first Periodic Safety Review (PSR) in the late 1990s, covering both the at-power and shutdown conditions as well as fuel handling operations.

Summary of findings for the earthquakes at Hunterston B

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 per year. There are also discussions on the margin to failure of this equipment. It demonstrates that:

- The design basis earthquake was defined in the 1990s using an extensive study of historical earthquakes and local geology. It corresponds to an infrequent event.
- The design basis earthquake is reviewed by the periodic safety review process, most recently in 2006, 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 shutdown the reactor and provide post-trip cooling remains available following an infrequent seismic event.
- The plant has suitable processes in place to ensure it remains compliant with its licensing basis.
- There is an un-quantified safety margin implied by the process of seismic qualification, and no cliff-edge (i.e. a large change in impact for a small change in hazard) effects are expected for events up to twice as severe as the design basis.

The seismic safety case is based on the provision of a line of protection with redundancy for the infrequent design basis earthquake, and two lines of diverse protection with redundancy 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 conservatism, 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 fuel damage to be expected.
- 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.

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

² Assumed to mean tectonic plate boundary

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, 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.

Summary of finding for external flooding at Hunterston B

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

- Sufficient margin exists between the maximum design basis flood (4.84m Above Ordinance Datum (AOD)) and the physical elevation of the main nuclear island (>7.9m AOD).
- 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 shows that the methodology used to calculate the design basis flood for Hunterston B has been constructed using independent expertise based on well regarded sources of information. The methodology has also been constructed with appropriate conservatism, 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.
- 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.
- 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 managing beyond design basis risks, 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.

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

Extreme Weather

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

in this report the UK nuclear industry should consider them in the light of all extreme hazards, particularly for plant layout and design of safety-related plant.”

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

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

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

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

The findings of this work are summarised below.

Summary of findings for Extreme Winds at Hunterston B

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 event with a probability of 10^{-4} p.a. Equipment required to fulfil the essential safety functions is either located inside buildings which are qualified against infrequent wind, or qualified directly. The safety case has been assessed against the latest codes and is robust.

Summary of findings for Extreme Ambient Temperatures at Hunterston B

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 four possible events; high temperatures and low temperatures, sea temperature and snow loading. The safety case demonstrates that most equipment is expected to remain functionally available or fail-safe when subjected to the high or low ambient temperatures considered in the design basis. Operator actions play a large part in ensuring that during extreme air temperature events sufficient safety related plant remains available. Seawater temperature is primarily a commercial concern and changes in temperature will not impact nuclear safety. The reactor and other buildings containing essential equipment have been assessed against snow loading and demonstrate sufficient margin.

A climate change report predicts by 2030 there will be a rise in the expected maximum air temperature which may impact on plant life extensions.

Summary of findings for Lightning at Hunterston B

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

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 (LEMP) which are addressed as part of the Electro-Magnetic Interference / Radio Frequency Interference hazard and are not considered here.

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

Summary of findings for Drought at Hunterston B

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 on the civil structures and the effect of the hazard on the main electrical earthing system.

Drought is currently not considered as a formal hazard, as it is difficult to quantify. The primary defence against drought is that it is slow to occur compared with the 24 hour mission time of the station.

Overview of Combination of Hazards

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

Loss of Electrical Power and Loss of Ultimate Heat Sink

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

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

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

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

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

This chapter is based around a number of specified scenarios and the timescales to failure once all lines of protection have been eliminated. This chapter therefore considers severe / "cliff edge" changes in risk.

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

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

- Loss of off-site power is an event considered within the Hunterston B safety case and provisions are made to support the essential safety functions for 24 hours.

- In the event of loss of grid, there are sufficient supplies of fuel oil for the diesel generators to continue operating under required load for at least a 48 hour mission time.
- At Hunterston B, 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 provisions are made to support the essential safety functions.
- There are provisions off-site that can be deployed to station in 10 hours that would provide power generation capability and aid in continued post-trip cooling of the reactor.
- The current robustness and maintenance of the plant is compliant with its design basis against loss of electrical power. However, steps can be taken to improve the resilience of the plant for a beyond design basis event.
- Several means of preventing the loss of reactor cooling water by blockage of the water intakes are employed at Hunterston B including drum screens and chemical control.
- There exist diverse alternate heat sinks for essential cooling in case of loss of the primary ultimate heat sink.
- The current robustness and maintenance of the plant is compliant with its design basis for loss of the primary ultimate heat sink. However, steps to improve the resilience of the plant following a beyond design basis event should be considered.
- The current robustness and maintenance of the plant is compliant with its design basis for loss of the electrical supplies and primary ultimate heat sink. However, steps to improve the resilience of the plant following a beyond design basis event should be considered.
- In either the event of both loss of grid or station black out, sufficient cooling can be maintained to the station fuel route areas for a 72 hour mission time.
- In the event of loss of the primary ultimate heat sink there is adequate alternate heat sink provision available to the station fuel route.

Severe Accident Management

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

“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, widespread 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 Stress Test report explored the organisation and management measures which are in place for the 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 following the completion of the Stress Test reports and an appropriate programme of work formulated.

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 to extreme hazards 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

Hunterston B

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 Energy³ 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.

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

0.2 Scope of Stress Test

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

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

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

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

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

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

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

0.3 EDF Energy's Nuclear Sites

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

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

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

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

Power Station	Type	Net MWe	Construction started	Connected to grid	Full operation	Accounting closure date
Dungeness B	AGR	1040	1965	1983	1985	2018
Hinkley Point B	AGR	820	1967	1976	1976	2016
Hunterston B	AGR	820	1967	1976	1976	2016
Hartlepool	AGR	1190	1968	1983	1989	2019
Heysham 1	AGR	1160	1970	1983	1989	2019
Heysham 2	AGR	1235	1980	1988	1989	2023
Torness	AGR	1230	1980	1988	1988	2023
Sizewell B	PWR	1188	1988	1995	1995	2035



Figure 0.1: Map of the UK showing EDF Energy nuclear power stations.

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

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

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

- There should be a transparent bias on the side of health and safety. For duty holders, the test of 'gross disproportion' requires erring on the side of safety in the computation of health and safety costs and benefits.
- Whenever possible, standards should be improved or at least maintained, thus current good practice is used as a baseline - the working assumption being that the appropriate balance between costs and risks was struck when the good practice was formally adopted.
- Hazards are regulated through a safety case regime requiring an explicit demonstration in the safety case that control measures introduced conform to the ALARP principle.

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

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

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

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

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

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

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

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

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

The second wave of periodic safety reviews, referred to as periodic safety review 2, commenced in 2002 with a review process that was broadly similar to periodic safety review 1 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 diversity⁴ where required and that at least one line of protection remains available in all permissible plant states. The type of protection required is based on the frequency of the event, with more frequent events requiring protection with a higher level of integrity. These rules have been developed based on sound engineering principles and the likely reliability of the system if the rules are applied.

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

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

- Initiating events are defined as Frequent if they have an estimated frequency of occurrence greater than once in 1,000 years. 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 however there must be one line of protection.
- Initiating events are defined as Infrequent if they have an estimated frequency of occurrence less than or equal to once in 1,000 years. 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} pa.
- Events whose estimated frequency of occurrence is judged to be less than 10^{-5} pa are not assessed against the Deterministic Principles, however the reasonable practicability of providing protection for such events is considered.

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.

Initiating events which, in the absence of protection, would lead to a dose of less than 1 ERL⁵ 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 a series of documents called Technical Specifications (or Tech Specs) which include all of the limits and requirements for normal operation of the plant both at power and shutdown. In addition to the requirements and limits the Tech Specs also include actions to be taken if they are not met.

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

- (i) The 'normal maintenance' state is one in which the level of essential plant availability is defined in Technical Specifications as being allowed to exist for consecutive period of 31 days.
- (ii) The 'urgent maintenance' state, as defined in Technical Specifications, will have an action completion time significantly less than 31 days, typically between 36 and 72 hours. It reflects a lower state of plant availability than the normal maintenance state. Whenever practicable, maintenance and testing shall be planned so as not to introduce an urgent maintenance state.
- (iii) If the plant availability falls below the urgent maintenance state, then there is a need for 'immediate remedial action' within short timescales, either to restore essential plant or achieve safe shutdown of the reactor.

0.5.2 Probabilistic Principles (NSP 3)

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

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

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

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

The Probabilistic Nuclear Safety Principles used by EDF Energy are based upon two premises. The first premise is that a risk of fatality for any identified individual member of the public of $<10^{-7}$ p.a., from all accidents at a single reactor, is

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.

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:

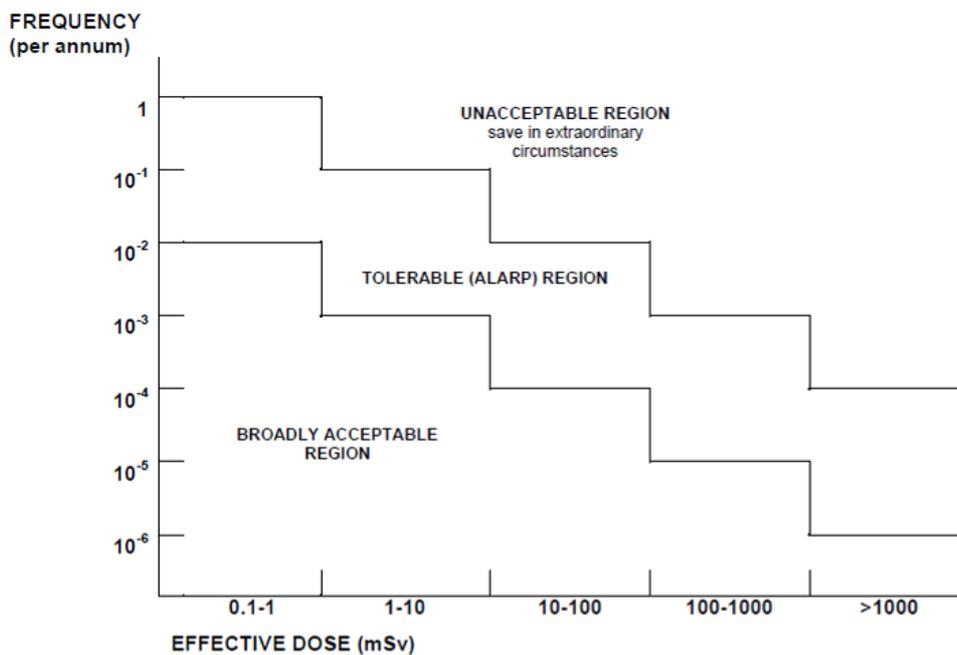


Figure 0.2: Surrogate risk regions as a function of frequency and effective dose.

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, 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 in 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 exceedance⁶ of greater than or equal to once in 1,000 years. 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 one line of protection.
- External hazard events are defined as Infrequent where they have an annual probability of exceedance of between once in 1,000 year and once in 10,000 year event. For any infrequent event there is at least 1 line of protection to perform any essential function and that line is provided with redundancy, during any normally permissible state of plant availability, unless it is shown not to be reasonably practicable.
- External hazards events with an annual probability of exceedance of less than once in 10,000 year event 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 Off-site 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 off-site 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

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

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 walkdown 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 walkdowns 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. Walkdowns 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, walkdowns 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. This review and its findings are detailed in Chapter 6 alongside the subsequent reviews.

All applicable agreements and contracts designed as contingencies to support severe accident mitigation were identified and comprehensively reviewed. Walkdowns 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 Hunterston B

Hunterston B

1 General Data about Hunterston B

1.1 Site characteristics

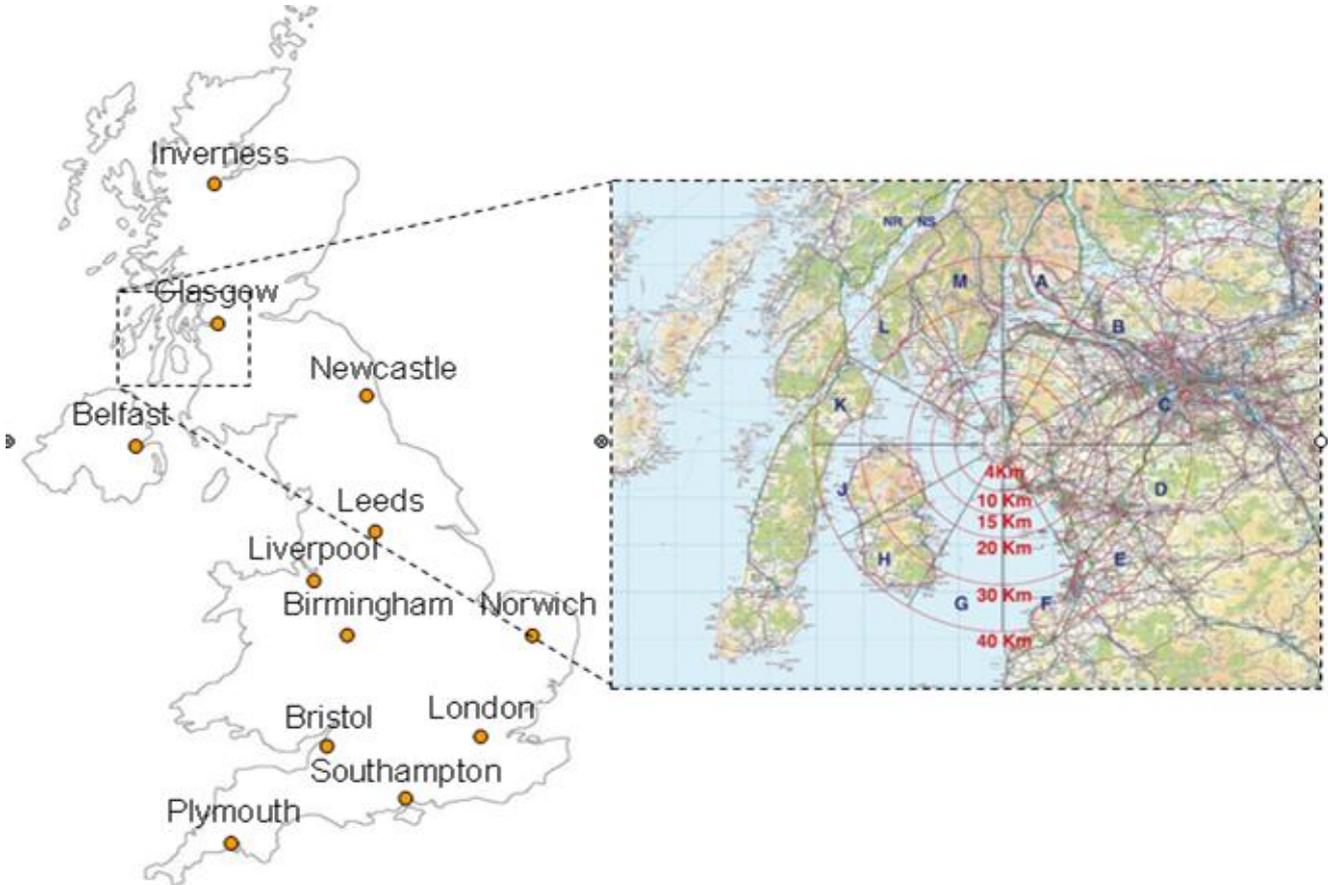


Figure 1.1: Location of Hunterston B

Hunterston B is a twin reactor Advanced Gas Cooled (AGR) station is located about 3km northwest of West Kilbride in North Ayrshire, Scotland. Construction commenced between 1967 and 1976. The end of generation is currently scheduled for 2016, although a life extension could see power generation until 2021, but this has not yet been confirmed.

Hunterston A is a separate nuclear licensed site which is neither owned nor operated by EDF Energy plc or any of its subsidiary companies. However, Hunterston A and B were historically together on a single licensed site, sharing some administrative and, to a much lesser extent, operational facilities. Nearly all linked services (water, electrical) between the two stations have been removed or removal works are planned to be completed in the near future.

1.2 Main characteristics of the unit

Table 1.1: Details for HNB Reactor

Hunterston B	
Type	AGR
Station Net Electrical Output (Design)	1190 MWe
Construction started	1967
Connected to grid	1976
Full operation	1976
Criticality	1976
Reactor Thermal Power (Current)	1320 MW(th)
Owner	EDF Energy
Operator	EDF Energy
Accounting closure date	2016

1.3 Systems for providing or supporting main safety functions

Advanced gas-cooled reactor technology differs significantly from that of light water reactors (or the boiling water reactor at Fukushima) and is unique to the UK. The advanced gas-cooled reactor core is assembled from high purity graphite bricks. These are keyed together in layers, and are arranged in a polygonal structure with an approximate overall diameter of ten metres and height of eight metres. Circular channels in the bricks allow passage of fuel elements, coolant and control rods. The graphite also acts as a moderator. The fuel in an advanced gas-cooled reactor is slightly enriched uranium dioxide which is contained within stainless steel cans. The fuel is cooled by 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/m³ (million Watts of thermal power per cubic meter of reactor volume) when compared with approximately 100MWth/m³ 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.

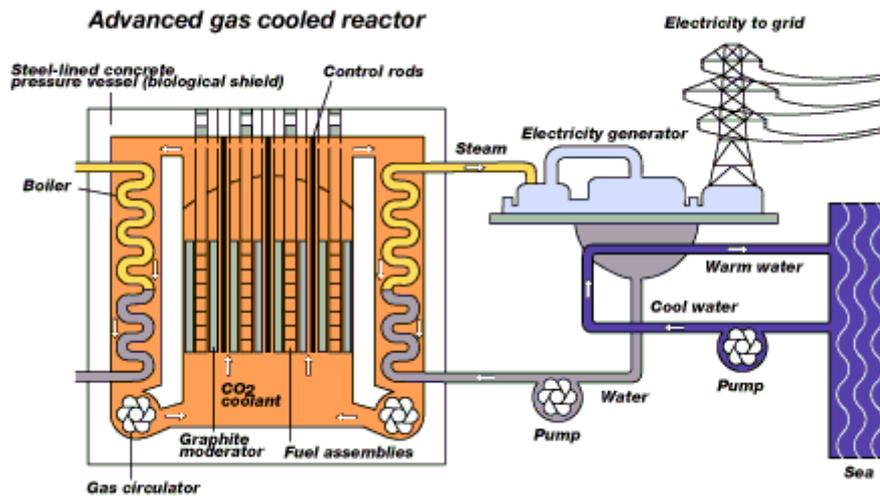


Figure 1.2: AGR showing internal components and the primary ultimate heat sink (seawater)

Fuel Handling

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

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

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

1.3.1 Reactivity Control

1.3.1.1 Reactivity Control - Reactor Core

Reactivity control in advanced gas-cooled reactors is achieved using the following systems:

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

1.3.1.2 Reactivity Control – Fuel Storage and Transport

All operations involving storage or movement of nuclear fuel on-site which could conceivably constitute a criticality hazard (except when resident in the reactors) are assessed to make sure accidental criticality cannot occur. All such operations are therefore controlled by means of Criticality Safety Certificates for each location or operation. These certificates restrict the quantities of fuel accumulated, U^{235} 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 ultimate heat sink

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

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

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

Post-Trip Control

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 feedwater systems which pump water through the boiler tubes.

If the gas circulators fail and the reactor is pressurised, the fuel can be cooled by natural circulation providing the boilers continue to be cooled by the feedwater systems. All advanced gas cooled reactors have at least two diverse post-trip feedwater systems with redundancy and diversity in their electrical supplies.

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

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

The provision of adequate post-trip cooling requires a number of active systems to be shutdown 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 back-up diesel generators.

Primary Coolant Heat Transfer

The primary coolant, CO₂ 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 and require off-site power (grid) to be available. If grid supplies are unavailable, the gas circulators can be powered by the diesel generators.

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

The CO₂ primary coolant is topped up using storage tanks. Liquid CO₂ from the tanks passes through steam heated vaporisers and into the CO₂ distribution system, then eventually into the reactor gas circuit. The CO₂ 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 CO₂ is sufficient to repressurise 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 System

The main boilers act as the primary to secondary heat transfer surface within the reactor pressure vessel. There is considerable excess capacity in the boiler system: with forced primary coolant circulation, a fed main boiler unit in a single reactor quadrant is sufficient to adequately cool the core with a pressurised primary circuit.

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

In normal operation, boiler feedwater is pumped from the condenser to the boilers and steam flows from the boilers to the turbine. The main boiler feed pump is driven by the steam leaving the boilers.

Following a reactor trip, condensate supplies to the deaerator cease and the level falls. An electrically driven pump is used to maintain the deaerator level by transferring water from storage tanks, until the condensate system can be re-established. There is sufficient decay heat to generate enough steam to run the main boiler feed pump for approximately an hour post-trip. However, the operators would normally switch to an alternative electric feed pump after a few minutes, which would allow better control of boiler pressure and gas outlet temperature.

If the condensate system is lost immediately post-trip, the ability to re-circulate feedwater is also lost and therefore steam is released through boiler valves to atmosphere. This does not reduce the effectiveness of the post-trip cooling, and there is sufficient water stocks to operate in this 'once-through' manner for an absolute minimum of 24 hours.

Feed Systems

Main Feed System

The purpose of the system is to provide main feedwater supply to the boilers during power operations and post-trip. Although in practice the main feed system will be used to provide feed for most faults post reactor trip, this is only claimed for risk mitigation within the safety case.

The main feed system is required to provide feedwater to the boilers during normal power operation and to provide high pressure feedwater to the boilers following a reactor trip. It has been designed with adequate margins and safeguards to supply clean deaerated water to the boilers at suitable temperature and pressure over the full load range and to cool the reactor by way of the boilers at shutdown and following a trip occurrence.

Post-trip boiler feed is normally provided by the start/standby boiler feed pumps, which are electrically driven requiring off-site electrical grid supplies, and draw their water supply from the deaerator.

Emergency boiler feed system

The purpose of the system is to provide post-trip feed to the boilers. For most faults the system is claimed as the first line of feed within the deterministic safety case, although in practice feed will be provided by the standby boiler feed system with the low pressure feed system only being required if the start/standby boiler feed fails or is unavailable post-trip.

The emergency boiler feed pumps have been sized so that one pump is sufficient to supply adequate feedwater to remove reactor shutdown and stored heat following a reactor trip. The low pressure feed system has been designed to be independent from the main feed system so that any single failure cannot invalidate both systems.

Back-Up Boiler Feed System

The purpose of the back-up boiler feed system is to provide post-trip feed to the boilers when the other feed systems are unavailable. This system is completely independent, segregated and/or qualified to take account of internal and external hazards of the other feed systems, and is powered by direct diesel driven pumps. The system is claimed by the safety case as a means of providing a supply of feedwater for most faults post reactor trip. Like the emergency boiler feed system it requires the boiler to be depressurised. Feedwater is taken from dedicated back-up feedwater tanks. Manual initiation of the back-up feed system is required.

The back-up feed system would be expected to be used in conjunction with pressure vessel cooling system to provide reliable natural circulation post-trip cooling on a pressurised reactor.

Additional Feed System

Condensate and Feedwater System

The role of the condensate and feed heating system is to provide treated feedwater to the deaerator from the condenser. The water is then routed to the main boilers by the main boiler feed pump, the start and standby boiler feed pumps or the emergency boiler feed. During reactor outages, the system is also claimed as part of the man access cooling system, in which emergency boiler feed is used in a recirculatory mode.

The condensate and feed heating system is provided to regulate the flow of feed to the deaerator and maintain sufficient reserve of acceptable quality feedwater during power operation and a following a reactor trip.

Decay Heat Boiler Feed System

The primary function of the decay heat boiler feed system is to remove excess heat from the reactor after a trip or shutdown, allowing the main boilers to be released from cooling duty. The decay heat boiler feed system also has a role in reactor start-up, removing excess heat prior to bringing the main boilers into service.

Cooling Water Systems

Main Cooling Water

The operational duty of the main cooling water system is to remove heat from the turbine condensers, and hence the system has no essential safety role.

The general service water is a demineralised water system which provides cooling to various items of plant in the turbine hall, such as the Start & Standby Boiler Feed Pumps and heater lift pumps. Its safety significance is primarily as a potential trip initiator. The general service water is cooled by the seawater auxiliary cooling water system.

Reactor Cooling Water System

The safety function of the reactor cooling water system is to provide a seawater heat sink to the pressure vessel cooling system and reactor auxiliary cooling system during at power and post-trip operation. The two systems in turn remove

excess heat from the pre-stressed concrete pressure vessel and gas circulators to maintain them within safe operating limits. The reactor cooling water system also provides cooling to the pond cooling secondary circuit.

The design intent for the reactor cooling system is to provide sufficient flow rates to adequately cool the reactor auxiliary cooling system, pressure vessel cooling system and pond cooling secondary circuit systems via the system heat exchangers during at-power operation. Post-trip, the heat loading and therefore, the required flow rates are significantly reduced.

In the event of total loss of reactor cooling water, the reactor would be tripped and the diverse cooling system, which is grid independent, would provide the heat sink for the pressure vessel cooling system and reactor auxiliaries cooling system.

Diverse Cooling System

Each reactor has a diverse cooling system which provides a diverse heat sink for the reactor auxiliaries and pressure vessel cooling systems in the event of loss of reactor cooling water. The system mirrors the twin circuits of the reactor auxiliaries cooling system and pressure vessel cooling system. Each circuit consists of a diesel engine driving diverse reactor auxiliaries cooling pumps and pressure vessel cooling pumps, pumping water to the diverse cooling system heat exchangers. The diverse cooling system heat exchangers are cooled by their own cooling circuit pumps driven by the same diesel engines, rejecting heat to atmosphere in forced air cooling towers supplied by diesel backed electrical supplies.

Reactor Auxiliaries Cooling Water System

The safety function of the reactor auxiliaries cooling water system is to supply cooling water in twin closed circulation circuits to maintain the temperatures of the reactor auxiliaries at acceptable levels to ensure their continuing operation and to prevent their failure from excessive temperatures.

The key safety role of the reactor auxiliaries cooling water system is to maintain the temperatures of the reactor auxiliaries at acceptable levels to ensure their continuing operation and to prevent their failure due to excessive temperatures. This applies to both normal and post-trip operation. The system is required to operate continuously.

Townswater System

Townswater is primarily used on the station for the usual domestic purposes and as a cooling and process medium for various plant installations.

Its safety related function is to top up the reserve feedwater tanks and the back-up boiler feed tank. The diesel driven townswater pumps ensure the availability of adequate feed stocks to the back-up boiler feed tanks by providing a means of utilising the contents of the million gallon townswater tank under loss of grid and other conditions.

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 diesel generated 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

Many of these systems consume stocks such as fuel for the 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 off-site 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.

Beyond this period it is claimed that adequate arrangements can be established for any required essential supplies to be brought to site.

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 direct diesel-driven feed system at Hunterston B offers a diverse means of providing secondary coolant circulation from the other feed systems, all of which are reliant on electrical 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. It is acknowledged that some passive parts of the heat transfer chain are not diverse; the boilers are an example of this.

Probabilistic safety assessment for reactor systems provides an indication of whether the systems deliver diversity. Any significant weaknesses in the system relating to diversity would be revealed during the assessment process. The probabilistic safety assessment for Hunterston B supports the view that the integrity of the reactor protection systems is satisfactory and that the overall risk from reactor operation is both tolerable and compliant with the as low as reasonably practicable principle.

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 CO₂), 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 primary ultimate heat sink.

Table 1.2: The heat transfer chains for each stage of fuel storage and handling

Stage of fuel storage and handling	Handling with fuelling machine	Buffer storage	Dismantling	Storage in ponds
Primary cooling circuit	CO2 by natural circulation to fuelling machine body	CO2 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 seawater cooling system	None	Once-through seawater cooling system
Ultimate heat sink	Ambient air	Sea	Ambient air	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 1.3: loss of cooling scenarios for each stage of the fuel storage and handling process

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	Even with loss of forced air flow, natural cooling effects mean fuel safety limits will not be breached.	Boiling of water in the ponds followed by overheating of fuel
Assigned safety limit	n/a	Boiling dry of storage tube water jackets	n/a	Boiling of pond water
Minimum time to reach safety limit	n/a	Not less than 24 hours for the hottest fuel	n/a	At least several days 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. However, it is noted that there is a potential threat of deterioration to the pond concrete before boiling temperatures are reached. This would increase the rate of water loss and hence the demand on topping-up of pond water until cooling can be restored. Potential improvements to mitigate this issue are being considered.

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

AGRs 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.

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

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

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

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

1.3.4.1 System descriptions

Pre-Stressed Concrete Pressure Vessel

Coolant gas, which transports heat from the reactor core to the boilers, is enclosed within the reactor coolant pressure boundary inside the reactor. The reactor coolant pressure boundary performs an essential safety role by preventing the release of reactor coolant gas (CO₂) to the outside environment. The pre-stressed concrete pressure vessel, its steel liner and penetrations form the primary components of the reactor coolant pressure boundary and together, they provide a barrier against any escape of the reactor gas and thereby maintain gas pressure at a level sufficient to ensure adequate fuel cooling under all normal operating and credible fault conditions. The pressure vessel also performs a secondary safety role by providing radiation shielding, thereby minimising radiation doses to station personnel.

Pressure Vessel Cooling System

Each reactor has a twin circuit pressure vessel cooling system which supplies treated cooling water to sets of pipes in each reactor quadrant, which are welded to the pre-stressed concrete pressure vessel liner and penetrations in order to maintain these below their temperature constraints. The reactor cooling water system provides the normal heat sink for this system. In the event of loss of grid, pressure vessel cooling system is backed by the station diesel generators and hence pressure vessel cooling system would remain available. In the event of a loss of grid and failure of the diesel generators, the cooling role would be provided by the diverse cooling system which is grid independent.

1.3.5 AC power supply

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

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

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

The reliability of on-site power is assured by providing sufficient independence and redundancy of diesel 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 1.4 Further details on plant required to provide essential safety functions.

System	Seismic Qualification	Fuel Provision	Water Provision
Essential Diesel Generators (11kV)	System designed to function following a seismic event	10 days with a pressurised reactor	No water used
3.3kV Diesel Generators	System designed to function following a seismic event	10 days with a pressurised reactor	No water used
415V Diesel Generator	System not qualified to function following a seismic event	10 days with a pressurised reactor	No water used
Diesel Driven Back-Up Feed System	System designed to function following a seismic event	At least 24hrs	At least 24hrs
DC Battery Support System	The 110 V dc system is designed to function following a seismic event	No fuel used	No water used

1.3.5.1 Off-site Power Supply and Station Earthing

Off-site power supplies connect to the Hunterston B site via the 400kV and 132kV switch houses.

The 400 kV switch house at Hunterston B contains 400 kV switchgear in a single busbar open terminal arrangement. The 132 kV switch house is the source of the two independent grid based supplies to the Hunterston B main electrical system. The station transformers at Hunterston B are connected to either side of the bus-coupler circuit breaker and can be selected by isolators to either main or reserve busbars.

The generator transformers together with their associated 400kV cable sealing-ends and HV connections and local control cubicles are located in weather-proof buildings outside the turbine hall.

The station earthing system is made up of three earth rings formed around the turbine hall/control building and each of the reactor buildings. These are interconnected with each other and also with a number of earth parks located around the perimeter of the B station complex. The main earthing system is interconnected with the 400kV and 132kV earthing systems.

1.3.5.1.1 Off-site power supply reliability

Table 1.5 presents loss of off-site power events which have occurred at Hunterston B.

Table 1.5: Loss of off-site power events at Hunterston B.

Date	Time	Duration	Reactor Trip	Weather	Description
22/1/93	0956	22 minutes (but 2.5 hours before station reconnected)	yes	Adverse	High winds, rain and sleet showers resulted in faults on all four incoming circuits due to flashovers on insulators suffering severe salt pollution. NUPER report cited 'instabilities' but it is considered that these were due to a loss of continuity rather than being evidence of 'effective loss'.
27/12/98	0021	28 minutes (but 1 hour 10 minutes before station reconnected)	yes	Adverse	High winds gave rise to a large amount of salt deposition on insulators; 'all electrical grid connections progressively lost'.
27/12/98	1107	4 hours	Already Tripped	Normal	Salt pollution was still extant from the previous incident (although 'wind had dropped'). Weather conditions dampened the salt deposited on insulators leading to more multiple flashovers. Following the loss of off-site power event earlier in the day, restoration was slow because of the electrical plant line-up on the station.

Loss of off-site power is recognised within the station safety case as a frequent initiating event. 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. Primary coolant flow can be achieved by natural circulation together with feedwater flow to the boilers, and is effective at providing post-trip cooling. Although forced primary coolant flow is the design intent.

Following the first two events shown in Table 1.5, forced primary coolant circulation was established via electrical power from on-site diesel generators.

The third event in Table 1.5 occurred on the same day as the previous loss of off-site power event. By this time normal levels of post-trip cooling had been in service for over 10 hours and decay heat levels had fallen to around 10MW. Immediately prior to the second loss of off-site electrical supplies, adequate post-trip cooling was being provided by the

decay heat systems on both reactors. Following this loss of off-site supplies, it was necessary for the operators to manually reconfigure essential electrical supplies from the diesel generators

Natural circulation cooling was established on Reactor 3 within half an hour of grid loss, but took over two hours to establish on Reactor 4. After about three hours, forced cooling had been restored to both reactors from the diesel generator supplies, and off-site electrical supplies were restored shortly after that.

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

The unit transformers are located outdoors in dedicated transformer compounds on opposite sides of the turbine hall. They are of the oil immersed type; the oil being cooled in radiator banks over which air is blown by thermostatically controlled fans. The oil is circulated through the radiators and transformer tanks by totally immersed circulating pumps.

The station transformers are located outdoors in dedicated transformer compounds on opposite sides of the turbine hall building. They are of the oil immersed type; the transformer oil being cooled by circulation through two banks of separately mounted air-cooled radiators.

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

1.3.5.2 Power Distribution inside the Plant

Power distribution inside the plant is carried out at lower voltages than the grid connections. Supplies at 11kV, 3.3kV and at lower voltages are provided on a unit and station basis as part of the 'main electrical system' as follows.

11kV Supplies

With grid supplies available, the 11kV system is designed to provide power supplies as necessary, depending upon operating conditions, to the essential post-trip cooling plant and to energise lower voltage systems via the 11/3.3kV auxiliary and station auxiliary transformers. Under post-trip conditions the 11kV station boards support operation of essential post-trip cooling plant and supplies to the 3.3kV station auxiliary boards using 132kV grid supplies if these are available.

3.3kV Supplies

The 3.3kV system is designed to supply the directly connected 3.3kV system loads and to interconnect the 11kV unit and station board supplies to the various 415V unit and station associated essential and non-essential systems via their associated 11/3.3kV auxiliary transformers and 3.3kV/415V services transformers.

415V AC Supplies

Although some high power pumps/motors are supplied directly from the 11kV/3.3kV systems, a large number of cooling and feed systems require lower power demands and are therefore operated at 415V. With grid-derived supplies at the 11kV and 3.3kV voltage levels the supplies at 415V AC are supported via 3.3kV/415V transformers or via a combination of 3.3kV AC/240V DC transformer/rectifiers and 240V DC/415V AC Motor Generators. The latter arrangement is battery backed and forms part of the 'no break' back-up power sources.

Low Voltage Supplies

Low voltage supplies – 110V DC, 110V AC and 50V DC – are normally energised via transformers and transformer/rectifiers from the 415V AC system. These typically support control and indication functions.

1.3.5.2.1 Main Electrical System – Cable and Equipment Locations

The main 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 throughout the station, generally in the area of the equipment they support.

Table 1.6: Main Electrical Equipment locations at Hunterston B.

Equipment	Location
11kV Boards	Main switch room
11kV/3.3kV unit and station auxiliary transformers	Either side of the turbine hall
3.3kV Boards	Main switch room
3.3kV/415V transformers & boards	Essential switchroom
3.3kV/415V transformers & boards	Essential switchroom
3.3kV/415V transformers & boards	'B' Diesel House
3.3kV/415V transformers & boards	'B' Diesel House

1.3.5.2.2 Main Electrical System – Performance in Hazards

The main 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 generally resilient to these. If grid supplies are unavailable, power will not be available via the main electrical system as described above.

While the main electrical plant, including the grid and generator connections and unit, station and station auxiliary transformers, is generally well segregated on a unit basis, this segregation does not extend to the 11kV and 3.3kV. Effective segregation would be difficult or impossible to achieve and a justification for this aspect of the design is dependent upon a demonstration that the risk of loss of the 11kV and 3.3kV switchgear is low. In respect of external hazards the main switchgear flat and switchboards are qualified against the infrequent (10⁻⁴ pa) seismic hazard, and due to their position in the control building are expected to be unaffected by extreme wind and flooding events.

1.3.5.3 Primary On-Site Back-up Power Supplies

As outlined above, certain sections of the main electrical system which supply essential plant required for cooling a shutdown reactor have back-up power supplies. 'No break' essential supplies are battery-backed and are intended for immediate post-trip essential functions such as control, instrumentation and essential short term cooling. Diesel-backed 'short break' supplies are available to support essential cooling functions which are re-instated once the diesel generators have started and run up to speed.

The stress test report format suggests that 'primary' on-site back-up power supplies and 'diverse' on-site back-up power supplies are addressed in both this section and Section 1.3.5.4. However, the safety cases of the AGR power stations consider the issue of diversity at a functional level, i.e. diversity is sought for frequent faults and hazards between 'lines of protection' including those which support post-trip cooling. It may be appreciated that the provision of diversity at the functional level does not necessarily imply a requirement for diversity in the sources of power supplies for the main electrical system, even though such diversity may be demonstrable. At many AGRs, including Hunterston B, a functionally capable 'line of protection' for post-trip cooling is provided by a stand-alone diesel powered back-up cooling system which operates largely independently of the main electrical system. Together with natural circulation of the primary coolant and a source of feedwater for the boilers, satisfactory post-trip cooling may be achieved without making a

significant call on the main electrical system. For that reason, the means of providing back-up power to the essential parts of the main electrical system is addressed in this section only.

Back-up 11kV Supplies

The 11kV diesel generators are designed to supply the essential systems during loss of off-site power. The 11kV 'A' diesel generators are also designed to support the 3.3kV system directly if either of 3.3kV diesel generators 3A or 4A are unavailable following a reactor trip.

The four 11kV diesel generators are started automatically by the reactor shutdown sequencing equipment following every reactor trip. The automatic sequence applied to the diesels by the reactor shutdown sequencing equipment is determined by the availability of grid derived supplies from the 11kV station boards, the reactor conditions and the overall availability of the 11kV and 3.3kV diesel generators. If grid supplies remain healthy following reactor trip then the diesels are subsequently manually shutdown.

Each diesel day service tank is sized to give at least 6 hours full load running in the event of failure of the fuel make-up from the bulk storage tanks. The bulk fuel storage tanks for the 11kV and 3.3kV diesel generators provide a total usable fuel storage capacity of 159,000 gallons. The technical specifications require the bulk fuel stocks to be maintained above 62,500 gallons to meet a specified requirement for 10 days continuous running of the diesel generators required to maintain satisfactory post-trip cooling under prolonged grid loss conditions with both reactors pressurised.

Back-up 3.3 kV Supplies

The 3.3kV diesel generators are designed to supply their own 415V auxiliaries via their 3.3kV/415V auxiliaries transformers, the 240V DC system via the 3.3kV/240V DC transformer rectifiers and all other essential system loads via the 3.3kV/415V 'A' essential transformers in support of post-trip cooling in the event of a reactor trip accompanied by loss of grid supplies. The diesel generators are also rated to allow the connection of additional loads, not strictly associated with post-trip cooling but that would be advantageous in preserving the station commercial security during prolonged grid disconnection events.

Back-up 415 V Supplies

Under normal reactor operating conditions, electrical supplies at 415 V are derived from the 3.3 kV boards. To support the essential safety function of post-trip cooling, 415 V supplies are 'backed-up' in three ways:

- 415 V Essential 'no-break' supplies
- 415 V 'A' Essential short break supplies
- 415 V 'B' Essential short break supplies

415 V Essential 'no-break' supplies

The function of the 415V AC no-break supply system is to provide continuity of electrical supplies to AC loads in the event of interruptions and disturbances affecting the station main electrical supply system. These 'uninterruptible' supplies are essential for both nuclear safety and the prevention of plant damage

415 V 'A' Essential short break supplies

The 415V 'A' essential short-break system comprises two 415V switchboards. Each switchboard is supplied from the 3.3kV station board system via a parallel pair of 3.3kV/415V essential services transformers. Each switchboard is fully rated for the whole of the system load and to allow a transformer to be removed from service at any time, each transformer is also fully rated for the whole of the system load.

Diesel backed supplies at both 11kV and 3.3kV levels can provide back-up supplies to the 3.3kV station boards which feed the 415V 'A' essential short break system as outlined above.

415 V 'B' Essential short break supplies

The 415V 'B' essential short-break system includes two switchboards. Each switchboard is normally supplied from the 3.3kV station board system via a parallel pair of 3.3kV/415V essential services transformers. Each switchboard together with its associated parallel pair of 3.3kV/415V essential transformers is fully rated for the whole of the system load.

The 'B' switchboards supplies are backed by three 415V diesel generators. However, should two diesel generators become unavailable, the automatic sequencing equipment, in conjunction with the interconnector, will configure the system to ensure both boards are supplied from the remaining diesel generator. Each diesel generator is fully rated for the whole load to be applied to the 415V 'B' essential system in the event of a reactor trip associated with loss of grid.

110V dc and 50V dc 'no break' supplies

Battery-backed 110V DC and 50V DC supply systems are also provided to support short term switching, indications and telecommunications for in excess of 30 minutes until diesel-backed supplies are restored.

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

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 main electrical 11kV and 3.3kV switchboards are located in the central area of the main switchgear flat. While a localised fire presents a potential threat to these parts of the essential electrical system, external hazards (e.g. flood, seismic) are not assessed to present a significant challenge to these parts of the system. The 415V 'B' essential system is well segregated from these parts of the 11kV and 3.3kV equipment.

The 11kV and 3.3kV diesels and their fuel supplies are located externally to the reactor building. The switchboards, switchgear and diesel generators for both 11kV and 3.3kV supplies are qualified against the infrequent 1 in 10,000 year seismic event. The diesel generators and their diesel oil supplies are not expected to be adversely affected by an infrequent extreme flood (10^{-4} p.a.) due to their elevated location on the site.

The 415V essential supplies (no-break, 'A' and 'B' systems) including the 'B' diesels are qualified against the 1 in 10,000 year seismic event. The 415V 'B' essential diesel generators and their diesel oil supplies are not expected to be adversely affected by infrequent extreme flooding (10^{-4} p.a.) due to their elevated location on the site.

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

The 240V batteries have a capacity to support the 415V essential 'no break' supplies for at least 30 minutes. 3.3kV essential supplies to the 3.3kV / 240V DC transformer/rectifiers would be expected to be restored via 11kV/3.3kV diesel generators well within this time in the event of a loss of off-site power.

The bulk fuel storage tanks for the 11kV and 3.3kV diesel generators provide a total usable fuel storage capacity of 159,000 gallons. The technical specifications require the bulk fuel stocks to be maintained above 62,500 gallons to meet a specified requirement for 10 days continuous running of the diesel generators required to maintain satisfactory post-trip cooling under prolonged grid loss conditions with both reactors pressurised.

Fuel for the 415V 'B' essential diesel generators is stored in a tank farm outside the diesel house, comprising two 182,000 litre capacity bulk storage tanks and in individual 5,000 litre capacity service tanks associated with each engine. The technical specifications require the bulk fuel stocks to be maintained above 21,000 gallons (~95,500 litres) to meet a specified requirement for 10 days continuous running of the 415V diesel generators.

1.3.5.4 Diverse On-Site Back-up Power Supplies

The stress test report section headings draw a distinction between primary back-up power supplies and 'diverse' on-site power supplies. A demonstration of defence in depth does not necessarily require the presence of diversity in sources of electrical supply. Nevertheless, it may be appreciated that the back-up sources of electrical supply at Hunterston B are extensive, with a total of nine diesel generators supporting generation at three voltage levels exhibiting redundancy and segregation; the latter being between the 415V 'B' essential system and the higher voltage diesel generators.

Diversity of 'power supplies' in the broader sense of 'motive power' rather than 'electrical power' may be demonstrated at Hunterston B in respect of the secondary essential safety functions supporting post-trip cooling, i.e. primary coolant flow and secondary coolant flow. Providing the primary circuit is pressurised, primary coolant flow may be achieved without external motive power, i.e. by natural circulation. Motive power is also required to deliver a flow of feedwater to the boilers but this may be achieved without recourse to the essential electrical system. The back-up boiler feed system at Hunterston B has feed pumps which are directly driven from diesel engines. No external electrical supplies are required; the back-up boiler feed pumps may be started manually local to plant.

In addition to the back-up boiler feed, the diverse cooling system provides an alternative means to cool the pressure vessel cooling system and reactor auxiliary cooling system which is independent of the grid and the normal station diesel backed electrical system.

1.3.5.4.1 Diverse On-Site Back-up Power Supplies – Cable and Equipment Locations

An alternative source of motive power from the electrical supplies to support post-trip cooling is provided by the back-up boiler feed system. This is independent of the electrical system. The back-up boiler feed pumphouse is well segregated from all parts of the essential electrical system.

1.3.5.4.2 Diverse On-Site Back-up Power Supplies – Performance in Hazards

Diverse electrical back-up supplies are not provided at Hunterston B. However diverse provision of the essential safety function of post-trip cooling is provided by the back-up boiler feed system. Its location on the site offers protection against significant inundation from the sea and modifications currently underway are designed to secure resilience against an infrequent (10^{-4} pa) seismic event.

1.3.5.4.3 Diverse On-Site Back-up Power Supplies – Time Constraints

Diverse electrical back-up supplies are not provided at Hunterston B. However diverse provision of the essential safety function of post-trip cooling is provided by the back-up boiler feed system. Localised back-up boiler feed diesel tanks provide for operation in excess of 24 hours although it would be expected that continuous running times in excess of 10 days would be possible given manual replenishment of these tanks from bulk diesel stocks elsewhere on-site.

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) 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. Additional time would then be required to deploy this equipment.

1.3.5.5.1 Potential Connections to Neighbouring Units/Plants

Hunterston B is a twin unit station in which a number of the station systems are shared between the two units. The extent of integration is considerably greater than that seen in other multiple unit plants which are merely repetitions of a single reactor design. The AGR is designed such that the two reactors share the same charge hall building and, the electrical supply systems are shared to an extent.

The facility of cross-connecting similar electrical distribution boards in the main electrical system between the two units at 11kV and 3.3kV level is included in the plant design. This is not invoked under normal operating conditions but provides a degree of flexibility in exceptional circumstances. Cross connection between units is also possible at lower voltages but is again carried out exceptionally.

The primary back-up electrical supplies (see Section 1.3.5.3) are designed to supply both units simultaneously.

Hunterston B has historically shared some power supplies from the neighbouring Hunterston A station. However Hunterston A is now being decommissioned and it is no longer possible to expect any significant sources of electrical power to be provided by the Hunterston A station due to gradual removal of interconnections.

1.3.6 Batteries for DC Power Supply

Section 1.3.5 identifies the significant DC batteries at Hunterston B used to support the 'no break' essential systems. These are the 240V DC batteries, designed to support essential systems for a limited time (up to 30 minutes) by which time it would be expected that diesel-backed supplies would be on line. There are also batteries within the 110V DC and 50V DC supply systems which are provided to support short term switching, indications and telecommunications for in excess of 30 minutes until diesel-backed supplies are restored.

1.4 Significant differences between units

There are no significant differences between units at Hunterston B

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 practicable' 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.

Chapter 2 - Earthquakes

Hunterston B

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 line⁷ 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 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 with plant modification planned/carried out were necessary as part of the first periodic safety review in the late 1990s, covering both the at-power and shutdown conditions as well as fuel handling operations.

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

2.1 Design basis

2.1.1 Earthquake against which the plant is designed

2.1.1.1 Characteristics of the design basis earthquake (DBE)

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

- For any infrequent initiating event, there should be at least 1 line of protection to perform any essential safety function, and that line should be provided with redundancy. The magnitude of an infrequent earthquake corresponds to a severity consistent with a return frequency of 10^{-4} per annum (p.a.). This is often referred to in the seismic safety cases as the ‘bottom line’ earthquake.
- 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 however there must be one line of protection. Frequent initiating events are defined as more frequent than 10^{-3} p.a.

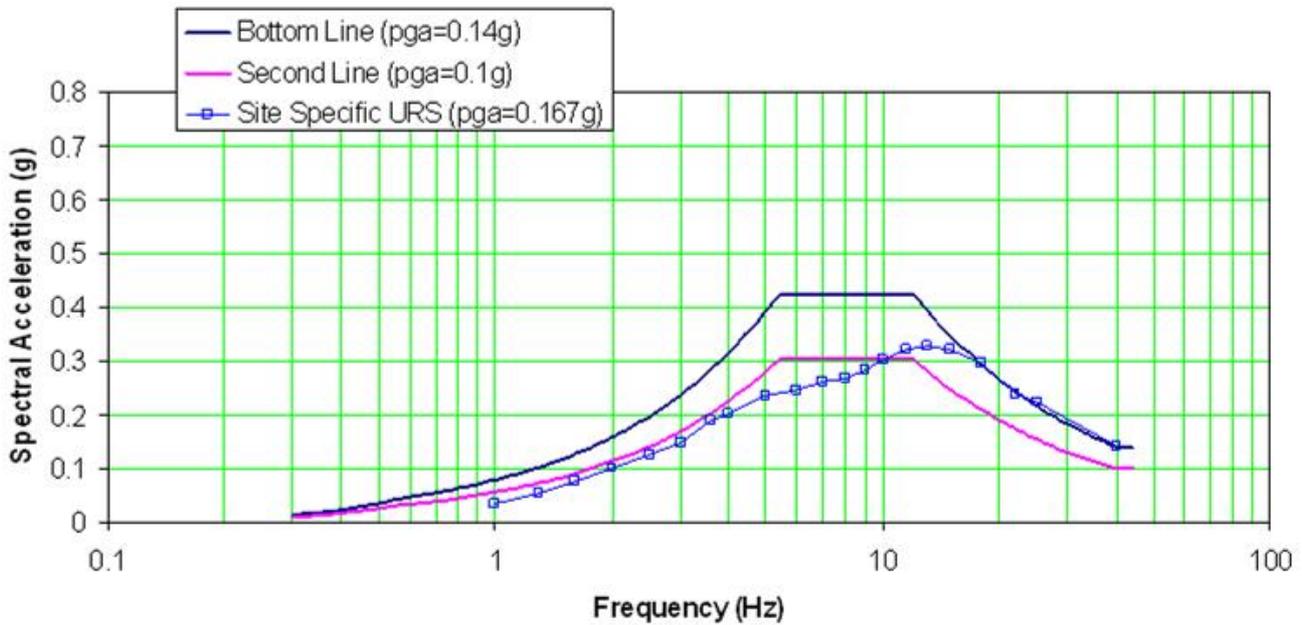
The actual site specific Peak Ground Acceleration (PGA) for the infrequent earthquake at Hunterston B is 0.167g Uniform Risk Spectrum (URS). However the seismic safety case has been developed to be consistent with the corresponding case at Hinkley Point B, where the infrequent earthquake is taken as one with a peak ground acceleration (PGA) of 0.14g Principia Mechanical Ltd. (PML) hard site response spectrum. It can be seen from Figure 2.1 below that the 0.14g PML is a conservative representation of the infrequent site specific earthquake. In practice, the 0.1g PML response spectrum is a close match to the site-specific URS (with a PGA of 0.167g) throughout the range of frequencies (1 Hz to 10 Hz) that are most important for structural response at industrial sites such as Hunterston B. The majority of the safety case for infrequent earthquakes at Hunterston B is based on use of 0.14g PML; however there are a few areas of the case where qualification to this level is not reasonably practicable, where qualification to 0.1g PML has been implemented.

Following normal convention for PML spectra the vertical accelerations have been taken to be 2/3 of those acting horizontally. The URS was obtained from site-specific evaluation in 1991 using the seismic hazard working party methodology which is described below.

The design basis earthquake at Hunterston B for a frequent event has an assumed PGA of 0.1g Principia Mechanical Ltd. spectrum in accordance with IAEA guidelines.

⁷ Assumed to mean tectonic plate boundary

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 shutdown and post-trip cooling was initiated subsequent to the earthquake. The tsunami was the cause of the majority of the plant failures.



Hunterston B Ground Motion Specification

Horizontal, 5% damping

Figure 2.1: Hunterston B 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} pa). This is identified as the bottom line event, i.e. the most onerous event for which bottom line plant provides protection. Bottom line plant and structures are those plant and structures required to provide a single line of protection during the infrequent, more onerous seismic event. The bottom line plant is required to perform the essential safety functions of trip, shutdown, and post-trip cooling; the bottom line structures are those that must withstand the infrequent earthquake to maintain the reactor in a coolable geometry. Bottom line plant and structures also provide one of two lines of protection against frequent events.

Seismic Hazard Assessment Methodology

The methodology for assessing the seismic hazard at each site was developed in the early 1980s by a group known as the seismic hazard working party. The seismic hazard working party was chaired and co-ordinated by Central Electricity Generating Board (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 in the UK as the URS and are used to define the infrequent seismic hazard at the reactor sites.

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

- 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.
- Specifying parameters describing factors such as the rates of activity in these zones, source depths and attenuation parameters. These are specified conservatively.
- 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.
- 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	
3 May 1998	Jura, Scotland	3.5 ML	
4 March 1999	Arran, Scotland	4.0 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

Many seismic events have occurred in the UK since the first periodic safety review of Hunterston B. Only two events within the innermost zones of the Hunterston B seismic zone model were large enough to merit macroseismic surveys, those on Arran (4 ML) and Jura (3.5 ML). In the case of the Arran event, the isoseismal 4 skirts the Ayrshire coast close to Hunterston. At this intensity level, it would be reasonable to expect the earthquake would have been felt at the site, but station staff were not aware of the event. Clarification on the nature of the felt area was therefore sought from the British Geological Survey. The event was not detected by the seismic monitoring equipment on the site and this is consistent with a low level of ground motion. The Jura event had a somewhat lower local magnitude (3.5 ML compared with 4.0 ML for the Arran event) but had a larger area within isoseismal 4, namely about 4000 square kilometres. None of these events were sufficient to trigger the seismic alarm at the station (set at 0.05g)

These reviews concluded that the events that were considered did not give cause to reconsider the validity of the design basis earthquake.

Geological Information on-Site

A complete review was carried out of the information on the soil and rock conditions below the site. These were reviewed to establish the range of properties which were used for the soil structure interaction analyses.

The solid geology of the site is formed by rocks of the Upper Old Red Sandstone of the Devonian or early Carboniferous periods of the Newer Palaeozoic Era. Where the rocks are overlain with superficial deposits, these consist generally of interbedded medium dense, dense or very dense sand or gravel and firm or stiff sandy silty clay, laminated silty clay or sandy silty clay with gravel, some of which may be naturally occurring, but are generally considered to be made ground.

The sandstones in the rock strata contain intrusions of basalt and also contain agglomerate as a pyroclastic deposit within the sedimentary sequence of the sandstones. Apart from these irregularities, the rock beneath the site is fairly uniform sandstone over the whole area of the site with the top surface of the rock varying in level between +6 and -10m Ordinance Datum (OD).

A volcanic vent filled with basaltic lapilla tuff occurs to the south of the site and excavations for the Hunterston B site revealed a similar vent of up to 100m in diameter. The area is also traversed by dykes and sills of igneous origin.

As well as the existing soil/rock information for the Hunterston A and B stations, a series of cross hole shear wave velocity measurements was carried out nearby in the sandstone. This work was commissioned for the proposed dry fuel store at Hunterston. The work was extrapolated to the Hunterston B site. The report also confirmed the use of Principia Mechanics Ltd hard ground spectrum as being appropriate for Hunterston B site.

Seismic Source Model and Sensitivity Studies

A number of studies have been carried out on the Hunterston Peninsula to determine the site specific expected ground motion. The first study was carried out for the Hunterston A Magnox Station Long Term Safety Review. This report connected a number of studies including a jointly funded contract on United Kingdom seismicity. One of the significant conclusions of this study was that the UK exhibited regional variations and that there were slight differences between the Hunterston seismicity and the UK as a whole. That is, Hunterston exhibited lower ground acceleration for any given annual probability of exceedance. For example, at annual probabilities of exceedance of 1 in 1,000 and 1 in 10,000 year events, Hunterston's peak free field horizontal acceleration are 0.08g and 0.17g respectively, compared with 0.09g and 0.19g for the UK as a whole.

A second study was commissioned in 1991 prior to the periodic safety review of the Hunterston B AGR station, which is sited adjacent to the Hunterston A Magnox station. The results of this study confirmed that the seismic hazard at Hunterston is somewhat below the average for the United Kingdom, with the infrequent (10^{-4} pa) exceedance probability lying between 0.16g and 0.17g. This report also generated the expected Hunterston uniform risk spectra and showed

that when compared to the 1981 PML hard ground spectra anchored to 0.17g, the URS are lower at moderated frequencies.

The zonation for the 1991 study was based on an earlier seismic zonation of west and central Scotland in which a square area of side 250 km was established, bounded to the south-east by the Southern Uplands Fault. This was subdivided into four equal square zones corresponding to the southern, western, northern and eastern sectors, with Hunterston situated close to the centre of the southern zone.

For the northern, eastern and western zones, the conventional Poisson model was used to establish the range of possible activity rates from the observed earthquakes. However, in the southern zone (the most significant one for the hazard at the site), no events with magnitudes greater than 4.0 ML had been documented. It was therefore judged that a range of scenarios should be considered to ensure that the hazard was not underestimated as a result of the scarcity of data. The mean activity rate predicted by the conventional Poisson model was therefore taken as the lower bound activity rate for the southern zone, whilst the upper bound was based on the pessimistic assumption that the activity rate is equivalent to that which would result if the seismicity were evenly distributed over all four zones and then concentrated in an area one third smaller.

No site-specific sensitivity studies were carried out, but the usual parameter uncertainty was included in the logic-tree formulation. Furthermore, the seismic source model was deliberately chosen in a pessimistic way to ensure that the predicted seismic hazard was suitably robust and conservative to use for engineering purposes.

After joint discussions between the licensees and the regulator, it was decided to adopt common input motions for the assessment of the Hunterston B and Hinkley Point B plant, systems and structures as discussed earlier in this section.

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.

As noted above the 0.14g PML response spectrum has been used for the majority of the safety case from infrequent seismic events, whereas the site specific earthquake corresponds to 0.1g PML. Thus there are significant margins in the case as a result

The original seismic hazard source model for the site had activity rates based on the number of events above a threshold magnitude of 4.0 ML, chosen to ensure completeness of the database. The historical time period began in AD 1600 and, allowing for higher threshold magnitudes in earlier historical periods, the effective time period of observations was 196 years. During this period, 11 events above 4.0 ML were observed in the four zones, 7 in the North zone, 3 in the east zone, 1 in the west zone and none in the south zone (i.e. the zone in which the site is actually located). In the period since 1990, as demonstrated above, there have been no further events above the threshold magnitude in any zone and the observation period has increased by 21.5 years. Consequently, if the seismic hazard assessment were repeated today, the activity rates would be lower than previously assessed and the expected seismic hazard level could clearly not have increased. This conclusion is robust because, even if the Arran event had been over 4.0 ML, the current observed activity rate for the south zone would be about 0.0046 events per year (1 event in about 217.5 years). This rate is at the lower end of the pessimistic range of activity rates included in the original seismic hazard model (from 0.0048 to 0.021 events per year) for the zone, which indicates that a 4.0 ML event on Arran would still be consistent with the original model parameters.

None of these events were sufficient to trigger the seismic alarm at the station (set at 0.05g). This is consistent with the seismic attenuation relationships used in the seismic assessment of the site. To put this into context, the largest seismic acceleration recorded to date by a strong motion recorder is 0.02g. This was recorded only 15 km from the source of the Melton Mowbray earthquake of 28 October 2001, which had a local magnitude of 4.1. Therefore, it is not surprising that the acceleration levels at Hunterston due to the smaller magnitude and more distant events on Arran and Jura were below the alarm setting.

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

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

2.1.2 Provisions to protect the plant against the design basis earthquake

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

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

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

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

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

2.1.2.1.1 Operating Reactors

Infrequent Event

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

Frequent Event

As well as the infrequent hazard event, a less onerous but more frequent hazard magnitude is defined against which two lines of protection are demonstrated, where this is reasonably practicable. As described in Section 2.1.1 above, the design basis earthquake at Hunterston B for a frequent event is taken to be one which has an assumed PGA of 0.1g Principia Mechanics Ltd. (PML) Spectrum, this being representative of a frequent earthquake (10^{-3} pa), i.e. the lower limit of the frequent band defined in the nuclear safety principles.

No formal qualification is judged to be necessary for plant to survive ground accelerations below a damage threshold. For Hunterston B, a peak ground acceleration of 0.03g is well below this threshold and equates to an expected frequency of once in 100 years (10^{-2} pa). Events more frequent than 10^{-2} pa are therefore judged to contribute negligible risk of damage.

Thus the seismic safety case considers appropriate essential systems which are diverse to the bottom line plant and demonstrates that these are qualified to withstand 0.1g PML, where reasonably practicable. This 'second line' plant and the safety case that surrounds it are not central to this report, since the focus of this review is on extreme events.

Essential Safety Functions

Essential safety functions are required to prevent, protect or minimise potential radiological consequences of an initiating event such as an earthquake. In order to achieve a safe shutdown post an infrequent earthquake. The following essential safety functions are required:

- Reactor trip
- Reactor shutdown
- Post-trip cooling and monitoring

The case is based on demonstrating that the essential functions of trip, shutdown, post-trip cooling and monitoring can be provided for an infrequent bottom-line seismic event (corresponding to a peak free field horizontal ground acceleration of 0.14g combined with a pessimistic spectrum).

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

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 generally designed on fail-safe principles; both these systems will remain available (or fail-safe) to provide protection for any faults generated by the infrequent 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 primary shutdown system is assured.

Post-Trip Cooling

The bottom-line line post-trip cooling protection is based on natural circulation with boiler feed provided by the back-up boiler feed system and pressure vessel cooling provided by the diverse cooling system. The following sub sections address the functionalities required to support this claimed post-trip cooling.

Pressure Boundary

In order to support this claim, it was necessary to carry out seismic assessment, and where necessary, plant modification of the following plant and structures to ensure the integrity of the pressure boundary:

- The pre-stressed concrete pressure vessel, liner and penetrations. The assessments included the CO₂ bypass plant and the reactor safety relief valve pipework.
- Small bore pipework connected to the reactor.

- Boilers.

Assessments have been carried out to ensure that non-essential plant would not pose an interaction threat to the pressure boundary.

Gas Flow Path

The modelling for natural circulation cooling assumes that the normal gas flow paths around the circuit remain unaffected. Detailed seismic assessment was carried out for the core and associated support and restraint structures to demonstrate the integrity of cooling flow and control rod entry paths. In addition, detailed analysis was carried out to confirm the integrity of the fuel assembly, boiler support and boiler internal components following a bottom-line seismic event.

Boiler Feed

The manually initiated back-up feed system has been designed and installed to be qualified against the infrequent seismic event. The back-up boiler feed pumps are direct diesel driven pumps, designed to feed the main boilers at low pressure. Depressurisation of the boilers is achieved manually using the boiler depressurisation valves. The back-up boiler feed system provides adequate feed flow to support natural circulation.

Pressure Vessel Cooling System

The pressure vessel cooling system is seismically qualified for the infrequent design basis seismic event. The pressure vessel cooling system is cooled by the reactor cooling water system which is not seismically qualified to bottom line.

The diverse cooling system has been designed and installed to perform this role. Operator action is required to put the diverse cooling system into service.

Consequential Boiler Tube Failure

There is a safety case which identifies that a seismic event can lead to a consequential boiler tube failure, albeit with a relatively low consequential probability. This arises as a result of the boiler pressure and system loads that occur on boiler components as a result of a reactor trip, together with seismically induced stress in the boilers. As a result, systems structures and components which have a role in protecting against the consequence of boiler tube failures have already been seismically qualified or currently ongoing under normal business.

Seismic events during on load refuelling

An existing assessment has previously identified that seismically induced movement of the fuelling machine in an extreme event, has the potential to create a breach in the reactor pressure boundary at the seal area between the reactor and the fuelling machine. There is a safety case outlining the provision to prevent and limit the potential for radiological release. As a result of this work is already being carried out as part of normal business to seismically qualify flash CO₂ plant.

Forced Gas Circulation

The reactor gas pressure should be maintained in support of effective natural circulation cooling. Although the primary seismic safety case is based on natural circulation, as noted above, there is the possibility that a breach in the pressure boundary may occur as a result of on load refuelling operations or small bore pipework failure. Therefore seismic assessment (and where necessary, modification) has been previously carried out to enable the appropriate systems to be claimed for manual start/operation following a bottom-line seismic event using local to plant actions where necessary.

In addition operating instructions have been put in place to support the claimed manual restoration of gas circulators following establishment of post-trip boiler feed.

In line with the commitment referred to in the section above on seismic events during on load refuelling, significant additional qualification work has been carried out aimed at providing additional robustness in bottom line seismic events.

Essential Stocks

The safety approach at EDF-Energy stations requires sufficient stocks of consumables to be held to enable essential functions to operate autonomously for a sufficient time to reasonably allow replenishment from off-site sources before they are used up, as discussed in Section 2.1.2.3.3 below.

Minimum quantities of these essential consumables have been determined and are specified in the relevant technical specifications.

Post-Trip Monitoring

In general, the equipment in the central control room has not been functionally qualified to withstand a bottom line seismic event and is not claimed as essential plant. Whilst the control room is expected to remain habitable, should it become unusable for any reason then an alternative monitoring station exists to provide a single area from which the status of the trip, shutdown and post-trip cooling of the two reactors can be monitored. This alternative provides the operator with post-trip indications and has been designed to withstand the infrequent level event. It has an uninterruptible power supply and is powered by a seismically qualified on-site AC power supply. Local plant indications may also be available but are not claimed for the bottom line seismic event.

Civil Structures

The plant that constitutes the various essential systems is housed in a number of reinforced concrete, steel-framed and masonry structures on-site. Whilst the structures themselves do not perform an active safety function, they may adversely affect the performance of the safety-related equipment. The structures have therefore been assessed against the requirement to maintain support to the safety-related equipment and to not cause incidental damage through interaction effects.

Other outlying buildings housing essential equipment are also qualified to the bottom line seismic event.

2.1.2.1.2 Shutdown Cooling

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

The shutdown cooling safety case claims that cooling will be achieved by restoration of gas circulators with main boilers being fed using the back-up 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.

As discussed in Section 2.1.2.1.1, it has previously been identified that seismically induced movement of the fuelling machine in an extreme event, has the potential to create a breach in the reactor pressure boundary at the seal area between the reactor and the fuelling machine. There are provisions in place to limit the potential for radiological release. As a result of this issue work is already being carried out to seismically qualify appropriate CO₂ plant.

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 (excepting the effect of a potential pressure boundary breach noted above)

- Buffer storage - cooling systems are seismically qualified
- Dismantling - loss of cooling is tolerable as natural cooling is adequate
- Storage in ponds - cooling system is not seismically qualified. Timescales to recover cooling are as per Chapter 1.

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

The severity of the earthquake used in the safety case to represent the infrequent design basis earthquake with a return frequency of 10^{-4} p.a. 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 (referred to in Section 2.1.2.1).

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

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

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

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

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

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

2.1.2.2.1 Operating reactor

Trip

If there are no plant faults requiring automatic trip, then the operator will perform a controlled shutdown or manually trip the reactor. The guardlines are qualified or will fail-safe as described in Section 2.1.1.1.

Shutdown

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

Post-trip Cooling

For the primary case, manual initiation of back-up boiler feed is claimed to be achievable from the central control room or local to plant.

The safety case currently assumes that inlet guide vanes are frozen following the seismic event. Pre-trip positions are suitable for post-trip cooling but manual operation of inlet guide vanes local to plant is also claimed if required to achieve forced gas circulation.

In the event of small bore pipe failure causing a very small depressurisation fault, manual initiation of emergency boiler feed pumps and manual restart of gas circulators is claimed in order to provide forced gas circulation. This requires a number of local to plant actions. This also applies if a breach has occurred as a result of the earthquake whilst the fuelling machine is connected to the reactor, although the claimed timescales for restoration of gas circulators is shorter. Appropriate operator actions relating to boiler feedwater are required after a few hours; other actions may also be required depending on the detailed nature of the fault sequence.

Station procedures have been amended to take account of the required operator actions. As some of these actions require local to plant operations, extended timescales for their completion has been included in the safety case.

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 the totality of the required actions and the way these might be influenced by the emergency arrangements taking due account of the human factor 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, and it is considered that this should be reviewed. This issue has been included in Consideration 2.1.

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

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

2.1.2.3 Protection against indirect effects of the earthquake

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

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

The seismic qualification methods used in EDF Energy (see Section 2.1.2.1) include consideration of 'interaction threats'. In other words, when considering the functional capability of systems, structures and components, the potential for the failure of nearby plant, whose functionality may not have been seismically qualified (on the basis that such functionality is non-essential) is considered. In this way, if earthquake induced failure of nearby plant can cause failure of the essential function, then reasonably practicable remedial action is taken.

Failure of the low pressure 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.

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

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

The safety case assumes that consequential loss of grid occurs for both frequent and infrequent seismic events. The safety case approach in EDF Energy Nuclear Generation is to ensure that adequate stocks of consumables are held on-site to last at least 24 hours. The usual approach is for the minimum stock levels quoted in technical specifications to be those that correspond to this 24 hour 'mission period'. It is implicit in the safety case that company emergency arrangements would provide replacement consumables within the 24 hour period to enable the plant to be managed safely. Note that in general, normal stocks levels are higher than the limits specified in technical specifications, 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. This is discussed further in Chapter 6.

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

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

The Local Resilience Forums are the local authority body in the UK with responsibility for providing emergency response in the community.

A review of site access following external hazards has been carried out. At Hunterston it is postulated that the bottom-line seismic event would only involve damage to some ancillary buildings and that roads on-site would remain passable.

The main access road to Hunterston B is in good condition and confidence in its design and current condition is provided by the fact that it was used at the time of construction of Hunterston B, in order to facilitate the delivery to site of heavy site construction loads, and that it is currently considered adequate for the transport of the new heavier design fuel transport flasks.

The view that there is no significant potential for the prevention of road access following a seismic event is further supported by a recently completed review of the risk of blockage of the road from the A78 roundabout to the site main gate and inside the power station site.

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

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

Conclusion HNB 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).

Worldwide experience is that in urban environments fires, 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, 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.

The reactor coolant pressure boundary is expected to remain intact, so there is not expected to be a significant hot gas release hazard. In the unlikely event of small bore branch failure, the resulting hot gas release effects should be small. In the event of an earthquake occurring during on-load refuelling, there may be significant environmental effects arising from hot gas release in the charge hall. However there is not plant essential for reactor post-trip cooling in that area.

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

Conclusion HNB 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 HNB 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 modification proposals address whether plant affected by the proposal is claimed as seismically qualified and whether the modification could have a deleterious effect on that qualification or any other seismically qualified equipment. The procedure therefore reduces the risk that the seismic safety case is compromised by changes to the plant and structures.

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

The review carried out as part of within design basis review identified inconsistencies in fleet guidance on housekeeping standards.

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

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

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

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

2.1.3.4 Specific compliance check already initiated by licensee

The checks carried out following the events in Fukushima have confirmed that the safety case is based on the provision of a line of protection with redundancy for the infrequent design basis earthquake, and two lines of diverse protection with redundancy in each line, for the frequent design basis earthquake. These cases are considered 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 walkdowns that whilst being compliant with our existing safety case requirements, did not meet industry best practices. The fleet guidance on housekeeping standards lacks clarity in the seismic area. The associated record keeping requirements also need clarity. A number of commitments were made as a result of the 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 HNB 2.9: The reviews undertaken and the actions identified therein, have confirmed that Hunterston B is compliant with the current licensing basis, although a few improvements have been identified.

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

2.2 Evaluation of safety margins

The experiences at Fukushima Dai-ichi outline the significance of the plant experiencing events more severe than were considered within the design basis earthquake. The EDF Energy Nuclear Safety Principles for the 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 10^{-4} pa within the design basis safety case.

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

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

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

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 (HCLPF). Higher reliability is expected for new plant designed according to code-based methods. In any case, even where 'high confidence of low probability of failure' is not strictly achieved, margins will be sufficiently great that there will be no disproportionate increase in risk for more severe seismic events.

The justification for this assertion lies in the concept of seismic fragility functions. Figure 2.2 is a typical fragility curve for a system, structure or component which has been seismically qualified. It shows the way the probability of failure increases as the severity of the earthquake increases. Curves like this can be used quantitatively in seismic probabilistic safety assessment. In deterministic seismic cases, the curves are used by the concept of the level at which there is a high confidence in the low probability of failure (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.

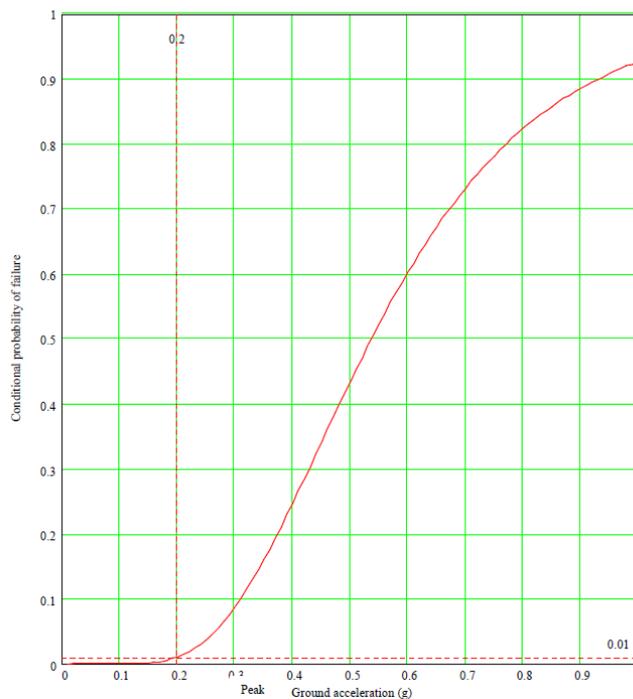


Figure 2.2: Mean Fragility Curve for Typical System Qualified to 0.2g PGA

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 HNB 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 design basis earthquake, which for Hunterston B is 0.28g PGA. The seismic hazard assessment reports for the site indicates that this increased level of ground motion has a probability of between 10^{-5} and 10^{-6} per year.

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 HNB 6.1 raised in Chapter 6 will lead to further insights into this issue.

Clearly, where there are known issues with the robustness of the plant to withstand the within design basis infrequent earthquake, the margins available for those systems, structures and components may be reduced. These known issues are a subject of further work as detailed in Section 2.1.

2.2.2 Range of earthquake leading to loss of containment integrity

AGRs are not provided with a containment structure, so this question does not apply. However the reactor pressure boundary does have a containment role, although its main role is to maintain the density of the CO₂ primary coolant. The qualification of the reactor pressure boundary for design basis earthquake is discussed Section 2.1.2.1.1. Therefore the comments in Section 2.2.1 above relating to margin to failure also apply to here.

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

There are no dams or large water courses within the vicinity of Hunterston B, and although there are large bodies of water surrounding the site, 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 Department of the Environment, Food and Rural Affairs (DEFRA) in 2005 to evaluate the tsunami risks to the UK. The study concluded that the probability of a tsunamigenic seismic event in UK coastal waters was very low and that if it did occur the likely coasts affected would be eastern England and Eastern Scotland. Tsunamis could be generated with the potential to affect Hunterston, but these would be associated with seismic events originating in areas remote from the Station such as the plate boundary west of Gibraltar. 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 Hunterston 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 flooding risk at Hunterston B 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 HNB 2.12: There is not a credible risk posed to UK plant from a beyond design basis earthquake and consequential beyond design basis flood.

2.2.4 Potential need to increase robustness of the plant against earthquakes

EDF Energy undertook 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.

Section 2.1.3.4 discusses the scope and findings of the specific seismic aspects for within the design basis review. The findings of the seismic aspects for the beyond design bases review is 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 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 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.

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. However in line with reviewing the potential for consequential fire, noted in Section 2.1.2.3.4, feasibility to enhance the seismic capability of unqualified fire systems could be considered.

It was noted across the fleet that the pond structures are seismically qualified but that the pond cooling systems are not necessarily qualified owing to the relatively low decay heat of the AGR fuel ponds. This is considered acceptable for the DBE, however, feasibility to enhance the robustness of pond cooling systems could be considered.

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

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.

A number of potential areas for improvement were identified by the review.

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

Consideration HNB 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 conservatism, 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

Hunterston B

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 chapter assesses the margins of the existing design basis, as well as the existing flood protection in place at Hunterston B Nuclear Power Station. It demonstrates that:

- Sufficient margin exists between the maximum design basis flood (4.84m Above Ordinance Datum - AOD) and the physical elevation of the main nuclear island (>7.9m AOD).
- 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 shows that the methodology used to calculate the design basis flood for Hunterston B has been constructed using independent expertise based on well regarded sources of information. The methodology has also been constructed with appropriate conservatism, 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 managing beyond design basis risks, 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 Hunterston B site, the protection provided against and the compliance route by way of which Hunterston B 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 all items important to safety should be constructed above the level of the design basis flood, with account taken of wind wave effects and effects of the potential accumulation of ice and debris, where practicable, as a defence-in-depth measure against site flooding.” (The concept of defence-in-depth is explained in Chapter 1). It is important to note that EDF Energy sites can accept a limited degree of flooding and provide means for draining off the flood water with the intention of providing suitable margins (see Section 3.2.1).

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

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

3.1.1.1 Characteristics of the Design Basis Flood (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.

For Hunterston B the characteristic flooding events considered as part of the fault schedule are:

- Frequent rainstorm.
- Infrequent rainstorm (i.e. mean rainfall of 70mm in one hour, 90.5mm in two hours.).
- Frequent snowmelt.
- Infrequent snowmelt.
- Frequent wave overtopping in conjunction with tidal conditions.
- Infrequent wave overtopping in conjunction with tidal conditions.

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 (i.e. 10^{-4} pa). Provisions to protect the plant against the design basis flood and compliance are considered against this infrequent event within this chapter.

The infrequent design basis flood is as follows:

- Significant water level being 4.84 AOD.
- Rainfall for a 1 hour storm period and a 2 hour storm period is 70mm and 90.5mm respectively.
- No threat judged from snowmelt and tsunamis.
- Threat from climate change effects is considered as part of significant sea level.

3.1.1.2 Methodology used to evaluate the design basis flood

Hunterston B geography

Hunterston B is located near West Kilbride in North Ayrshire in Scotland. The general ground level for the Hunterston B site is 6.1m AOD (minimum).

The shoreline to the north and west sides of the station site consists of a wide shore platform (100m and 500m wide respectively) which effectively dissipates wave energy and protects the site. The site itself is protected from flooding from the sea by a revetment (i.e. a natural embankment strengthened and protected along its length by large stones). Across the site there are numerous gullies and downpipes that remove the surface water run-off from buildings and paved areas and discharge such arisings into the station drainage system.

Original methodology employed at Hunterston B

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.

The original methodology employed to evaluate the external flooding threat to Hunterston B consisted of a review of existing data and assessments presented in a long term safety review report published for Hunterston A. Following on from this report further studies have been carried out, resulting in the production of two more reports, both of which form the foundation of the design basis flood for Hunterston B. The reports focused on wave overtopping and general flood events since this present the most onerous scenario. Available meteorological data was reviewed with respect to precipitation and the assessment of relevant meteorological and hydrological data in relation to wave overtopping of sea defences. A detailed analysis of existing site drainage was carried out and an appraisal of existing sea defences was performed. A detailed topographical survey of the site was also carried out. The objectives of the review was to obtain predictions of extreme flood levels over the Hunterston site, identify Hunterston B safety related plant within flooded areas and assess whether loss of, or damage to, the plant would result in a significant radioactive release. Fuel route plant items whose failure due to flooding could lead to a significant radiological release were also considered. The methodologies used to calculate water levels associated with the various source of external flooding are presented below. The results of any subsequent reviews where it is considered that these are significant to the conclusions of this report are also presented.

Wave Overtopping

The prediction of tidal levels appropriate to the Hunterston site is based on the use of Admiralty tide tables. The most appropriate site with values available is Millport. The relevant tidal levels which form the basis for this part of the assessment are the:

- Mean High Water Spring (MHWS) 1.78 m AOD
- Highest Astronomical Tide (HAT) 2.36 m AOD

These levels can be further elevated by a storm surge. The Department of Energy, Offshore Installation; Guidance on Design Construction and Certification 4th Edition, gives estimates of 50 year return positive surge elevations for the UK. For Hunterston B the predicated surge is extrapolated for a 10,000 year return period giving a resulting maximum still water level of 3.98m AOD.

A detailed topographic survey was carried out as part of a wave overtopping study and established the crest of the revetment as varying along its length with a maximum of 5.88m AOD. The crest drops to 4.0m AOD at the northern portion of the site, and at the southern extremity of the site the crest level is 4.62m AOD. Recent trends in land mass movement also affect long term forecasting, but generally indicate a rising mass in the north of the UK which serves to counter the magnitude of rises in sea levels. The available records for Millport indicate an ongoing rise in sea level of some 0.94 mm per year. Assuming a 50 year life for the station would add 47 mm to the determined levels. This is minor and when compared with the inherent conservatism of the still water calculation, can readily be neglected.

To define fully the potential extent of site flooding due to sea effects it was necessary to add in the effect of waves. The maximum fetch appropriate to the Hunterston site is assessed as being 20 km in a north-easterly direction from Arran. The northern part of the study area is more sheltered and a fetch length of 4 km is appropriate. For the infrequent event with a 20 km fetch the appropriate wave height is 4.1 m. With the shorter fetch of 4 km this reduces markedly to 1.9 m. These figures relate to deep water and take no account of shallow water effects, bed friction and refraction and are thus conservative.

For the determination of maximum overtopping effects the infrequent maximum still water level (3.98m AOD) has been combined with a 1 in 100 year wind speed wave effect. This is considered to be a conservative method of a combination of extreme events and is more onerous than the extreme case. Due to local site topography, overtopping only occurs at the northern and southern extremities of the foreshore sea defences. In addition, in order to ascertain the extent of inundation on the site due to a more frequent event, a 1 in 100 year still water level has been combined with the 1 in 100 year wind speed wave effect. The results of this study indicate that the resultant overtopping would give rise to a local flood level of 4.84m AOD.

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. In the first Hunterston B periodic safety review, relevant historical records of seismically generated tsunamis were assessed and it was concluded that over the past 400 years only two seismic events are of note. These events, 1580 Great London and 1755 Lisbon, produced tsunamis which affected the south coast of England. No historical records of seismically generated tsunami have been recorded on the west coast of Scotland. This fact, together with the local geography of the area which includes Cumbrae, Arran, Kintyre and Ireland, would preclude the formation of a tsunami which could threaten Hunterston B. The risk from submarine-slide tsunamis was identified as being relevant to the east coast of the mainland with 3 major events being recorded emanating from the Norwegian Sea Area. The first periodic safety review concluded that no risk is presented to the station from these tsunamis. The probability of a tsunami occurring with an effect on the Hunterston site is considered to be significantly less than infrequent event. Comment is also made that local geology precludes the formation of a suitable landslide. The hazard of seiches (an oscillating wave in an enclosed body of water which may have a period from a few minutes to a few hours and is usually a result of seismic or atmospheric disturbances) is considered to be insignificant.

In 2003, just prior to the occurrence of the Indian Ocean tsunami, the Society of Earthquake and Civil Engineering Dynamics (SECED) held a seminar on this topic. The state of research on UK tsunamis was summarised at the meeting and it was confirmed that the tsunami heights and run up values assumed in the first periodic safety review were still supported. In the light of the 2004 event, consideration was given to underwater slumps involving huge quantities of material (around 3,500 cu km) off the coast of Norway and to mega-tsunamis involving volcano collapse in the North Atlantic. It was confirmed that the existing assessment remained valid. The particular events of the Indian Ocean tsunami and their impact on the Kalpakkam nuclear power plant on the east coast of India were also considered. It was judged that there were no new lessons to be learnt from this event that would be applicable to Hunterston.

At around the time of the second periodic safety review, the Department for Environment, Food and Rural Affairs (DEFRA) commissioned two assessments of the tsunami threat. The first of these assessments concluded that tsunami threats were possible from a number of sources including an earthquake in the North Sea, earthquake in the western Celtic Sea, tsunami associated with the plate boundary west of Gibraltar (referred to as the Lisbon-type event) and a landslide associated with the Canary Islands, but noted that, all major centres of population have flood defence infrastructure designed to cope with the expected range of surges. The follow-up study reviewed in more detail the tsunami hazard for the UK and Irish coasts associated with the Lisbon-type event and the North Sea event. It concluded that even after such significant events, only the most south-westerly coast of the UK may incur sea level elevations marginally in excess of the 1 in 100 year extreme sea level predictions. These findings do not challenge the assumptions that have been made with respect to tsunamis.

In conclusion, there is no credible source of a tsunami that could affect Hunterston B. This is in agreement with the arguments presented in the safety case.

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

Rainfall

The Meteorological Office provided details of rainfall events associated with return frequencies ranging from 1 p.a. to 10^{-4} p.a. For each of these return frequencies the Meteorological Office applied those procedures recommended in the Flood Studies Report of 1975. The analysis produced rainfall values of 70 mm for a 60 minute storm duration and 90.5 mm for a storm of 120 minute duration. Both values refer to an infrequent (10^{-4} p.a.) event. These design values for rainfall were then combined with an extreme tide level corresponding to the Highest Astronomical Tide at Millport. This provided a worst case drainage outfall boundary condition. Independent verification of the existing surface water drainage system was completed and confirmed that general site standing water levels do not exceed 50 mm when no run off is assumed. These levels are assumed to be located adjacent to existing surface water drainage manholes around the main buildings, and are below main building ground floor levels. It is considered that all safety-related plant would remain available in this case.

Snowmelt

Assessment of previous studies and the appraisal of available data indicated that no significant snowfall events are experienced by the power station site. The site is coastal, and the prevailing south westerly wind generally mitigates the effects of snow. It is considered that the effects of snowfall particular to the site at Hunterston are readily bounded by the rainfall and wave overtopping effects.

It is therefore judged that there would be no threat to safety related equipment at the station 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. Therefore EDF Energy are not concerned that snowmelt will pose a more significant threat to the safe and reliable operation of nuclear power stations than it does today.

Climate Change Adaptation

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

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

Sea-level rise

Based on research completed by the Intergovernmental Panel on Climatic Change (IPCC), a pessimistic estimate of future sea level rise of 6 mm per year was assumed in the first Periodic Safety Review undertaken. For the length of time until the next Periodic Safety Review was due in December 2006, the research concluded that the rate of sea level rise would require approximately 70 mm to be added to the standing water levels determined. When this is added to the determined sea levels no significant effects could be seen to occur within the B Station boundary.

More recent reports published by the Met Office in 2004 discussed the effect of climate change and show a global mean sea-level increase of between 4 and 14 cm from 2004 until 2020s. This is supported by an IPCC study in 2001 predicting a mean global sea-level rise of a maximum approximately 13 cm by 2023. Another report produced by the Met Office (2007) provided similar information to that presented previously, 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 Meteorological Office report commissioned by British Energy (at the time) in 2003 found that expected changes in UK climate during the operational lifetime of UK nuclear generating plants are predicted to be small, indeed insignificant, in comparison with the natural variability of parameters such as wind and rainfall. More significant changes are expected with respect to wave and storm surge heights towards the end of the decommissioning period, but this was outside the scope of the most recent periodic safety review.

However, work subsequent to the second periodic safety review indicated a sea level rise due to climate change of approximately 0.99m at Hunterston B over the current century. This indicated that flood levels could rise to 4.97m AOD by 2016. This depth is still not adequate to threaten the main Hunterston B nuclear island at 7.9m AOD; however the cooling water pumphouse at 4.916m AOD would be flooded with consequential loss of the system inside. The increased flood levels due to climate change do not change the nuclear safety arguments as the flooding is infrequent and therefore loss of cooling water systems remains tolerable given that the diverse cooling system remains available.

Wave Height Increase

Given the conservatism in the wave height calculation based on a 20km fetch, discussed in the Wave Overtopping section above, the wave height increases are negligible, as a more appropriate fetch length was determined to be 4km.

Physical Margin

There is a 3.05m margin between the conservatively judged 10^{-4} p.a. bounding flooding event and the lowest elevation of the main nuclear island plant.

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 Hunterston B 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 input from two of EDF Energy's contract partners who are specialists in this area, and will complete prior to the end of 2011.

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

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

Consideration HNB 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, until the period of 2035.

Conclusion HNB 3.3: There is no credible source of a tsunami that would affect Hunterston B. 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 following a frequent and infrequent external flooding event, the following essential 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 3.1 for the following events:

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

Table 3.1: Claimed Line of Protection for an Infrequent External Flood

Type of Claim		Main - Deterministic
Trip		Guardline equipment remains available
Shutdown		Main shutdown system
GCRO Protection		Reactor shutdown sequencing equipment
Post-trip Cooling	Gas Circulation	Forced Circulation
	Boiler Venting	Low pressure vents
	Boiler Feed	Emergency boiler feed system
	Feedwater Source	Deaerator & reserve feedwater
	RACW / PVCW Heat Sink	Diverse cooling system
Essential Monitoring		CCR

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 guardlines and the reactor shutdown sequencing equipment are not at risk from external flooding due to their location.

Shutdown

The main shutdown system is claimed for both bottom line and second line events. The main shutdown system has an extremely high reliability conservatively limited to 10^{-5} failures per demand by a hypothetical common mode failure. There is not a credible flooding risk to the main shutdown system. No claim is, therefore, made on the enhanced shutdown system or on nitrogen injection, following a flooding event with a return frequency of less than 10^{-2} p.a. as the main shutdown system is confidently expected to function.

Post-Trip Cooling

The emergency boiler feed system is claimed as the bottom line post-trip feed system. The second line of defence is provided by the back-up boiler feed system. The primary source of feedwater for the emergency boiler feed pumps comes from the associated reactor’s deaerator. In the event of the deaerator make-up not being available, long term provision of water to the emergency boiler feed system comes directly from the reserve feedwater tanks .

Boiler depressurisation is required before the emergency boiler feed system and the back-up boiler feed system can be utilised. Reduction in pressure is achieved by operation of the low pressure vents.

For gas circulation, forced circulation is claimed as the bottom line defence. For the second line of defence, natural circulation is claimed for the frequent event and although not formally claimed for the infrequent event, is assumed to be available.

Provision of long term feed is normally via the million gallon townswater tank which is not formally claimed. A new back-up feedwater tank is currently being constructed which will provide a claimable source of long term feed. The new tank is being constructed at the highest area of the nuclear licensed site.

The safety case concedes loss of reactor cooling water for the infrequent overtopping event. However, cooling to the gas circulators for forced gas circulation and pressure vessel cooling should remain available supported by the diverse cooling system.

The safety case assumes loss of grid in an external flooding event. Electrical supplies would be provided from the emergency diesel generators and from back-up battery systems. None of these systems would be threatened by an external flooding event and each system has significant redundancy and cross-connectivity.

Essential Monitoring

The central control room would not be susceptible to even very extreme flooding around the Hunterston B station buildings. The assessment has shown that infrequent rainfall events will not pose a threat to the main buildings. The infrequent wave overtopping event could however result in depths of up to 100mm around the Magnox Hunterston A station buildings and the Hunterston B station administration buildings, including the emergency control centre. However, even if this level of flooding were to put the alternative indication centre out of action, the central control room would continue to permit monitoring to be carried out following the infrequent event.

Shutdown Reactors

The impact of external flooding on a shutdown reactor is considered as part of the shutdown safety case. The safety case concedes loss of reactor cooling water for the infrequent overtopping event. However, forced gas circulation and pressure vessel cooling should remain available via the diverse cooling system.

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 cooling water systems, which support buffer storage cooling. However the fire hydrant system provides back-up cooling in such an event.

Conclusion HNB 3.4: 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

The shoreline to the west and north sides of the station site consists of a wide shore platform (100m to 500m wide respectively) which effectively dissipates wave energy and protects the site. The site itself is protected from flooding from the sea by a revetment (i.e. a natural embankment). At the north end of the revetment, north of the drainage outfall, the foreshore has been strengthened with a rock embankment and 40m long section of paved revetment in the form of stone sets. At the south end, the foreshore to the north of the cooling water intake jetty has been strengthened with a short length of gabion wall. The crest of the revetment varies from a maximum of 5.88m AOD to 4.0m AOD (minimum) at the northern portion of the site. At the southern extremity of the site the crest level is 4.62m AOD. The site rises away from the revetment in the landward direction.

Topography & drainage

The surface at the Hunterston B site slopes at approximately 1 in 30 to 1 in 10 towards the sea with a more steeply sloping sandstone layer beneath. The topography combined with the impermeability of the local geology generates high run-off of surface water from the land. Across the site there are numerous gullies and downpipes that remove the surface water run-off from buildings and paved areas and discharge such arisings into the station drainage system. There is a general fall in ground levels from the Hunterston B site to the Hunterston A site and the surface water is discharged

via stormwater outlets located to the west of the site. The primary safety related role of the surface and storm drainage is to provide a hazard reduction role. It reduces the effects of flooding from storm water and other local flooding hazard sources and is judged to be adequate to protect against infrequent external flooding from the landward side.

Conclusion HNB 3.5: The flood defence provisions for Hunterston B are suitable and robust in the event of an external flood event.

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

Operating instructions

In the case of external flooding, the operator is expected to take action. The reactor may require manual shutdown as a result of the hazard in the case of infrequent external flooding. The operator is given instructions to protect the plant from the flooding hazard.

The station operating documents specify actions to be taken following warning of external flooding to prevent, or limit damage to essential plant.

The claims made on the operator actions are not onerous in the event of a severe flood, before the reactor is shutdown. 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 cooling water plant and or the reactor cooling water system is such that the operation of the reactor unit is no longer possible then the reactor will be tripped. At this stage the bulk of the actions occur at the significantly higher elevations where the plant sits.

Conclusion HNB 3.6: 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 24h mission time is presented within Chapter 5.

A review of site access following external hazards has been carried out. During the infrequent high tide seawater flooding event, some areas surrounding the Hunterston B site could become flooded, including parts of the main site access roads, although access should remain available via the farm access road which pass over the elevated land east of the station. After the 24 hour mission period circumstances should be such that access to site will be available for essential supplies.

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

Conclusion HNB 3.7: Access to the Hunterston B site and deployment of personnel has been considered as part of the emergency response and it is considered this continues to be appropriate.

3.1.3 Plant compliance with its current licensing basis

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

All modifications are implemented using 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 is 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 Hunterston B covers the maintenance of the sea defences and site flood protection.

The second periodic safety review identified the need for an ongoing programme of inspection of the foreshore. However, it has been judged that foreshore inspection is not necessary since there would be adequate time for remedial action by operators because essential systems are remote from the foreshore. The safety case concurs with this argument and further argues that only dramatic changes to the foreshore could have a significant effect on extreme sea levels. It is nevertheless proposed in the second periodic safety review that foreshore inspections should form part of the regular LC28 inspections. This would provide consistency with Hinkley Point B. As the safety case does not rely on structures to prevent the ingress of seawater to essential plant, there is no requirement for any related LC28 inspections. The inspection schedules have been examined and these do include an appropriate level of attention to external drainage, although the emphasis is clearly on the effects on the building structure rather than site drainage. For example, a typical Inspection Guideline for External and Internal Drainage is as follows:

- Blockages – Drains shall be checked for blockages. All drains should run freely with no evidence of debris which could lead to future blockages.
- Manhole Covers – The condition of all manhole covers and channel covers shall be checked.
- Brickwork and Mortar – The condition of brickwork and mortar shall be checked for signs of distress

Recent LC28 reports have been consulted, paying particular attention to those relating to lower parts of the site, no issues connected with site drainage have been identified.

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

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

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

Within the processes outlined above there are mechanisms for identifying any areas of concern or anomalies. These may take the form of a commitment from the productions of a safety case, justification 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 HNB 3.8: There are no outstanding issues identified related to the external flooding safety case.

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

In light of the events at the Fukushima Dai-ichi plant, as responsible operators EDF Energy Nuclear Generation have carried out reviews at each of the sites as required by the Board.

Scope

The 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 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.

Summary of Hunterston B Findings

All tasks were completed. With regard to flooding, the actions below were identified and are in progress:

- There are no immediate safety issues that would compromise the existing design basis accident withstand capability.
- A small number of minor deficiencies have been identified, which require timely resolution. Corrective actions have been identified to address these areas for improvement.

Conclusion HNB 3.9: The reviews undertaken and the actions identified therein, have confirmed that Hunterston B is compliant with the current licensing basis.

3.2 Evaluation of safety margins

An estimation of the safety margins against external flooding is presented below outlining that Hunterston B 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 between the main safety related plant and the design basis flood. There is also shown to be adequate defence-in-depth.

3.2.1 Estimation of safety margin against flooding.

Cliff edge effects are not assumed to occur on the site once the margin for sea wall overtopping has been exceeded. However the return period for such 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. Large physical margins and drainage capacity exist to demonstrate the resilience of the plant.

Physical Margins

The Hunterston B site including the main safety related plant and buildings forming the nuclear island are relatively high in terms of the site flood levels. Although the ground level of the cooling water pumphouse and the adjacent area is located at a level of approximately 4.91m AOD, the Reactor building is located at a level of approximately 7.9m AOD. The turbine hall is generally located at a level of approximately 7.9m AOD; however areas do exist in the north west corner where the ground level reduces in height to approximately 6.23m AOD. The design basis flood from wave overtopping at Hunterston B station is 4.84m AOD. There is therefore sufficient margin available within design basis with the possible exception of the reactor cooling water system.

Conservatism within the Methodology

The methodologies used to estimate the extreme event were taken from the Department of Energy as used for Offshore Installations. The methods utilise an extrapolation of both total standing water levels and the surge components out to 1 in 10,000 year levels, which is considered a conservative approach. This infrequent storm is then coupled with a 1 in 100 year wind. Again this is considered conservative.

The resulting water levels are such that, even after adding climate change assessments undertaken for Hunterston B that there is more than sufficient margin available on-site.

The current periodic safety review document highlighted the conservative nature of the previous overtopping assessment which considered an infrequent tidal return frequency together with a 1 in 100 year wind return frequency. Topography of the Hunterston B site allows drainage from higher ground under gravity directly to the sea. The site is also protected from wave overtopping by the revetment. There is therefore sufficient margin demonstrated within the design basis.

It is important to note that any sensitivity within the Hunterston B external flooding methodologies will only affect the frequency of the loss of the cooling water pumphouse and are therefore associated with the higher frequency events, rather than the design basis events considered here. The margins between the infrequent flood levels and the main nuclear island are significant enough to give confidence that seawater flooding of essential plant other than the cooling water systems is an incredible event, even if the methodologies were not as conservative as judged.

Lines of Protection

In extreme external flooding events, essential plant items will not be affected with the possible exception of the cooling water pumps. Therefore in all but a loss of cooling water 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 3.2 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. In such an event, the main safety related plant will be powered from emergency diesel generators and from back-up battery systems. These are all protected by their location within the reactor building as outlined above. This is further discussed in Section 3.1.2.1. Therefore, in a beyond design basis event, there is expected to be sufficient margin.

Table 3.2: Claimed Lines of Protection for an Infrequent External Flood as well as Defence-in-Depth measures that demonstrate further protection.

Type of Claim		Main – Deterministic	Defence-in-Depth
Trip		Guardlines	Main guardline
Shutdown		Main shutdown system	Alternative shutdown system (+N ₂ Injection)
Gas circulator run on protection		Reactor shutdown sequencing equipment	Quadrant protection equipment
Post-trip Cooling	Gas Circulators	Forced gas circulation	Natural circulation
	Boiler Venting	Low pressure vents	Diverse boiler venting Turbine leg drains*
	Boiler Feed	Emergency boiler feed pumps	Back-up boiler feed system
	Feedwater Source	Deaerator & reserve feedwater tanks	Back-up boiler feedwater tank as well as Townswater*
	RACW / PVCW Heat Sink	Diverse cooling system	Townswater*
Essential Monitoring		Central control room	Alternative indication centre

*Townswater and Turbine Leg Drains are not claimed as formal deterministic lines of protection within the safety case; however they are outlined in the table as they provide additional Defence-in-Depth.

Conclusion HNB 3.10: The review has shown that there are suitable and sufficient margins present within the methodology and plant for compliance with the current safety case. There is also sufficient margin for a beyond design basis flood.

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

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.

Section 3.1.3.4 discusses the scope and findings of the specific flooding aspects for Hunterston B within the design basis review. The findings of the flooding aspects for 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.

Scope

The 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 this 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.

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

Summary of Findings

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

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

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

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

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

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

Conclusion HNB 3.11: 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 HNB 3.2: Consideration should be given to the feasibility of additional temporary or permanent flood protection for essential safety functions.

Consideration HNB 3.3: 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 conservatism, 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.

The bounding case for external flooding at Hunterston B is seawater waves overtopping the revetment. The methodology for the external flooding case demonstrates that seawater flooding on the site is nearly incredible. There is a 3.05m margin between the conservatively judged 10^{-4} p.a. bounding flooding event and the lowest elevation of the main nuclear island plant. Additionally, the site is on a hill and therefore rainwater will flow into the sea.

Chapter 4 – Extreme Weather

Hunterston B

4 Extreme Weather

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 Hunterston B 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 of 1 in 10,000 per year at the site.

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

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

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

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 are 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 Hunterston B for these hazards is discussed in what follows.

Extreme Wind

The hazard presented to the station from normal wind loading was considered and designed for during the design stage of the station. The original building design threshold was a wind loading severity commensurate with a wind with a probability of exceedance of 0.02 per year (one in fifty years). The extreme wind safety case required adequate reactor protection against an extreme wind with a probability of exceedance of 1 in 10,000 years or infrequent event and a less onerous, more frequent second line event. Subsequent to the first periodic safety review, it was shown that the global factors of safety on building structures that had been adopted for the 1 in 50 year event bounded the 1 in 1,000 year event.

The wind standard CP3 Chapter V: Part 2: 1972 was used to derive wind speeds corresponding to the infrequent and frequent events. This method is essentially a static approach which makes no explicit allowance for the potential dynamic response of the building. A basic, 3 second gust, wind speed is first derived from an isopleth map for the UK. Various factors are then applied to the generic speed to allow for local features such as the local terrain, ground roughness, building size and height, period of exposure and the return period of the wind, and wind direction. For certain structures, frictional drag must also be taken account of but at Hunterston B, the aspect ratio is such that these effects can be neglected.

Extreme Ambient Temperatures

Ambient air temperature records have been used from the Hunterston site gathered since 1964 and these have been supplemented by data from Millport (3km to the north), Dalry (11km to the east) and Rothsay (17km to the Northwest). The recorded data for ambient air temperatures has been subjected to an extreme value analysis, which is an extrapolation method using experienced temperatures to allow derivation of extreme values, and this method has produced the values tabulated below.

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 Frequency
Frequent	-17.5 °C	+33.3 °C	1 in 1,000 year
Infrequent	-22.2 °C	+36.2 °C	1 in 10,000 year
Extreme Sea Temperature	-3 °C		1 in 10,000 year

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.

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

Provisions were made in the original design of the station to protect against lightning but this was not formally considered as a hazard at that time and was not assessed as such in the station safety reports. In the first periodic safety review, the lightning protection provisions were reviewed and a comparison was made of the codes used during construction against modern versions. Following the subsequent review during the second periodic safety review it was concluded that the design of the earthing and lightning protection systems were adequate for the operation of the station until at least 2016.

Conclusion HNB 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

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

Perhaps more than any other hazard, drought will be characterised as developing over a long period of time. One consequence of this is that mitigation can be put in place prior to the event. It is likely also that the duration of the event will extend significantly beyond the mission time.

The current safety case requirement for the back-up boiler feed system is that this should be available to provide back-up feedwater to each reactor for 24 hours. Failure to have sufficient stocks available to satisfy this requirement results in the need for a controlled reactor shutdown.

It is considered as highly unlikely that extreme drought could prevent the station from meeting its essential safety functions. This conclusion is further supported by the following facts:

- Reactor cooling water is provided from a seawater intake, with adequate diversity, which is not susceptible to low tide levels or drought.

- Adequate water reserves exist in the station, with adequate diversity, for the main boiler units, which could provide at least 24 hours of essential post-trip cooling supply without the townswater mains make-up system being available.

Any effects of drought on soil conditions or building foundations are considered to be very gradual, with time being available to allow a safe plant state to be achieved before significant loss of essential systems occurs. This is judged not to be a significant issue at Hunterston B where the main foundations are founded directly on rock and overlying deposits which have not been prone to settlement.

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

Conclusion HNB 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 station is founded on suitable 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.

4.1.1.1.1 Extreme Wind

There is an explicit safety case for the extreme winds hazard for Hunterston B which forms part of the consolidated Internal and External Hazards safety case for the plant. Although the consequences of any hazard, including other consequential hazards, are normally dealt with as part of the case for the initial hazard, the effects of wind blown missiles has been dealt with as part of the overall missiles hazard where it has been shown to be bounded by other more severe missiles.

Tornados have been considered and a tornado wind speed for the infrequent event has been defined. This speed is bounded by the straight line infrequent wind.

Work was carried out in 1985 to determine the frequency and intensity of tornados in the UK. 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 HNB 4.3: Tornados have been assessed in the second periodic safety review and no significant shortfalls have arisen.

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

The extreme wind assessment of structures for the first periodic safety review was undertaken against CP3 Chapter V-2: 1972, "Code of Basic Data for the Design of Buildings – Loading – Wind Loading", but it was recognised that a new wind code was in preparation, which was to be based on BRE Digest 346. Therefore an assessment against BRE Digest 346 was undertaken, for certain buildings and it was concluded that the CP3 derived loadings bounded the BRE derived loadings for buildings <20m high. It was considered that only for certain elements of the charge hall and Deaerator would the BS6399 wind code indicate higher wind loadings than those derived using CP3. However this conclusion was only valid on the assumption that there were no significant differences between the BRE and BS6399 wind code.

Although the BS6399 wind code was based on the BRE Digest, differences were established during the code's development.

Subsequent work was undertaken for Torness periodic safety review and this makes comparisons between CP3 Chapter V and the new BS6399 code. The comparison of standards undertaken for the Torness periodic safety review was based on BS6399 Part 2: 1997, but a later amendment was made in 2002. Therefore the validity of the above conclusions reached was dependent on the effect of the BS6399 2002 amendment.

The PSR2 review therefore identified a shortfall to investigate further the validity of the CP3 assessments that primarily provide support to the existing safety case when judged against the current BS6399 standard. This shortfall has now been addressed by a re-assessment. The objective of this assessment was to re-substantiate the buildings and exposed plant claimed by the wind loading safety case against the latest version of the wind loading code, BS6399-2: 1997 (2002).

Again it was found that BS6399-2: 1997 (2002) generally estimates lower wind pressure loads than CP3 for the site and wind loading events considered. There were however a number of instances where increased global wind loadings were derived using BS6399. For each of these instances, the original periodic safety review assessment was reviewed to establish whether the conclusions of that assessment would be affected. In all cases, it was found that the overall stability of the affected structures would not be affected.

Climate change means that local weather patterns and the average conditions associated with them may change over time. Future prediction of change to wind characteristics is relevant when considering the extreme wind hazard. A Met Office report commissioned by EDF Energy finds that by the 2020s spring and autumn wind speeds will have decreased by 2% to 4% and winter speeds will vary by about plus or minus 2%. These changes are small in the time period under consideration and although changes in wind speed are predicted, it is judged that nuclear safety is not at any further risk from extreme winds due to climate change.

Conclusion HNB 4.4: For extreme wind loadings there is a current design basis which has been reviewed as part of the periodic review process. The existing safety case remains valid and secure when assessed against the most recent standards.

Consideration HNB 4.2: A review of the programme of work in place to respond to the extreme wind hazard design basis methodology should be incorporated in to the next periodic safety review. Any significant nuclear safety issues arising from the programme of work should be addressed as appropriate.

4.1.1.1.2 Extreme Ambient Temperatures

There is an explicit safety case for extreme ambient temperatures for Hunterston B which forms part of the consolidated hazards safety case for the plant.

A study of extreme ambient conditions for the Hunterston site was carried out as part of the Hunterston A Station, long term safety review. That study was supplemented in 1993 by a report commissioned by Scottish Nuclear from the Meteorological Office which used data gathered mainly from the Hunterston site since 1964.

For the Hunterston B Station, the extreme ambient temperature hazard was specifically addressed in the first periodic safety review which concluded that, subject to certain reservations, "in conditions of extreme high or low ambient temperature there would be at least two lines of protection against all fault conditions within the design basis... these extreme conditions do not add significantly to the frequency of fault-initiating events." The reservations referred to, have now been addressed.

The purpose of the second periodic safety review was to confirm the adequacy of the case up to the following review in 2016. As part of the scope for the second periodic safety review the nature of the hazard was reviewed and the fundamental nature of the hazard was not considered to have changed since the initial review save that factors like global climate change may have affected the severity of the hazard.

The first periodic safety review case considered buried pipework and pipework in trenches. It was generally considered that buried pipework would be prevented from freezing. It was noted that some of the back-up boiler feed pipework was carried in trenches but this was protected by trace heating.

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 2010/11) consideration has again been given to the design basis temperatures for all EDF Energy nuclear stations and these have been confirmed as robust. A climate change report has recently reviewed the methodologies for:

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

Extreme Ambient Temperatures

The review of extreme ambient temperatures, carried out as part of the first periodic safety review, was used as the basis of the consolidated statement of the extreme ambient temperatures safety case which was included in the Hunterston B, internal and external hazards safety case. The summary of the extreme ambient temperature safety case presented here is based on the original periodic safety review as modified by the final safety case. Bounding temperatures have been derived appropriate to both infrequent (10^{-4} p.a.) ambient temperature extremes, and for the more frequent temperature events.

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

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

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

Extreme Seawater Temperatures

The second periodic safety review noted that it was not clear that extreme seawater temperatures had been rigorously derived and the relevant plant confirmed against these. Hence, this review recommended that extreme seawater temperatures be determined for the infrequent hazard level and the relevant plant be confirmed as able to withstand these.

The response to this shortfall confirms that there is no safety case claim on the cooling water system. The reactor cooling water system is recognised as vulnerable to frequent failure and there are therefore two diverse lines of protection available. It has therefore been deemed unnecessary to rigorously derive the extreme seawater temperatures and confirm the relevant plant against these, particularly since the effect of thermal inertia in seawater is such that the range of upper and lower temperatures is very short and both slow and predictable. The time taken to reach the lower temperatures (several days) means that there would be ample time to seek expert advice and take mitigating actions (extreme weather is a standing agenda item in the Daily Operations Focus Meeting). Furthermore, a surface water freezing incident in the vicinity of the cooling water intake is not considered to present a problem, as the duct is sufficiently well submerged.

Conclusion HNB 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 seawater 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 a moderate increase in expected extreme temperature may occur during the lifetime of the station.

Consideration HNB 4.3: Monitor and review the extreme ambient temperatures following the publication of the climate change adaptation report and consider these as part of plant life extension for all AGR stations.

Snowloading

Snow loading was not considered in the review of the original design or in the first periodic safety review, however the issue of snow loading was considered as part of the civil structures in the second periodic safety review. Snow loading was derived using BS6399-3:1988 and BRE Digest 332.

An over-stress of the turbine hall roof decking had been identified a further study was carried out to quantify to what extent. It has been confirmed that whilst the decking may fail, until the critical failure loading is reached the decking will continue to provide lateral restraint to the purlins and that at failure, the loading on the purlins will be reduced by the snow and decking falling into the building. The purlin integrity will not be challenged and it has been judged that the debris and snow falling into the turbine hall would not pose a significant threat to essential plant.

For an event with a probability of exceedance of 1 in 10,000 year event, the snow loading has been taken as 0.91kN/m².

A 2010 Met Office report on snow loading commissioned by EDF Energy identified the depth of snow expected at Nuclear Generation sites from an event with a return frequency of 1 in 50, 1,000 and 10,000 years. The best estimate uniform snow loading on the ground for Hunterston B is predicted to be 0.67kN/m² for an infrequent event, which is bounded by the value assumed for assessment of the buildings.

A climate change review 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 UKCIP09'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 UKCIP09 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 it does today.

Conclusion HNB 4.6: Snowloading has been considered in second periodic safety review and with only shortfalls of a low safety significance being identified.

Consideration HNB 4.4: Consideration should be given to whether a snow loading hazard case is required and whether all aspects of the snow hazard, such as 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 whilst these extreme hazards were not explicitly addressed at the infrequent event level in the original design basis, assessments have been back-fitted as part of the first periodic safety review and these have been tested and further developed as part of the second periodic safety review.

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 the second periodic safety review indicated that these were unlikely to present significant threats to the continued safe operation of the plant.

4.1.1.4 Consideration of potential combination of weather conditions.

This section considers the potential for weather events that have been considered to arise individually within this 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 extreme infrequent event in combination with another event is considered to be of such low probability that the risk is judged to be acceptable. On this basis, unrelated coincident hazards can be discounted.

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

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

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

The Potential for Wind to Cause Internal Hazards

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

Extreme Wind Combining with Other External Hazards

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

The Potential for Extreme Ambient Temperatures to Cause Internal Hazards

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

Extreme Ambient Temperatures Combining with Other External Hazards

- Extreme Ambient Temperatures Combining with Lightning

Combined Hazards Involving Lightning or Drought

The safety cases that are currently being developed for the lightning and drought hazards will include consideration of combined and consequential hazards. In advance of those cases being completed, combinations of this sort have been considered; it has been judged that no significant threat will be posed to reactor safety from such combinations.

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 HNB 4.7 Combinations of hazards have been considered in the Hunterston B and Hinkley Point B safety cases, where they were judged not to impact adversely on nuclear safety. These findings are broadly applicable across the AGR fleet.

Consideration HNB 4.5: 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 HNB 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 HNB 4.6: 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 the 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.

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

Season Preparation

A procedure is in place which is used at Hunterston B to promote safe and reliable operation during meteorological and environmental conditions encountered through the year. This procedure supplies a process for the assessment of Station readiness for seasonal conditions for summer and winter seasons. This procedure also supplies guidelines that have been developed to assist senior station staff in making decisions affecting the plant status and the provision of appropriate resources necessary for safe operation or shutdown of reactors during periods of severe weather. The measures taken at different seasons are given below.

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

Table 4.2: Actions taken during the approach to summer to mitigate the effect of extreme weather conditions

Threats	Risk / Risk areas	Mitigation
High ambient temperatures	Central control room, auto control and computer systems overheat Reactor Circ Hall boiler levels and Turbine Hall operating areas become difficult working environments.	Check air conditioning systems. Review defects. Repair defects. Check station heating and ventilation systems. Complete confirmation checklist. Review defects. Repair defects. Ensure heating and ventilation fans in service, filters clean and warming steam off.
High sea temperatures	Turbine condenser cooling water outlet temperature limit approached	Assess environmental limit and possible load restrictions. Target 4 Main cooling water pumps in service Assess performance of reactor and turbine coolers. Rod/clean coolers and repair defects.

Threats	Risk / Risk areas	Mitigation
	Performance of cooling water coolers deteriorates	

Table 4.3: Actions taken during the approach to winter to mitigate the effect of extreme weather conditions

Threats	Risk / Risk areas	Mitigation
Low ambient temperatures	Chemical pipework & outside water systems freeze. Diesel generator cooling systems freeze Essential plant areas	Check operation of trace heating systems. Complete confirmation checklist on all systems. Repair defects. Check concentration of antifreeze in engine cooling systems. Assess defects in Passport. Repair leaks. Check operation of essential plant space heating and availability of portable space heaters
Ice/Snow	Site vehicles Road gritter and road salt Dispatch of Road Flasks	Check vehicles operationally ready Check operation and salt stock level Confirm road and railhead serviceable
Storm – high winds	Loss of Grid Site access problems Flood in combination with tide and heavy rainfall Flying debris on-site	Check the availability of all plant essential to ensuring electrical supplies and the safe shutdown of the reactors should off-site power be lost. Confirm alternative access route viable Ensure site and access road surface water drainage systems fully operational. Check cooling water pumphouse doors and sump pumps. Repair defects. Confirm sandbags/cofferdams available. Survey site buildings and roofs. Repair defects and clear/secure loose material.

4.2.1.1 Extreme Wind

The lines of reactor protection as identified for this hazard are shown in Table 4.4.

Table 4.4: Lines of Protection against Extreme Wind Hazards

Essential Function		Infrequent (More Onerous) 10 ⁴ p.a. event
Trip		Guardline equipment remains available
Shutdown		Main shutdown equipment
Post-trip Cooling	Boiler Venting	All boiler routes remain functionally capable
	Boiler Feed	All post-trip feed systems remain functionally capable
	Gas Circulation	Forced gas circulation Natural circulation
	Feedwater Source	Deaerator Reserve feed tanks Back-up boiler feedwater tanks

Essential Function	Infrequent (More Onerous) 10 ⁻⁴ p.a. event
	Townswater

Trip and Shutdown

It is considered that loss of grid would occur before the onset of extreme wind speed corresponding to an infrequent event, resulting in a reactor trip via the gaurdlines, due, for example, to circulator underspeed or under-voltage. It is therefore considered that the reactor would have tripped and shutdown before the most extreme wind gusts are experienced by the station.

The reinforced concrete structure of the control building would not be significantly affected by extreme wind loadings, and that all essential plant areas would be adequately protected.

Post-Trip Cooling

All plant has been assessed against the infrequent hazard. The grid has been assumed to be lost therefore the safety case does not consider start/standby boiler feed pumps to be available.

Following the trip, the reactor shutdown sequencing equipment re-configures the 11kV system to supply the unit and station boards, and starts three circulators. Thus the diesel generators will maintain make-up supplies to the deaerator. For forced circulation, inlet guide vanes are required to be in reactor shutdown sequence positions, although these may be established manually. For natural circulation, the inlet guide vanes positions are adequate.

The fault does not lead to increasing reactor pressure pre-trip. If required to do so, the operators would have up to 90 minutes to initiate feed/boiler venting to prevent safety relief valve lift. For gas circulator run on protection, both the reactor shutdown sequencing equipment and the quadrant protection equipment activate both the main and the secondary circuit boards.

The back-up boiler feed system and station fire tender pump have stand-alone dedicated power supplies. The long term feedwater supplies to the back-up boiler feed system are from the million gallon townswater tank. However, if available, the supplies from the reserve feedwater tanks would be preferred.

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

The diverse cooling system is not claimed for this hazard as sufficient claimed lines of protection are already in place. The diverse cooling system is the bottom line protection for a seismic event, however the likelihood of an infrequent seismic event combining with this hazard is of such low probability that the risk is judged to be acceptable.

Essential Monitoring

It is considered that the central control room would remain available for post-trip monitoring actions, due to the capability of the control block and reactor building to withstand extreme wind loadings without significant failures. Furthermore, the diverse alternative indications centre has been shown to remain available as back-up in the extremely unlikely event that the central control room became inoperable.

Electrical Supplies

The back-up diesel generator house, fuel tank farm and fuel pumphouse have been assessed against the infrequent wind hazard and no structural failures have been predicted. The auxiliary transformers are considered to be adequately protected due to their partially shielded location and substantial design.

Shutdown Cooling

The consolidated hazards shutdown safety case noted it had been shown by a deterministic approach that there is sufficient protection available against the infrequent hazard.

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. Refuelling operations are not permitted during high winds.

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

The nuclear safety related structures have been assessed against the extreme wind hazard in accordance with the provisions of the relevant limit state design codes; appropriate partial factors of safety on load and materials have been applied, characteristic (lower bound) material strengths have been adopted and, hence, the structures will exhibit essentially elastic behaviour. If elastic limits were to be exceeded, the onset of non-linear behaviour would not necessarily threaten the structural integrity or functionality of the buildings. However, without carrying out non-linear stress analyses and detailed consequences of failure studies for the individual buildings, it is difficult to rigorously establish what level of increase in the design basis wind would result in a loss of essential safety functions. Even if localised failures of individual structural elements or building components were to occur, the consequences of failure would be dependent upon the nature and extent of failure and the resulting degree of interaction with essential plant and services. It can be argued with confidence, however, by having assessed the nuclear safety related structures against the provisions of limit state design codes, that the buildings will possess inherent reserve strength margins such that design basis extreme wind does not represent a fundamental safety limit or cliff-edge scenario.

Conclusion HNB 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 HNB 4.7: 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

The lines of reactor protection for extreme ambient temperatures are shown in Table 4.5 which has been based on the fault based view for the hazard.

Table 4.5: Lines of Protection – Extreme Ambient Temperatures

Essential Function		Extreme Infrequent Ambient and Sea Temperature
Trip		All trip systems remain available
Shutdown		Main shutdown system
Post-Trip Cooling	Boiler Venting	Low pressure vents Diverse boiler venting Turbine leg drains
	Boiler Feed	Emergency boiler feed system Back-up boiler feed system
	Gas circulation	Forced gas circulation Natural circulation
	Feedwater Source	Deaerator Reserve feedwater tank Back-up boiler feedwater tank Townswater

Extreme Low Ambient Temperature

No particular single line of protection is identified in the safety case as being claimed for the infrequent hazard. It is noted that extreme low temperatures do not arise as a sudden event but rather develop over a period, giving the operator considerable time to take evasive action if this is possible and appropriate. The impact of extreme low ambient temperatures has been considered as this affects plant and equipment housed in occupied buildings, unoccupied buildings and in fully exposed locations. Loss of grid has been considered to occur during extreme low ambient temperature.

Trip

Essential reactor trip systems, in addition to the reactor shutdown sequence equipment are located in central areas where local environmental temperatures are similar to the average bulk indoor temperature. Normally energised electrical equipment will have sufficient self-heating to prevent failure due to low temperatures and the equipment is generally fail-safe.

Shutdown

The main shutdown system has a high level of redundancy and is designed to fail-safe principles, for which no credible fail-to-danger modes have been identified.

Post-Trip Cooling

The claimed bottom-line circulation is natural circulation. The heat exchanger and pumping units for the pressure vessel cooling system required to support natural circulation is located in relatively warm indoor plant areas and would not be significantly affected by very low outdoor temperatures.

In addition the essential electrical supplies required for pressure vessel cooling operation are judged to remain functional under extreme low outdoor ambient temperatures. Natural circulation can therefore be claimed following the infrequent event. The pressure vessel cooling system relies upon the cooling water system to provide a heat sink. The cooling water

system will remain available during periods of infrequent low ambient temperatures and infrequent low seawater temperatures.

Forced gas circulation is claimed for second line primary cooling. All circulator ancillary equipment is located indoors local to the circulators and is therefore not at risk from extreme low temperatures. The gas circulators require coolant from the reactor auxiliary cooling system, and as with the pressure vessel cooling system, the reactor auxiliary cooling system heat exchangers are located in relatively warm indoor plant areas. The reactor auxiliary cooling system is reliant on essential electrical supplies that can be provided by the back-up diesel generators which will remain available during periods of infrequent low temperature.

Equipment contained within unoccupied and unheated buildings are provided with some protection by the envelope of the building in which they are housed. Additionally, protection is afforded by trace heating provisions and, in the case of tanks, immersion heaters in the cooling systems and lubricating systems for diesel engines. In cases where it may be necessary to bring in portable space heaters, appropriate operating procedures are in place.

Some equipment are located in places where they are fully exposed to external conditions. Exposed pipework is protected by trace heating systems and lagging, and work is ongoing under normal business to assess the suitability of this protection. Limited pipework is not covered by trace heating and in these cases routines are in place to re-circulate water through the pipework and back to the tank in outside areas should this be required. Operating Procedures are in place to ensure that sufficient plant will remain available to provide two lines of post-trip cooling in the event of severe or prolonged cold weather.

The diverse cooling system is not claimed for this hazard as sufficient claimed lines of protection are already in place. The diverse cooling system is the bottom line protection for a seismic event, however the likelihood of an infrequent seismic event combining with this hazard is of such low probability that the risk is judged to be acceptable.

Essential Monitoring

The central control room will be unaffected by infrequent extremes, enabling operators to obtain essential post-trip indications. The alternative indication centre is considered to provide a back-up in the highly unlikely event that essential plant monitoring is lost from the central control room. It has been specifically designed to withstand extreme ambient temperatures.

Electrical Supplies

Post-trip electrical supplies for reactor shutdown sequencing equipment controlled plant are provided by the back-up diesel generators. The back-up boiler feed systems and the station fire tender pump have stand alone dedicated electrical supplies. The long term feedwater supplies to the back-up boiler feed system are from the million gallon townwater tanks, however, if available, the supplies from the RFTs would be preferred.

A further potential cause for concern is the effect of extreme cold on diesel fuel; sufficient "waxing" to prevent flow of the fuel through fine filters could occur at temperatures of -4°C (Summer grade fuel) or -12°C (Winter grade).

The manufacturers of the installed diesels have confirmed that extremely low ambient temperature (down to -22°C) would not have a significant effect on their performance. Ongoing work is being undertaken to ensure diesel fuel stocks remain available for use.

Shutdown Cooling

The consolidated hazards shutdown safety case noted that there will be diversity for all shutdown cooling functions since reactor reseal and repressurisation provides additional depth of protection for depressurised shutdown states.

The safety case does not consider the effects of extremely low ambient temperature on building temperatures if the extreme low ambient temperature event occurred when both reactors have been shutdown for an extended period of time. This may represent a more onerous challenge as there will be less heat produced by the plant to mitigate the extremely low ambient temperatures.

Operator Actions during Low Ambient Temperatures

If the external temperature falls below 0°C, the following actions are taken until the external temperature returns to above 0°C;

- Ensure that there is circulation in the reserve feedwater tanks
- Ensure that there is circulation through the million gallon townswater tank and associated exposed external pipework and that the pumphouse room heaters are operating.
- Ensure that the back-up cooling system heating is operating, including system pipework trace heating, water storage tank heaters, diesel water cooling system heaters and pumphouse room heaters.
- Ensure that the reactor auxiliaries/pressure vessel diverse cooling system heating is operating, including pipework trace heating, make-up water tank heaters, cooling tower basin heaters, plant room heaters. If the external temperature falls below minus 12°C, run the pumps to input extra heat into the system.

It is also required that temporary space heating be provided to maintain internal temperatures above 0°C within the diesel houses. Additional surveys are carried out to ensure that temperatures are above 0°C within the;

- Charge hall
- Circulator halls
- Cooling pond
- Flask handling bay
- Turbine hall boiler feed pump bay
- Cooling water pumphouse

If temperatures cannot be maintained generally at this level, temporary space heating is to be brought in to ensure that vulnerable essential plant remains available for immediate operation. Also, if the temperature in the vicinity of any safety related crane falls to minus 5°C, all load movements by crane in that area are stopped.

If the external temperature falls below the infrequent level, the technical specifications require that it be established that there is sufficient availability of essential plant to support continued operation at power and that agreement be obtained from a specialist engineer for operation at power to continue. If these requirements cannot be met, a controlled reactor shutdown is carried out.

Air intakes are also monitored during heavy snow to ensure that they are clear.

Extreme Low Seawater Temperature

All other systems are assumed to behave similarly to extreme low ambient temperature. However, extreme low seawater temperatures could result in limited surface freezing around the cooling water intake but the intake duct is sufficiently well submerged for this not to present a problem.

Extreme High Ambient Temperature

The safety case considers that infrequent high ambient temperatures will not have any significant effects on the availability of the reactor protection systems (trip, shutdown and post trip cooling) and hence, two lines of protection should always be available. It is noted that extreme ambient temperatures do not arise suddenly and without prior warning.

Trip and Shutdown

Essential reactor trip and shutdown plant in addition to the reactor shutdown sequence equipment are located in central areas of the control block and reactor building, the local environmental temperatures being similar to the average bulk indoor temperature. Battery rooms also have thermostatically controlled heating to maintain local temperatures within design values.

In the unlikely event of a rapid temperature excursion the station computers may become unavailable, resulting in some loss of plant monitoring and indications. In this event there would still be sufficient instrumentation to enable safe reactor trip and shutdown. Note that the defeat of interlock hazard trip in the safety room incorporates a local ambient temperature input to ensure that the trip units do not operate above their rated temperature.

Post-Trip Cooling

Relatively brief high temperature excursions, likely to arise from limiting extreme ambient temperature events, are not expected to cause equipment or cable failures. Mechanical plant and structures are in most cases capable of continuous operation in high temperatures and high voltage electrical equipment has been designed to sustain operation in high temperatures. Reactor trip system consists of electrical and electro-mechanical components and would not be adversely affected by high ambient temperatures. Essential electrical plant and control and instrumentation plant are generally rated for operation to an ambient temperature of 40°C. The most important items of control and instrumentation equipment, including the guardlines, are housed in rooms of the control building and are served by the central control room air conditioning system.

It is possible that extreme high temperatures could result in temporary discomfort for central control room staff and could potentially cause premature ageing of cables. However, neither of these effects is judged likely to give rise to equipment failures. All essential cooling functions will retain adequate cooling capacity in the event of extreme high seawater temperatures. Electrical supplies and long term supplies to the back-up boiler feed system are the same as for extreme low ambient temperature.

The diverse cooling system is not claimed for this hazard as sufficient claimed lines of protection are already in place. diverse cooling system is the bottom line protection for a seismic event, however the likelihood of an infrequent seismic event combining with this hazard is of such low probability that the risk is judged to be acceptable.

Essential Monitoring

Electrical components are specified for operation up to 40°C but they are expected to be able to withstand 60°C or above without prompt failure. Additionally all the equipment for the alternative indication centre was designed to withstand extreme infrequent high temperatures and the alternative indication centre equipment in the circulator hall was designed to withstand 75°C. It has been claimed that two lines of protection for monitoring will remain available during infrequent high temperatures. Note that in addition to the central control room and the alternative indication centre, monitoring is available local to the plant.

Electrical Supplies

All essential electrical supplies are qualified to 40°C which is above the infrequent extreme ambient temperature. Electrical supplies to the essential electrical systems can be provided by the back-up diesel generators in the event of loss of grid.

Shutdown Cooling

It is judged that the extreme ambient temperature hazard does not present a more onerous challenge to a shutdown reactor than one at power, as both natural and forced circulation are assumed to be available.

Fuel Route

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

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

Extreme Ambient Temperature Safety Margin

A safety margin 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 diesel generators fail would be a possible cliff edge as the cooling of the plant would be compromised. This is discussed in Chapter 5. This is mitigated by operator actions.

Conclusion HNB 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 HNB 4.8: 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 conservatism 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 HNB 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 HNB 4.9: Consideration should be given to the prioritisation of the ongoing production of the lightning and drought safety cases.

4.2.1.4 Human Factors Assessment

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

Consideration HNB 4.10: Consider reviewing whether comprehensive human factors assessments are required for operator actions undertaken during extreme weather conditions.

4.2.1.5 Mitigating Actions

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

Conclusion HNB 4.13: The predictable nature of the extreme weather hazards discussed in the chapter allows operator actions to be taken to help mitigate the effect of the hazard.

Consideration HNB 4.11: 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 has been subject to review as part of the second periodic safety review and will be reviewed again in the third periodic safety review for the station. Whilst those the second periodic safety review 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.

One shortfall concerned the upgrading of lightning protection afforded to the methane trailer plant. This proposal has been considered but the balance of risk was judged such as to preclude any modification.

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 4.6: Gaps Identified by Adaptation Report

Gap Identified by Adaptation Report	Suggested Adaption Option
Some chemicals and oils are volatile and/or degrade at extreme air temperatures	Investigate options for cool chemical/oil storage to protect against extreme ambient temperatures
Some stations are more likely to exceed their thermal discharge consents	Liaise with 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 townswater (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

The 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.

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

The 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 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.

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 HNB 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 HNB 4.12: Consideration should be given to all stations receiving site specific weather forecasts.

Consideration HNB 4.13: 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 event with a probability of 1 in 10,000 years. Equipment required to fulfil the essential safety functions is either located inside buildings which are qualified against infrequent wind, or qualified directly. The safety case has been assessed against the latest codes and is robust.

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. Seawater temperature is primarily a commercial concern and it is judged incredible that changes in temperature will impact nuclear safety. The reactor and other buildings containing essential equipment have been assessed against snow loading and demonstrate sufficient margin.

The climate change adaptation report predicts by 2030 there will be a rise in the expected maximum air temperature which may impact on plant life extensions. 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 24 hour mission time of the station.

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

Hunterston B

5 Loss of Electrical Power and Loss of Ultimate Heat Sink

Severe damage of the reactor is prevented by the essential safety functions of reactor trip, shutdown and hold-down, adequate post-trip cooling 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 focuses on prevention of severe damage to the reactor and to the irradiated fuel under various loss of electrical power and loss of ultimate heat sink scenarios, including all last resort means and an evaluation of times available to prevent severe damage in various circumstances.

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

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

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

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.

This chapter is based around a number of specified scenarios and the timescales to failure once all lines of protection have been eliminated. This chapter therefore considers severe / "cliff edge" changes in risk.



Figure 5.1: High voltage electricity pylons connecting Hunterston B to the Electricity Grid

5.1 Nuclear power reactors

The Essential Safety Functions at Hunterston B are briefly described below.

Trip and Shutdown

For a reactor at power, the trip systems are via the guardlines. The main provision for shutdown is the main shutdown system which comprises 81 control rods which, when power supplies are removed from the clutches, fall under gravity into the core. These systems are designed to fail-safe on loss of power.

Post-Trip Cooling

Post-trip cooling is usually provided by forced 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 CO₂ 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 provided boilers are fed. In an unpressurised reactor natural circulation cannot provide a sufficient amount of post-trip cooling.

Post-trip feedwater is normally provided to the boilers by the start and standby boiler feed pumps with water from the deaerator, the start and standby boiler feed pumps requires grid supplies. Various other feed systems are available and are mentioned later in this document.

The pre-stressed concrete pressure vessel provides a robust containment for the reactor primary coolant (CO₂). The pre-stressed concrete pressure vessel is cooled by the pressure vessel cooling water systems, which requires both electrical supplies and a heat sink.

Monitoring

Monitoring is provided in the central control room or the alternative indications centre

5.1.1 Loss of electrical power

Whilst the primary design intent for post-trip cooling of an Advance Gas-cooled Reactor (AGR) is for forced circulation of the primary coolant using gas circulators, a key feature of AGRs that needs emphasising here is their ability to tolerate loss of the gas circulators: acceptable post-trip cooling can be achieved by natural circulation, provided the reactor remains pressurised and main boilers are fed. Pressure vessel cooling system operation at Hunterston B is desirable, but not essential. The power requirements to operate these systems are relatively low.

5.1.1.1 Loss of Off-site Power

This scenario proposes a loss of off-site power supply, which constitutes a loss to the station's reactors all of the electrical power supplied by the National Grid network system.

The off-site power should be assumed to be lost for several days. The site is isolated from delivery of heavy material for 72 hours by road, rail or waterways. Light, portable equipment can be assumed to arrive to the site from other locations after the first 24 hours.

The off-site power supply, i.e. the grid network, is described in detail in Chapter 1 (Section 1.3.5.1) which also provides an outline of the on-site distribution (Section 1.3.5.2). A loss of off-site power event is considered within the safety case and there are installed plant provisions as described below to deliver the essential safety functions.

Loss of off-site power or loss of grid is primarily characterised by the loss of either 132kV grid, 400kV super grid or both. Therefore, a loss of grid will lead to a loss of one or more quadrants of gas circulation. A reactor trip will result from a loss of grid.

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*

Operating reactor

Loss of off-site power will result in a turbine trip with a subsequent reactor trip. The reactor shutdown sequencing equipment automatically starts the back-up diesel generators and re-instates electrical supplies to all the essential systems. The reactor shutdown sequencing equipment then automatically restores post-trip cooling using gas circulators and boiler feed from emergency boiler feed pumps. Note the high pressure start/standby boiler feed pumps are not re-instated in these scenarios.

The diesel generators have the capacity to power post-trip cooling to all 4 quadrants of both reactors if they all start. Only two diesel generators are required to support minimum post-trip cooling on both reactors.

The diesel generators and the auxiliary systems, including the automatic sequencing equipment, is maintained and tested in accordance with the maintenance schedule. Technical specifications set down the availability requirements for these systems.

Post-trip Monitoring

The central control room would remain fully functional in this scenario, the supplies being provided initially by the no-break supplies and subsequently taken over by starting of the diesel generators.

Shutdown cooling

Cooling on a shutdown reactor is achieved using forced gas circulation and feeding of main boilers from emergency boiler feed pumps or later use of the decay heat loops or the back-up boiler feed system. In the event of loss of off-site power, the starting of the normal back-up AC power sources would provide the necessary electrical power for all these systems.

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*

Technical specifications require sufficient stocks of consumables to support operation of the essential systems for at least 24 hours.

The company's emergency arrangements include provisions for securing replenishment of consumables from off-site suppliers before on-site stocks are exhausted. This is discussed further in Chapter 6.

Fuel Oil Stocks

11kV & 3.3kV

For the 11kV and 3.3kV diesel generators fuel oil capacity, there are three bulk storage tanks, with minimum fuel stocks, there is sufficient fuel to provide post-trip cooling on a pressurised reactor for ~10 days.

It should be noted that these figures exclude additional stocks held in day tanks.

415V

For the 415V diesel generators fuel oil capacity there are two bulk storage tanks each. With minimum fuel stocks, there is sufficient fuel to provide post-trip cooling on a pressurised reactor for ~10 days.

It should be noted that these figures exclude stocks held in day tanks.

Back-Up Boiler Feed System

The 3 back-up boiler feed pumps are diesel driven, each pump having an associated fuel oil tank. The consumption rate expected with one pump running continuously is one tank (based on minimum stock level) every 24 hours.

72 hour Mission Time

The scenario postulated by the stress test means that consideration needs to be given to a 72 hour mission time, which is significantly beyond the current design basis

Conclusion HNB 5.1: Loss of off-site power is an event considered within the Hunterston B safety case and provisions are made to support the essential safety functions for 24 hours.

Conclusion HNB 5.2: In the event of loss of grid, there are sufficient supplies of fuel oil for the diesel generators to continue operating under required load for at least a 48 hour mission time.

Consideration HNB 5.1: Consideration will be given to the practicability of extending safety case mission times by either providing additional on-site storage facilities or additional diverse means to replenish stocks.

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

A loss of off-site power combined with loss of ordinary back-up AC power (the essential electrical system) event is considered within the safety case and there are installed provisions to deliver the essential safety functions.

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

Operating reactor

The station's design basis includes provisions to take account of the possibility of loss of off-site power and common mode failure of the diesel generators. As noted earlier, post-trip cooling can be provided by natural circulation, which requires the main boilers being fed. The back-up boiler feed consists of 3 direct diesel driven pumps designed to feed main boilers on both reactors simultaneously, should the need arise. The diesel engines used in this system are diverse and segregated from the diesel generators which provide the primary means of electrical supply in the event of loss of off-site supplies. The back-up boiler feed diesels are started by their own dedicated battery systems. The main boilers need to be depressurised to enable the back-up boiler feed system to be effective. The diverse boiler vents have been provided as a means of depressurising the boilers which is diverse from the normal system, namely the low pressure vents. The back-up boiler feed system is brought into service manually either from the central control room or, if necessary, local to plant.

In line with the common approach to the 24 hour mission time for all essential functions, a minimum of 24 hours worth of fuel oil and boiler feedwater are provided by the back-up boiler feed and implemented by specific technical specification requirements.

In the event of cooling by natural circulation, pressure vessel cooling will be provided by the diverse cooling system. This system has its own dedicated diesels which are diverse and segregated from the main electrical back-up diesels. The diverse cooling system is brought into service from the central control room, or locally if necessary.

Post-trip monitoring

In the event of loss of off-site power and common mode failure of the 11kV diesel generators, the central control room would remain functional provided the 3.3kV or 415V diesel generators start and operate satisfactorily. In the event of failure of the entire essential electrical system, operators would need to use the alternative indication centre. The alternative indication centre provides sufficient indications to monitor the effectiveness of post-trip cooling in the unlikely event that the central control room was untenable or all its functionality is lost. The instruments in the alternative indication centre are powered by an independent power supply unit, but is also backed up by a diesel generator. Therefore the alternative indication centre would remain functionally capable in this scenario.

Shutdown cooling

In the event of loss of off-site power and failure of all the normal back-up diesel generators, recovery would depend on the plant state.

If the reactor pressure was > 10 bar(g), cooling by natural circulation could be achieved by using the back-up boiler feed system. This system has its own dedicated diesel driven pumps which are not reliant on the normal back-up power sources.

If the reactor pressure was <10 bar(g), the reactor would need to be resealed and repressurised. Electrical supplies would be provided from portable generators held on-site during an outage.

Conclusion HNB 5.3: At Hunterston B, 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 provisions are made to support the essential safety functions.

5.1.1.2 Battery capacity, duration and possibilities to recharge batteries

As noted at the start of this chapter, electrical power is not required to circulate the primary coolant in these scenarios. Natural circulation cooling is supported by boiler feed derived from direct diesel driven pumps. The battery systems are there to support control and instrumentation and lighting requirements and for the no-break system provide support while the ordinary or diverse AC power supplies start up.

Batteries are 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. The back-up boiler feed diesel driven pumps also have a hydraulic start mechanism.

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

Hunterston B is not provided with permanently installed diverse back-up AC power sources. The approach for providing diversity in the event of common mode failure of the ordinary back-up AC supplies is to provide direct diesel drive to the main essential functions.

The alternative indication centre has its own diesel generator to provide its AC supplies. If this power source were also lost as part of the scenario, then there would be a loss of post-trip monitoring provisions. In itself this would not lead to severe core damage but would impede management of the recovery. In this situation, reliance might need to be placed on the off-site assistance referred to in Section 5.1.1.3.2 to enable post-trip cooling to be managed.

It should also be noted that whilst the diverse cooling system pumps are all driven directly by diesel engines, the cooling tower fans that provide the heat sink to atmosphere are powered by dedicated diesel generators. Thus if this AC power source were also lost as part of the scenario, the performance of pressure vessel cooling would be impaired. Note that whilst such cooling is desirable under natural circulation conditions, in these very low frequency scenarios, it is not essential.

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

As noted previously in Section 5.1.1.2.2, there is no reliance on battery power to circulate the primary coolant in this situation, although it would have a role in control & instrumentation and emergency lighting.

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 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.

Conclusion HNB 5.4: There are provisions off-site that can be deployed to station in 10 hours that would provide power generation capability and aid in continued post-trip cooling of the reactor.

5.1.1.3.3 Competence of shift staff to make necessary electrical connections and time needed for these actions. Time needed by experts to make the necessary connections.

As it is beyond design basis, there is no formal requirement for the training of shift staff to connect the off-site generators to the station. However, all shift staff go through a structured training programme for their normal duties and specific additional training for the roles they perform as part of the emergency arrangements.

In addition to this the AGR twin reactor design means that there is a relatively large complement of shift staff present, who cover a variety of the plant areas. It is therefore anticipated that the disciplines required for carrying out the necessary work to connect off-site supplies to the plant would be present on-site 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.

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

Operating reactor

In the unlikely event of complete station black out on a pressurised reactor, including all diesel driven pumps, the important structural failures would not occur until after many hours, if boiler feed can be restored before any structural failure then the situation is recoverable and severe core degradation should not occur. This time would be extended if a controlled blowdown 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 one hour before being lost, then the timescale on which feed needs to be restored to prevent structural failure would be increased by several more hours.

Shutdown cooling

For a depressurised reactor the minimum cooling requirements require forced circulation unless operator action to reseal the pre-stressed concrete pressure vessel and repressurise the primary coolant is successful. Neither of these are possible under station black out conditions.

The timescales available are dependent on the particular state. If the reactor is pressurised and is only recently shutdown, the timescales will be similar to those for the operating reactor given above. When the decay heat has reduced to the point that the reactor can be depressurised and an air atmosphere introduced into the reactor, then sufficiently more time is available than the operating case (described above) to restore core cooling to prevent a significant release. If the reactor could be resealed, the time available to restore core cooling to prevent a release would be again significantly extended.

Consideration HNB 5.2: 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 robust 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-engineering in order to improve mitigation measures
- Further transient analysis of severe accident scenarios

Chapter 6 contains further considerations for additional emergency back-up equipment to mitigate against the effects of beyond design basis loss of electrical power. Alternative indication centre has a dedicated diesel generator and a mobile back-up diesel which is shared with the access control point.

Conclusion HNB 5.5: The current robustness and maintenance of the plant is compliant with its design basis against loss of electrical power. However, steps can be taken to improve the resilience of the plant for a beyond design basis event.

Consideration HNB 5.3: Consideration should be given to providing a second dedicated diesel generator for the alternative indication centre.

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 functions

The stress-test review of the various scenarios for 'loss of ultimate heat sink' at Hunterston B 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 ultimate heat sink scenario are considered in Section 5.1.4.

Seawater is drawn from the Firth of Clyde through coarse bar screens, along a tunnel before emerging into the fore bay. The water is then drawn through fine drum screens before passing into the draught tube immediately preceding the four main cooling water pumps. The reactor cooling water pumps also derive their suction from these draught tubes. There are four fine drum screen chambers, each uniquely associated with one main cooling water pump. Each drum screen chamber is preceded by two penstocks, allowing the drum screen chamber and draft tube to be de-watered.

- 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.

- It is the reactor cooling water which has a safety role as it provides the heat sink for the reactor auxiliaries cooling system and the pressure vessel cooling system.

Note that the central control room functionality would not be affected in this scenario, so the normal provisions for monitoring post-trip cooling are available.

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

Maintaining the primary ultimate heat sink not only has important safety significance to the reactor plant, but it also has a strong commercial driver to ensure that the station continues generating electricity. Therefore efforts are made to ensure availability of the primary ultimate heat sink.

Coarse and fine screens are provided as noted above. The fine screens are continuously backwashed to prevent blockage. Fouling of the drumscreens is indicated directly in the central control room by differential pressure indications and alarms and by the effects on cooling water pump pressures, motor currents and turbine vacuum.

Fouling of the coarse screens results in a reduction in the forebay levels. Three of the coarse screens are fitted to winches allowing for the coarse screens to be raised if they should become blocked.

Hunterston also undertakes chemical dosing, using sodium hypochlorite, of the cooling water system to discourage marine growth.

Conclusion HNB 5.6: Several means of preventing the loss of reactor cooling water by blockage of the water intakes are employed at Hunterston B 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 reactor cooling water supplies. This is a loss only of the seawater heat-sink.

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

Operating reactor

Complete loss of reactor cooling water is considered in the safety case as a within design basis, infrequent initiating event. Drum screen blockage is considered as a frequent initiating event but this is not a permanent loss of all reactor cooling water, so the case claims various recovery actions. The focus of these reports is on severe events so drum screen blockage will not be considered further here.

In the event of complete loss of reactor cooling water the reactor will be tripped manually on the appropriate alarms or automatically as a result of plant faults. Post-trip cooling will be provided by natural circulation with main boilers fed by the back-up boiler feed system as described in Section 5.1.1.2. The back-up boiler feed system takes feedwater from on-site water tanks and discharges the resulting steam to atmosphere. There is no reliance on seawater cooling systems for this function or for cooling of the back-up boiler feed pump diesels.

As noted in Section 5.1.1.2, pressure vessel cooling system is required when natural circulation is claimed. In this scenario pressure vessel cooling system cooling will be provided by the diverse cooling system. This system is a recirculatory system with an air heat exchanger. The diverse cooling system is brought into service from the central control room, or locally if necessary. Note that whilst pressure vessel cooling system is desirable to cool the pre-stressed concrete pressure vessel and its penetrations, under very low frequency scenarios, it is not essential.

Shutdown Cooling

The only significant impact that complete loss of reactor cooling water would have on the plant claimed for cooling on a shutdown reactor would be to affect the heat sink for reactor auxiliaries which provides cooling to the gas circulators. The diverse cooling system would be brought into service to provide an alternative heat sink.

Conclusion HNB 5.7: There exist diverse alternative heat sinks for essential cooling in case of loss of the primary ultimate heat sink.

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

The design basis post-trip cooling claimed in these faults and described in Section 5.1.3.2.1 above are all achievable by manual actions in the central control room and are claimed to be completed within one hour of the reactor trip. As noted in Section 5.1.1.3.4, many hours are available to restore post-trip cooling to prevent severe damage to the reactor. Note that this time can be extended by partially depressurising the reactors via the blowdown route.

For faults on a shutdown reactor, the arrangements ensure that all permitted states allow sufficient time for the required recovery actions. As mentioned earlier, when the decay heat has reduced to the point that the reactor can be depressurised and an air atmosphere introduced, then sufficiently more time is available than the operating case to restore core cooling to prevent a significant release.

Water Stocks

If both reactors remain pressurised, operators are able to cutback boiler feed immediately post-trip following the station operating instructions. Assuming minimum water levels and feed cutback, water stocks in the deaerator and reserve feedwater tanks will last approximately 58 hours (2.4 days).

Additional water stocks are held in the back-up boiler feed tank and million gallon townwater tank. Assuming the same cut back feed consumption rate, these stocks will last approximately 118 hours (4.9 days).

5.1.3.3 Loss of the primary ultimate heat sink and the alternate heat sink

This event proposes the loss of all seawater, townwater and any on-site air based cooling systems through failure or unavailability. This is a total loss of all otherwise available cooling via any systems available.

5.1.3.3.1 External actions foreseen to prevent fuel degradation

Operating reactor

In the event that the reactor cooling water and back-up boiler feed system and diverse cooling systems all failed, the key action required would be to restore feedwater to at least one boiler on each reactor. Note that whilst pressure vessel cooling system is desirable to cool the pre-stressed concrete pressure vessel and its penetrations, in these very low frequency scenarios, it is not essential. In these situations it is likely that reliance would be placed on procuring off-site assistance and provisions to reinstate boiler feed (see Section 5.1.1.3.2) to support natural circulation in the reactor.

Shutdown Cooling

In the event that the reactor cooling water and back-up boiler feed system and diverse cooling systems all failed, recovery would depend on the shutdown reactor plant state:-

If the shutdown reactor was fully depressurised, then the optimum strategy would be to reseal the reactor and repressurise it. In this scenario, station electrical supplies are available for resealing operations. Repressurisation can be achieved with normal use of the CO₂ plant. If there is a problem in establishing pumped vaporised CO₂ as a consequence

of the initiating event, repressurisation can be achieved by using flash CO₂, which only requires local to plant manual valve configurations. A source of boiler feed would be required, so in this situation, it is likely that reliance would be placed on procuring off-site assistance and provisions to reinstate boiler feed (see Section 5.1.1.3.2) to support natural circulation in the reactor.

If the shutdown reactor was already sealed, then only part of the above set of actions would be required.

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 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.

5.1.3.3.2 Time available to recover one of the lost heat sinks or to initiate external actions and to restore core cooling before fuel damage: consideration of situations with various time delays from reactor shutdown to loss of normal reactor cooling state

If the primary ultimate and alternative heat sinks are lost boiler feed and forced gas circulation would be lost. On a pressurised reactor the high natural circulation flows would transfer heat efficiently from the core to structures, potentially leading to failures of key components and an escalation of the fault scenario before the onset of severe fuel damage simply from overheating.

Depending on the station design and on the fault conditions, boiler supports or core supports are likely to fail first, only after many hours of no post-trip cooling.

For this total loss of cooling scenario if a viable boiler feed can be restored before significant structural failure, the situation is recoverable and severe core degradation should not occur. This time would be extended if a controlled blowdown 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 one hour before being lost, then the timescale on which feed needs to be restored to prevent structural failure would be increase by several more hours.

The timescale to potential failure of the structures can be increased by depressurising the reactor and limiting the transfer of heat from the fuel to the reactor components, however this will have the affect of decreasing the time to fuel failure from overheating.

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 as well as a complete station black out comprising loss of off-site power supply as well as loss of all back-up AC supplies.

If loss of primary ultimate heat sink coincided with station black out, but the alternate heat sink is still available, then back-up boiler feed system could provide minimal cooling to the reactor and boiler venting to air. 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. This statement applies to a reactor which was operating before the fault, as well as one that is in shutdown cooling mode.

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 driven pump systems. In this case, the estimate is that important structural failures would occur after many hour of no cooling, if boiler feed can be restored before then any significant structural failures, the situation is recoverable and severe core degradation should not occur. This scenario is the same as the loss of primary ultimate heat sink and alternative heat sink scenario addressed in Section 5.1.3.3 above.

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

Hunterston B is an advanced gas-cooled reactor and therefore has no water in the primary circuit.

The loss of the CO₂ gas, which is used as the AGR primary coolant, is covered under the station depressurisation fault safety case. The case takes account of possible loss of off-site power, but does not include coincident loss of 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 the resultant hot CO₂ 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.

This section considers measures that could be attempted to provide the necessary power supply to provide a coolant heat sink to remove decay heat from the reactor and from the irradiated fuel.

As noted earlier in Section 5.1.1.3.2, the current EDF Energy position is that a common store of off-site generation and diesel powered pumping equipment is available for the fleet. There is a set of emergency equipment replicating the core response equipment used on-site with additional special items to enable force 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 in 10 hours following the declaration of an off-site nuclear emergency activation (see Section 6.1.2.1).

5.1.4 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 heat sink scenarios. The AGR design is generally tolerant to the loss of the primary ultimate heat sink as a result of the inherent capacity to transfer heat to atmosphere. Hence, fewer specific issues have been identified when compared with the loss of electric supplies scenarios.

It should be noted that a consideration to extend the availability of essential stocks for severe accident scenarios is raised in Section 5.1.3.2.2.

Chapter 6 contains further considerations for additional emergency back-up equipment which would mitigate against the effects of a beyond design basis loss of all ultimate heat sinks.

Conclusion HNB 5.8: The current robustness and maintenance of the plant is compliant with its design basis for loss of the primary ultimate heat sink. However, steps to improve the resilience of the plant following a beyond design basis event should be considered.

5.1.5 Licensee Review of Robustness

EDF Energy undertook a number of 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 mandatory evaluations.

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 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, 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, 24 hours seems a short mission time for essential stocks.

Disabling reactor cooling while shutdown in air at the AGRs 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 repressurised, both of which require electrical supplies

Loss of non essential equipment will provide additional challenges for longer term events. 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 HNB 5.9: 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 to improve the resilience of the plant following a beyond design basis event should be considered.

Consideration HNB 5.4: 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 following scenarios are considered for each facility:

- Loss of external power supplies (grid)
- Loss of on-site back-up generation and grid
- Loss of heat sink
- Loss of on-site back-up generation and grid and primary heat sink

5.2.1 Loss of electrical power

The loss of electrical power is primarily a concern as regards the effect on cooling systems for the various stages of fuel handling and storage. Loss of power to handling systems is generally acceptable as the fuel will be held in a safe state, or manual back-up systems are available to manually operate the relevant drives. The impact of loss of power is summarised in the table below:

Table 5.1: The impact of loss of power on fuel route

Stage of fuel storage and handling	Handling with fuelling machine	Buffer storage	Dismantling	Storage in ponds
Effect of loss of grid	Back-up power available	Back-up power available	Back-up power available	Back-up power available
Effect of loss of grid and on-site generation	Manual operation available for movement of fuel, cooling is passive	Cooling can be provided by diesel driven pumping systems or systems with stand-alone generation	Cooling lost but passive cooling acceptable (see Chapter 1)	Cooling lost, timescales to recover as per Chapter 1. Note that diesel driven pumps can top up water level.

Conclusion HNB 5.10: In either the event of both loss of grid or station black out, 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.

Consideration HNB 5.5: To improve resilience of decay store cooling, consider possible enhancement options in respect to guidance to operators, fault recovery techniques, and improved understanding of credible consequences.

Consideration HNB 5.6: To improve resilience of pond cooling and make-up, consider possible enhancement options in respect to guidance to operators, replenishment of lost pond water, and standalone pond cooling facilities having no dependence on any other station supplies or systems.

5.2.3 Loss of the ultimate heat sink

For the various stages of fuel handling and storage, loss of the primary ultimate heat sink could affect the ability to cool the fuel. Where this is critical, alternative heat sinks are provided. In the effect of loss of all heat sinks, the timescales to restore cooling are as discussed in Chapter 1. The impact of loss of heat sink is summarised in the table below. Note that heat sinks shaded green are not affected by a loss of grid and on-site generation (Station Black Out).

Table 5.2: The impact of loss of heat sink on fuel route

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
Secondary heat sink	-	Fresh water from mains	-	-
Tertiary heat sink	-	Air	-	-

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

The preceding sections have shown that there are robust provisions for design basis loss of the primary ultimate heat sink. Furthermore, there are also arrangements for mitigation of the effect of loss of the ultimate heat sink beyond design basis.

Generic measures set out in Section 5.1.4 to increase robustness of the plant in case of loss of the primary ultimate heat sink would also increase robustness of the fuel route plant areas

The specific issues for the fuel route plant areas are raised below.

Conclusion HNB 5.11: In the event of loss of the primary ultimate heat sink there is adequate alternative heat sink provision available to the station fuel route.

Consideration HNB 5.7: To improve resilience of buffer store cooling, consider possible enhancement options in respect to guidance to operators, fault recovery techniques, and improved understanding of credible consequences.

Consideration HNB 5.8: To improve resilience of pond cooling and make-up, consider possible enhancement options in respect to guidance to operators, replenishment of lost pond water, and standalone pond cooling facilities having no dependence on any other station supplies or systems.

Chapter 6 – Severe Accident Management

Hunterston B

6 Severe Accident Management

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

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

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

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

This chapter will explore the organisation and management measures which are in place within EDF Energy to deal with severe accidents.

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

6.1 Organisation and arrangements of the licensee to manage accidents

EDF Energy Nuclear Generation has a robust organisation and has emergency arrangements that have been developed and maintained to respond effectively in the unlikely event of an emergency.

There are three main obligations that underpin EDF Energy Nuclear Generation’s approach to an emergency:

Moral – we have a moral duty to protect both personnel and the public. We must have robust emergency plans and their use demonstrated to outside agencies and the public.

Legal - under the Nuclear Installations Act 1965, the Ionising Radiation Regulations 1999 and Radiation Emergency Preparedness & Public Information Regulations 2001 we must ensure safe operations and make arrangements to respond to an off-site nuclear emergency. Our Nuclear Site Licence Condition 11 states: “...the licensee shall make and implement adequate arrangements for dealing with any accident or emergency arising on the site and their effects...”

Commercial – a safe company is also a successful company, so it is in our interests to have robust emergency arrangements.

In addition, EDF Energy Emergency Arrangements are approved by the Office for Nuclear Regulation under a license instrument.

Processes and practices are in place to ensure ongoing development and maintenance of the emergency arrangements.

EDF Energy Nuclear Generation’s emergency arrangements form part of a line of defence for the improbable event that robust measures have not been sufficient in preventing. The emergency arrangements are designed to deal with events which, though very unlikely, are reasonably foreseeable. All EDF Energy Nuclear Generation’s sites have operator plans as defined by Regulation 7 of Radiation (Emergency Preparedness & Public Information) Regulations. These provide the principles of the site emergency arrangements and the site emergency response guidelines for emergency role holders. These detailed plans are designed to be sufficiently scalable to provide the base from which an extended response to more serious events can be developed.

Regulation 9 of Radiation (Emergency Preparedness & Public Information) Regulations explains the requirement on the Local Authority to prepare an off-site plan for any premises with an operator’s emergency plan. The off-site emergency plan is an integrated emergency management document to bring together the emergency arrangements of all the off-site agencies with a role to play in the intervention of an off-site nuclear emergency. EDF Energy supports external stakeholders ensuring an integrated approach to emergency management.

6.1.1 Organisation of the licensee to manage the accident

All of EDF Energy Nuclear Generation power stations' emergency arrangements are developed in line with an EDF Energy Integrated Company Practice; where clear responsibilities and accountabilities are published, highlighting the specific roles assigned within the business to manage the emergency arrangements.

The objectives of the emergency arrangements are:

- To enable the situation and the extent of hazards to people and the environment, on-site and off-site to be determined, in order to provide protection measures and reassurance.
- To enable the event to be managed on-site so as to ensure that a safe and stable plant condition is established.
- To notify those off-site who need to be informed.
- To provide advice to those off-site organisations who have the responsibility for the protection of the public and the need for protective measures to be taken, if any.
- To provide information about the event to the public through the media.
- To enable the business of the company to be secured.

It is an EDF Energy Nuclear Generation policy that the emergency arrangements will be generic and similarly implemented across all nuclear sites and other locations. Locally agreed exceptions to the generic emergency arrangements can occur which take into account geographical or specific local issues. Standards used for managing the emergency arrangements will be traceable back to national and internationally recognised practices or quality standards. The aforementioned process ensures continuously improving arrangements and so optimum intervention at any given time.

Emergency Preparedness Engineers oversee the establishment and maintenance of emergency arrangements at each of EDF Energy's nuclear power station utilising central guidance in the form of company processes and procedures. The emergency arrangements are regularly reviewed, experience is captured, lessons identified and proposed changes are adequately considered and communicated before implementation.

6.1.1.1 Staffing and shift management in normal operation

Maintaining adequate staffing levels is critical to the organisation's ability to maintain its essential functions. Posts and roles essential to the continued safe operation of the nuclear fleet have been identified and, should it become necessary, actions will be taken to implement an 'essential staff only' regime to ensure the continued manning of essential posts and roles by suitably qualified and experienced personnel.

It should be noted that based on learning from other external events, emergency scheme staff with a decision making role will be EDF Energy employees who are suitably qualified and experienced personnel. It is permissible following the completion of the required training for contract staff to fulfil supporting roles within the emergency scheme.

The number of persons on a normal station day shift is approximately 500-600 people, this includes contract staff. During an outage this figure will increase.

6.1.1.2 Plans for strengthening the site organisation for accident management

In line with the companies generic approach to emergency planning, each EDF Energy Nuclear Generation power station adopts the emergency organisation depicted below (figure 6.1):

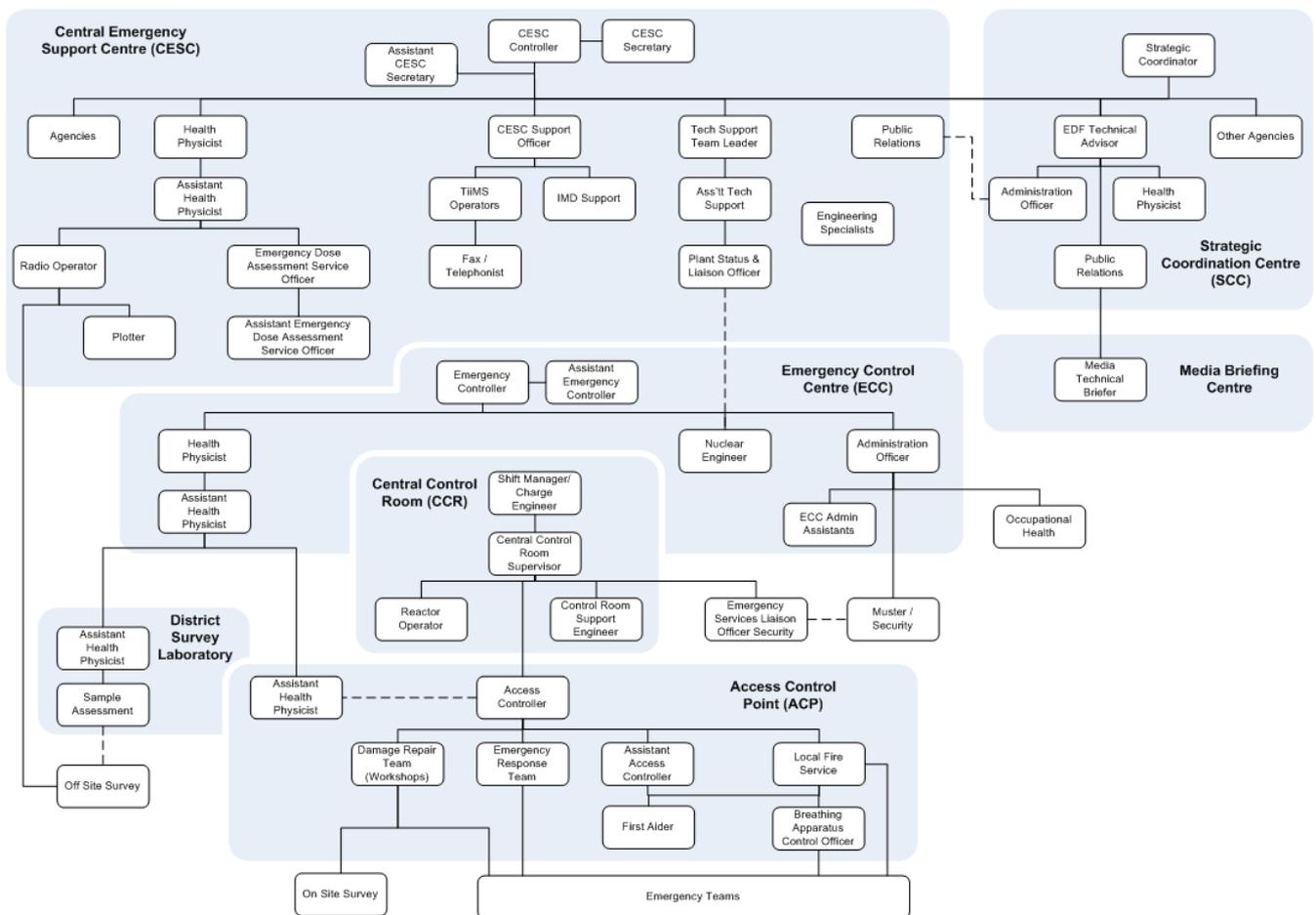


Figure 6.1: EDF Energy Generic Emergency Response Organisation

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, 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 Hunterston B 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.

There is a dedicated fixed access control point at Hunterston B. There is also an Alternative Mobile access control point available for deployment.

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 been passed on effectively.

The generic 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

Procedures

A suite of documents are utilised as part of emergency arrangements to control both preparedness and response activities to comply with applicable legislation.

Preparedness is defined as the organisational structure and associated activities that develop and maintain the emergency response capability.

Response is defined as the organisational structure and activities that are used when an emergency situation occurs. These include compliance documents, e.g. specifications, response guidance handbooks and emergency preparedness procedures.

The standard distribution of emergency planning materials is via electronic medium. Hard copy distribution is kept to a controlled minimum and primarily for storing at response locations. Symptom based emergency response guidelines and severe accident guidelines are available for supporting responders. The symptom based emergency response guidelines provide non-mandatory advice to the Emergency Controller and his supporting team on the management of beyond design basis faults in order to regain control of safety functions. The severe accident guidelines provide advice on the management of faults escalating towards severe or imminent fuel damage.

Training

The training modules within the EDF Energy Nuclear Generation Generic Emergency Scheme Training Framework are based on the training needs analysis of tasks described in the Emergency Plan and Emergency Handbook. The modules cover a discrete area of procedures, skills and/or knowledge. A module may meet the needs of a number of different role holders who need knowledge or skills in that subject area. Within each module the objective may be differentiated by role. Testing of equipment is carried out by undertaking training modules specified for each emergency scheme role. This is managed and recorded via the standard EDF Energy electronic system.

The EDF Energy Nuclear Generation process for training is outlined in the steps below:

Role Orientation

All role holders will receive orientation for their new role irrespective of whether they are new to EDF Energy, emergency scheme or moving between roles. There are three main elements to this:

- Familiarisation with facilities.
- Provision of practical information, e.g. notification arrangements.
- Analysis and delivery of required training for those moving between or taking on an additional role.

Initial Training and Assessment:

Each emergency role will have a separate route through the training programme for their centre although several elements will be common across roles.

The programme is made up of modules drawn from the matrix of generic Emergency Scheme Training. The programme will involve both national and local provision and include some combination of:

- Role specific mentor guide and job aid.
- Attendance on courses, e.g. breathing apparatus training.
- Use of flexible learning materials, e.g. overview, centre/task specific modules.
- Local mentoring.
- Role observation.
- Role shadowing.
- Assessment.

Most station role holders initial training will be provided on-site using multiple methods with some provision of courses for station role holders on a national basis, i.e. the Nuclear Power Academy. Training will conform to the standards and expectations set by EDF Energy.

Assessment of initial training will be undertaken module by module, as an integral part of that training. The method of assessment selected will be appropriate to the objectives and the content covered, but may include a combination of the following:

- Paper or computer based tests using appropriate questions.
- Observed practical tasks or procedures in a realistic setting.
- Questioning by a certified instructor, assessor or internal regulator.

As part of qualification for role, all role holders will demonstrate suitability for and competence in role by participating in a shift exercise or equivalent. The prospective role holder will undertake the role in full and be observed by an assessor who will normally be an experienced practitioner in that role.

Continuing Assessment and Training

To maintain competence and compliance, the core competences for each emergency role will be assessed over a three year cycle. All role holders will be assessed on every competence for their role during this period. In addition there may be a small number of fundamental, personnel safety related competences for some roles that need to be assessed annually e.g. use of Breathing Apparatus.

The role specific mentor guide issued for each role acts as a log book for recording competence. Assessment of core competences will use a number of methods:

- Observation of tasks in exercises and performance assessments events.
- Observation of tasks set in a refresher training session, e.g. simulator.
- Use of computer-based knowledge checks.
- Paper-based tests drawn from initial training.
- Questioning by assessors, i.e. to cover scenarios outside of the scope of a specific exercise/event.

The assessment of core competences will be carried out by:

- Current emergency role holders who have met the requirements of the Umpire/Assessor role. Assessors will have normally completed training specific for Umpires & Assessors .
- Contracted personnel who provide assessment in specialised key skills or tasks that fall outside of EDF Energy Nuclear Generation core business, e.g. fire fighting, command and control.

Accrediting role holders

Emergency arrangements training, follows the company systematic approach to training. However, as a non accredited programme, a graded approach is adopted with the methodology tailored to the needs of the emergency scheme and role holders.

The above approach to training has recently been introduced and moves the company towards a more focused training programme. Hunterston B are in the process of aligning with the company process associated with emergency scheme training.

Hunterston B B Power Station 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
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	Every 3 years

Exercise Type	Description	Frequency
	designate Strategic Coordination Centre facility.	
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 HNB 6.1: EDF Energy has detailed robust arrangements for Emergency Response which are subject to a programme of continuous improvement and exercised as required by standard procedures and regulatory demand.

Based on the learning from the Japanese Earthquake, the subsequent EDF Energy Emergency Nuclear Generation review of Station Safety Cases and examination of the associated risks on plant, it is not believed the fundamental risk profile on the nuclear power station has changed. Therefore current arrangements remain fit for purpose. However, as part of EDF Energy standards we ensure any lessons identified by real events and exercises (internal/external) are reviewed and built upon within our arrangements.

Consideration HNB 6.1: EDF Energy will consider how lessons identified from Japan and credible beyond design basis events can be reflected in our facilities, procedures, training and exercise programmes. Utilising experience from other emergency response organisations and the military, EDF Energy will consider enhancement of its staff welfare, human factors and emotional aspects associated with emergency response.

6.1.2 Possibility to use existing equipment

6.1.2.1 Provision to use mobile devices (availability of such devices, time to bring them on-site and put them into operation)

Each nuclear power station has self sufficient mobile back-up feed pumps. Equipment is inspected and maintained under a maintenance contract to ensure readiness. The contract also includes initial response support arrangements for the deployment of the equipment to the affected site. The equipment has bi-monthly, six monthly and annual inspection programmes to maintain the health and state of readiness of plant. The pumps are serviced annually by swapping out the pump with a spare.

There is a set of emergency equipment replicating the core response equipment used on nuclear power stations with additional special items to enable cooling to be restored to a reactor. A detailed inventory of the equipment is held by the Central Emergency Support Centre. This equipment is located remotely off-site and held centrally within the UK on trailers to be transported to the affected site within a 10 hour timeframe following the declaration of an off-site nuclear emergency. The activation of the trailers is tested weekly. The call to mobilise the trailers by the Central Emergency Support Centre alerts drivers under contract to be ready to move out from the depot, fully loaded, within an hour of the call. A team is also mobilised which travels directly to the affected site to prepare for the arrival of the trailers. They are then able to execute plans using the equipment available. An additional vehicle is also deployed to provide fuel.

Once a site declares an off-site nuclear emergency the Emergency Plan is initiated and an emergency response organisation within the company and external agencies is mobilised. This includes the Central Emergency Support Centre which brings together a team of experts to deal with the emergency. In a severe accident situation the Technical Team at the Central Emergency Support Centre, supported by the central technical organisation would consider the strategies and formulate an implementation plan. It is the Central Emergency Support Centre organisation which is able to mobilise the trailers, procure other equipment consumables. To aid the procurement process there is a standby team of procurement specialists who are part of the Central Emergency Support Centre arrangements.

Based on the location of the trailers the current deployment time to site would be approximately 4 hours. The lessons identified from the Japanese Earthquake so far highlight the associated issues that degradation of external infrastructure can have on access to and egress from site. The original intent of the off-site equipment focused on specific issues with the plant. The events in Japan have shown that all areas of plant vulnerable to an off-site hazard should be taken into account when designing the off-site equipment requirement.

6.1.2.2 Provisions for and management of supplies (fuel for diesel generators, water, etc)

One of the roles of the Central Emergency Support Centre is to coordinate EDF Energy's 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.

Conclusion HNB 6.2: EDF Energy has a range of on and off-site equipment which it can use to respond to emergencies which could affect the site. The provision of this equipment and support is a maintained and formal process within the organisation. This includes arrangements to maintain the essential supply of consumables during and emergency. Based on the lessons from Japan there are areas where EDF Energy could consider further enhancements to equipment and its critical supply.

Consideration HNB 6.2: EDF Energy will consider further resilience enhancements to its equipment and critical supplies which take onboard lessons of extendibility and issues that prolonged events could present. Extensive work has already begun to highlight updates to equipment, its location and deployment.

6.1.2.3 Management of radioactive releases, provisions to limit them

As part of the existing company Emergency Arrangements there are plans in place for the management of radioactive releases and provision to limit the effects of them.

At HNB the primary reactor gas blowdown System allows the reactor 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 Reactor Gas Blowdown System so that the activity is reduced to a safe level. Blowdown occurs via the various blowdown routes and may pass through particulate filters and the main iodine adsorption plant, before being discharged to atmosphere via the main exhaust.

System integrity, the provision of non-return valves, and operations in accordance with station operating instructions will prevent potentially contaminated/combustible gases being vented from one reactor to the other.

A DEPZ 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 DEPZ 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 DEPZ consistent with the concept of 'extendibility'.

A number of emergency preparedness activities take place within the DEPZ around EDF Energy Nuclear Generation sites. As part of the company's responsibility under REPIR, 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 emergency 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 the their local power station.

6.1.2.4 Communication and information systems (internal and external)

The station has substantial diversity of communications media to ensure requirements are met during a response situation. The on-site links include the use of the station's routine telephone networks - Private Automatic and Branch exchange lines, and a number of BT telephone lines together with dedicated direct wire telephones linking the on-site response centres. Across the nuclear power station the 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's 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 (EMI) / Radio Frequency Interference (RFI),
- 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 HNB 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 recognised 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 recent report was produced on all EDF Energy existing nuclear stations radio systems.

Hunterston B Station is in the process of replacing their UHF system with a digital system. This has not yet been commissioned for use by the emergency teams because of a requirement to be used with breathing apparatus. It is currently being utilised by the site security teams and has proved to be successful. Notable advantages of the system are;

- Optimised architectural design by Arciva.
- Simple system.
- Possible to use as back-up to other stations due to channel range.
- Voice recording, allowing post emergency analysis and logging.
- 24/7 support to site.

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 HNB 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 HNB 6.3: EDF Energy to consider enhancing current telephony and communications systems to increase levels of resilience of key technological components based on learning from Japan.

6.1.3.3 Impairment of work performance due to high local dose rates, radioactive contamination and destruction of some facilities on-site.

The existing Emergency Arrangements recognise that there is the potential for radiation levels, in some extreme instances, providing access challenges on-site.

If this is ever the case then remote access would be required or the installation of an appropriate level of shielding. If radiation levels are such that some access is possible then this access will be time restricted. This would impair the recovery operation particularly if operations are time consuming and would therefore require staff rotation after a certain time spent exposed to high levels of radiation. Existing plans acknowledge and make provision for these eventualities.

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 HNB the central control room is located in an area where habitability would not be directly impacted by an external flooding issue for staff already located in the facility. The central control room indications are not fully seismically qualified and hence operator actions may be required locally to verify instrument readings by other means, e.g. checking against the seismically qualified indications in the alternative indication centre.

In the event that the central control room becomes untenable an alternative indication centre serves as an alternative to the control room. This facility allows operators to monitor the activity of the reactors but does not allow them to take any remote action.

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 HNB 6.5: In extreme circumstances some on-site facilities may become unavailable. EDF Energy 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 HNB 6.4: EDF Energy will consider a review of its mobile facilities and the resilience of equipment contained within.

6.1.3.6 Feasibility and effectiveness of accident management measures under the conditions of external hazards (earthquakes, floods)

There will be a number of issues associated with the effectiveness of accident management measures should they occur under the conditions of external hazards. These include:

Emergency Services Support - the availability of emergency services support is unknown with the potential that services will also be responding to a wider emergency. The tasks of the site Emergency Team at the power station will need to be supplemented by specialists; such as the Fire and Rescue Service when the event develops beyond the limits of capability or require specialist equipment. It is a requirement of the Regulator that emergency services and standby support must be active on-site within 60 minutes of a declaration.

Under conditions of external hazard there is an increased risk that attendance of responders external to the site within 60 minutes of emergency declaration will not be met. To improve resilience under such conditions EDF Energy will consider off-site resources in appropriate locations to facilitate the emergency response including provision of equipment and staff.

Access to site - (issues responded to as part of Section 6.1.3.1) an associated issue related to access to site is the availability of personnel to resource ongoing shifts particularly in the instance of a prolonged emergency. Under the conditions of an external hazard it is likely trained staff will be unavailable due to their own homes or family members being affected.

Off-site monitoring - there is an established process for providing off-site countermeasures advice to protect the public during a release of radiation from a site involving mobile sampling vehicles. One of the lessons identified from the Japanese Earthquake was the inability of off-site monitoring vehicles to access pre-determined monitoring locations and determine the levels of radiation that were being discharged off-site.

Conclusion HNB 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 HNB 6.5: EDF Energy should consider reviewing existing arrangements to ensure the principles of extendibility are adhered to.

6.1.3.7 Unavailability of power supply

The loss of power supply to nuclear power stations would impinge on the response to accidents and so EDF Energy Nuclear Generation has redundancy in the essential electrical supply system at both nuclear power stations and key sites supporting emergency response, such as the Central Emergency Support Centre.

Following loss of the external power grid, back-up options such as diesel generators and batteries ensure electrical supply to essential plant equipment. This includes the facilities required for Emergency Arrangements.

6.1.3.8 Potential failure of instrumentation

The primary failure mechanism by which instrumentation would be lost is loss of power. Most indicating instruments/sensors have a designated power supply. This may be a dedicated supply to the instrument or it may be derived from the instrument signal loop. The availability of instrumentation for information on plant status and control of plant systems is crucial to the management of the plant within the design-basis. For this reason station-critical systems have diesel- and battery- backed supplies to provide sufficient indication of the station parameters to monitor shutdown. A detailed review has been undertaken and this did not identify any issues within the design basis.

For managing severe accidents, the company documentation gives a list of plant parameters which aid assessing the Critical Safety Functions. The Emergency Controller, on advice from site experts and the Central Emergency Support Centre, would specify which instruments gave information on these parameters. If all of the instruments giving information on a particular Critical Safety Functions were disabled by plant damage, it is probable that a minimum set could be recovered by improvised connections and dedicated power supplies. Consideration is being given to holding equipment, off-site, to reinstate instruments and remotely telemeter the indications.

6.1.3.9 Potential effects from the other neighbouring installations at the site

Advanced gas-cooled reactor 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.

Hunterston B is situated adjacent to Magnox owned Hunterston A site which is working through a decommissioning process. The radiological hazard from Hunterston A station is considerably reduced. However, conventional hazards must still be taken into account.

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 HNB 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 HNB 6.6: Further mitigation against the effects of beyond design basis accidents could be provided by additional emergency back-up equipment. This equipment could be located at an appropriate off-site location close to the station to provide a range of capability to be deployed in line with initial post-event assessment. This equipment may include the following capabilities:

- Electrical supplies for plant facilities.
- Emergency command and control facilities including communications equipment.
- Emergency response/recovery equipment.
- Electrical supplies for lighting, control and instrumentation.
- Robust means for transportation of above equipment and personnel to the site post-event.
- Equipment to provide temporary shielding and deal with waste arisings from the event

6.2 Maintaining the containment integrity after occurrence of significant fuel damage (up to core damage) in the reactor core

Reactor shutdown systems, containment integrity and reactor cooling act together in order to ensure, as far as is reasonably practicable, fuel damage and fission product release do not occur.

In advanced gas-cooled reactor designs there are three barriers preventing the release of radioactivity into the atmosphere during steady state and transient operation. These are:

1. The fuel matrix.

2. The fuel clad and

3. The primary circuit (pressure vessel / containment).

The single phase carbon dioxide coolant cannot undergo a sudden phase change as a result of an unexpected rise in temperature or pressure. This means that there can be no sudden discontinuity of cooling under fault conditions, and changes in flows, temperatures and pressures would progress slowly.

The coolant pressure may fall in case of a major leakage to the atmosphere, but the core cannot become uncovered as could occur in a pressurised water reactor.

If an advanced gas-cooled reactor is exposed to a depressurisation accident of the carbon dioxide coolant, forced circulation of the coolant, together with defined boiler feed, continues to provide adequate core cooling. Also, in the event of loss of boiler feed, the large heat sink represented by the graphite moderator and other reactor internals, provides long timescales before impermissible fuel temperatures are reached.

In the unlikely event that, post-trip, a fault is not controlled by the design basis, engineered protection, either because of multiple plant failures or an initiating event beyond the design basis, the mandatory station operating instructions would be suspended and the accident managed using advice from either the symptom based emergency response guidelines or the severe accident guidelines. The symptom based emergency response guidelines advise on managing beyond-design-basis accidents when the fuel is still substantially intact and there is a reasonable prospect of re-instating the minimum plant needed to contain fission products. For this reason, the advice is based on best-estimates of timescales for irreversible damage and of the minimum plant requirements, in contrast with design-basis requirements which have substantial margins.

If severe fuel damage has occurred, or is anticipated, or if applying symptom based emergency response guidelines advice has not controlled fission product release, the Emergency Controller would consult the severe accident guidelines for advice on limiting the release. The severe accident guidelines advice is broadly based, to deal with unanticipated situations, and uses existing plant in standard and innovative techniques. In addition, some advice calls for equipment and material not normally held on-site.

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

Consideration HNB 6.7: 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 over pressurisation 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, water introduced by an additional shutdown system would act as a neutron absorber to prevent re-criticality and ensure long term holddown.

In very severe accident conditions extra absorber may be needed to protect against increasing reactivity. It should be noted that this would not occur until well in to the severe accident sequence.

Any actions to cool the core will be extremely beneficial, as would steps to cool and preserve the core supports or to prevent control rod withdrawal in the extremely unlikely event of the core supports collapsing.

6.2.4.2 Operational provisions

It can be seen from the description of the various plant items available that the primary documents relating to holddown 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 would 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 depressurisation and significant fuel damage. Reinstating or preserving that part of the vessel cooling system for the penetrations would protect their containment function. The guidelines advises that in the event of loss of normal pumping systems, improvised use of fire pumps would restore adequate vessel cooling even if dried-out vessel cooling pipework has reached temperatures well above boiling.

Failing this, advice is given for removing outboard insulation from the penetrations and improvising cooling air-blast or water-spray.

6.2.7 Measuring and control instrumentation needed for protecting containment integrity

The central control room provides a single source of alarm and plant information for both reactors and turbine units and associated common plant.

Facilities are provided to monitor and control aspects of plant operation including reactor start-up and operation at power, trip, shutdown and post-trip cooling. The central control room also performs the duty of a communications facility in the event of an emergency.

An alternative indication centre provides a single area from which the status of the trip, shutdown and post-trip cooling of the two reactors can be monitored in the event of hazards that may have rendered the central control room untenable. The alternative indication centre receives a sub-set of the signals provided to the central control room which are buffered to ensure that damage to the central control room does not result in loss of signals to the alternative indication centre.

Instrumentation for Containment integrity

Instrumentation is required for all critical safety functions for protecting containment integrity. The pressure vessel is fitted with temperature, pressure and flow instrumentation.

Loss of electrical power to this instrumentation will cause the readings to be lost. Consequently, restoring electrical power to this instrumentation is incorporated in considerations detailed below.

6.2.8 Measures which can be envisaged to enhance capabilities to maintain containment integrity after occurrence of severe fuel damage

For the advanced gas-cooled reactor design, the timescales under which severe accident damage occurs is greater than for light water reactor where, in a similar accident, as shown by Fukushima, severe fuel damage occurs very quickly. This significant delay means that for a range of beyond design basis initiating events, either the symptom based emergency response guidelines advice on restoring cooling, or the severe accident guidelines advice on improvising cooling, is likely to be successful. For cases where cooling cannot be restored, they advise on maintaining or improvising containment of fission products released from the degrading fuel. In the guidelines there is also advice on blocking breaches in the vessel and on constructing an ad hoc filter.

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

The findings of the severe accident management aspects are discussed below on a fleet wide basis; this is because the learning from each of the sites is judged to be applicable across the stations

Scope

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

Summary of Findings

All advanced gas-cooled reactors have a suite of symptom based emergency response guidelines designed to manage a beyond design basis fault. The scope of these documents only covers the operating reactors at the site.

In addition, severe accident guidelines have been specifically designed to provide guidance for the management of events beyond the current design basis of the stations when a degraded core is likely or has occurred.

The severe accident guidelines have been developed through incorporating the understanding derived from both real events and dedicated research experimentation into a set of suggested mitigating actions in the event of a severe accident postulated on a generic basis.

There is the opportunity to improve the documentation and training provided for severe accident management using the experiences of the people in the Tokyo Electric Power Company (operators of the Fukushima Dai-ichi plant) as this is one of the very few events where such documentation has been used in a real situation.

Conclusion HNB 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 HNB 6.8: EDF Energy should consider a review, extension and retraining for the symptom based emergency response guidelines

Consideration HNB 6.9: Consideration should be given to providing further mitigation against the effects of beyond design basis accidents. This could be provided by additional emergency back-up equipment. This equipment should provide additional diverse means of ensuring robust, long-term, independent supplies to the sites. This equipment should be located at an appropriate off-site location close to the station to provide a range of capability to be deployed in line with initial post-event assessment. This equipment may include the following capabilities:

- **Equipment to enable pressure vessel cooling.**
- **Supply of suitable inert gas for primary circuit cooling (AGR only).**
- **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.**

6.3 Accident management measures to restrict the radioactive release

6.3.1 Radioactive releases after loss of containment integrity

6.3.1.1 Design provisions

Reactor shutdown systems, containment integrity and reactor cooling act together in order to ensure, as far as is reasonably practicable, fuel damage and fission product release do not occur.

In advanced gas-cooled reactor designs there are three barriers preventing the release of radioactivity into the atmosphere during steady state and transient operation; these are the fuel matrix, fuel clad and the pressure vessel.

6.3.1.2 Operational provisions

Emergency planning and actions will be put into effect and will have a major role to mitigate the consequences of a radioactive release.

For a severe accident, to restrict the radioactive release, the severe accident guidelines advise on repairing breaches, strengthening the vessel, and on improvising filters to remove fission products from released gases. Advice on strengthening the pressure vessel is aimed at preventing melt through of the basemat via penetrations, preventing failures of large numbers of penetrations as temperatures increase and blocking paths for activity release through concrete.

Loss of containment integrity would mean that there is a high probability of increased radiation levels off-site. Throughout an off-site nuclear emergency EDF Energy Nuclear Generation and independent experts will be utilising the information they receive to produce advice that will protect the public. The methodology for producing this advice is as follows. Emergency Reference Levels are part of Health Protection Agency – Centre for Radiation Chemical and Environment guidance. This agency provides guidance on introducing countermeasures in the early stages of an emergency and the emergency reference levels show what dose to an individual could be averted if the countermeasure is taken. These levels are based on dose saving and do not take into account the dose already accrued. There are different risks associated with each countermeasure depending on:

- the site location.
- the type of installation.
- conditions at the time of the accident.

For this reason, there are ranges of dose for the introduction of each countermeasure.

The Lower Emergency Reference Level

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.

The Upper Emergency Reference Level

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 seawater to maintain water levels would have no impact on criticality safety.

Wider impact on dose rates

There is only very limited ranges on-site where there would be an impact on 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 HNB 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 HNB 6.10: Consideration should be given to providing further mitigation against the effects of beyond design basis accidents by the provision of additional emergency back-up equipment. This equipment could provide additional diverse means of ensuring robust, long-term, independent supplies to the ponds. This equipment could be located at an appropriate off-site location close to the station to provide a range of capability to be deployed in line with initial post-event assessment. This equipment may include the following capabilities:

- Equipment to enable fuel pond cooling.
- Emergency command and control facilities including communications equipment.
- Emergency response/recovery equipment.
- Electrical supplies for lighting, control and instrumentation.
- Water supplies for cooling from non-potable sources.
- Robust means for transportation of above equipment and personnel to the site post-event.

It would be appropriate, if this equipment was developed and in any case to capture learning from events in Japan to review and where necessary revise the documentation and training provided for severe accident management in the fuel route plant areas.