



EU Stress Test

Dungeness B

Save today. Save tomorrow.



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

Glossary	5
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	17
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	22
0.7 Mission Time and Offsite Support	24
0.8 Beyond Design Basis Events and Accident Management	24
0.9 Emergency Response Arrangements	25
0.10 Mandatory Evaluations	25
1 General Data about Dungeness B	28
1.1 Site Characteristics	28
1.2 Main Characteristics of the Dungeness B Reactors	28
1.3 Systems for Providing or Supporting Main Safety Functions	29
1.3.1 Reactivity Control	30
1.3.2 Heat Transfer from the Reactor to the Primary Ultimate Heat Sink	31
1.3.3 Heat Transfer from Spent Fuel Pools to the Primary Ultimate Heat-sink	35
1.3.4 Heat Transfer from the Reactor Containment to the Primary Ultimate Heatsink	36
1.3.5 AC Power Supply	37
1.3.6 Batteries for DC Power Supply	42
1.4 Significant Differences Between Units	42
1.5 Scope and Main Results of Probabilistic Safety Analyses	42
1.5.1 Probabilistic safety assessment: The advanced gas-cooled reactor approach	42
2 Earthquakes	44
2.1 Design basis	44
2.1.1 Earthquake against which the plant is designed	44
2.1.2 Provisions to protect the plant against the design basis earthquake	49
2.1.3 Compliance of the plant with its current licensing basis	58
2.2 Evaluation of safety margins	59
2.2.1 Range of earthquake leading to severe fuel damage	61
2.2.2 Range of earthquake leading to loss of containment integrity	62
2.2.3 Earthquake exceeding the design basis earthquake for the plant and consequent flooding exceeding design basis flood	62
2.2.4 Potential need to increase robustness of the plant against earthquakes	62
2.3 Summary	63
3 External Flooding	66
3.1 Design Basis	67
3.1.1 Flooding against which the plant is designed	67
3.1.2 Provisions to protect the plant against the design basis flood	76
3.1.3 Plant compliance with its current licensing basis	81
3.2 Evaluation of safety margins	82
3.2.1 Estimation of safety margin against flooding	82
3.2.2 Potential need to increase robustness of the plant against flooding	83

3.3	Summary	84
4	Extreme Weather	87
4.1	Design Basis	89
4.1.1	Reassessment of weather conditions used as design basis	91
4.1.2	Conclusions on the Design Basis	95
4.2	Evaluation of safety margins	95
4.2.2	Potential need to increase robustness of the plant against extreme weather conditions	102
4.3	Summary	104
5	Loss of Electrical Power and Loss of Ultimate Heat Sink	107
5.1	Nuclear power reactors	108
5.1.1	Loss of electrical power	108
5.1.2	Measures which can be envisaged to increase robustness of the plant in case of loss of electrical power	113
5.1.3	Loss of the ultimate heat sink	113
5.1.4	Measures which can be envisaged to increase robustness of the plant in case of loss of ultimate heat sink	117
5.1.5	Licensee Review of Robustness	117
5.2	Spent fuel storage pools	118
5.2.1	Loss of electrical power	118
5.2.2	Measures which can be envisaged to increase robustness of the plant in case of loss of electrical power	119
5.2.3	Loss of the ultimate heat sink	119
5.2.4	Measures which can be envisaged to increase robustness of the plant in case of loss of heat sink	120
6	Severe Accident Management	122
6.1	Organisation and arrangements of the licensee to manage accidents	122
6.1.1	Organisation of the licensee to manage the accident	123
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	141
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	144
6.2.4	Prevention of re-criticality	145
6.2.5	Prevention of basemat melt through	145
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	146
6.2.8	Measures which can be envisaged to enhance capabilities to maintain containment integrity after occurrence of severe fuel damage	146
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	149
6.3.3	Measures which can be envisaged to enhance capability to restrict radioactive release	151

Glossary

AC	Alternating Current
AGR	Advanced Gas-Cooled Reactor
ALARP	As Low As is Reasonably Practicable
AOD	Above Ordnance Datum
ASME	American Society of Mechanical Engineers
ASREP	AGR Safety Review and Enhancement Programme
ASREP	Safety Review and Enhancement Programme
BGS	British Geological Survey
CEGB	Central Electricity Generating Board
DC	Direct Current
DEFRA	Department for Environment, Food and Rural Affairs
DNB	Dungeness B
EDF	Electricity de France
ENSREG	European Nuclear Safety Regulators' Group
HSE	UK Health and Safety Executive
IAEA	International Atomic Energy Agency
IPCC	Intergovernmental panel on Climate Change
NSP	Nuclear Safety Principle
ONR	Office for Nuclear Regulation
PML	Principia Mechanica Ltd
PSA	Probabilistic Safety Analysis
PSR	Periodic Safety Review
PWR	Pressurised Water Reactor
SNUPPS	Standard Nuclear Power Plant
SOER	Significant Operating Experience Report
SZB	Sizewell B
TEPCO	Tokyo Electric Power Company
URS	Uniform Risk Spectrum
WANO	World Association of Nuclear Operators

Executive Summary

Dungeness 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 Dungeness 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”.

This report raises some ‘considerations’. These are defined as ‘Opportunities to further examine potential enhancements to plant, process or people for beyond design basis scenarios’.

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

Earthquakes

In the Office for Nuclear Regulation (ONR) Interim Report into the Japanese Earthquake and Tsunami, it is stated that “The extreme natural events that preceded the accident at Fukushima - the magnitude 9 earthquake and subsequent huge tsunami - are not credible in the UK. We are 1,000 miles from the nearest fault line² and we have safeguards in place that protect against even very remote hazards.”

With the exception of Heysham 2 and Torness, the advanced gas-cooled reactors were not originally designed to withstand earthquakes. Sizewell B, a pressurised water reactor, was based on the Standard Nuclear Power Plant design and the standard design included qualification against earthquake. However, for the pre-Heysham 2/ Torness advanced

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

² Assumed to mean tectonic plate boundary

gas-cooled reactors, seismic safety cases were developed 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.

Summary of findings for earthquakes at Dungeness B

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

- The design basis earthquake was defined as that corresponding to an infrequent event using an extensive study of historical earthquakes and local geology.
- It is not judged credible that a local earthquake would be powerful enough to produce a tsunami. This judgement is supported by a detailed study undertaken by DEFRA in 2005 to evaluate the tsunami risks to the UK.
- The design basis earthquake is reviewed by the periodic safety review process, most recently in 2007, which concluded that it was still valid in the light of modern standards and data.
- Protection of plant from seismic effects is provided through a qualification process which ensures the plant needed to safely shut down the reactor and provide post-trip cooling remains available following the infrequent seismic event.
- Suitable processes are in place to ensure that the plant remains compliant with its licensing basis.
- No cliff-edge (i.e. a large change in impact for a small change in hazard) effects are expected for events up to twice as severe as the design basis.

The seismic safety case is based on the provision of a line of protection with redundancy for the infrequent design basis earthquake, and two lines of diverse protection with redundancy in each line, for the more frequent. 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.

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

External Flooding

In the Office for Nuclear Regulation's (ONR) interim report on the Japanese Earthquake and Tsunami Implications for the UK Nuclear Industry, recommendation 10 is:

"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, 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 beyond the scope of this report. Any further references to floods in this report concerns the external flooding hazard.

Summary of findings for external flooding at Dungeness B

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

- At Dungeness B the bounding case for the infrequent event design basis is rainfall. The methodology calculates that the extreme event will give a water level which is equal to or greater than some building thresholds, however the equipment which forms the bottom line of protection is located in buildings above flood level or on plinths, i.e. bottom line protection would remain available during a design basis flood.
- 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.
- The sea defences are adequately sized to maintain essential function availability during the Design Basis Sea States.
- During extreme rainfall events the predicted maximum site flooding level is conservatively calculated to be 5.54m Above Ordnance Datum (AOD). Essential function availability is maintained by the action of the passive site drainage system and drainage of water through the shingle.
- The methodology used to calculate the design basis flood for Dungeness B has been conservatively constructed using independent expertise based on well regarded sources of information.
- The methodology for determining the design basis flood and the 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.
- Although the equipment needed to maintain the essential safety functions are qualified against the design basis flood, the margin to failure has not been explicitly derived. For the purposes of beyond design basis risk management a consideration has been raised to quantify the physical margin to failure.

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.

Summary of findings for extreme winds at Dungeness B

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

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

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

Summary of findings for extreme ambient temperatures at Dungeness 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 current design basis for extreme ambient temperatures has not been robustly defined. A consideration has been raised by this report to redefine the design basis using modern techniques and data.
- Analysis of climate change shows that the expected extreme ambient temperatures will exceed the current design basis by 2030.
- Within the current design basis at least one line of protection is demonstrated to remain available.
- A safety margin cannot be defined for extreme ambient temperatures. Tech Specs ensure that the plant is shutdown while the temperature is still within the allowable range.

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 changes in temperature will not impact nuclear safety. Buildings containing essential equipment have been assessed against snow loading and demonstrate sufficient margin. Where this has not been shown, failure of the building has been shown to be acceptable.

The Climate Change Adaptation Report predicts by 2030 there will be a rise in the expected maximum air temperature beyond the current design basis. This has been raised as a consideration by this report.

Summary of findings for lightning at Dungeness B

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

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 these are not considered here.

- Work is currently being undertaken to produce a formal lightning safety case.

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 Dungeness 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 has been addressed.

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.

- Work is currently being undertaken to produce a formal drought safety case.

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.

Combinations of hazards at Dungeness B

Some combinations of hazards have been considered in the safety case for Dungeness B. However a systematic consideration of all the possible combinations of hazards has not yet been undertaken, and work is underway to do so.

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 considers the impact upon the reactor essential safety functions due to the above scenarios and considers 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 findings for loss of electrical power and loss of ultimate heat-sink at Dungeness B

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

- At Dungeness 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 adequate provisions are made to support the essential safety functions.
- A permanently installed, diverse additional boiler feed system can provide post-trip cooling of a pressurised reactor under a station black out scenario.
- Whilst arrangements exist to provide resilience against some station black out scenarios at Dungeness B, there is currently no explicit station black out safety case.
- For a depressurised reactor, sufficient cooling cannot be provided under a station black out scenario because forced gas circulators and equipment necessary for reseal and repressurisation would be unavailable.
- During station black out, the back-up battery supplies are not required to provide boiler feed in the long term.
- There are provisions off-site that can be deployed to station within 10 hours that would provide power generation capability and aid continued post-trip cooling of the reactor.
- Following a severe accident event, actions required by shift staff could be hindered by conditions on-site. Mitigation of this is provided in the form of centralised emergency support and procedures for beyond design basis events.
- Analyses modelling severe accident scenarios have previously been carried out. These have been used for the examination carried out in this report. It has been noted that reconfirmation of these analyses and additional sensitivity studies would be beneficial.
- In the event of a loss of the heat sink, there are sufficient stocks of cooling water for a period of at least 24 hours.
- The current robustness and maintenance of the plant is compliant with its design basis for loss of the ultimate heat sink. However, steps to improve the resilience of the plant following a beyond design basis event should be considered.
- The current robustness and maintenance of the plant is compliant with its design basis against loss of electrical supplies and ultimate heat sink. However, steps can be made to improve the resilience of the plant for a beyond design basis event.
- Whilst there are no vulnerabilities identified in the current design basis for the fuel route against loss of electrical power, loss of ultimate heat sink or both, further resilience enhancements could be envisaged.

Severe Accident Management

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

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

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

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

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

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

Dungeness 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 interim report focuses on significant lessons for the safety of nuclear power stations operating in the UK and proposals to build new ones. It looks at the evidence and facts, as far as they were known at that time, to establish technically based issues that relate to possible improvements in safety and regulation in the UK. It also indicates some lessons for international arrangements for such systems.

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

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

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

0.2 Scope of Stress Test

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

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

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

As well as the existing safety justifications, this Stress Test considers the response of the plant and the claimed safety measures to challenges of a severity in excess of those already covered in the station Safety Cases. The nature of the challenges has been defined considering the issues that have been highlighted by the events that occurred at Fukushima Dai-ichi, including combinations of initiating events and failures. These include the directly relevant hazards such as earthquake and flooding (from tsunamis and other sources) and other extreme weather conditions, potentially more relevant to the UK such as high winds and extreme ambient temperatures.

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.

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

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

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

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

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

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

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

0.3 EDF Energy’s Nuclear Sites

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

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

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

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

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



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

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

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

The UK Health and Safety at Work Act leads to legislation made under the Act that may be absolute or qualified by expressions such as the need for duty holders to ensure “reasonable practicability”. (As Low As is Reasonably Practicable - ALARP). The term reasonably practicable allows for a cost benefit analysis to be used when determining the actions to be taken in response to an identified risk, or for a comparison to be carried out with “good practice” in similar circumstances. The preventative measures taken should however be commensurate with the magnitude of the risk. Both “practicable” and “reasonable 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' 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

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.

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

- Initiating events are defined as Frequent if they have an estimated frequency of occurrence greater than 10^{-3} /year. For any frequent initiating event there are at least 2 lines of protection to perform any essential function, with diversity between each line, during any normally permissible state of plant availability, unless it is shown not to be reasonably practicable.
- Initiating events are defined as Infrequent if they have an estimated frequency of occurrence less than or equal to 10^{-3} /year. For any Infrequent Initiating Event there is at least 1 line of protection to perform any essential function and that line is provided with redundancy, during any normally permissible state of plant availability, unless it is shown not to be reasonably practicable. As a minimum, during any permissible state of plant or equipment unavailability for testing or maintenance, there should be at least one line of protection to perform any essential function for any initiating event with a frequency of greater than or equal to 10^{-5} /year."
- Events whose estimated frequency of occurrence is judged to be less than 10^{-5} /year are not assessed against the Deterministic Principles, however the reasonable practicability of providing protection for such events is considered.

Initiating events which, in the absence of protection, would lead to a dose of less than 1 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.

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

0.5.2 Probabilistic Principles (NSP 3)

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

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

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

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

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

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

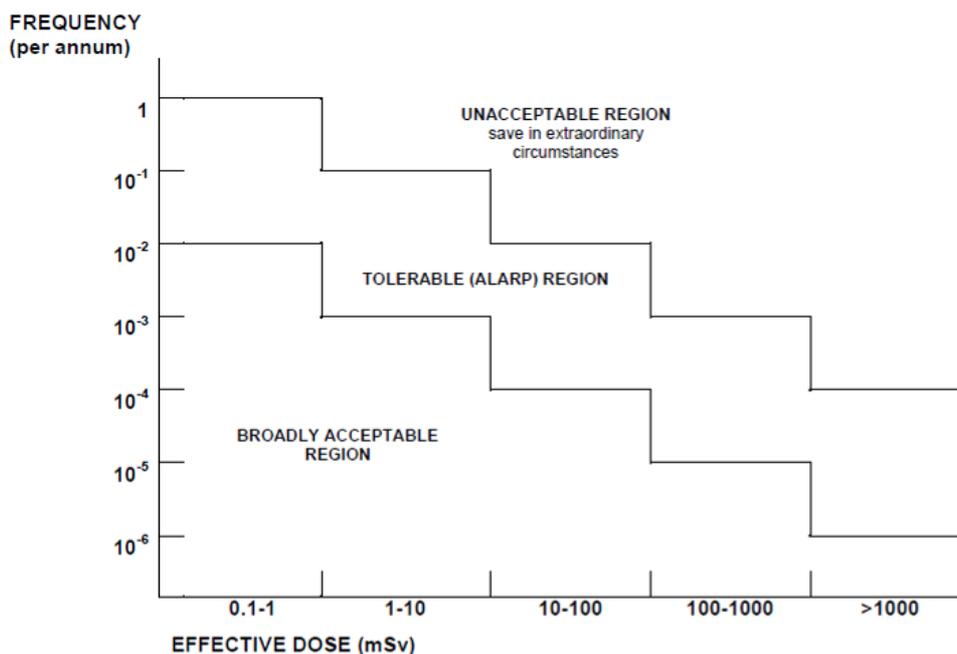


Figure 0.2: Surrogate risk regions as a function of frequency and effective dose.

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

0.5.3 Shutdown Cooling Criterion

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

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

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

0.6 Specific Assessment and Design Against Hazards

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

The main reason for categorising the hazards in this way is that internal hazards are faults for which EDF Energy can have a direct influence in limiting the magnitude and frequency of the hazard by, for example, minimising quantities of flammable materials or ensuring hazardous equipment is suitably segregated. External hazards are those which initiate

independently of EDF Energy's operations and to which EDF Energy have limited (such as industrial hazards) or no (such as meteorological hazards) control over the magnitude or frequency of the hazard event.

The nature of the event at Fukushima Dai-Ichi and therefore focus of this Safety Report are the natural external hazards. Unlike other faults they cannot be prevented and so, as far as defence 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 10^{-3} . For any frequent event there are at least 2 lines of protection to perform any essential function, with diversity between each line, during any normally permissible state of plant availability, unless it is shown not to be reasonably practicable, recognising that there should always be at least 1 line of protection.
- External hazard events are defined as Infrequent where they have an annual probability of exceedance of between 10^{-3} and 10^{-4} . For any infrequent event there is at least 1 line of protection to perform any essential function and that line is provided with redundancy, during any normally permissible state of plant availability, unless it is shown not to be reasonably practicable.

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

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

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

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

0.7 Mission Time and Offsite Support

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

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

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

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

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

0.8 Beyond Design Basis Events and Accident Management

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

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

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

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

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

0.9 Emergency Response Arrangements

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

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

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

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

0.10 Mandatory Evaluations

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

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

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

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

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

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

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

Chapter 1 - General Data about Dungeness B

Dungeness B

1 General Data about Dungeness B

1.1 Site Characteristics



Dungeness B is a twin reactor advanced gas-cooled station situated on the Kent coast approximately 30km south-west of Dover. It was the first commercial advanced gas-cooled reactor to commence construction (1965) and started generating power in 1983. End of generation is currently scheduled for 2018. The power station is built on a large area of open shingle, measuring 12 km by 6km. The three small towns on the headland nearest the power station are Lydd-on-Sea, Greatstone-on-Sea and Littlestone-on-Sea, which lie to the north on the east coast of the Dungeness headland.

Dungeness B is operated by the licence holder – EDF Energy Nuclear Generation Ltd, a subsidiary company of EDF Energy plc. The Dungeness B plant with its twin reactors adjoins Dungeness A Power Station, a twin unit Magnox Station. The latter has ceased generation and is being decommissioned. Dungeness A is a separate nuclear licensed site which is neither owned nor operated by EDF Energy plc. However, Dungeness 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 are planned to be removed in the near future.

1.2 Main Characteristics of the Dungeness B Reactors

The station consists of two reactor units with a shared services unit for services, instrumentation and control, and a shared turbine house. Each reactor drives a single 660 MW turbine generator set. The two reactors are served by one fuelling machine operating within a common charge hall. The primary circuit of each reactor is contained within a post-tensioned concrete pressure vessel.

Table 1.1: Specific details of Dungeness B reactor

	Reactor 21 and 22
Reactor Type	Commercial Reactor
Model	Advanced Gas-Cooled Reactor
Owner	EDF-Energy
Operator	EDF-Energy
Capacity Net	520 MWe (per reactor)

Table 1.2 Construction and Operation details for Dungeness B

	Reactor 21	Reactor 22
Start Construction	1 October 1965	1 October 1965
Criticality	4 December 1985	23 December 1982
Grid Connection	29 December 1985	3 April 1983

1.3 Systems for Providing or Supporting Main Safety Functions

Reactor Systems

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

The reactor core is contained within a cylindrical pre-stressed concrete pressure vessel with top and bottom caps. On the inside of the concrete there is a gas tight steel liner. Normal operating pressures are 30bar to 40bar.

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

Compared with light water reactors, the advanced gas-cooled reactor energy power density is low, approximately 2.5MWth/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 increase 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.

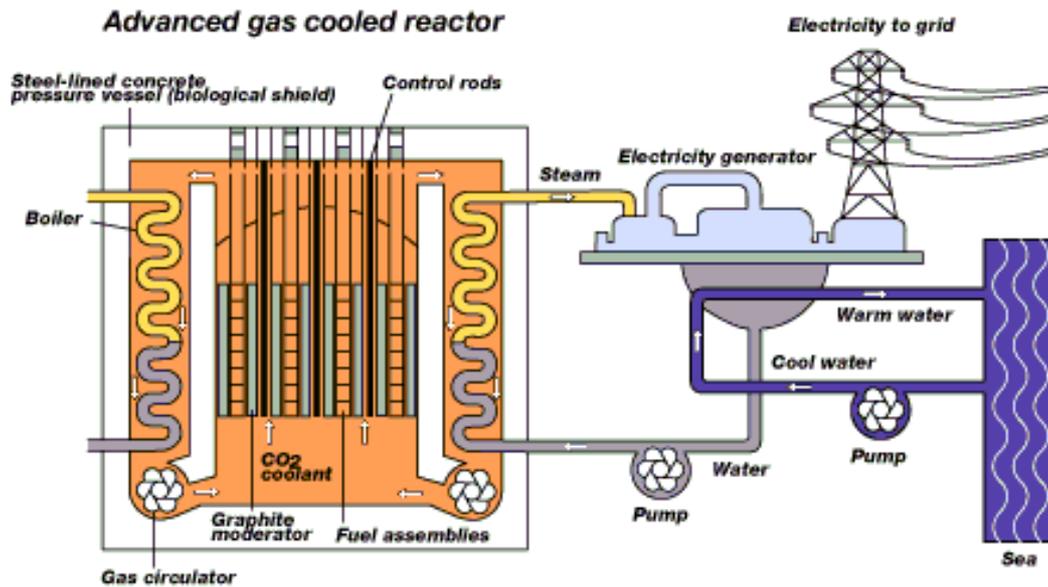


Figure 1.1: Simplified AGR showing internal components and the ultimate heat sink

Fuel Handling

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

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

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

1.3.1 Reactivity Control

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 in any one location, ^{235}U enrichment, the presence of additional moderators (e.g. graphite or water from fire extinguishers) and flammable materials. They also specify procedures to be followed in the event of fuel damage.

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

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

1.3.2 Heat Transfer from the Reactor to the Primary Ultimate Heat Sink

1.3.2.1 Means of Heat Transfer from the Shutdown Reactor to the Primary 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. Feedwater 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, decay heat removal is via the main boilers with each being fed with feedwater from either normal feed systems or the back-up feed systems. The steam generated in the boilers by decay heat is either returned to the main condenser or discharged to atmosphere via safety relief valves in the boiler (whereby the atmosphere is used as an alternative heat sink).

Post-Reactor 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 continues 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. diesel, carbon dioxide, feedwater). This is on the basis that within that timescale it would be possible to obtain the required stocks to go beyond 24 hours. In reality, available stocks are normally provided for longer than 24 hours.

The provision of adequate post-trip cooling requires 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 a number of different diesel generators systems.

Primary Coolant

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 circulator main motors which are supplied by off-site power (grid). Heat from the circulator oil systems is rejected to a cooling system which uses the sea as the ultimate heat sink. If grid supplies are unavailable, alternate electric motors powered by diesel generators can drive the gas circulators.

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 Systems

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

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

In normal operation, boiler feedwater is pumped from the condenser to the boilers (via a deaerator) and steam flows from the boilers to the turbine. 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 for approximately one 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 are sufficient water stocks to operate in this 'once-through' manner for at least 24 hours.

Feed Systems

Main feed systems

The purpose of the main feed system is to provide feedwater to the boilers both during power operations and post-trip and is a system with inherent inbuilt diversity. The main boiler feed pump can only operate for a limited period post trip and is only claimed for risk mitigation within the safety case. An additional electric boiler feed pump is claimed by the safety case as a means of providing a supply of feedwater for most faults post reactor trip. The main boiler feed system normally re-circulates feedwater through the condenser, but can also use water stored in tanks in a once-through manner.

Following a reactor trip, the main boiler feed pump would normally remain in service until the operator transfers to the electric boiler feed pump if grid supplies are available. In the event of the main feed system being unavailable (e.g. following a loss of grid), one of the systems described below would be used.

Emergency boiler feed system

The purpose of the emergency boiler feed system is to provide post-trip feed to the boilers, and comprises of a set of steam driven pumps and a set of diesel generator backed electric pumps. The feedwater is the same as that used for the

main feed system, described above. For most faults the system is claimed as a first line of feed within the deterministic safety case. The steam powered pumps can only operate for a limited period post trip. In the longer term post trip feed is provided by the diesel generator backed electric pumps.

Direct diesel-driven feed system

The purpose of the direct diesel-driven feed system is to provide a high-pressure back-up feed supply for post-trip cooling of the boilers which does not depend on electrical supplies. The system is automatically initiated by a combination of trip detection equipment. The water used is taken from a separate set of tanks. This feed system is entirely independent of the other feed systems. This feed system was an addition to the original design of the Station, and was specifically designed against the infrequent earthquake and other external hazards.

Back-up feedwater system

The purpose of the back-up feed system is to provide post trip feed to the boilers when the other feed systems are unavailable. This system is completely independent of the other feed systems, and is powered by diesel generators. The system is claimed by the safety case as a means of providing a supply of feedwater for most faults post reactor trip. This system may also be connected by spool pieces to provide make-up for the reactor tertiary shutdown system. The ultimate heat sink for the back-up feed system is the atmosphere, as the water passes through the boilers once and is then discharged as steam.

Manual initiation of the back-up feed system is required, and the boilers must first be depressurised. With forced circulation, the quantity of water in the back-up feedwater tank is sufficient to remove the shutdown decay heat from both reactors for a period of at least 24 hours. If additional water is required, it can be drawn from nearby lagoons which contain a large quantity of water.

Cooling Water Systems

Main cooling water

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

Seawater cooling Water

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

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

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

Back-up cooling water system (lagoons)

The system design is to provide a safety related, on-demand (though with plant status determining heat loading) back-up cooling system with redundant pump capacity and cooling capacity that feeds supported systems which are systematically divided into two half systems.

It has been designed such that as a minimum, one pump could provide cooling water flow following a double reactor shutdown although two pumps would normally be started. The system is designed to support the safe removal of excess heat from the reactors.

The water is taken from nearby lagoons. Water usage is managed to support at least 24 hours of operation, and the system is confidently expected to operate for longer.

Townswater cooling water system

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

- Gas circulator main motors;
- Fuel handling facilities; and
- Boiler feed pumps.

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

1.3.2.2 Layout of Heat Transfer Chains

Plant systems which support primary coolant heat transfer are generally located close to the primary circuit although there are some systems, for example the seawater cooling water and back-up cooling water which both support forced circulation cooling, which are located outside of the reactor building. Similarly, it may be appreciated that electrical supplies to support forced circulation (power to circulator motors and power to auxiliary cooling systems) will also originate externally buildings. 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).

1.3.2.3 Heat Transfer Time Constraints

The length of time for which heat transfer systems may continue to be supported depends on a number of factors. If off-site power supplies are available, not only are electrical supplies supported without time constraints but feedwater may also be re-circulated. A continued loss of off-site power supplies is likely to require reactor heat transfer to be supported by consumable water supplies and consumable fuel oil supplies. Fuel oil consumables are relevant to direct diesel-driven pumps and also to the provision of diesel-backed electrical supplies.

Table 1.3: Minimum feedwater Stocks.

Feedwater Source	Timescale	Comments
Water for electric feedwater pumps.	The specified reserves for these systems are sufficient for 12 hours forced circulation post-trip cooling	The 12 hour time period and associated reserve originates from the original plant safety case requirements
Water for back-up feedwater pumps	The specified reserves are sufficient for 24 hours of forced circulation post-trip cooling of two reactors	This quantity is not sufficient for 24 hours natural circulation cooling of both reactors, but topping up this tank using nearby lagoons is available.
Water for direct diesel driven feedwater system	The specified reserves are sufficient for 24 hours of natural circulation post-trip cooling of two reactors (one of which is assumed to depressurise slowly, requiring enhanced feed flowrate).	Topping up this tank using nearby lagoons is available, but a make up connection is required.

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 Dungeness 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 analysis for reactor systems provides an indication of whether the systems deliver diversity, and any significant weaknesses in the system relating to diversity would be revealed during the assessment process. The probabilistic safety analysis for Dungeness 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 Primary 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 CO₂) 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.

Stage of fuel storage and handling	Handling with fuelling machine	Buffer storage	Dismantling	Storage in ponds
Primary cooling circuit	CO ₂ by forced circulation to fuelling machine body	CO ₂ by natural circulation	CO ₂ by forced circulation	Pond water circulated by cooling system
Secondary cooling circuit(s)	None	Recirculating cooling water circuit; and Once-through sea water cooling system	Recirculating cooling water circuit; and Once-through sea water cooling system	Recirculating cooling water circuit; and Once-through sea water cooling system
Ultimate heat sink	Ambient air	Sea	Sea	Sea

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

Stage of fuel storage and handling	Handling with fuelling machine	Buffer storage	Dismantling	Storage in ponds
Potential impact of loss of cooling	Natural circulation is effective unless fuel is part way in reactor.	Boiling of water in the secondary circuit followed by overheating of fuel	Even with loss of cooling water systems, natural cooling effects mean fuel safety limits will not be breached.	Boiling of water in the ponds followed by overheating of fuel
Assigned safety limit	n/a	Boiling dry of storage tube water jackets	n/a	Boiling and/or loss of pond water
Minimum time to reach safety limit	n/a	Not less than 21 hours for the hottest fuel	n/a	Several days

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 Primary Ultimate Heatsink

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

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

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

The pre-stressed concrete pressure vessel contains the reactor and primary coolant gas and the boilers. Its concrete walls act as a biological shield so that the radiation levels outside the pre-stressed concrete pressure vessel are minimal. A steel liner forms a gas-tight membrane on the inside to maintain an integral pressure boundary with the many penetrations. These penetrations, amongst other things, allow water to enter the boilers and steam to exit as well as provide routes for instrumentation and refuelling operations.

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

A dedicated cooling system serves the pre-stressed concrete pressure vessel. Cooling water flows around the pressure vessel through a network of pipes which are connected to the pressure vessel, vessel liner and the vessel penetrations. The ultimate heat sink for this cooling system is the sea.

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

1.3.4.1 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. There are also safety relief valves which can be opened to reduce the pressure if required. The pressure vessel also performs a secondary safety role by providing radiation shielding, thereby minimising radiation doses to station personnel.

Vessel cooling systems

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

1.3.5 AC Power Supply

Electricity produced by Dungeness 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/gas turbine generators).

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

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

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

System	Seismic Qualification	Fuel Provision	Water Provision
Main Diesel Generators (3.3 kV)	System not qualified to withstand a seismic event	12 hours but can be extended to 24 hours if non-essential equipment shutdown	Water cooled using recirculating cooling water. On loss of grid connection this system is direct-diesel pumped with fuel stocks for 30 hours.
Back-up Diesel Generators (3.3 kV)	System designed to function following an infrequent seismic event	More than 24 hours	No water used (air cooled)
Further Back-up Diesel Generators (415V)	System designed to function following an infrequent seismic event	More than 24 hours	No water used (air cooled)

Table 1.4: Further details on plant required to provide essential safety functions.

1.3.5.1 Off-site Power Supply and Station Earthing

The Dungeness B grid connections comprise the Dungeness 400kV and 275kV substations, the 400kV/275kV supergrid transformers and the 400kV and 275kV cable connections to the 400kV/23.5kV Generator and 275kV/11.8kV Station Transformers respectively.

The 400kV substation has four connections to the grid system whilst the 275kV substation consists of four busbar sections. The interconnection between the 400kV and 275kV busbars is made by two 400kV/275kV 750MVA supergrid transformers.

The principal function of the grid interface is to transfer the generated power from the Turbine Generators to the 400kV transmission network and to provide electrical power supplies from the 275kV transmission system to the station Main Electrical System 11kV Station Boards.

1.3.5.1.1 Off-site power supply reliability

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

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

Date	Time	Duration	Reactor Trip	Weather	Description
16/10/87	0406	12.5h	yes	Intense	Hurricane, loss of grid connection several times between 0406-1930hrs
26/01/90	1533	14 mins	yes	Adverse	Following a period of severe weather and intermittent tripping and reclosing of Ninfield 1&2 and Sellindge 1&2 over-head lines, a total loss of grid transmission lines occurred. This led to a Reactor 22 trip on rate of change of Boiler Gas Outlet Temperature, and a simultaneous reactor trip at Dungeness A station.

Date	Time	Duration	Reactor Trip	Weather	Description
16/03/91	1134	31 mins	-	Normal	A complete loss of Station Electrical Supplies occurred due to the loss of the 275kV substation during testing by the National Grid Company whilst both reactors were in a shutdown state.

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 does not rely on off-site power. Post-trip cooling requires the provision of both primary and secondary coolant flow. Natural primary coolant circulation together with feedwater flow to the boilers (requiring electrical power) is effective although forced primary coolant flow (also requiring electrical power) is the design intent. In the reactor trip events shown in Table 1.5, forced primary coolant circulation was established via electrical power from on-site diesel generators.

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

Cabling between the transformers and grid substations is via underground tunnels. The provision of ventilation and sump pumps serves to maintain acceptable environmental conditions within the tunnels. Fire protection is provided in the grid substations and in parts of the cable tunnels. However, the fire protection systems have no essential safety duty in respect of preserving the integrity of the grid connection since the causes of off-site power loss are likely to arise externally to the site. 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 substations 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. The power distribution from back-up supplies and diverse back-up supplies are addressed in Sections 1.3.5.3 and 1.3.5.4. Supplies at varying voltages are provided on a unit and station basis as part of the ‘main electrical system’ as follows.

11kV Supplies

Two 11kV Unit Switchboards associated with each reactor derive their supplies from transformers connected to the main generator connections. These unit supplies are only available from the generator output and cannot be supplied from the grid via the generator transformers.

There are interconnectors provided between the station and unit boards to allow station supplies to be used for start-up or shutdown of the unit. Interconnectors are also provided between the three station transformers to allow each to provide redundancy. The 11kV station transformer derived supplies are the preferred source of supply for post trip cooling plant.

3.3kV Supplies

The unit and station electrical supplies required to operate at this voltage are divided into two separate systems both providing distribution at 3.3 kV. One is the 3.3kV unit auxiliaries board (one per reactor) and the other is the 3.3kV station auxiliary boards (of which there are six).

415V AC Supplies

The 415V switchboards are derived via transformers from the appropriate 3.3kV Unit Auxiliary or Station systems.

'No-break' Systems

Four 500V DC batteries provide no break supplies either directly as DC or via motor-generator sets as AC. This system provides secure no-break supplies of limited duration (approximately 25 minutes) to essential loads. Following starting of the diesel generators or restoration of grid supplies, the batteries are recharged and the supported loads continue in service uninterrupted.

The provision of 'no-break' systems consisting of batteries and chargers ensures that control, instrumentation and some other systems continue to function during the changeover from grid to diesel generator supplies. Thus, the systems will be started once the appropriate diesel generators are running.

1.3.5.2.1 Main Electrical System – Cable and Equipment Locations

Cabling at 11kV runs between the switchboards and their associated unit and station transformers. Cabling at 11kV and 3.3kV runs from the services building to the external 11kV/3.3kV unit and station auxiliary transformers.

1.3.5.2.2 Main Electrical System – Performance in Hazards

Electrical supplies via the transformers are therefore expected to be maintained following localised initiating hazard events, e.g. single transformer fire. The transformers are designed for external duties and are not expected to be affected by rainfall. Some protection against site flooding is provided by bunds surrounding the transformers but this is not claimed to be effective under conditions of gross site inundation. Alternative electrical supplies are likely to be available via back-up electrical supplies (see section 1.3.5.3). External transformers are not seismically qualified; resilience against seismic events is provided by the back-up electrical supplies.

The 11kV and 3.3kV supplies are grouped together in two switch rooms; each supplying its respective unit. Localised hazards which could disable supplies from either switch room are credible (e.g. fire, steam release). Back-up supplies via diesel generators or an alternative switch house are available in such instances. In general, the equipment in the services building is not seismically qualified since loss of off-site power is assumed in a seismic event. Severe flooding events are unlikely to affect the 11kV and 3.3kV boards within the services building which are well above flood level. Similarly, the 415V AC boards are not seismically qualified but may be assumed to be unaffected by severe site flooding.

The 110V DC Gas Circulator Tripping Supplies are battery backed and are seismically qualified. These supplies provide protection against gas circulator run-on by delivering a secure electrical supply to trip the gas circulator breakers in the event of a reactor trip.

1.3.5.3 Primary On-Site Back-up Power Supplies

Dungeness B has a number of separate back-up electrical power supplies which supply different items of plant supporting post-trip cooling.

The first of these systems is the main back-up for the grid-backed main electrical system and is designated as the primary on-site back-up power supply. It is supported by diesel generators and is a 'short break' supply, i.e. power is only available after the diesels have started and the necessary electrical switching has been completed. The 'no break' battery backed system enables the starting and switching required to configure electrical supplies.

Two further back-up electrical power supplies provide diverse sources of power which in general add defence in depth to the electrical supply provision for most initiating faults and hazards. However, for a limited number of specific faults/hazards which could adversely affect the on-site back-up, these latter systems may be claimed to provide essential electrical supplies to support post-trip cooling equipment and are considered to be diverse permanently installed on-site sources for back-up power supply.

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

Most of the electrical equipment comprising the primary on-site back-up power supplies is located within the main buildings. Essential diesel generators and their fuel supplies are located nearby.

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

Localised hazards which could disable sections of the primary on-site back-up power supplies are credible (e.g. fire, steam release). In general, the primary equipment is not seismically qualified. Alternative diverse supplies have been qualified to remain available in such circumstances. Severe flooding events are unlikely to affect the 3.3kV boards and battery rooms.

Similarly, the lower voltage distribution boards will be unaffected by severe site flooding. The diesel generators and their diesel oil supplies would not be adversely affected by infrequent extreme flooding.

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

The 500V batteries within the Guaranteed Supplies system have a capacity to support the related provision of 415V and 110V AC power supplies to essential plant for at least 25 minutes by which time the diesel generators will have taken over supplying these loads. The 500V batteries also support the diesel starting equipment including the compressors for the starting air receivers.

The primary diesel generators have fuel supplies which will maintain all four generators supporting essential loads for a minimum of 12 hours. However, one generator provides sufficient power and therefore sufficient stocks exist for much more than 24 hours.

1.3.5.4 Diverse On-Site Back-up Power Supplies

In addition to the primary on-site back-up power supplies, provision of further electrical supplies is made to address those faults and hazards which threaten the operation of the primary on-site back-up power supplies. These systems are considered as diverse on-site back-up power supplies.

There are two independent diverse on-site back-up power systems, each consists of a 'short-break' system backed by diesel generators. Each diesel generator is housed in its own container, which incorporates the radiator, starting system, control panel and fuel tank. The fan-assisted radiators operate on a closed loop system and do not depend upon station cooling water services.

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

Where main and back-up cables are brought into common areas cabling is segregated in separate routes. Where complete physical segregation between main and back-up cables is not possible, they are separated as far as practicable and fire retardant cables are used for the back-up system. The cables are segregated along separate routes where diversity of supply is a requirement.

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

The diverse on-site back-up power systems provide independent electrical supplies available under the major station fault conditions, designed to operate in the presence of major site hazards such as fire, steam release, hot gas release, seismic events and turbine disintegration. Design redundancy criteria determine that the required loads may be met with one out of three diesel generators available.

The diverse on-site back-up diesel generators have no specific design features to provide protection against external flooding. The systems are located above the infrequent external flood level, and although the floor of the building housing one system lies marginally below this level, it is considered that low level flooding of the building will not disable the equipment contained within.

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

Both diverse on-site back-up power systems contain batteries which support a number of different dc supplies. Their role is to support essential switching, indication and lighting functions until the systems' respective diesel generators have completed their starting and run up sequence. Battery capacities are therefore limited.

The diesel oil stocks are sufficient to support operation (and power supplies to both reactors) for a mission time of at least 24 hours.

1.3.5.5 Further Available Back-up Power Supplies

1.3.5.5.1 Potential Connections to Neighbouring Units/Plants

Dungeness 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 advanced gas-cooled reactor 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. The facility for cross connection between units is universal at the 3.3kV level; any 3.3kV supplies board may be connected to its equivalent on the other unit. Cross connection between units is possible at lower voltage levels but requires multiple rather than single connections.

The 'no break' system may be cross connected between units at the 500V dc battery level. The facility to link electrical boards within the diverse on-site back-up power systems is also included in the system design.

Dungeness B has historically had a facility to obtain some separate power supplies from the neighbouring Dungeness A station. Although some cross connection capability may remain in the short term, the decommissioning of Dungeness A has resulted in a programme of removing such cross connection capabilities. This programme is expected to be complete in the near future.

1.3.6 Batteries for DC Power Supply

Section 1.3.5 identifies the significant DC batteries at Dungeness B. Although there are batteries in the primary and diverse on-site back-up power systems, they are mostly provided to support short term switching, indications and lighting (and some other functions) for a brief period until diesel-backed supplies are restored. They do not have significant capacity to support motive power for the large electric motors. The batteries are required to support systems until the diesel generators have started and run up.

1.4 Significant Differences Between Units

There are no significant differences between the two reactors (Reactor 21 and Reactor 22) at Dungeness B.

1.5 Scope and Main Results of Probabilistic Safety Analyses

1.5.1 Probabilistic safety assessment: The advanced gas-cooled reactor approach

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

Probabilistic safety analysis is a structured and comprehensive analytical methodology which is used in the assessment of safety critical systems. It allows 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.

Probabilistic safety analysis does not invent new faults to those identified through deterministic safety cases on the station fault schedule. Instead probabilistic safety analysis gives further insight to the complex nature of some fault sequences, 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).

Probabilistic safety analysis 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

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

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

Overview

This report covers the definition of the design basis earthquake and the equipment which is expected to survive an infrequent earthquake. 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. An infrequent event corresponds to an event with a return frequency of 10^{-4} per annum.
- The design basis earthquake is reviewed by the periodic safety review process, most recently in 2007, 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 unquantified safety margin implied by the process of seismic qualification, and no cliff-edge effects are expected for events of up to twice the design basis.

2.1 Design basis

2.1.1 Earthquake against which the plant is designed

2.1.1.1 Characteristics of the design basis earthquake

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

- For any infrequent initiating event, there should be at least one 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. This is often referred to in the seismic safety cases as the ‘bottom line’ earthquake.
- For any frequent initiating event, there should normally be at least 2 lines of protection to perform any essential safety function with diversity between each line. Frequent initiating events are defined as more frequent than 10^{-3} per annum.

At Dungeness B, the infrequent earthquake results in a peak ground acceleration of 0.21g uniform risk spectrum soft site response spectrum. The uniform risk spectrum was obtained from site-specific evaluation in 1991 using the seismic hazard working party methodology.

⁷ Assumed to mean tectonic plate boundary

The current design basis earthquake at Dungeness B for a frequent event has an assumed peak ground acceleration of 0.1g Principia Mechanical Ltd Spectrum in accordance with International Atomic Energy Agency (IAEA) guidelines.

It is important to note that this figure of 0.1g was adopted in accordance with IAEA guidelines and is a conservative figure as the actual worst site specific earthquake that could be expected in 1,000 years is 0.08g using the seismic hazard working party methodology. Only where as low as reasonably practicable assessments have shown this is not practicable have the second line plant items (those items claimed against the frequent event) been qualified against the less onerous 1 in 1,000 per year uniform risk spectrum. It is also worthy of note that a significant proportion of the second line plant has been seismically qualified to the more onerous 1 in 10,000 per year uniform risk spectrum.

According to a Tokyo Electric Power Company (TEPCO) report, the maximum recorded peak ground acceleration 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.

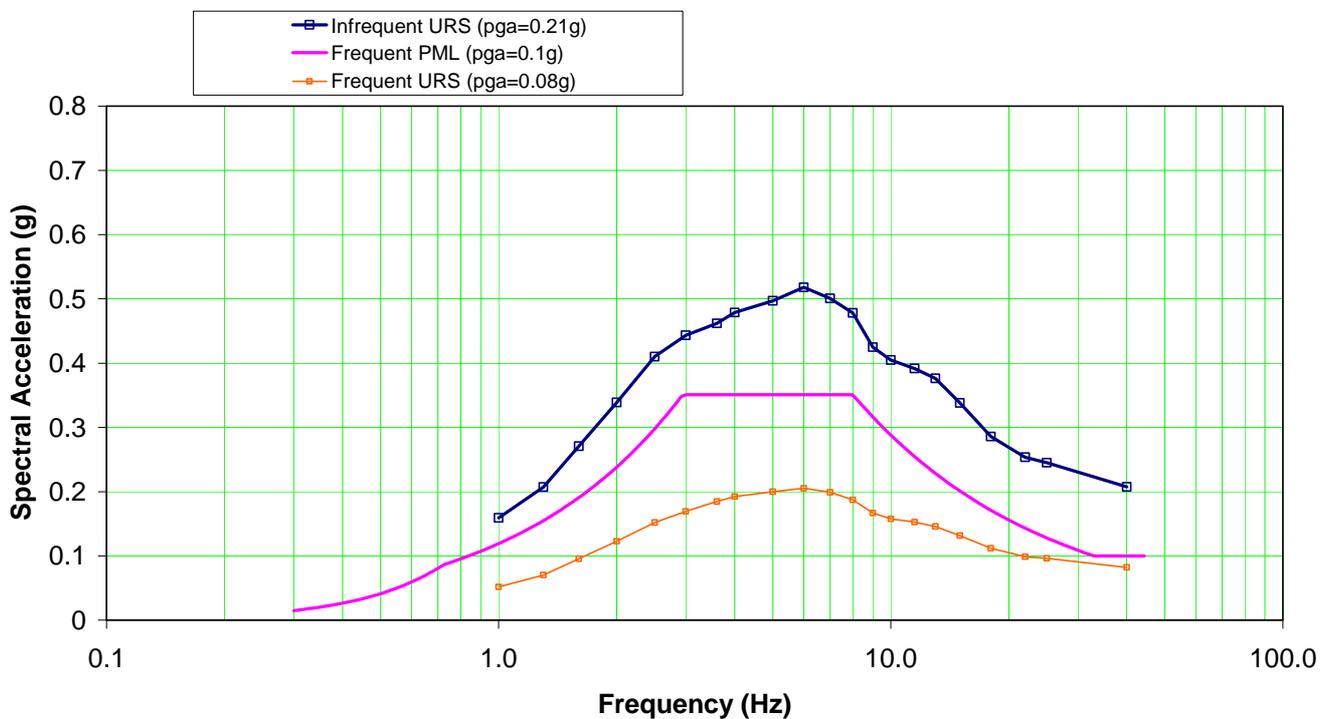


Figure 2.1: Dungeness B Ground Motion Specification showing Infrequent Uniform Risk Spectrum (URS), Frequent Principia Mechanical Ltd (PML) and Frequent URS spectral accelerations.

2.1.1.2 Methodology used to evaluate the design basis earthquake

Infrequent Event

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

Seismic Hazard Assessment Methodology

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

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

- 1) Compilation of a seismic source model in which seismic source zones and specific faults surrounding the sites are represented. The model takes in to account a variety of data sources.
- 2) Specifying parameters describing factors such as the rates of activity in these zones, source depths and attenuation parameters. These are specified conservatively.
- 3) Computation of the hazard level at the site. The approach is a probabilistic one and takes full account of uncertainties in the model parameters in order to provide appropriate safety margins.
- 4) Sensitivity studies to confirm that the results are not unduly sensitive to model or parameter variations, in order to ensure that appropriate margins to safety are present.

The Seismic and Geotechnical Database Section 1.3 provides further details of the Seismic Hazard Assessment Methodology, which is applicable to all EDF Energy’s Nuclear Generation sites in the UK.

Historical Data

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

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

Table 2.1: Significant Recent Historical UK Earthquakes

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

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

Review of Local Seismic Events

Figure 2.2 shows the tectonic framework around the Dungeness Site. To derive the site specific design basis earthquake, the seismological data for the region was investigated. The earthquakes that were felt at Dungeness from 1158 to 1992 are shown in Table 2.2

Seismic Source Model and Sensitivity Studies

The site specific seismic hazard was established by deriving a hazard model which defined zones around the site. Three alternative area zone source geometries were constructed for the region around Dungeness. They shared the same outer zone boundaries, but differ in respect of the subdivision of the local inner zones around the site. The zones differ in their representation of the southern part of the region, to ensure the most conservative representation was considered.

Sensitivity studies were carried out and in general reduced the predicted level of ground motion. Even extremely pessimistic scenarios gave only small increases in the predicted motion. For example, assuming a maximum surface magnitude of 7.0 Ms in every zone (greater than any historically recorded earthquake in the region) gave only a 0.01g increase in predicted peak ground acceleration for an infrequent event, although the effect was somewhat greater for the spectral acceleration at 1Hz.

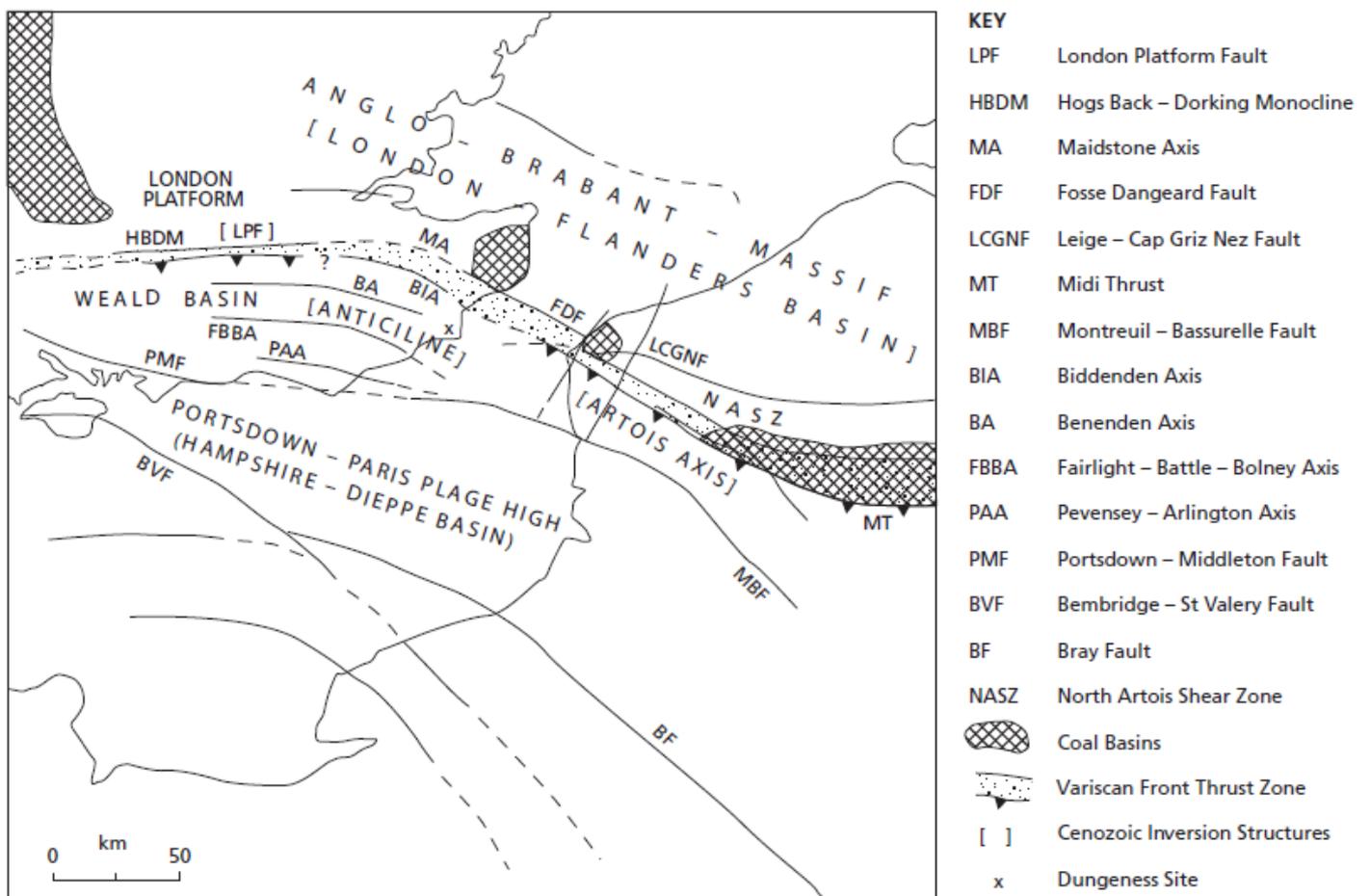


Figure 2.2: Tectonic framework of the Dungeness Region.

Table 2.2: Earthquakes felt at Dungeness from 1158 to 1992.

Date	Location	Magnitude (Ms)
1299	North Downs	4.0
1382	Off North Foreland	5.3
1580	Straight of Dover	5.4
1756	Ashford	3.0
1776	Off South Foreland	4.1
1983	Dungeness	<2.5

A review of seismic hazards for Dungeness was carried out during the second Dungeness B periodic safety review in 2007 to confirm the validity of the seismic hazard derivation.

The review considered seismic events that had occurred since the seismic hazard working hazard site specific evaluation. Within a 100km radius of Dungeness there had been two events with a magnitude of greater than 3.0 ML. There was a magnitude 3.6 event in Boulogne on 14 December 1991 and a magnitude 3.1 event in the Strait of Dover on 27 January 1998 that were 70km and 50km from Dungeness respectively. Within the 200km radius there were another two events of magnitude 3.2 in 1994 and 1999. These events were all below the threshold for events considered by the original seismic hazard assessment.

By comparison with the findings of the reviews for other EDF Energy sites and given that the events local to Dungeness were below the threshold for the original seismic hazard assessments, it was concluded that the recent seismic events did not have a significant effect on the Dungeness B hazard assessment and that it remained valid.

In 2007 an earthquake with a magnitude of 4.2 ML occurred with its epicentre directly adjacent to Folkestone, approximately 10 miles from Dungeness. Earthquakes of this magnitude have a recurrence interval of around five years over the whole of the UK. However, the recurrence interval for an earthquake of this magnitude specifically at Dungeness is much higher than five years. This event caused damage to brickwork of houses and cracking of internal plaster in the Folkestone area. The peak ground acceleration recorded of 0.1g at 10Hz is less than the frequent uniform risk spectra value of 0.15g at this frequency as shown in Figure 2.1. The effect of this event on the magnitude of the design basis earthquake is being considered under normal company business.

Geological Information on Site

The Gravel stratum consists of fine to coarse gravels in two units, the storm beach and the upper shoreface deposits. The lower unit contains variable amounts of sand matrix with some interbedded seams or lenses of sand. The upper unit generally contains no sand matrix, and sand seams or lenses are rare. The sand stratum of the superficial deposits is predominately of fine to medium grain size. It often contains some beds of finer material such as clayey silts or silty clays. A thin gravel layer is often present at the base of this unit. The Hastings Beds consist generally of very weak mudstones and siltstones with some sandstones, and bands of lignite at some levels.

Table 2.3: The approximate average stratum boundary levels in metres relative to Ordnance Datum (O.D.) (Newlyn) at the Dungeness sites.

	Dungeness A	Dungeness B
Ground Level	+5.5	+5.5
Base of Gravel	-8.5	-7.0
Base of Sand	-33.5	-33.5
Hastings Beds	-33.5 to approx -100	

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.

The frequent event design basis earthquake is 0.1g Principia Mechanical Ltd, in accordance with IAEA guidance and this exceeds that with a probability of 1 in 1,000 per year which for this site is 0.08g uniform risk spectra. This shows a clear margin and is therefore a pessimistic representation of a frequent event. Only where an 'as low as reasonably practicable' assessment have shown this is not practicable have the second line plant items been qualified against the less onerous frequent uniform risk spectra. It is also worthy of note that a significant proportion of the second line plant has been seismically qualified to the more onerous infrequent uniform risk spectra.

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

The information presented in the preceding sections shows that the methodology used to calculate the design basis earthquake for Dungeness B has been constructed using independent expertise based on well regarded sources of information. Furthermore it has been reviewed periodically in line with company process and regulatory expectations, including in the periodic safety review where no issues with the design basis earthquake were identified. The methodology has been constructed with appropriate conservatism, margins and sensitivity studies employed.

Conclusion DNB 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.

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 design basis earthquake and assessment of potential safety margin.

EDF Energy Nuclear Generation now has seismic safety cases for all of its advanced gas-cooled reactors covering both the at-power and 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.

The following section first describes the current safety case and plant items required for safe shutdown and cooling of all plant areas on the Dungeness B site. The second part of the section is where the evaluation of robustness of the Dungeness B plant is described.

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 (defined as an earthquake with a return frequency of once in 10,000 years (10^{-4} p.a.) 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. Note also that it is very likely that much of the other plant would survive an event and that the operators are instructed to use the most appropriate systems that remain available and therefore the following description of protection presents the worst case assumptions.

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 Dungeness B for a frequent event is taken to be one with has an assumed peak ground acceleration of 0.1g Principia Mechanical Ltd Spectrum, this being more conservative than the site specific frequent uniform risk spectra.

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 the 0.1g Principia Mechanical Ltd, where reasonably practicable. This ‘second line’ plant and the safety case that surrounds it is not discussed further in this report, since the focus of this review is on the extreme events.

Essential Safety Functions

Table 2.4: Equipment claimed to provide essential function following infrequent event

Essential Function		Equipment Qualified Against Infrequent Event
Reactor Trip		Guardline equipment
Reactor Shutdown		Main shutdown system
Pressure Boundary		Pressure vessel and penetrations with claim on gas circulator seals
Post-trip cooling	Boiler venting	A boiler vent route
	Boiler Feed	A post-trip feed system
	Gas Circulation	Natural circulation (pressure support via CO ₂ injection is available if required)
	Vessel Cooling	Back-up vessel cooling system
Monitoring		Alternative monitoring location and control room

The following summarises the function and operation of the systems identified in Table 2.4.

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 main shutdown system is assured.

Post Trip Cooling

The bottom line post trip cooling protection is based on natural circulation with boiler feed provided by direct diesel-driven boiler feedwater system, whilst pressure vessel cooling is provided by a further cooling water system.

Gas Circulation

Primary Circuit Cooling is based on natural circulation, which relies on ensuring suitable primary circuit pressure. It is therefore necessary to demonstrate that the primary coolant pressure boundary remains secure, such that there will not be a significant loss of gas following seismic events, and that the natural circulation of gas through the core will not be impeded by damage to the structures internal to the pressure vessel, including the core itself.

The safety case demonstrates that all the pressure boundary components, namely the pressure vessel, penetrations and large- and small-bore pipework, are capable of withstanding the infrequent seismic loading. In order to maintain the pressure boundary, the gas circulator seals must remain effective; this is achieved by either the running seal or the stationary seal. Both seal systems require pressurised oil systems to be active, which are also qualified against an infrequent earthquake.

The modelling for natural circulation cooling assumes that the normal gas flow paths around the circuit remain unaffected. As discussed above, 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.

Pressure Vessel Cooling

The vessel cooling system (using back-up pumps) and its heat sink are seismically qualified to withstand infrequent level events and ensure the integrity of the pressure vessel.

Boiler Feed

The direct diesel-driven boiler feedwater system is a once through high pressure feed system and is qualified to withstand the infrequent level seismic event. The boiler discharge route is via safety relief valves, which are also qualified against the infrequent event. Natural circulation relies on feed being provided to at least two of the four boiler quadrants.

Monitoring

In general, the equipment in the control room has not been functionally qualified to withstand a bottom line seismic event, and is not claimed as essential plant, although the control room is expected to remain habitable. Should for any reason the control room need to be evacuated, there is an alternative monitoring location and control room providing a single area from which the status of the trip, shutdown and post-trip cooling of the two reactors can be monitored.

The alternative monitoring location and control room provides the operators with post-trip indications and has been designed to withstand the infrequent level event. The alternative monitoring location has an uninterruptible power supply which is also seismically qualified. Local plant indications may also be available but are not claimed for the infrequent seismic event.

Electrical supplies

The majority of the plant claimed by the safety case to mitigate against seismic hazard is powered from two separate diesel generator backed seismically qualified systems. There is defence in depth in that both systems can supply the gas circulator oil systems, which gives added confidence in the operation of these systems, which are required to ensure the reactor pressure boundary following the seismic event.

One of these diesel generator backed seismically qualified power source supplies the control and instrumentation for the diesel driven feed system, and the CO₂ make-up facility.

Safety-Related Buildings

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.

Essential Stocks

The safety approach at EDF-Energy stations requires that sufficient stocks of consumables are held to enable essential functions to operate for at least 24 hours. Replenishment of stocks to enable the essential plant to continue operating is expected to commence within the 24 hour period, as discussed in Section 2.1.2.3.3 below. All essential stocks and associated systems have been qualified to Bottom-line level. These are:

- Water for boiler feed.
- Water stocks for essential equipment cooling.
- Fuel oil for back-up generators and the direct diesel feed system.
- Liquid CO₂ for the CO₂ make up plant.

Minimum quantities of these essential consumables, to ensure a 24 hour mission time, have been determined and are specified in the relevant Technical Specifications. Replenishment of stocks will commence within 24 hours. See Chapter 6 for discussion of emergency arrangements.

2.1.2.1.2 Shutdown Cooling

When a reactor is tripped and the 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.

The bottom line post trip cooling described above is also claimed for the scenario where a seismic event occurs when a reactor is shutdown. For a shutdown pressurised reactor, natural circulation is available straightaway. However, during a reactor outage, 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 normally provided by forced gas circulation. Following a seismic event, forced gas circulation may be lost and therefore cooling can only be achieved through natural circulation. With the reactor shutdown in a depressurised state (either in air or CO₂) cooling by natural circulation is not possible. Recovery from loss of forced circulation on a depressurised reactor would require resealing of any open penetrations and repressurisation of the reactor to a level which supports adequate natural circulation cooling.

The shutdown safety case describes the various penetrations that could be opened during a shutdown and the activities required to complete reseal and repressurisation. The case is based on permitting penetrations to be opened once the decay heat has reached a level where it can be demonstrated that for all of the required reseal operations, sufficient time exists to complete the actions and repressurise the reactor before a safety limit is reached. All of the plant claimed during the reseal activities is qualified against the hazard and will remain available, these include:

- Electrical supplies
- An air extract system to maintain adequate environmental conditions local to the reactor
- Service air from a local compressor
- Emergency lighting
- Required lifting equipment.

The arrangements and required actions are detailed in Recovery Plans and post-fault recovery procedures with nominated reseal teams available to enact the reseal operations within the required time.

Once the reactor is resealed it is repressurised using the CO₂ system. Sufficient CO₂ is available in the tanks to repressurise one reactor and to maintain the pressure support to both reactors for the mission time of 24 hours. Additional stocks of CO₂ will be delivered to site within the 24 hour time period. This is discussed further in Chapter 6.

2.1.2.1.3 Fuel Route

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

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

- Handling with fuelling machine – forced cooling may be lost but natural cooling maintains acceptable fuel temperatures;
- Buffer storage - cooling systems are seismically qualified
- Dismantling - loss of cooling is tolerable as natural cooling is adequate
- Storage in ponds - 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 design basis earthquake and assessment of potential safety margin.

The severity of the earthquake used in the safety case to represent the infrequent design basis earthquake with a return frequency of 1 in 10,000 per year 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 Design Basis earthquake have been qualified using conservative methods (referred to in Section 2.1.2.1).

Conclusion DNB 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 this situation. The actions on indication of seismic activity are described in Station Operating Instructions. There is a seismic alarm in the control room to alert the operators to seismic activity. These actions have been reviewed as part of the safety case production to ensure that sufficient time is available to complete the tasks.

2.1.2.2.1 Operating reactor

Trip

If plant faults which would normally lead to automatic trip do not successfully result in a reactor trip then there are two lines of operator trip available via the guardlines. The operator can perform this action in the control room and the safety case conservatively allows ample time for this to occur. Following a less significant seismic event the operator will assess the plant damage and proceed with a controlled shutdown.

Shutdown

Operation of the main shutdown system is completely fail-safe and requires no operator action. As part of the post-trip actions the operator will attempt to confirm that the control rods have entered the core.

Post-trip cooling

Manual initiation of the direct diesel-driven boiler feed system, either from the control room, alternative control room or local to plant is claimed as described in Section 2.1.2.1.1. Feed stocks are available for 24 hours provided that manual flow cutback is implemented. Local indications of boiler feed flow rate to each boiler are available. Additional feed supplies can be sourced from back-up systems using temporary hoses connected to the feed tanks.

The operators are required to engage the stationary seal. If the stationary seal oil pump is not running on a gas circulator then the seal can be applied using a temporary hose from an adjacent operational gas circulator stationary oil system. There are several hours available to complete this.

The reactors are expected to remain pressurised and therefore pressure support should not be required. All penetrations and connections with refuelling equipment have been seismically qualified including all small-bore reactor gas lines, e.g. instrument lines and burst can detection pipes. However, whilst there is no specifically identified likely failure site, the safety case allows for a limited reactor pressure boundary breach, and the CO₂ make-up supplies are seismically qualified.

Equipment cooling is provided by a back-up cooling water system. Operator action is required to operate isolation valves to connect this system to the normal equipment cooling ring main, although this does not have to be done immediately.

2.1.2.2.2 Shutdown Cooling

The operations on a shutdown reactor are broadly similar to those for a reactor at power, except when reseal and repressurisation is required. This scenario is discussed in Section 2.1.2.1.2.

2.1.2.2.3 Fuel Route

See Section 2.1.2.1.3 for details of the fuel route systems.

2.1.2.2.4 Summary

The actions identified above may need to be carried out in conjunction with actions from a number of other procedures. The number of actions would be increased if one of the reactors is shutdown and depressurised or if unexpected failures occurred. Measures have been put in place to ensure the availability of additional staff for resealing and re-pressurising a shutdown and depressurised reactor. Human factor reviews have also been carried out in support of the at power and shutdown reactor seismic safety cases. The second periodic safety review in 2007 did not identify any concerns relating to the ability of the operators to carry out the actions in the required timescales.

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

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

2.1.2.3 Protection against indirect effects of the earthquake

2.1.2.3.1 Assessment of potential failures of heavy structures, pressure retaining devices, rotating equipment, or systems containing large amount of liquid that are not designed to withstand design basis

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

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

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

Seismic Assessment of Interactions

Seismic interaction is the physical interaction of any structures, piping or equipment with a nearby essential plant item caused by the relative motions from an earthquake. An item of plant or structure that could pose such a threat to an essential system is commonly known as a seismic interaction.

Seismic interactions were identified during a seismic walkdown of the essential systems. There are numerous types of interaction, for example, pipework/valves, cranes/lifting hoists, electrical cabinets, cables and cable supports. Other types of interaction are the buildings themselves or other associated structures, for example firebreak walls, masonry walls, walkways/platforms. Unrestrained items such as trolleys and storage cabinets can be noted as interactions. Heating, ventilation and air conditioning systems and fire fighting pipework are also a potential spatial hazard.

Other types of plant were also investigated that could cause additional hazards initiated as a consequence of seismically induced loads, for example pressurised tanks of cold gas could lead to missile generation or the flooding with freezing and or toxic/asphyxiant gas. Other storage tanks were also investigated with reference to the risk from consequential flooding and risk of fire.

Where issues were identified during the walkdowns, they were appropriately addressed. The general approach to the qualification of the majority of seismic interaction hazards was to secure the anchorage or support for the item, or to increase its structural flexibility to allow the postulated seismic movements without resulting in damage to nearby essential plant.

Missiles

The only significant source of missiles identified was disintegration of the rotors of the main turbines. Worldwide experience reported in a survey of the performance of 91 steam turbines (experiencing seismic events with assessed horizontal accelerations in the range 0.1g to 0.6g) is that turbines are not seriously damaged and missiles are not generated. Although direct seismic damage to the turbines is therefore judged unlikely, there is the possibility of a seismically induced fault condition leading indirectly to turbine disintegration. If the seismic event results in a loss of grid with the reactor and turbine not being immediately tripped, then the turbine speed could increase in response to the loss of load. This scenario was judged to be an infrequent sequence, requiring only one line of protection.

The turbine is protected by a governor, which should trip the turbine if it fails to control the increase in speed, and by two mechanical over-speed bolts. Only the mechanical bolts system is claimed for the seismic case, and this has had a seismic review, noting that the system is designed for high levels of vibration (as it is located close to the turbine) and is fail-safe on loss of hydraulic oil (or pipework breach).

Turbine over-speed bolts also protect against gross gas circulator over-speed and over-pressurisation of the pressure cylinder dome caused by turbine over-speed.

The only other source of potential missile generation caused by a seismic event is the failure of unqualified pressure vessels. It was concluded by the second periodic safety review that there was no credible threat to essential plant.

Seismically Induced Internal Flooding

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.

Buffer store cooling

Spent irradiated fuel transferred from the reactors and retained in the buffer store pending disposal is cooled by the pressurised CO₂ gas within the buffer storage tubes. The CO₂ gas is in turn cooled by circulating water systems using sea water as the ultimate heat sink. In the event of unavailability of this water cooling, a back-up cooling system can provide full cooling to the CO₂ gas in the buffer store tubes. In order to further support confidence in the security of the back-up system, a review has been conducted into the potential for issues to affect the availability of this water supply. The back-up cooling water is supplied to the buffer store system by pipework leading into the reactor building from a pumphouse located at the external secure water source (the lagoon). The only credible concern identified is of events such as earthquakes causing damage to the supply pipe (e.g. due to impact of collapsing structures, etc).

In the highly unlikely event of coincident loss of both the back-up and normal cooling water systems, there is scope for site engineers to arrange for temporary means to maintain cooling flow to the Buffer Store cooling system by use of available resources such as fire hoses and portable pumps. These ad-hoc arrangements would facilitate the priority recovery efforts to effect any necessary repairs to a damaged pipe, etc.

Conclusion DNB 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.

Consideration DNB 2.2: Consider investigating whether the single long small bore pipe providing the make up to the decay store could be vulnerable to interaction hazards.

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. Electrical supplies to essential equipment, including those supporting fuel route safety functions, are provided by seismically qualified supplies. On this basis loss of grid is not significant as the grid-only powered systems are not claimed to be available following a seismic event.

The safety case approach in EDF Energy is to ensure that adequate stocks of consumables are held on site to last at least 24 hours. This includes boiler feedwater, CO₂, and diesel generator fuel. The usual approach is for the minimum stock levels quoted in technical specifications to be those that correspond to this 24 hour 'mission period'. It is implicit in the safety case that company emergency arrangements would provide replacement consumables within the 24 hour period to enable the plant to be managed safely. Note that in general, normal stocks levels are higher than the limits specified in the specifications, therefore the most probable scenario would be that more than 24 hours would be available to replenish consumables.

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

Conclusion DNB 2.5: Consequential loss of grid has been considered as part of the safety case. Electrical supplies to essential equipment are provided by two sets of 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. The review of emergency arrangements is discussed in Chapter 6.

A review of site access following external hazards has been carried out. A survey of the approaches to site was completed and the review concluded that potential blockages would be limited such that arrangements for rapid access to appropriate plant and equipment for temporary repairs and clearing earth, rubble, trees, etc, would allow a route to be re-opened within the 24 hour mission period. It noted that limited differential settlement could not be ruled out at Dungeness during an extreme seismic event. However, whilst some damage to local roads constructed on shingle in the vicinity of Dungeness B was possible, it is expected to only ever be limited in extent and severity and not to render the roads un-passable.

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

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

Conclusion DNB 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).

To claim a system as seismically qualified, along with the qualification of the essential plant, it also must be demonstrated that the system is not threatened by any seismic interactions.

Steam Release

Steam pipework is not considered essential plant for the seismic safety case; the route for the release of steam being considered of secondary importance once the water has passed through and cooled the boilers. Steam release may potentially disable electrical plant, feed control valves, boiler depressurisation valves and the gas circulator oil systems, and hence a number of modifications have been being undertaken to protect the plant.

Walkdowns of the steam pipework were completed to support the safety case and all of the large bore pipework was found to be acceptable for the infrequent event. Also, the majority of the small bore pipework as originally designed and installed was shown to be acceptable for the infrequent event. Although the seismic safety case is tolerant of the simultaneous failure of a few small-bore pipes the small-bore pipes have been modified to remove any seismic vulnerability.

Worldwide experience of welded pipework which is exposed to seismic events is that damage in earthquakes is very rare and, failure of more than a very small number of steam pipes as a result of an earthquake would not be anticipated. The likelihood of such failures including any pipework, for which failure is claimed to be incredible, is therefore very small, particularly so as the Incredibility of Guillotine Failure welds in this pipework are subject to enhanced inspection and acceptance criteria.

Hot Gas Release

To support natural circulation the safety case cannot tolerate significant leakage and thus appropriate qualification of the pressure boundary has been undertaken. Therefore, the effect of a hot gas release as a consequential hazard need not be considered further.

Cold Gas Release

The effects of cold gas cloud dispersion on the essential plant were not shown to be significant.

Seismically Induced Fire

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

Conclusion DNB 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 DNB 2.3: 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 a 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. The tool available to carry out these checks is a database of all the equipment on site, identifying the level of hazard qualification and the means by which the equipment has been qualified.

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 inspections. Specific entries are included in the maintenance schedule for selected plant items and for a number of the systems, safety system reviews are also specified. The reviews are included on the maintenance schedule and are carried out at frequencies of between three and five years, depending on the system.

Seismic walkdowns have been added to the maintenance schedule at Dungeness B.

The review carried out as part of the within design basis evaluation referred to in Section 2.1.3.4 below, also identified a lack of fleet guidance on housekeeping standards.

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

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

The equipment needed to reseal the reactor (as discussed in Section 2.1.2.1.2), including an air compressor, will be assembled before penetrations are opened. It is a requirement of the safety case that this air compressor is subjected to a seismic walkdown by suitably qualified and experienced personnel to demonstrate it will remain functional after a seismic event.

Each gas circulator has a seismically qualified stationary seal oil system. If the stationary seal oil pump on a gas circulator failed, the stationary seal could be closed using interconnecting hoses to an adjacent circulator's functioning seal oil pump. These hoses are stored on a trolley and kept local to the plant.

2.1.3.3 Potential deviations from the 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.

Where areas of concern are identified they are captured and tracked using the Company's corrective action and work planning processes. No significant issues, concerning both bottom line and second line equipment, worthy of highlighting in this report were identified.

Conclusion DNB 2.8: There are no significant issues identified with the seismic safety case.

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.

Mandatory Evaluation

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

Within design basis evaluation

Scope

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

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

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

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

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

Conclusion DNB 2.9: The reviews undertaken as part of the within design basis evaluation, and the actions identified therein, have confirmed that Dungeness B is compliant with the current licensing basis, although a few improvements have been identified.

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

2.2 Evaluation of safety margins

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

The nuclear safety principles also state that the integrity of protection against the infrequent External Hazard should ideally be demonstrated with a margin that could be argued to accommodate an appropriate more severe level of

hazard. This is included to ensure there is no 'cliff edge' such that in the event of an earthquake slightly more severe than the design basis earthquake, unacceptable consequences would not occur.

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

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

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

The justification for this assertion lies in the concept of seismic fragility functions. Figure 2.3 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 analysis. 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. A high confidence in the low probability of failure acceleration value is set such that there is a high confidence (95%) of a low probability (5%) of failure. In practice this implies an overall probability of failure at the high confidence in the low probability of failure value of 1%. For new plant that is designed to resist earthquakes, the more onerous design code requirements imply a probability of failure of less than 0.1%.

So in Figure 2.3 below, the high confidence in the low probability of failure value is a peak ground acceleration of 0.2g. If plant has been qualified, it is taken that the level to which the plant is qualified is the earthquake at which the plant should not fail, i.e. there is a low probability of failure, and this corresponds to the concept of the high confidence in the low probability of failure value. Thus plant qualified to 0.2g, effectively has a high confidence in the low probability of failure value of 0.2g.

The important point here is that the shape of the curve for systems which have been designed with a seismic capability tends to be similar, although the curve will be shifted to the left or right depending on the level of earthquake for which the plant has been designed. Inspection of Figure 2.3 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.

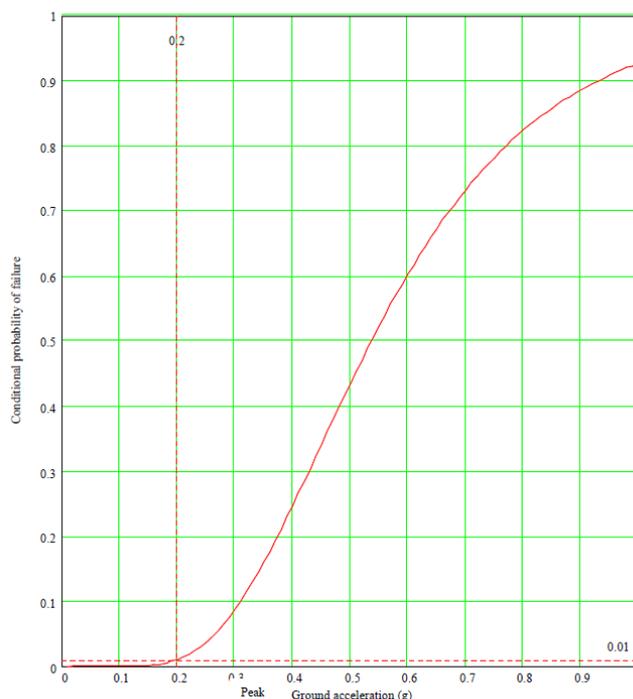


Figure 2.3: Mean Fragility Curve for typical System Qualified to 0.2g peak ground acceleration.

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

Conclusion DNB 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

Reactor Structures and Bottom Line Systems

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 Dungeness B is 0.21g peak ground acceleration. The seismic hazard assessment reports for the site indicates that this increased level of ground motion has a frequency of between 1 in 100,000 and 1 in 1,000,000 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 be 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 DNB 6.2 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.

The qualification of equipment has been carried out using conservative methods. In some circumstances these conservative methods when first applied have indicated areas of concern which required more detailed analysis to demonstrate adequate performance against the design basis earthquake and 'high confidence of low probability of failure'.

One such case is the pressure vessel at Dungeness B. Each pre-stressed concrete pressure vessel sits on a castellated support wall that is cast integral with the foundation raft. The bottom of the vessel includes a circular support ring of mean radius approximately 8 m and a thickness of approximately 1 m. The vessel and the support wall are separated by rubber bearing pads that are designed to transmit direct thrust and accommodate lateral movement of the vessel due to pre-stress, pressure and temperature. The calculated movements of the vessel are relatively large because of the flexibility of elastomer support pads. This in turn leads to potential vulnerabilities of any attached items such as penetrations and gas circulators for more severe events. It is judged therefore that one of the first items to fail in a significant Beyond Design Basis event would be the vessel or multiple penetrations.

As mentioned previously, post-trip cooling relies on maintaining the reactor pressure boundary such that natural circulation can be supported. If the vessel fails or multiple penetrations fail then natural circulation could not be achieved. In these circumstances it is likely that the response actions outlined in severe accident guidelines would need to be invoked (see Chapter 6).

2.2.2 Range of earthquake leading to loss of containment integrity

Advanced gas-cooled reactors 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 Dungeness B Power station 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 Dungeness 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. On this basis the shingle bank is not formally seismically qualified (although gross failure is unlikely to occur).

The other sources of flooding considered at Dungeness B 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 flooding risk at Dungeness 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 DNB 2.12: There is not a credible risk posed to UK plant from a beyond design basis earthquake and consequential beyond design basis flood.

2.2.4 Potential need to increase robustness of the plant against earthquakes

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

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

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

The beyond design basis evaluation

Scope

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

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

Summary of findings from the beyond design basis evaluation

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

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

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

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

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

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

Consideration DNB 2.5: Consideration should be given to enhancing the robustness of pond cooling systems within the advanced gas-cooled reactor fleet.

2.3 Summary

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

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

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

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

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

Chapter 3 – External Flooding

Dungeness B

3 External Flooding

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

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

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

Overview

In line with the statement quoted above from the ONR report, the Stress Test focuses on the External Flooding hazard. Within EDF Energy Nuclear Generation, the External Flooding hazard is defined as 'Extreme rainfall, snowmelt, 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 beyond the scope of this report. Any further references to floods in this report concerns the external flooding hazard.

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

- The sea defences are adequately sized to maintain essential function availability during the Design Basis Sea States.
- During extreme rainfall events the predicted maximum site flooding level is conservatively calculated to be 5.54m Above Ordnance Datum (AOD). Essential function availability is maintained by the action of the passive site drainage system and drainage of water through the shingle.
- The methodology used to calculate the design basis flood for Dungeness B has been conservatively constructed using independent expertise based on well regarded sources of information.
- The methodology for determining the design basis flood and the 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.
- Although the equipment needed to maintain the essential safety functions are qualified against the design basis flood, the margin to failure has not been explicitly derived. For the purposes of beyond design basis risk management a consideration has been raised to quantify the physical margin to failure.

3.1 Design Basis

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

3.1.1 Flooding against which the plant is designed

The International Atomic Energy Agency (IAEA) recommends that the “plant layout should be based on maintaining a ‘dry site concept’, where practicable, as a defence-in-depth measure against site flooding.” 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.

The characteristics of the Design Basis Flood at Dungeness B are described below based on a frequency of occurrence of 1 in 10,000 per year, defined as an infrequent event. For Dungeness B the design basis flooding events considered are:

- Maximum rainfall and snowfall.
- Overtopping of the sea defences for the following extreme sea states:
 - Combined extreme wave height and still water level.
 - Combined wave height and extreme still water level.
 - Combined extreme swell height and still water level.
 - The probable maximum tsunami event (at high water spring tide).
- Outflanking of sea defences.

There are no reservoirs in the vicinity of the station which could introduce floodwater into the site.

Dungeness B was the first commercial scale advanced gas-cooled reactor power station to begin construction and is located on the Dungeness headland in the south east of Kent, England. In order to describe the characteristics of the design basis flood, a description of the site is required; this is detailed in Chapter 1. The general level of the reactor building and turbine hall is at 5.5m AOD and the site is higher than the surrounding land. The design basis flood states have been calculated as:

- Extreme sea states are bounded by the maximum tsunami (at high water spring tide) at a level of 8.7m AOD. This would result in a minimal amount of water overtopping the shingle bank.
- Rainfall for a 1 hour storm (the bounding case) produces on-site flooding to a maximum height of 5.54m AOD.
- The threat of snowmelt is judged to be bounded by rainfall.

3.1.1.2 Methodology used to evaluate the design basis flood

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 design basis for Dungeness B was for 1 in 250 year tide and storm surge events. This was substantially revisited in an updated flooding safety case in 1994, the details of which are presented below.

Rainfall

Rainfall data was collected from many different locations throughout the UK and using statistical analysis the total rainfall as a function of return frequency was determined (see Figure 3.1). The short duration extreme rates of rainfall are in excess of the design capacity of the surface drainage system and therefore some flooding would be expected to occur.

The flood height associated with the infrequent rainfall flooding event was determined by using a three-dimensional computer model of the site. The model was used to determine the height of flood waters conservatively assuming that no surface flow to the surrounding lower lying areas occurred. The volume of water remaining and therefore the height of water on site was calculated as the total rain falling on the site less the water lost through the drainage pipes, soakaways and infiltration to the shingle. Loss of grid and therefore surface water pumps was assumed. It was found that a one hour storm caused the highest flood water, as the intense rainfall is greater than the drainage capacity. For longer duration storms, where a greater total volume of rainfall is predicted, and for more frequent events, the rate of rainfall is less than the design capacity of the drainage system. The loss through soakaways and the shingle is greater than the rate of rainfall and therefore flooding would not be expected.

The calculation to determine maximum flood heights was last performed in 2010 following some changes to the site layout. The flood level following a one hour infrequent rainfall was determined to be 5.54m AOD. This calculation includes much conservatism; including assuming no flooding of open spaces below buildings or within trenches occurs.

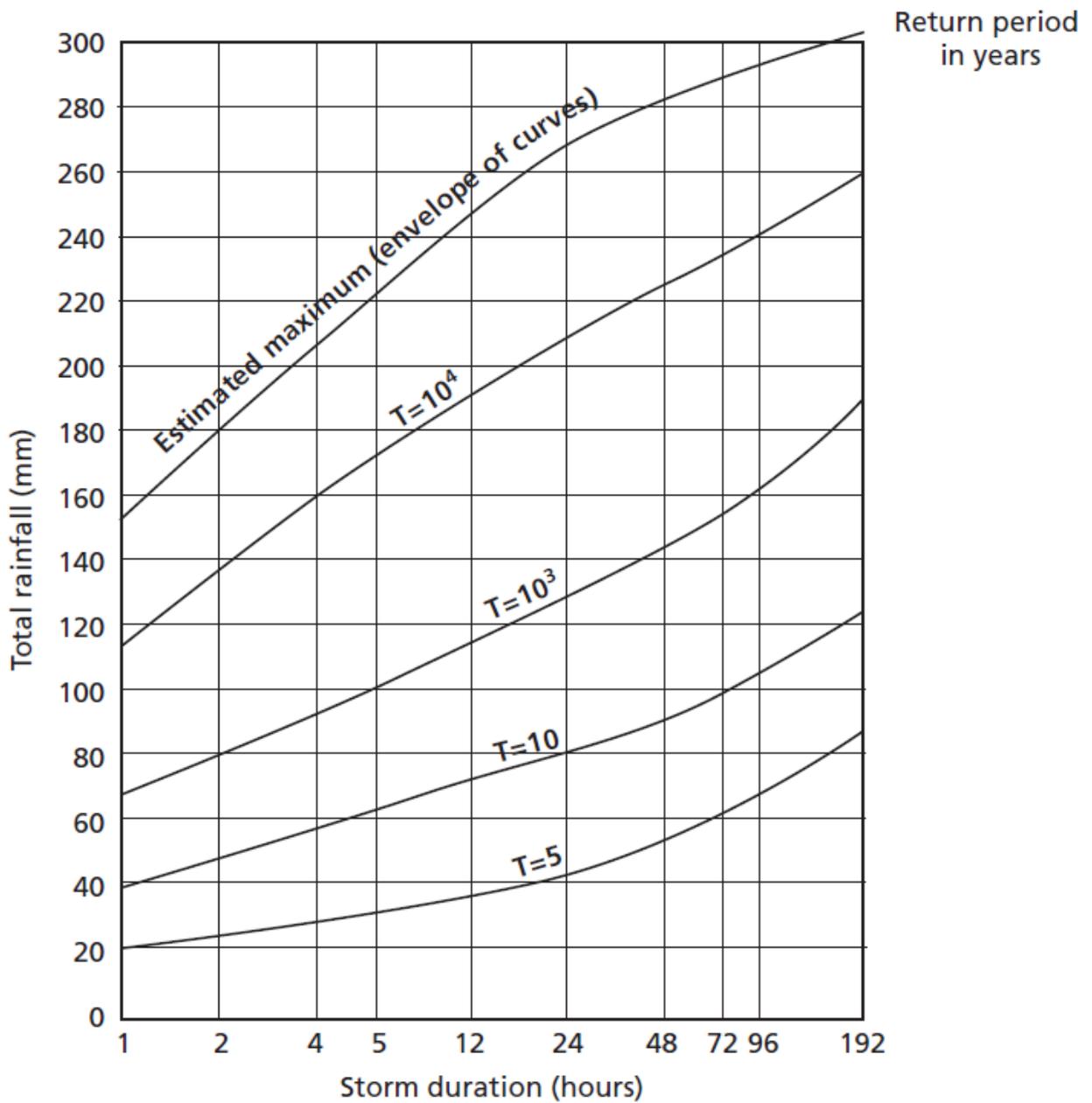


Figure 3.1: Total Rainfall for duration and return period for Dungeness.

Snowmelt

The flooding hazard from snowmelt was derived by considering the likelihood of significant snowfall coincident with a high groundwater level (which is influenced by the sea still water level). The normal groundwater level is sufficiently low that the snowmelt would simply drain off into the ground and not flood the site. The argument was made that the occurrence of snowfall and extreme still water levels are independent events and so the frequency of snowmelt sufficient to flood the site is beyond the design basis.

Recent work has indicated that the snowfall calculations included in the safety case may not be conservative. Further work is being undertaken to assess the implications for snow loading of buildings (see Chapter 4) but in addition it will reconsider the flooding case from snowfall.

Extreme Sea States

As mentioned previously, the design basis sea states have been calculated by considering combinations of wave conditions, still water conditions, swell and tsunami. The derivation of each of these states and how they have been combined are addressed in turn below:

Extreme Wave Conditions

Due to the position of Dungeness, being exposed to long westerly fetches over a bay where refraction effects may be important, it was necessary to derive, in effect, two wave climates and to combine them. The climates required are those for wave generation and for wave refraction and shoaling. The wave sets were then vectorially summed to obtain the predicted wave climate at Dungeness. Both climates were obtained using two commonly used computational models. A summary of the results are shown below.

Table 3.1: Extremes of Wave Height. The most significant waves come from the South and the West; hence the external flood defences are more extensive in this direction.

Return Period (years)	Wave Height (m AOD) by Direction (°N)			
	All	90-140	140-205	205-270
1	3.20	1.05	3.20	1.59
10	3.86	1.32	3.84	1.79
100	4.46	1.55	4.44	1.93
1000	5.01	1.77	4.98	2.05
10000	5.52	1.97	5.50	2.15

Extreme Still Water Conditions

The still water levels or tidal conditions were based on twenty years of recorded data from Dover (1971-1990). This was adjusted to be valid for Dungeness by adding the predicted astronomical tides at Dungeness and the modified surge levels from Dover. In order to obtain the astronomical tides, the harmonic constituents for Dungeness were required. Water level records taken at Dungeness for the period July 1983 - May 1985 were analysed and Astronomic tides at Dungeness for the full period of recordings at Dover were then calculated and by adding the modified surge levels from Dover, 20 years of combined surge and predicted tides were obtained and an extremes analysis provided the extreme values of total water level and surge level for the site which are shown in Table 3.2.

Table 3.2 lists water levels for various directions and return periods, the directional component is as a result of the surge. The maximum still water level is predicted to be 5.44m AOD for the infrequent event.

Table 3.2: Extremes of Still Water

Return Period (years)	Still Water Level (m AOD) by Direction (°N)			
	All	90-140	140-205	205-270
1	4.49	4.17	4.31	4.46
10	4.75	4.45	4.47	4.65
100	4.94	4.70	4.76	4.94
1000	5.19	4.94	5.04	5.19
10000	5.44	5.18	5.32	5.44

Joint Probability of Waves and Water Levels

The most severe coastal events are generally as the result of the combination of high waves and high water levels occurring together. The joint probability of high waves and water levels occurring has therefore been studied.

The correlation between high waves and high water levels will usually lie between the two extremes of complete dependence, which would assume a 1 in 100 year event would comprise a 1 in 100 year wave coupled with a 1 in 100 year water level, and complete independence, which would assume a 1 in 100 year event would comprise a 1 in 10 year wave coupled with a 1 in 10 year water level. In reality the two will be partially dependent to an extent which is best determined from analysis of actual data. This analysis was undertaken using a computational program.

The joint probability analysis takes the hourly recorded wave and water levels from the time series data set and selects the wave heights at each of the high tides. A scatter diagram relating high tide levels and simultaneous wave height predictions is produced giving the relationship between the wave and water levels. Probabilities are then extrapolated to extremes, using standard extrapolation methods, firstly by fixing the water level and calculating wave heights and secondly, by fixing wave heights and calculating water levels. The extremes of wave height and water level are then plotted on a graph and smooth curves fitted linking combinations of waves and water levels with equal return frequencies. An example of these graphs is given in Figure 3.2.

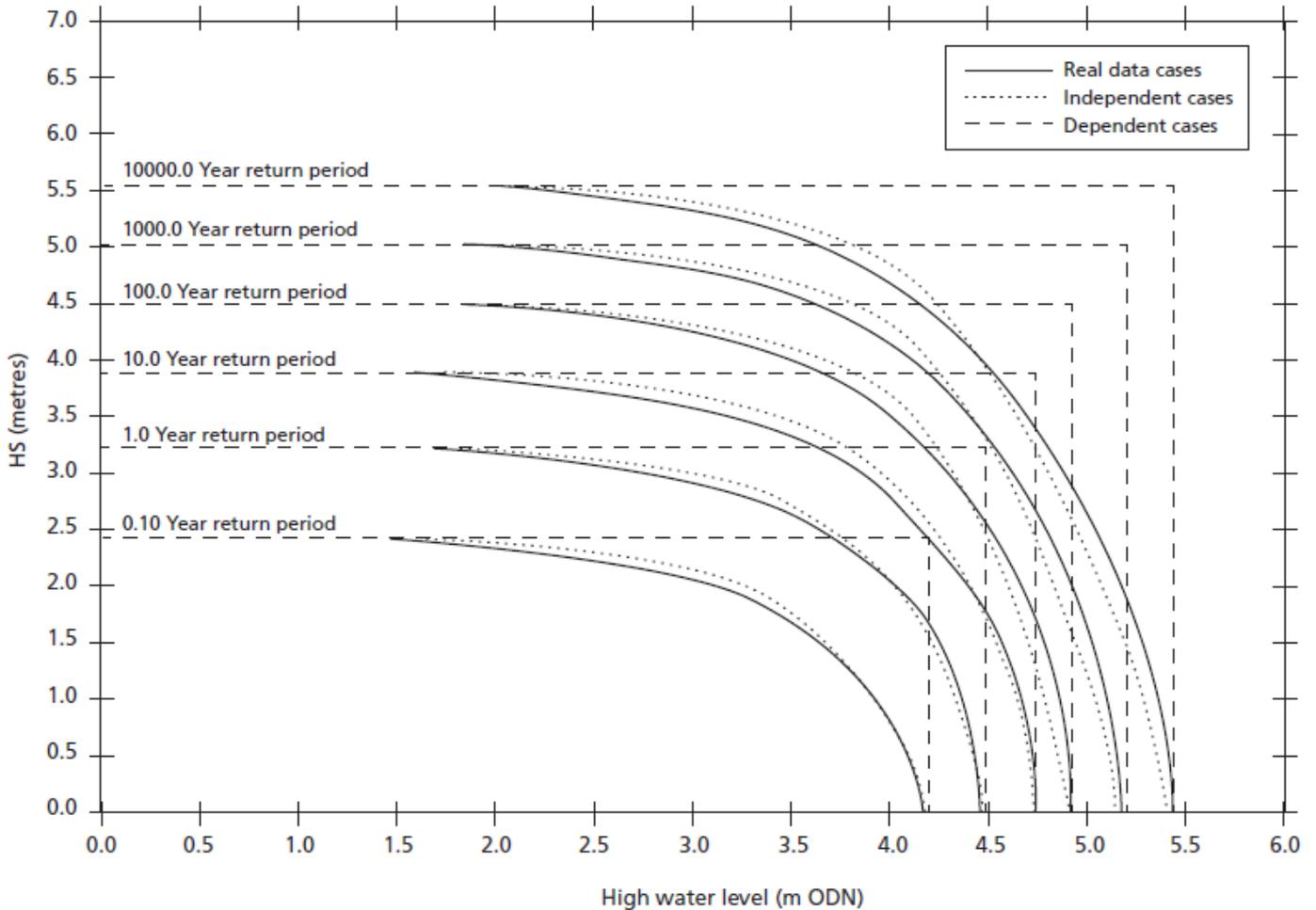


Figure 3.2: Extremes of wave height and water level. The total extreme sea height can be calculated by the addition of the high water level and the wave height (Hs). Note: Ordnance Datum Newlyn (ODN) is the same as AOD used in the rest of the report.

Swell

Swell is long period wave energy not directly related to recent or local wind conditions. It may be due to decaying storms generated several days previously. Although swell wave heights are usually small, the long wave period means that the associated run up and sediment transport may be significant. Swell may be generated in either the Atlantic or the North Sea and can be identified from wave records when the energy spectrum has two distinct peaks, the lower frequency one being the swell constituent. Single peaked spectra may also be indicative of swell when the energy is low frequency and the weather conditions are not appropriate to storm waves.

The methods used to derive a data set and extremes for swell waves at Dungeness are based upon a Met. Office model with results from Dover converted to Dungeness and extrapolated to extremes. The results are given below, where the swell wave height is used to calculate the run up. The total water height is calculated by combining the run up height and the Mean High Water Spring level of 3.6 m AOD.

Table 3.3: Extremes of Swell

Return Period (Yrs)	Swell Wave Ht (m)	Run Up (m)	Total Water Level (m AOD)
1	0.99	2.34	5.94
10	1.19	2.70	6.30
100	1.52	3.03	6.63
1000	1.72	3.32	6.92
10000	1.79	3.59	7.19

Design Basis Sea States

The table below gives a selection of the design basis sea states which were statistically derived and represent combinations of wave height, still water level and swell that occur with a return period of 1 in 10,000 years. Many other combinations exist and these are simply provided to give indicative values for the design basis sea state. These values were then used to assess the adequacy of the sea defences which are described in Section 3.1.2.2.

Table 3.4: Design basis sea states

No.	Description	Significant Wave Height (m)	Still Water Level (m AOD)	Period (s)
1	Combined extreme wave height and still-water level	5.45	2.0	9
2	Combined wave height and extreme still-water level	2.6	5.0	6.3
3	Combined swell height and still-water level	1.79	3.6	14.5

Flooding risk from tsunami

Tsunamis are long period waves that are produced from geological rather than meteorological events, principally submarine earthquakes, but also volcanic activity and submarine or shoreline landslides. A pessimistic estimate of the height of a tsunami at Dungeness B was derived based on a review of historic tsunamis along the south coast of England. The maximum tsunami height recorded was estimated to be approximately 3m (above the normal sea level) at the entrance to the English Channel from the 1755 Lisbon Earthquake. It is worth noting that no evidence of similar wave heights from this event were found for the Dungeness area, which is therefore a conservative assumption.

Based on the timescale over which records existed this event was estimated to occur with a return frequency of 1 in 1,000 years. To derive the height of the infrequent 1 in 10,000 year event the conservative tsunami wave height was combined with the mean high water spring tide level of 3.6m AOD (which exists for much less than 10% of the time). The tsunami wave is assumed to be amplified by a further 2.1m as a result of shoreline interactions giving an overall tsunami wave height of 8.7m AOD. The overtopping of sea defences with various profiles and heights was modelled assuming this maximum wave height. Very limited overtopping of an 8m AOD shingle bank was shown to occur and therefore the sea defences were built up to in excess of this level.

At around the time of the second periodic safety review, the Department for Environment, Food and Rural Affairs (DEFRA) commissioned two assessments of the tsunamis threat. The first of these assessments into the threat posed by tsunamis concluded that threats were possible from a number of sources (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). The follow-up study reviewed in more detail the hazard for the UK and Irish coasts associated with the Lisbon-type event and the North Sea event. It concluded that, only the most south-westerly coast of the UK may incur sea level elevations marginally in excess of the 1:100 year extreme sea level predictions.

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

The safety case has not been updated to take account of this assessment. An update to the safety case to reflect the latest assessment of the risk of tsunamis at Dungeness is raised as a consideration by this report.

Review of Flooding risk from Outflanking

An additional source of potential flooding has been identified for the site, this being flood water arising from a breach of the sea defences to the West of the site with the resultant seawater outflanking the shingle beach fronting the Station and flooding the site from the westerly direction.

The shingle beach approximately ½ km from the western boundary fence is known to have been breached in the past, most recently during the winter storms of 1989/90. The shingle beach in the area of the breach is not subjected to the beach feeding which takes place along the Station frontage.

The extent of the flooding was obtained from the Environment Agency. The records showed no evidence of flooding directly on the Station site or in its immediate vicinity, however flooding elsewhere in the local area was quite extensive covering some 12-13km² and extending 3km inland. It is judged that the effects of more severe storms would be to cause more extensive flooding rather than flooding over a similar area but to a greater depth. This is supported by surveys of the backshore area of the Denge Marsh which show that there is little difference in the level of the shingle with the only increase being inside the site boundary fence south of the switch house. (The general site level is in excess of 5.5m AOD whilst the level of the shingle in the backshore area varies between 4.75m and 5.5m AOD).

The boundary to the west of the Station includes the site access road and car park which are raised above the level of the shingle to a height of 6.0m AOD. This can be regarded as providing a barrier and protection against the spread of shallow flood water.

Historical reports indicate that the seawater inundation took place only at high tides and that the total flooding was the result of over 12 hours of storm activity. This indicates that there is likely to be a significant amount of time from any initial flooding to flood water actually affecting the site.

Flooding from the East of the site is not considered to be a problem due to the significantly lower wave heights which approach from this direction (see Table 3.1). The still-water level would be essentially the same however the wave heights approaching from the East are significantly smaller than those from the South West due to the much shorter fetch lengths. The risk of flooding from this source is therefore far less.

Overall, flooding by outflanking is not considered to pose a significant threat to the Station. This is due to the very large area which would have to be affected before flood water would result on site and the long time judged to be required for any significant flood water to build up.

One of the back-up cooling water systems pumps water from lagoons near the site and the risk of outflanking on operation of this system, both in terms of the pumps and the mixing of seawater and other debris with the lagoon has not been considered in the safety case. The area around the Power Station is generally lower lying than the main Power Station site (OS maps show local spot heights of between 2 and 3m AOD and the pump house floor is 3.7m AOD). This issue is currently being addressed, however even if this back-up system was rendered unavailable, adequate cooling could still be achieved using the normal seawater system.

Climate Change Adaptation

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

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

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 in 1997.

More recent reports published by the Met Office in 2004 discussed the effect of global warming and climate change and show a global mean sea-level increase of between 40 and 140 mm from 2004 until 2020s confirmed by an IPCC study in

2001 predicting a mean global sea-level rise of a maximum approximately 130 mm by 2023. Another report produced by the Met Office provided similar information to that presented previously predicting a maximum global average sea rise of 140 mm by the 2020s with the assumption of a high emission scenario. The 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 Met 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 to wave and storm surge heights towards the end of the decommissioning period but this is many years in the future and the safety case demands will be very different.

For the second periodic safety review in 2007 more recent local sea level data was reviewed. The review concluded that the first periodic safety review estimate of 6mm per year (total rise of 180mm in the 30 year station life), on which the safety case is based, was conservative, and remained conservative until the end of the station operational life.

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 Dungeness 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 conservatism, 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.

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

Conclusion DNB 3.2: The flood defences at Dungeness B prevent the maximum credible tsunami resulting in damage to the plant.

Conclusion DNB 3.3: In line with Recommendation 10 of the Weightman Report, the design basis flood at Dungeness B has been confirmed, however further studies accounting for climate change have been initiated to reconfirm the design basis flood.

Consideration DNB 3.1: Consider updating the safety case to reflect the latest assessment of the risk of flooding due to tsunamis at Dungeness B.

Consideration DNB 3.2: In line with Recommendation 10 of the ONR report, flooding studies have been initiated for all eight stations. These studies re-evaluate the design basis flooding scenarios using the most recent data and taking account of climate change, they cover the period until 2035.

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.

3.1.2.1.1 Reactor at power

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

Table 3.5: Available Lines of Protection

Essential Function		Equipment Qualified Against Infrequent Event
Reactor Trip		Guardline equipment remains available
Reactor Shutdown		Main shutdown system
Pressure Boundary		Pressure vessel and penetrations with claim on gas circulator seals
Post-trip cooling	Boiler venting	All boiler vent routes remain functionally capable
	Boiler Feed	All post-trip feed systems remain functionally capable
	Gas Circulation	Forced primary coolant gas circulation or natural circulation
	Vessel Cooling	Vessel cooling system (using normal or back-up pumps)
Monitoring		Control room or alternative monitoring location

As external flooding events are often associated with high winds, grid supply is assumed to be lost as a result of this fault (but this is not claimed by the safety case).

With the exception of the grid dependent systems, all safety related plant is qualified against the infrequent event and this event is used to bound all higher frequency events. As described in Section 3.1.2.2, engineered barriers prevent water ingress to site from the design basis sea states and the maximum probable tsunami. Passive drainage systems and building thresholds ensure that the majority of the plant remains unaffected by extreme rainfall.

Trip

The guardline equipment (including control rod clutch relays, contactors and sensors) is located in buildings with sufficiently high thresholds to ensure that floodwater does not enter the buildings during any infrequent external flooding event. Reactor trip is not therefore affected by such events. An automatic trip is not expected as a result of an infrequent flooding event; the guardlines will remain available for manual trip (if required for operational reasons) or automatic protection for coincidental faults (such as loss of grid).

Shutdown

The main shutdown system has an extremely high reliability conservatively estimated as one failure per 100,000 operations. There is not a credible flooding risk to the main shutdown system from flooding as the equipment is located approximately 30m above the maximum flood level.

Post-trip cooling

Gas circulation

Gas circulation equipment is located in buildings not affected by an infrequent external flooding event. Two lines of protection remain available, forced circulation by gas circulators supplied by diesel generators or natural circulation. In the unlikely event that the normally used diesel generators are affected then sufficient forced gas circulation can be achieved using a second set of back-up diesel generators (located at a higher elevation).

Boiler Feed

Three boiler feed systems are provided.

- Following shut down, steam driven pumps are available to supply boiler feed and these are backed up by an AC powered system which takes over as steam supplies eventually become exhausted. None of this plant is at risk from extreme flooding events.
- A second boiler feed system supplied by diesel generators is also available. This system comprises equipment that is situated in locations that are not at risk from the infrequent flooding event.
- A third permanently installed and direct diesel-driven boiler feed system will also remain available. Again, this system comprises equipment that is situated in locations that are not at risk from the infrequent flooding event.

Vessel Cooling

The vessel cooling plant is located in an area unaffected by external flooding and will therefore remain available (both the main cooling pumps and the back-up pumps will be available). The heat-sink for vessel cooling is the seawater system which will remain available as the pumphouse threshold is above the infrequent flooding level.

Monitoring

Specific measures have been taken to address the threat of site flooding on the operation of systems at the alternative instrumentation monitoring location. The measures are:

- Location above maximum flood level.
- Provision of IP65 rated cubicles that can withstand jets of water from any direction.
- Provision of waterproof cables run in sealed cable trenches.

The building has a threshold of 6.55m AOD and the cubicles are on 150mm plinths with door openings a further 100mm above the top of the plinths. The equipment is not at risk from flooding.

The normal control room and all of the equipment associated with providing it with essential signals are also located above the maximum flood height and will remain available.

Two lines of post-trip monitoring will remain available during any infrequent extreme flooding event. Instrumentation local to the plant can provide a third line of post-trip monitoring if required.

3.1.2.1.2 Shutdown Cooling

As outlined in the section above, in the event of an infrequent flood it is expected that almost all systems will remain available other than grid based supplies. If the reactor is depressurised, forced gas circulation is necessary and electric motors backed by diesel generators will be available for this purpose. In the extremely unlikely event that the gas circulators fail, the reactor will need to be repressurised to establish natural circulation. All the equipment necessary to reseal (if required) and repressurise the reactor is expected to survive the flood, and may be operated without grid electrical supplies.

3.1.2.1.3 Fuel Route

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

Extreme external flooding could result in a loss of grid and therefore a loss of power to the pond cooling systems. Timescales to recover cooling are as per Chapter 1.

Conclusion DNB 3.4: There are appropriate lines of protection available for achieving and maintaining a safe shutdown state following a design basis flooding event. The flooding predictions need to be recalculated based on the best available techniques and information.

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

Sea Defence

The Dungeness B site is on the edge of an extensive flat shingle beach. The form of the ness has resulted from erosion in the south and deposition to the east.

The response of the beach to the design basis sea states was considered as part of the safety case. Modelling identified that a beach crest level of 8m AOD or above would limit the amount of water overtopping the defences to acceptable levels. In the mid 1990s the beach profile was built up to its current level of a minimum 8m AOD along its entire length. The crest is artificially maintained for about 875m west of the B station and up to a point just to the east of the A station boundary. The crest has been built up and is maintained to a minimum width of 12m in front of the A station, 20m in front of the B station reducing to 10m to the west. Figure 3.3 shows the height of the shingle bank in May 2010.

Between the shingle bank and the station frontage is an access road. To channel any water that overtops the shingle bank away from the B Station a 500mm bund wall was installed behind the access road in 1998. In addition a water tight gate was installed between the A Station and B Station. The A Station frontage is bounded by a 2m high reinforced concrete wall.

The seawater intake bund wall height (forebay and drumscreen wall) was raised specifically to contain the calculated water level rise due to the maximum tsunami (3m excluding the shoreline effects) and the mean high water spring level (3.6m AOD) described in the original safety case. The water ingress occurs due to rise in sea level in the forebay and drumscreen area from water entering through the intake tunnel. The measures described above prevent any significant quantity of seawater from entering the site, and therefore provides sufficient mitigation against the threat of ingress to the areas containing essential plant.

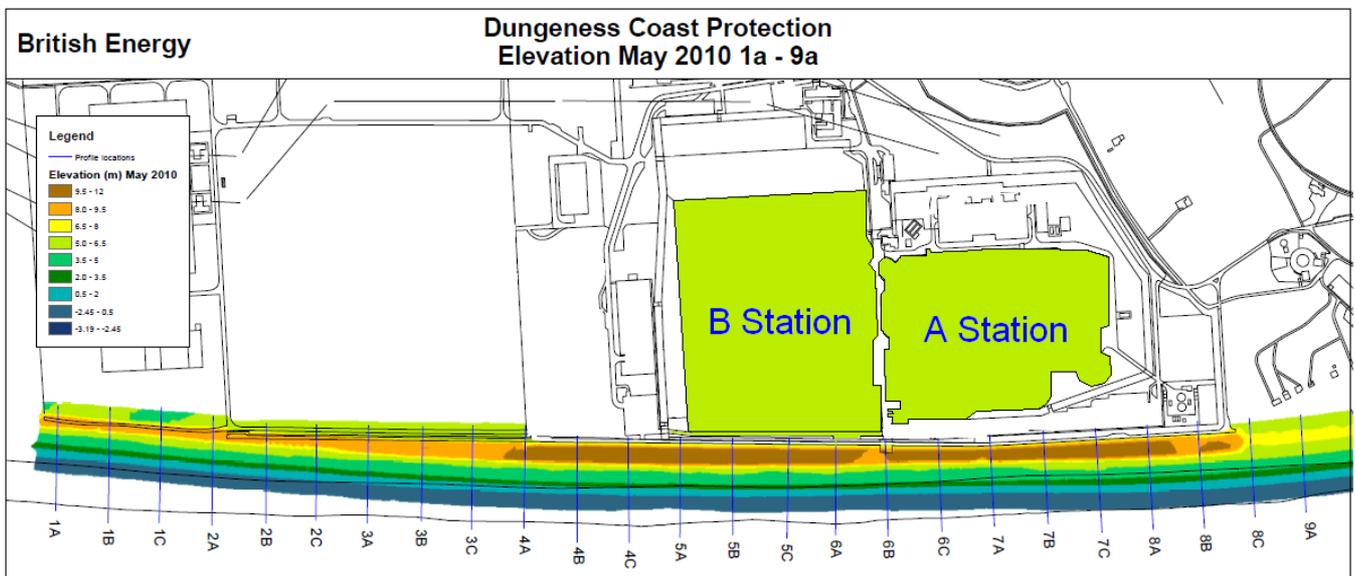


Figure 3.3: Dungeness Coast Protection



Figure 3.4: View of shingle bank looking east, showing access road, 2m high wall and end of bank as it tapers off just past the A station boundary.



Figure 3.5: View of shingle bank looking west at highest / widest point

Drainage System

The surface water drainage system collects all surface water from the site and discharges it to sea. All drainage originating from plant areas where there is a risk of contamination by oil is permanently routed to the site oil separator plant to remove the oil prior to discharge to the sea. However, the majority of the site drainage is through the main surface water drainage system which receives drainage from the roof drains, road drains, car parking areas and various sump pumps around the site. Water received into this system flows under gravity from the various legs of the system into a drainage main which directs it to the clean surface water section of the surface water pump house.

Under normal circumstances at periods when the sea level in the syphon recovery chamber is below the tidal flap on the drains outlet, the surface water pump house drains discharge under gravity. The tidal flap is fitted to prevent reverse flow of seawater from the syphon recovery chamber into the drain during a high tide. When the tide raises the level of water in the syphon recovery chamber the tidal flap will close and the surface water will back-up and overflow into the pump suction chamber. The pump suction chamber contains three automatically controlled pumps that discharge into the syphon recovery chamber at a level higher than any anticipated sea level. The pumps are arranged to discharge the full capacity of the drainage system, but are not designed to enable this flow coupled with a full oil/sprinkler water overflow conditions.

The discharge pumps are grid dependent so during the extreme rainfall event they are assumed to be lost. The drainage system will back-up until it reaches the level of a gravity fed surface water overflow channel, which carries excess water to the Dungeness A Station outflow.

In addition to the surface water drainage system there are a number of shingle soakaways on the south of the site that do not discharge in to the surface water drainage system. A certain amount of water also falls directly on to areas of shingle and so simply drains straight to ground.

Building Thresholds

The majority of buildings and the thresholds to the buildings are located above the maximum calculated flood level (5.54m AOD) and so are not at threat from site flooding. Section 3.1.2.1 shows that limited flooding can be tolerated while still maintaining a line of protection with which to trip, shutdown and cool the reactor.

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

Operating instructions

There are operating instructions which specify the operator actions to be taken in the event of extreme sea state or extreme rainfall. These were reviewed by the second periodic safety review, which considered that these actions were appropriate if carried out immediately on notification of expected flooding, and this notification will be given by the Shift Manager.

Should essential plant become unavailable (due to external flooding) then this will be covered by normal operating procedures which would require a controlled reactor shutdown in the event of essential plant availability falling below specified minimum requirements. This would occur while at least one line of protection is still available.

Conclusion DNB 3.5: The claims made on the operator for flooding events are not onerous if adequate warning is given of an extreme rainfall event or sea state. Further review of them has been undertaken as part of the response to the Fukushima Dai-ichi event and it is judged that the reliance on these claims continues to be appropriate.

Consideration DNB 3.3: Consider reviewing whether the operators could complete all the tasks required prior to an extreme sea state or extreme rainfall if insufficient warning was given.

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

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

A review of site access following external hazards concluded that unforeseen extreme external flooding events may have an impact on the site access road. Given the expanse of low lying land extending to the Romney Marsh area, the flood depths are not expected to be of great depth and to recede within the 24 hour period such that road access would be available using appropriate vehicles. This is discussed in more detail within Chapter 6.

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

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

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

3.1.3 Plant compliance with its current licensing basis

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

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

Inspection and maintenance 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 Dungeness B covers the maintenance of the sea defences and site flood protection, which consists of:

- Monthly visual inspection of the shingle beach crest along the station frontage. Also following storms and at least 2 weekly during periods of severe winds likely to cause significant erosion.
- Refurbishment of the shingle beach October-March annually, plus as required following storms. Beach feeding as required to maintain beach crest level of 8m AOD and width of 20m.
- Structural integrity inspection of the site bund walls, surface water chamber and syphon recovery chamber every 3 years
- Functional test of the watertight gates and the discharge route to the Dungeness A station every year
- Functional test of the tide flap valves every 6 months.

It is noted that EDF Energy does not currently have a licence for refurbishment of the shingle beach crest, which is required as it is located in a Site of Special Scientific Interest. The width and height of the shingle beach crest is currently in excess of the minimum required and a relicensing process to allow beach feeding to resume is being progressed.

Conclusion DNB 3.7: The flood defence provisions for Dungeness B are suitable and are appropriately inspected and maintained.

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

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

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

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

Conclusion DNB 3.8: Where issues are identified within the safety case, they are addressed under normal company processes and appropriate actions are undertaken on reasonably practicable timescales.

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

Mandatory Evaluation

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

The within design basis evaluation

Scope

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

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

Summary of site specific findings

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

Conclusion DNB 3.9: The reviews undertaken as part of the within design basis evaluation, and the actions identified therein, have confirmed that Dungeness B is compliant with the current licensing basis, although a few improvements have been identified.

3.2 Evaluation of safety margins

An estimation of the safety margins against flooding, where known, is presented below. As outlined previously the bounding case for this site is flooding from an extreme rainfall event. The safety case for external flooding is based on demonstrating that the methodology is suitably pessimistic.

3.2.1 Estimation of safety margin against flooding.

Physical margins (Reactor Equipment)

The safety case is based on demonstrating that all essential plant is located above a very pessimistically calculated flood height. However, the safety margin within the calculation of the flood height has not been explicitly determined. The model conservatively assumes that all of the water falling on to the site is contained. If the event were to occur then it is

expected that water would flow off the site, in particular to the north of the site where the land slopes away from the buildings. The land surrounding the site is mainly shingle and has a significant capacity to allow the water to drain away, even including the combined direct rainfall and run-off from the site.

The storage capacity in potentially flooded buildings with thresholds below the 5.54m AOD maximum flood height has not been calculated, which would also have an effect on reducing the maximum flood height. It is believed that there is significant margin between the calculated infrequent rainfall flood height and the actual effects of such an event on site. Work is ongoing to highlight the conservatism contained within the flood height calculation.

Loss of grid is assumed to be a consequence of flooding in the safety case. However, for flooding due to a rainstorm it is judged that the grid may not fail immediately and the surface water pumps would be available to clear flood water. This would reduce the maximum flood height resulting from the rainstorm.

The majority of building threshold levels are higher than the calculated flood level. This provides a margin between the maximum design basis flood height and the point at which the building would flood. However the exact flood height at which each item of plant will fail is not currently known and a consideration is raised by this report to conduct such a survey. This information could then be used to focus measures to increase resilience on the equipment at greatest risk.

In a beyond design basis rainfall event it is judged that there would be sufficient time for the operator to respond such that the reactor would be tripped and shutdown by operator action. The equipment necessary for reactor trip and shutdown is expected to survive limited flooding beyond the design basis. Even if building thresholds are breached some equipment may survive as it is mounted on plinths.

Given the conservatism in the flood height calculation and the physical maximum credible rainfall that can occur it is judged that total failure of all essential safety systems from flooding caused by rainfall is incredible.

As has already been discussed, the bounding design basis sea state considered by the safety case of a tsunami is believed to be conservative as more recent studies have shown that the risk from a tsunami is minimal at Dungeness. By designing the sea defences to cope with this event there is therefore an unquantified margin against significant site flooding from other beyond design basis sea states. As previously noted work is ongoing to review the hazards safety cases against lower frequency hazards, this will be used to understand the frequency of the event that could have the potential to significantly overtop the sea defences and lead to site flooding.

Conclusion DNB 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. However, the exact flood height for a beyond design basis event at which equipment will fail is unknown.

Consideration DNB 3.4: Consider reviewing the exact water level at which essential plant located within buildings will fail due to flooding.

Consideration DNB 3.5: Drainage of the site should be examined and the existing rainfall calculation revisited to highlight any margins. It should be ascertained whether the drainage would be compromised by a high sea state.

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

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

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

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

Scope

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

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

Summary of Findings

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

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

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

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

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

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

Conclusion DNB 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 DNB 3.6: Consideration should be given to the feasibility of additional temporary or permanent flood protection for essential safety functions where margins to flood levels are low.

Consideration DNB 3.7: Consideration should be given to enhancing the robustness of dewatering capability, in particular focusing on independence from other systems.

3.3 Summary

The information presented in the preceding sections shows that the processes for ensuring robustness of the plant for flooding events are well developed and implemented and give appropriate consideration to the requirement for margins. They make appropriate use of international experience and standards both nuclear specific and discipline specific.

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

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

At Dungeness the bounding case for an infrequent flood is caused by rainfall. The methodology calculates that the extreme event will give a water level which is equal to or greater than some building thresholds containing non-essential plant. However, the equipment which forms the bottom line of protection is located in buildings above flood level or on plinths and is thus protected from infrequent flooding. This line of protection could be used to safely shutdown the plant and provide post-trip cooling.

The methodology used in the calculations of the infrequent flood height assumes no water run off onto the surrounding land. Given that the site is at a higher level than the surrounding marshland, most of the water falling on site will run off-site. Therefore the calculations describe an unrealistically pessimistic scenario. It is concluded that the safety margin inherent in the methodology used to calculate the flood level is significant.

The shingle bank protecting the site from seawater flooding has large safety margins against the extreme seawater levels.

Chapter 4 – Extreme Weather

Dungeness B

4 Extreme Weather

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

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

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

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

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

The following section identifies the extreme weather events that have been identified as posing a potential threat to the Dungeness 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 advanced gas-cooled reactor fleet.

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

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

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

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

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

Overview

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).

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

Extreme Ambient Temperatures

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

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

- The current design basis for extreme ambient temperatures has not been robustly defined. A consideration has been raised by this report to redefine the design basis using modern techniques and data.
- Analysis of climate change shows that the expected extreme ambient temperatures will exceed the current design basis by 2030.
- Within the current design basis at least one line of protection is demonstrated to remain available.
- A safety margin cannot be defined for extreme ambient temperatures. Tech Specs ensure that the plant is shutdown while the temperature is still within the allowable range.

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. The Lightning Electro-Magnetic Pulse is addressed as part of that Electro-Magnetic Interference / Radio Frequency Interference hazard and is not considered here.

- Work is currently being undertaken to produce a formal lightning safety case.

Drought

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

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

- Work is currently being undertaken to produce a formal drought safety case.

Combinations of hazards

- Some combinations of hazards have been considered in the safety case for Dungeness B. However a systematic consideration of all the possible combinations of hazards has not yet been undertaken, and work is underway to do so.

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

4.1 Design Basis

The design basis which has been adopted for the extreme weather hazards is provided 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 probability of exceedance of 0.02 per year (1 in 50 years), in line with normal UK civil engineering practice at the time, using CP3 Chapter V: Part 2: 1952.

In 1996, to meet the new Nuclear Safety Principles, the extreme wind safety case was developed for the first periodic safety review and it required demonstration of adequate reactor protection against an infrequent extreme wind with a probability of exceedance of 1 in 10,000 per year and a less onerous, frequent 1 in 1,000 per year event.

The CP3 Chapter V Part 2: 1972 Standard was used to derive the wind loads corresponding to the infrequent and frequent events. The basic wind speed (i.e. the 3-second gust speed, 10m above ground in open level country, likely to be exceeded only once in 50 years) is first derived from an isopleths map for the UK. The design wind speed is then derived by multiplying the basic wind speed by factors to account for topography, ground roughness, building size and height above ground. The design wind speed is converted to a dynamic pressure, which is then multiplied by the appropriate pressure coefficients. The extreme design wind speed is determined for the appropriate exposure period and return frequency and, for design/assessment purposes, the appropriate partial factors of safety are applied for the ultimate limit state.

Plant that has been installed on site more recently was designed to BS6399-2:1997, which gives a basic wind speed at a height of 10m over completely flat terrain at sea level, with an annual risk of being exceeded of 0.02. The basic wind speed is converted to a site wind speed accounting for the altitude of the site, wind direction and seasonal factors (if required). The site wind speed is converted to an effective wind speed, this being the gust wind speed appropriate to the site exposure and the height of the building. This effective wind speed is then converted into an equivalent dynamic pressure and multiplied by pressure coefficients corresponding to the form of the building. The extreme design wind speed is determined for the appropriate exposure period and return frequency and, for design/assessment purposes, the appropriate partial factors of safety are applied for the ultimate limit state. Wind-borne missiles are considered to occur as a result of the frequent and infrequent winds described above.

Work is in progress to develop a safety case covering the threat of tornadoes. The calculated infrequent tornado intensity is not bounded by the straight-line infrequent wind. The results of the work carried out to date indicate that the tornado hazard is tolerable.

Extreme Ambient Temperatures

The station was designed using the normal design codes at the time which included a consideration of temperatures with a probability of exceedance of 0.02 per annum (1 in 50 years).

At the time of the first periodic safety review the need to assess the plant against extreme temperatures with a probability of exceedance of 1 in 10,000 per year was recognised. Estimates of the extreme high and low air temperatures were made based upon other stations as no detailed analysis had been performed for Dungeness B. For the infrequent hazard, the low and high extremes of air temperature were judged to be -16 °C and +36 °C for Dungeness B.

The frequent temperature range (usually calculated as occurring with a probability of exceedance of 1 in 1,000 per year) was taken to be the same as the 1 in 50 year range on the basis that the effects on the plant are insensitive to the exact extreme temperatures applied, as no cliff-edges were identified between the frequent and infrequent event other than the potential for freezing of water systems. This was calculated based on local historical information to be between -10 °C to +32 °C for Dungeness B.

The temperatures given above for the frequent and infrequent hazard correspond to a minimum or maximum temperature which is only likely to last for a period of a few hours.

A minimum sea temperature between 1°C and -2°C at Dungeness was judged in the first periodic safety review to be roughly consistent with a 1 in 10,000 year return frequency with high seawater temperatures of the order of 25°C.

Snow loading was evaluated generally in accordance with the provisions of BS6399-3 and the extreme events determined by applying a statistical factor to the 0.02 per annum (1 in 50 years) event basic snow load. For a frequent event the snow load on the ground has been calculated as 0.86 kN/m² and an infrequent event as 1.14 kN/m². Both uniform (blanket) and redistributed snow loads, due to drifting, have been considered. It has been calculated that the roofs of nuclear safety related structures can withstand frequent and infrequent uniform snow loads. They can also tolerate drifted snow loads, with the exception of the turbine hall, for which the roof decking is predicted to be overloaded in localised areas in the event of infrequent, and possibly frequent, snow drifts. However, the consequences of localised failure of the turbine hall roof have been shown not to affect nuclear safety of the plant.

Table 4.1: Extreme Ambient Temperature Design Basis

Event	Minimum Temperature	Maximum Temperature	Return Period
Extreme Air Temperature (Frequent)	-10°C	32°C	1,000 years
Extreme Air Temperature (Infrequent)	-16°C	36°C	10,000 years
Extreme Sea Temperature	-2°C		10,000 years

Lightning

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 stage and it was not assessed in the original station safety reports.

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 was 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.

Lightning has not been formally considered as a hazard and this led to a shortfall being raised in the second periodic safety review which required that a formal hazards safety case be produced for lightning. This work is ongoing and is currently assessed to be low priority as a result of the relatively low safety significance of the issue.

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

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 (compared to the mission time of 24 hours). One consequence of this is that mitigation can be put in place (where practicable) prior to the event. It is likely also that the duration of the event will extend significantly beyond the mission time.

Drought is a lack of water caused either by prolonged periods of hot or cold weather or by lack of rainfall. Such a hazard may affect the water levels held within the lagoons and the Townswater main supply to the station with a knock-on effect on the Station's water stock levels necessary for normal and post-trip cooling. In Station terms drought is primarily the unavailability of water supplies from the townswater main resulting in inability to stock up on water supplies. Minimum feedwater reserve levels are included in technical specifications. Failure to have sufficient stocks available to satisfy these specifications results in the need for a controlled reactor shutdown. In addition to the feedwater stocks, minimum water levels for the lagoons are also specified.

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:

- Seawater cooling heat sink is provided from a seawater intake which is not susceptible to low tide levels or drought. Therefore, there is no common mode failure of the seawater supply and the lagoons supply in terms of drought.
- Adequate water reserves exist in the station, with adequate diversity, for feedwater make-up, which could provide at least 24 hours of essential post-trip cooling supply without the townswater mains make up system available. Loss of main boiler feed would result in a demand to trip the reactor.

Any effects of drought on soil conditions or building foundations are considered to be very gradual, with time being available to allow a safe plant state to be achieved before significant loss of essential systems (including redundant and diverse systems) occurs. The general ground level at Dungeness B is 5.5m AOD, the level of standing groundwater is between 1m AOD and 2m AOD in the area of the reactor building. Beach Gravel forms the upper level of the local strata and extends from 5.5m AOD to -7m OD. The base of the concrete raft on which the reactor building sits is generally at -3.66m OD. It is evident therefore that an extreme change in groundwater level would be required before the ground under the reactor building is affected. A change of this magnitude is unlikely due to the Stations proximity to the sea.

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

Owing to the long timescales that will be available to respond to this hazard and its relatively low level of threat to safe operation, this hazard is not considered in any great detail in this EU Stress Test Report.

Conclusion DNB 4.2: Drought is difficult to quantify, although due to advance warning of the discontinuation of off-site water supplies ensure that there is sufficient time available to the operators to allow the appropriate actions to be taken.

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 for the extreme wind and extreme ambient temperature hazards.

4.1.1.1.1 Extreme Wind

The safety case for the wind loading hazard is based on the claimed lines of reactor protection being either protected from wind loading by virtue of being housed within qualified buildings, or being qualified directly against wind loading in the case of exposed plant.

Changes to the British Standards covering the design of structures in the major civil engineering materials were reviewed in 2007 as part of the second periodic safety review. It was concluded that the changes were not significant and did not affect the design integrity of the safety related structures at Dungeness B.

As noted previously, the assessment of extreme wind conditions has used different methods to determine the wind loads, this being dependent upon the age of the assessment. The majority of the structures were assessed using CP3 Chapter V Part 2: 1972 at the time of the first periodic safety review in 1996 but newer structures have been assessed against BS6399-2:1997. The second periodic safety review completed a comparison of the wind loading codes.

The second periodic safety review comparison concluded in broad terms that the wind loads to CP3 Chapter V Part 2: 1972 tend to bound those derived using the initial issue of BS 6399-2: 1997, and that the wind loads to BS 6399-2: 1997 (2002) bound those to the initial issue of BS 6399-2: 1997. However, no simple bounding comparison exists between CP3 Chapter V Part 2: 1972 and the current code BS 6399-2: 1997 (2002), although it was considered that, in some localised respects, wind loading to BS 6399-2: 1997 (2002) tends to be more onerous than the wind loading to CP3 Chapter V Part 2: 1972.

The second periodic safety review therefore identified a shortfall to investigate further the validity of the CP3 assessments when judged against the current BS6399 standard. This shortfall has now been addressed by a re-assessment, the objective of which was to re-substantiate the buildings and exposed plant claimed by the wind hazard safety case against the latest versions of the wind loading code, BS6399-2: 1997 (2002), and the relevant structural design codes. The

assessment concluded that existing safety case claims regarding the qualification of nuclear safety related structures against the second line and bottom line wind hazard remain valid and secure, when assessed against the more recent standards (e.g. BS6399-2: Wind Loads, BS5950: Structural Steelwork, BS8110: Reinforced Concrete, BS 5628: Structural Masonry).

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 major study, commissioned by EDF Energy, published in 2004, was undertaken by the Met. Office regarding the effects of climate change with respect to UK nuclear sites. A second study in 2006 presented quantitative predictions of climate change for five nuclear sites including Dungeness. For Dungeness, over the range of emissions scenarios modelled, the study predicts a clear increase in the average winter wind speed and a possible increase in the average summer wind speed. By 2080 the winter wind speeds in the vicinity of Dungeness are predicted to have increased by up to 6% (over land areas) and 8% (over sea areas). However, the study predicted that extreme wind speeds for the full range of return periods (up to a return period of 1 million years) will only increase by about 2.5% by 2080.

The above climate change work has recently been further supplemented by additional work for 2011. This work reviewed the recently produced UKCIP technical notes on storm projections (UKCIP 2009a) and probabilistic projections of wind speed (UKCIP 2011b) based on UKCP09 climate data and climate models. The latter study projects changes in monthly mean wind speed and excludes extreme wind speed. For this reason the UKCP09 probabilistic projections of wind speed are not suitable for assessing hazards caused by high wind speed. The former study (UKCIP storm projection) found that on balance the complex concurrent atmospheric and oceanic effects lead to little or uncertain changes in the frequency and intensity of storms over the UK thus providing no evidence that the severity of the risk will change significantly in the 21st century.

It was concluded that apart from keeping under review the projections for climate change, no specific actions were required relating to wind.

Conclusion DNB 4.3: For extreme wind loadings there is a current design basis. However, the national standards and the methodologies used to perform the hazard assessment have changed since the time of production of the safety case. Therefore, a re-assessment has been carried out adopting the relevant design codes and standards in force at the time of the second periodic safety review in 2007, and it is concluded that existing wind hazard safety case claims remains valid and secure.

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

4.1.1.1.2 *Extreme Ambient Temperatures*

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

Extreme Air Temperatures

The maximum and minimum ambient temperatures that define the infrequent hazard were originally derived using engineering judgement based on calculations undertaken for other stations. No further verification of the infrequent temperature limits has been conducted.

Most essential plant was originally designed in accordance with contemporary Central Electricity Generating Board standards at the time of construction, which typically specified a local working temperature range between 0°C and +40°C. It is, therefore, assumed that all essential plant will perform satisfactorily within this range unless there is a specific indication to the contrary. Because the plant would have been designed with margins of safety, there would be no 'cliff edges' and the plant would be expected to operate satisfactorily a few degrees outside the design range (subject to freezing of water-filled systems not occurring).

The local temperature of the equipment will depend on the location of that equipment, what type of building it is housed in, heat from nearby equipment and the effects of any local ventilation.

A 2011 Met Office report commissioned by EDF has recently reviewed the methodologies for extreme ambient (high or low) temperatures. The report examined and has taken 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 an increase in the predicted maximum temperature to 42°C by 2030. This is beyond the current design basis, and work is underway to revisit the original design basis to include this higher temperature.

Extreme Seawater Temperatures

The minimum seawater temperature associated with an infrequent hazard has not been verified. A consideration to review this position has been raised by this review, as part of the review of the extreme ambient temperature design basis.

Snow loading

For an event with a probability of exceedance of 1 in 10,000 per year, the uniform snow loading has been taken as 1.14kN/m² on the ground. A Met Office report on snow loading commissioned by EDF Energy predicted that, for Dungeness B, the uniform snow loading on the ground from an infrequent event would be 1.02kN/m², which is bounded by the value assumed for assessment of the buildings.

A Met Office report specifically written for EDF Energy sites included consultation with in-house specialist civil engineers and reported that the level of risk from snow loading was low.

The snow report 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 report 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 DNB 4.4: There is a current design basis for extreme ambient temperature which has been reviewed as part of the periodic review process. However, the design basis has not been validated. The design basis for air temperatures has recently been further reviewed for all sites as part of Climate Change Adaptation and it was identified that the expected infrequent high ambient temperature will be beyond the current design basis within the expected lifetime of Dungeness B.

Conclusion DNB 4.5: Snowloading has been considered in the second periodic safety review, with only shortfalls of a low safety significance being identified.

Consideration DNB 4.2: 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 have shown that whilst these extreme hazards were not explicitly addressed 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 a 1 in 10,000 per year design basis event cannot be easily derived (i.e., drought and lightning), this has been recognised and suitably pessimistic safety cases are in 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. Suitably conservative safety cases are being developed for the lightning and drought hazards but reviews carried out as part of the second periodic safety review indicated that these were unlikely to present significant threats to the continued safe operation of the plant.

4.1.1.4 Consideration of potential combination of weather conditions.

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

Hazards may combine together in a number of ways. One potential way involves the random coincident occurrence of hazard events, for example the occurrence of an external flood hazard at the same time as a dropped load incident within the station. In such a case there is no obvious connection between these events, causing one to arise 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 not been considered in the safety case. However, the Hunterston B and Hinkley Point B safety cases do formally consider combinations of hazards and the findings therein are broadly applicable across the advanced gas-cooled reactor fleet. They found that the majority of combinations of weather events lead to consequences no worse than those arising from an individual hazard with respect to the design basis. 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, based on the findings of the Hunterston B and Hinkley Point B safety cases, 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

At Dungeness B, some combinations of hazards and extreme winds have been considered under the second periodic safety review. The blockage of ventilation ducts by wind blown debris was considered. It was judged that there is adequate redundancy and segregation of the diesels to accommodate the effects of any credible disruption due to windblown debris. Failure of multiple tanks due to extreme wind has been considered to be bound by the seismic safety case. Where tanks are qualified against frequent or infrequent seismic events it is considered that multiple failures due to wind loading may be discounted. The main sources of potential flooding, including the main water and diesel stocks, are qualified or protected against infrequent wind loading. Finally, the risk to key personnel accessing the alternative monitoring location from wind blown debris was considered. The normal control room is also qualified against the bottom line hazard, and so use of the alternative monitoring location should not be necessary.

Conclusion DNB 4.6: There is no combined hazards safety case for Dungeness B. However, some combinations of hazards have been considered in the second periodic safety review. The work on combinations of hazards undertaken for other advanced gas-cooled reactor stations supports the judgement that combinations of hazards are no more onerous than the hazards occurring in isolation.

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

Fleet wide Review

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

Conclusion DNB 4.7: 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 DNB 4.4: Consideration should be given to evaluating the methodologies used to calculate the infrequent extreme ambient temperature and extreme wind event conditions and whether a fleet wide methodology should be adopted.

4.1.2 Conclusions on the Design Basis

Section 4.1 has confirmed that for the wind hazard, appropriate design basis events have been defined. A consideration has been raised to more formally consider the extreme ambient temperature design basis.

For the lightning and drought hazards, formal hazards safety cases are being developed but the nature of these particular hazards means that it is unlikely that infrequent events will be defined. Instead, it is likely that these hazards will be assessed against appropriate standards or, for worst envisaged consequences, as a surrogate for a design basis derived for a return frequency.

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

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

4.2 Evaluation of safety margins

This section considers the degree to which the existing safety cases include margins. It is noted however that the approach that is normally adopted in hazards analysis does not provide any estimation of the difference between the design basis condition and those conditions that would seriously challenge the reliability of the protection plant and

equipment. The section highlights what plant items are lost during the hazard, what essential safety functions are claimed to survive the hazard and any actions required to maintain the essential safety functions. The hazards that equipment is qualified against is listed in a database, which also states how the equipment has been qualified.

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

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 (for example, high wind speeds).

4.2.1.1 Extreme Wind

The potential effect of severe winds is to damage the buildings nearby or housing equipment providing essential safety functions. The detailed consequences of such building failures are difficult to determine with any great accuracy. The approach that has therefore been adopted for the infrequent wind speed is to demonstrate that the specific structures are capable of resisting the hazard.

In addition to the margin between the design basis condition and conditions which would challenge the protection equipment, there is a safety margin inherent to the standards used to define the design basis. That is, the conditions taken as the design basis are derived in a pessimistic manner. This is because limit state design methods, with partial factors of safety on load and materials, are used. These margins are not explicitly quantified.

4.2.1.1.1 Reactor at power

The potential for limited damage to internal plant, such as cabling, due to wind borne missiles is recognised but the claimed internal plant is either fail-safe or possesses adequate redundancy and segregation. It is reasonable to assume that wind speeds would have to exceed frequent levels to create and mobilise significant wind borne missiles that could damage external plant and structures. In the event of high / extreme winds, station operating instructions include an action to check outdoor areas for loose materials or temporary fixtures and to remove them to a secure indoor location.

Lines of Protection

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

Table 4.2: Lines of protection against the infrequent wind hazard

Essential Function		Equipment Qualified Against Infrequent Event
Reactor Trip		Guardline equipment remains available
Reactor Shutdown		Main shutdown system
Pressure Boundary		Pressure vessel and penetrations with claim on gas circulator seals
Post-trip cooling	Boiler venting	All boiler vent routes remain functionally capable
	Boiler Feed	Diesel generator supplied back-up feed system or direct diesel driven feed system
	Gas Circulation	Forced primary coolant gas circulation and natural circulation
	Vessel Cooling	Vessel cooling system (using normal or back-up pumps)
Monitoring		Control room or alternative monitoring location

The safety case assumes loss of grid and grid dependent systems (although the equipment itself is expected to survive). The lagoon based cooling system is not formally claimed to survive, as it has some short lengths of external pipe work which are difficult to absolutely prove would not be affected. However, there are two other diverse back-up feed systems available. The nitrogen injection system is not qualified against the frequent wind loading and will not be available and, as discussed in Chapter 3, the alternative main shutdown system is exceptionally reliable.

Trip

The Guardline systems are contained wholly within buildings which have been qualified to withstand the infrequent wind loading.

Shutdown

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

Post-trip Cooling

Forced gas circulation will remain available as the gas circulators equipment is located in a building qualified to withstand the infrequent wind loading. The electrical supplies for gas circulation can be provided by either of two diverse sets of diesel generators. The reactor pressure boundary will not be affected by the infrequent wind loading. Consequently, primary coolant circulation by natural circulation is also claimed as a line of protection. The gas circulator seals are assumed to be secure, either by continued operation of the running seals, or by manual application of the stationary seals. The stationary seals and the vessel cooling system are contained within qualified buildings.

The heat sink for the vessel cooling system is provided by seawater systems contained within buildings qualified against the infrequent wind load. Alternatively cooling can be provided by a back-up system supplied from diesel generators, both of which are contained within buildings qualified to withstand the infrequent wind load.

The back-up feed system claimed in the safety case, and the supporting electrical systems are within buildings which are qualified to withstand the infrequent wind load.

The provisions for post-trip cooling have been further enhanced by the installation of the direct diesel driven feed system whose buildings and water tanks have been qualified to withstand the infrequent wind loading.

Monitoring

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

Electrical Supplies

As mentioned above, the diesel generators which supply the systems above have been qualified against the infrequent wind 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.

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

- Checking the wind speed over every two hour period.
- Removing loose debris/scaffolding from around the site.

- Consider running back-up diesel generators.
- Half-fill any tanks that are empty due to maintenance (the added weight helps protect the tanks).
- Visually check all the exterior of all buildings and externally located plants.

4.2.1.1.2 Shutdown Cooling

It is judged that the extreme wind hazard does not present a more onerous challenge to a shutdown reactor than one at power. Forced gas circulation will remain available using the high speed motors. Reseal and repressurisation (to establish natural circulation) can also be achieved as all required equipment has been qualified to withstand the extreme wind loading.

4.2.1.1.3 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.

Extreme external winds could result in a loss of grid and therefore a loss of power to the pond cooling systems. Timescales to recover cooling are as per Chapter 1.

4.2.1.1.4 Wind Safety Margins

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 DNB 4.8: 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 DNB 4.5: Consideration should be given to defining the safety margin to equipment failure due to extreme wind, either directly or as a result of buildings failing.

4.2.1.2 Extreme Ambient Temperatures

Extreme ambient temperatures have the potential to disable the reactor's protection systems; because the temperature is either too high or too low to guarantee correct functioning of protection equipment. Extreme low temperatures are of particular concern to systems and structures that are located outside the reactor building, primarily equipment essential for post-trip cooling, which requires water in order to operate and for which there is the potential for freezing. There is also potential for the grid to be affected and hence the safety case for extreme ambient temperatures makes no claim on grid supplies or plant supported by grid only.

Extreme ambient temperature events are likely to develop over a protracted period and this will ensure that station staff has sufficient time to act in order to protect the plant against the effects, such that acceptable performance of essential plant can be assured. A range of measures are taken by the Station to mitigate the effects of the hazard, including lagging, trace heating, the provision of temporary heaters and the running of standby systems to prevent (or in extreme cases provide warning of) freezing.

The Technical Specifications require that actions be taken to confirm the availability of adequate lines of reactor protection in the event of extremes of temperatures arising. Ultimately, if the viability of the reactor protection cannot be confirmed, the specifications requires that a controlled shutdown be implemented. This should ensure that sufficient functional lines of reactor protection are available at all times.

4.2.1.2.1 Reactor at Power

Lines of protection

The safety case assumes loss of grid, therefore loss all grid dependent equipment unavailable post trip. However, if grid was not lost various trace and tank heating systems would be available, which would significantly increase the amount of equipment available and their margin to failure. The back-up feed system, which draws water from the lagoons is assumed to be unavailable for extreme low ambient temperatures.

The lines of protection claimed in the safety case are presented in Table 4.3.

Table 4.3: Lines of Protection from extreme ambient temperatures

Function	Equipment Qualified Against Infrequent Event	
Reactor Trip	Not required but manual trips remain available.	
Shutdown	Main shutdown system	
Pressure Boundary	Pressure vessel and penetrations with claim on gas circulator seals	
Post-trip cooling	Boiler venting	All boiler vent routes remain functionally capable
	Boiler Feed	Diesel generator supplied back-up feed system or direct diesel driven feed system (Lagoon derived water is available for high extreme temperatures)
	Gas Circulation	Forced primary coolant gas circulation and natural circulation
	Vessel Cooling	Vessel cooling system (using normal or back-up pumps)
Monitoring	Control room or alternative monitoring location	

Trip

The main guardline system is generally fail-safe in nature. However, it is considered that some aspects of this system are potentially vulnerable to high local temperatures. As a result, a second guardline system has been specifically designed to withstand an infrequent extreme ambient temperature event.

The second guardline equipment has been qualified to operate within specification up to a local temperature of 55°C. There are temperature sensors installed in the same location as the guardline designed to ensure that the guardline remains within the required temperature limits. If the local temperature of the guardline exceeds 45°C the reactor will be automatically tripped. The reactor will also be tripped if local temperatures fall to 0°C.

Shutdown

The main shutdown system is not vulnerable to extreme ambient temperatures due to its location deep within a building.

Post-trip Cooling

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

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

Gas circulation can be undertaken satisfactorily at local temperatures of 75°C. It is therefore expected that the gas circulators will operate satisfactorily at the assumed maximum external temperature of 36°C.

The vessel cooling system is judged not to be vulnerable to freezing during a low extreme ambient temperature event (-16°C).

The seawater cooling system cools plant such as some diesel generators, the gas circulator lubricating oil coolers and the reactor pressure vessel coolers. These systems are judged to survive the infrequent extreme ambient temperature, as the 'extreme weather procedure' ensures their availability.

The pressure vessel is a large civil structure, with a large thermal inertia, and the reactor building protects it from high and low temperature extremes. With an external ambient temperature of -16°C, the internal temperature would not drop below approximately +5°C. Therefore, all essential equipment within the reactor building are expected to be available during extreme low ambient temperatures.

The diesel backed boiler feed pumps and the supporting electrical supplies are protected from extreme low ambient temperatures by their location. Feed stocks are derived from storage tanks. Both the trace heating and tank heater are grid-based and their availability cannot be assured at extreme low temperatures. However, feedwater in the pipes could nevertheless be prevented from freezing in temperatures below -11°C by keeping the water circulating. Also, warm condensate could be directed to some of the tanks, and cold (but not freezing) water extracted for return to the main feed train. Furthermore, the need to monitor water stocks to ensure that freezing does not occur is included in the extreme weather procedure

In the extremely unlikely event that low ambient temperatures render seawater unavailable, either for cooling of auxiliary systems or for condensing recirculating boiler feed, boiler feed would still be available through the direct diesel-driven feed system. It is expected that such an event would be relatively slow to occur, and the reactor would already be shutdown.

The seawater intake is located at some depth below sea level, away from any surface ice. Therefore, it is judged that loss of cooling water through freezing of the sea is not credible.

Monitoring

Monitoring of essential functions can be carried out from either the control room or alternative monitoring location. The temperature within the control room is controlled by the heating and ventilation system. The alternative monitoring location, which is located in a separate building, can also be cooled by increased ventilation by opening windows, vents and louvres. Both locations are judged to be able to withstand the infrequent extreme high ambient temperature event.

Electrical supplies

There is a safety case requirement that the diesel generators are supplied with diesel fuel which is suitable for external ambient temperatures down to -16°C. The operator actions include considering running the diesels to ensure their availability during periods of low temperature.

Snow Loading

As discussed in Section 4.1.1.1.2, all buildings containing essential equipment have been qualified against infrequent snow loading. There is no explicit safety case identifying appropriate lines of protection against the frequent and infrequent snow loading hazard, and consideration should be given to developing such a case.

Operator Actions

Operator actions form an essential part of protecting the essential safety functions from extreme ambient temperatures. The local temperatures within the various rooms and buildings of the station are varied, but in general are likely to be higher than the ambient temperature. The operators manage the distribution of temperatures through the station with various actions, such as opening/closing windows and using fans or other temporary equipment, to maintain equipment temperatures within safe limits.

Low Temperature Risk and Standard Operating Procedure

There is a procedure triggered in the event that extreme weather conditions are forecast or are evident on site. Items contained in the procedure include:

- Checking the operation of trace heating (powered by grid-based supplies);
- Measures to prevent the freezing of cooling water systems.

The procedure also includes a requirement to run certain items of standby plant in low ambient temperature conditions (such as the back-up diesel generators and back-up feed system).

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

High Temperature and Standard Operating Procedure

If ambient air temperatures in excess of 30°C are expected within the next 48 hours, the operator actions listed in a procedure are to be carried out in order to reduce the risk to nuclear safety (trip, shutdown, post trip cooling and monitoring) plant. All operator actions involving the monitoring of hot indoor ambient conditions within a plant area are to be carried out mid afternoon, when the hottest conditions are expected.

Items contained in the procedure include:

- Actions to be taken to dissipate excess heat generation in buildings; and
- Actions to shutdown the reactor if countermeasures fail and temperatures in safety-related areas exceed 40 °C.

4.2.1.2.2 Shutdown Cooling

It is judged that the extreme high ambient temperature hazard does not present a more onerous challenge to a shutdown reactor than one at power. During an extreme low ambient temperature event, a shutdown reactor may be more susceptible to freezing than a reactor at power, therefore operator actions which are claimed to ensure plant availability are of greater importance. However, the effects on internal building temperatures have not been explicitly calculated. Forced gas circulation will remain available from the diesel generator backed electric motors. Reseal and repressurisation can also be achieved as all required equipment has been qualified to withstand extreme ambient temperatures.

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.

4.2.1.2.3 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. The only exception is that a loss of grid could lead to a loss of power to the pond cooling systems. Timescales to recover cooling are as per Chapter 1.

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

4.2.1.2.4 Ambient Temperature Safety Margin

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

Conclusion DNB 4.9: The safety margin of essential safety functions of the plant against extreme ambient temperature have not been defined. Cliff edge effects are also difficult to define for the extreme ambient temperature hazard.

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

4.2.1.3 Lightning and drought

Protection against lightning has been installed on the key buildings in accordance with appropriate standards. The 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 DNB 4.10: 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.

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 advanced gas-cooled stations. The review concluded that these actions were appropriate. However, this stress test 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 DNB 4.11: Operator actions undertaken during extreme weather events were reviewed in the second periodic safety review and were deemed appropriate.

Consideration DNB 4.7: Consider reviewing whether comprehensive human factors assessments are required for operator actions undertaken during extreme weather conditions.

4.2.1.5 Mitigating Actions

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

Conclusion DNB 4.12: The predictable nature of the extreme weather hazards discussed in the chapter allow operator actions to be taken to help mitigate the effect of the hazard.

Consideration DNB 4.8: Consider reviewing the seasonal preparedness measures currently undertaken to identify areas to increase robustness.

4.2.2 Potential need to increase robustness of the plant against extreme weather conditions

Each of the hazards that have been addressed in this Chapter have been subject to review as part of the second periodic safety review and will be reviewed again in the third periodic safety review for the station. Whilst the second periodic safety reviews identified some shortfalls with respect to the cases made, very little was found in terms of the need for potential enhancements of the plant robustness. Those shortfalls that have been raised have either been addressed and closed out or are still in process of being addressed.

Climate change has the potential to modify the severity of meteorological hazards and for this reason EDF Energy regularly monitors revisions to predictions. In 2011 EDF Energy undertook a climate change adaptation review. This considered the effects of predicted climate change on meteorological related hazards including those that have been considered in this Chapter. Considering the effect of climate change across EDF Energy's fleet of nuclear stations, a number of generic gaps were identified by the adaptation risk exercise. For each gap identified, a suggested adaptation

option was also specified, however these may not apply to every site. Based on these findings, EDF Energy has a number of initiatives that it will be progressing aimed at building on its existing adaptive capability. Over the next year, EDF Energy will be considering in detail its forward strategy with respect to these options. The areas relevant to this chapter are listed below.

Table 4.4: Gaps Identified by Adaption 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

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

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

The findings of the extreme weather aspects for the evaluations are discussed below on a fleet wide basis; this is because the learning from each of the sites is judged to be applicable across the stations.

This assessment was carried out very soon after the event and was primarily focussed on seismic and flooding hazards. Some consideration was given to other extreme events, commensurate with the level of impact of the hazard.

Within design basis evaluation

Scope

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

This assessment was carried out very soon after the event and was primarily focussed on seismic and flooding hazards. Some consideration was given to other extreme events, commensurate with the level of impact of the hazard.

Summary of Findings

The within design basis evaluation found that the systems essential to fuel cooling in an emergency situation in a within design basis event are correctly configured, lined up and in a suitable condition to be declared available/operable. No additional concerns were identified at station with regard to all hazards considered in this chapter.

Beyond design basis evaluation

Scope

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

This assessment was carried out very soon after the event and was primarily focussed on seismic and flooding hazards. Some consideration was given to other extreme events, commensurate with the level of impact of the hazard.

Summary of Findings

All stations have procedures for preparation for seasonal readiness and extreme weather events. In general they dictate allowable operations for weather conditions.

Some, but not all, of the stations receive site specific weather forecasts to enable preparation of plant for weather events.

All stations had some experience of within design basis adverse weather conditions such as heavy snow, localised flooding or prolonged heat and in reviewing that experience it was generally noted that some simple actions could provide benefit particularly with regard to station access.

Conclusion DNB 4.13: 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 DNB 4.9: Consideration should be given to all stations receiving site specific weather forecasts.

Consideration DNB 4.10: Consideration should be given to connecting the trace and tank heating systems to secure electrical systems.

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

4.3 Summary

The design basis for an infrequent extreme wind is based on demonstrating that buildings conform to relevant standards and codes for an infrequent event. Equipment required to fulfil the essential safety functions is either located inside buildings which are qualified against infrequent wind, or qualified directly. The safety case at Dungeness B 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 Building, Services Unit and Turbine Hall and others containing essential equipment have been assessed against snow loading and demonstrate sufficient margin. Where this has not been shown, failure of the building has been shown to be acceptable.

The climate change predictions are that by 2030 there will be a rise in the expected maximum air temperature beyond the current design basis. Re-evaluating the design basis maximum temperature has been raised as a consideration by this report.

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

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.

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

Dungeness B

5 Loss of Electrical Power and Loss of Ultimate Heat Sink

Potential damage to the fuel and reactor components is prevented by ensuring that the essential safety functions are always in place and available. These essential safety functions are reactor trip, reactor shutdown and hold-down, provision of adequate post-trip cooling and maintaining containment for the fuel and fission products. One of the main aspects of the Fukushima incident relates to the provision of adequate post-trip cooling and this is the main essential safety function that is affected by the scenarios considered in this chapter.

The focus of this chapter is on prevention of potential damage to the reactor and to the irradiated fuel under various loss of electrical power and loss of ultimate heat sink scenarios. This includes examination of all means available to supply post-trip cooling and an evaluation of timescales available to prevent potential damage in various stress-test imposed conditions.

The stress-test requires a consideration of 'Loss of Electrical Power', including sequential loss of the grid electrical supply, the station on-site normal (ordinary) electrical supplies and on-site diverse (alternative) electrical supplies leading to a 'Station Black-Out' scenario, where all station electrical supplies are lost.

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

It should be noted that many of the scenarios discussed in this chapter are beyond the design basis. This formally means that they occur with a frequency much less than 1 in 10,000 years. In fact, EDF Energy confidently expect that the scenarios in this chapter, especially those concerning the combination of station black out and loss of heat-sink, are not credible.

The Stress Test is applied to both the pressurised and allowable depressurised reactor states. In addition, the stress-test examines the plant requirements for maintaining cooling to station fuel route plant areas.



Figure 5.1: High voltage electricity transmission towers connecting Dungeness B to the electrical grid.

5.1 Nuclear power reactors

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

Trip, Shutdown and Hold-down

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

Post-Trip Cooling and Containment

Post-trip cooling is usually provided by forced CO₂ gas circulation. Forced gas circulation requires a supply of power from either the main electrical grid or the on-site back-up generators.

Natural circulation of the CO₂ gas is also possible and will provide suitable and sufficient gas circulation and heat transfer from the fuel to the boilers when the reactor is pressurised and without the need for electrical supplies. In a depressurised reactor natural circulation cannot provide a sufficient amount of post-trip cooling.

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

The pre-stressed concrete pressure vessel which encloses the reactor provides a robust containment for the reactor primary coolant (CO₂ gas). The pressure vessel cooling system requires both electrical supplies and a supply of cooling water to provide a heat sink.

Monitoring of the station reactor status is provided in the central control room and in an alternative on-site facility. Both of these monitoring facilities require electrical supplies.

5.1.1 Loss of electrical power

The stress-test review of the various scenarios for 'loss of electrical power' at Dungeness B and their impact on the plant that is required to carry out the essential safety functions are contained within this section and its sub-sections. Conclusions and judgements are made throughout the sections below and suggested 'Considerations' for improvement are identified.

The National Grid is the standard Alternating Current (AC) electrical supply source to most station electrical systems and normal station on-site supplies (used as a back-up AC electrical supply on loss of grid), are provided by diesel generators within several different functional electrical systems. Station battery power is provided for a number of these AC electrical systems to enable no-break supplies when switching from grid to station diesel generator supplies.

The provision of no-break electrical supply systems ensures that the required control and instrumentation systems continue to function during the short timescale change-over from grid to diesel generator supplies. Boiler feed and equipment cooling systems can tolerate a short electrical supply interruption while the diesel generators start.

5.1.1.1 Loss of off-site power

In this section loss of off-site AC power is considered, which constitutes a loss of all of the electrical power supplied by the National Grid. This event is considered within the safety case and there are installed plant provisions to deliver the essential safety functions.

5.1.1.1.1 Design provisions taking into account this situation: back-up power sources provided, capacity and preparedness to take them into operation

There is a safety case at Dungeness B covering loss of off-site power, which is considered to be a frequent event. It is also considered as a consequence of many other hazards, such as high winds or seismic events.

Loss of grid supplies will result in a turbine generator and reactor trip. This will result in a short temporary loss of power supply to plant providing boiler cooling water feed, CO₂ gas circulation and seawater cooling until diesel generator supplies are available.

On an operating reactor the normal trip and shutdown functions are not affected by loss of grid supplies. Gas circulation, boiler feed and pressure vessel cooling will be restarted from the station diesel generators electrical supplies system.

For a shutdown reactor the design provisions are the same as those discussed above for an operating reactor, although the reactor is already tripped and shutdown. If the reactor has been depressurised, provisions are available for forced gas circulation and reseal and repressurisation of the reactor to support natural circulation.

Each main diesel generator has separate and individual lubricating oil, fuel storage and main cooling systems. Bulk storage fuel oil tanks provide gravity feed to the diesel day tanks. For each set of diesels, a single diesel generator is capable of producing sufficient power to supply all the necessary essential functions, when the demanded load is managed by the operators.

All claimed systems are maintained regularly in accordance with maintenance schedules in order to ensure their continued compliance to the specification and design basis.

A diesel generator system programmed routine test is carried out on each engine system on a regular basis. Full engine and generator data is recorded and logged to assist in engine maintenance. The programme staggers the testing to ensure that availability remains at the required level.

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

The station safety case specifies that each main diesel generator must be capable of supplying full load for a period of 12 hours in the event of a loss of grid supply. The minimum usable fuel stocks held on-site are sufficient to supply enough power for the essential post-trip functions for 48 hours if the operators manage the electrical loading.

Longer mission times are not addressed in the current safety case. The normal operating stock levels are in excess of the minimum limits and therefore further margin would normally exist. The technical scope of the stress-test requires that loss of all off-site electric power supply to the site for several days is considered, wherein the site is isolated from delivery of heavy material for 72 hours by road, rail or waterways; portable light equipment can arrive to the site from other locations after the first 24 hours. EDF Energy safety cases are based on the demonstrated ability to provide essential stocks within 24 hours delivery time. Consideration could be given to enhancing the existing capability of the station to extend the current mission times; this could be achieved in a number of ways.

Conclusion DNB 5.1: Loss of off-site power is an event considered within the safety case and suitable provisions are made to support the essential safety functions.

Conclusion DNB 5.2: In the event of loss of grid, fuel oil supplies are sufficient for diesel generator electrical supplies for up to 48 hours.

Consideration DNB 5.1: Consideration should be given to enhancing the capability to extend mission times.

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

A loss of off-site AC power combined with loss of ordinary (normal) station back-up AC power 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

Power supplies to back-up post-trip cooling plant can be provided from diverse (alternative) diesel generators in the event of the main AC diesel generators being rendered inoperable. Back-up post-trip cooling plant is provided for CO₂ forced circulation, boiler feed, pressure vessel cooling, seawater cooling and control and indication systems. Sufficient redundancy is provided in the alternative diesel generator systems to provide the required minimum post-trip cooling via these back-up systems.

All claimed systems are maintained regularly in accordance with maintenance schedules in order to ensure their continued compliance to specification and design basis.

The conclusions and considerations arising from Section 5.1.1.1.2 relating to mission times for main on-site AC power supplies apply equally here for the alternate power supplies; the claimed mission time is 24 hours, although again it should be noted that in reality there would be more stocks than this present on site.

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

Conclusion DNB 5.4: The current robustness and maintenance of the plant is compliant with its design basis against loss of electrical power.

5.1.1.2.2 Battery capacity, duration and possibilities to recharge batteries

Battery supplies are not used to provide main feedwater or equipment cooling systems because this is not required.

The battery systems are used to support control and instrumentation, lighting and diesel generator starting amongst other systems. During a loss of off-site power with loss of the ordinary back-up power source, some batteries would not usually be recharged once exhausted. Batteries supporting starting of the alternative diesel generators are recharged by their respective systems while they are operating and it may be possible to recharge other batteries using the alternative diesel generators if the appropriate switchgear remains operable.

5.1.1.3 Loss of off-site power and loss of the ordinary back-up AC power sources and loss of permanently installed diverse back-up AC power sources

This stress-test scenario proposes a loss of off-site AC power supply as well as loss of the main back-up AC power supply and any other diverse generating systems. This is a total loss of all otherwise available power supply capacity.

At Dungeness B, this scenario would result in a station blackout as the station does not have further permanently installed generating capability.

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

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

For a pressurised reactor, primary circulation is achieved through natural circulation provided that sufficient boiler feed is available. At Dungeness B, a boiler feed system powered by direct drive diesel engines would remain available. This system is a high pressure system designed to be independent of, and segregated from, other feed systems as far as is practicable. The additional feedwater for both reactors is held on-site in dedicated tanks with sufficient water to support 24 hours of boiler feed to two reactors if flow is managed by the operators. The ability of the operator to complete this action could be compromised under a station blackout as control and instrumentation systems may not be available.

The pressure vessel cooling system would also be unavailable but overall vessel integrity would be retained.

On a shutdown and pressurised reactor the argument above applies. For a shutdown and depressurised reactor natural circulation is not achievable until the reactor is resealed and repressurised. The equipment required to reseal and repressurise the reactor relies on the provision of suitable power supplies.

Conclusion DNB 5.5: A permanently installed on-site system can provide post-trip cooling of a pressurised reactor under a station blackout scenario.

Conclusion DNB 5.6: Whilst arrangements exist to provide resilience against some station blackout scenarios, there is currently no explicit station blackout safety case.

Conclusion DNB 5.7: For a depressurised reactor sufficient cooling cannot be provided under a station blackout scenario because forced gas circulation and equipment necessary for reseal and repressurisation would be unavailable.

Consideration DNB 5.2: Consider making the reseal and repressurisation equipment available independent of installed on-site or off-site power supplies.

Consideration DNB 5.3: Consider the benefit of explicitly reporting the protection measures available for a station blackout.

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

Electrical power is not required to circulate the primary coolant in these scenarios. The battery power systems are used to support control and instrumentation, lighting and diesel starting (amongst other systems). The battery mission times would allow these functional requirements to be readily achieved given operator action to reduce the load on the batteries. Natural circulation cooling is supported by boiler feed derived from direct diesel driven pumps.

Although it may be possible to connect any surviving batteries to restart any surviving diesel generators, this has not been considered in the safety case and the operators have not been trained to perform the necessary operations. Ultimately, if no diesel generators are available there is no opportunity to recharge the batteries.

Conclusion DNB 5.8: No-break battery back-up systems are provided to supply control and instrumentation, lighting and diesel start-up functions. During station blackout, the back-up battery supplies are claimed for a minimum required duration in the current safety case. However, in reality durations may be longer than this with operator action taken to reduce battery loads.

Consideration DNB 5.4: Consider providing supply resilience and recovery actions which would give power supplies for essential control and instrumentation and lighting functions.

5.1.1.3.2 Actions foreseen to arrange exceptional AC power supply from transportable or dedicated off-site source

There is a set of emergency equipment that would support essential safety functions with additional special items to enable forced cooling to be restored to a reactor. This equipment is located remotely off-site and centrally within the UK on trailers to be transported to the affected site within an appropriate time frame following the declaration of an off-site nuclear emergency.

Conclusion DNB 5.9: There are provisions to deploy equipment to station within an appropriate time frame that would provide power generation capability and aid continued post-trip cooling of the reactor.

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

As it is beyond design basis, there is no formal requirement for the training of shift staff to connect the off-site generators to the station.

However, all shift staff go through a structured training programme for their normal duties and specific additional training for the roles they perform as part of the emergency arrangements. In addition to this the advanced gas-cooled reactor twin reactor design means that there is a relatively large complement of shift staff present, who cover a variety of the plant areas. It is therefore anticipated that the disciplines required for carrying out the necessary work to connect off-site supplies to the plant would be available and with the appropriate equipment would be able to carry out required actions for recovery. In a severe accident situation technical experts at the central emergency support centre would

support the technical staff on site by considering the strategies required and formulating a plan to implement those strategies.

Clearly the time then taken on-site to achieve the actions would be dependent on the extent of the work required, which would be a function of the damage to plant by the initiating events.

It is the central emergency support centre organisation which is able to mobilise the beyond design basis trailers, and procure other equipment or consumables. To aid the procurement process there is a standby team of procurement specialists who are part of the central emergency support centre arrangements (see Chapter 6).

Conclusion DNB 5.10: In a severe accident event, actions required by shift staff could be hindered by conditions on-site. Mitigation is provided in the form of the central emergency support centre and procedures for beyond design basis events.

Consideration DNB 5.5: Consider providing training, planning or pre-engineered arrangements in order to improve mitigation measures.

5.1.1.3.4 Time available to provide AC power and to restore core cooling before fuel damage: consideration of various examples of time delay from reactor shutdown and loss of normal reactor core cooling condition

Reactor Pressurised:

A boiler feed system remains available to supply boiler cooling water feed as it is a direct diesel driven pump system. It is judged that provision of minimum boiler feed for the mission time of 24 hours, followed by complete loss of post trip cooling would cause significant fuel damage after something approaching 3 days following station blackout. As mentioned previously, if operators are unable to manage feed flow, feedwater reserves may not be able to provide feed for 24 hours, in which case it is judged that the temperatures that would cause significant fuel damage would be reached in a slightly shorter time.

Reactor Shutdown and Depressurised:

For a depressurised reactor the minimum cooling requirements require forced circulation unless operator action is taken to reseal the pressure vessel and then repressurise the primary coolant to enable natural circulation.

Resealing and repressurising requires operators, equipment and electrical supplies to be available. Once the vessel pressure is greater than the natural circulation cut-off limit and boiler feed is established, then natural circulation cooling will be effective. Station symptoms based emergency response guidelines include recovery actions from limited or no post-trip cooling with the reactor pressurised and depressurised.

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

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

Conclusion DNB 5.11: Existing thermal-hydraulic analysis provides appropriate information on timescales relating to fuel and structural damage scenarios.

Consideration DNB 5.6: Consider providing new additional thermal-hydraulic analysis using the latest route and techniques.

5.1.2 Measures which can be envisaged to increase robustness of the plant in case of loss of electrical power

The preceding sections have shown that there are diverse and redundant provisions for design basis loss of power scenarios. Furthermore, where specific issues have been noted appropriate considerations are raised. These include, across the AGR fleet, consideration of:

- Extended availability of essential stocks
- Improved robustness of reseal and repressurisation arrangements
- Extended control and instrumentation and lighting resilience
- Improved training, planning and pre-engineered provisions in order to improve mitigation measures
- Further transient analysis of severe accident scenarios

Chapter 6 also contains further considerations for additional emergency back-up equipment which would mitigate against the effects of a beyond design basis loss of electrical power.

Conclusion DNB 5.12: The current robustness and maintenance of the plant is compliant with its design basis for loss of electrical power. However, steps to improve the resilience of the plant following a beyond design basis event are being considered.

5.1.3 Loss of the ultimate heat sink

A summary is given below of the reactor cooling systems and their associated key plant that support the essential safety function of provision of adequate post-trip cooling.

The stress-test review of the various scenarios proposed for 'Loss of Ultimate Heat Sink' at Dungeness B and their impact on the plant that is required to carry out the essential safety function is contained within this section and its sub-sections.

Conclusions and judgements are made throughout the sections below and suggested 'Considerations' for improvement are identified. Further potential improvements to the robustness of plant during this scenario are also considered.

The various cooling water systems provided at Dungeness B are described in Chapter 1.

In summary, the main systems are as follows:

- During normal operation, boiler feed is normally supplied by the main boiler feed system; this comprises recirculating boiler feedwater which has been cooled by seawater fed condensers which are supplied by the main cooling water system.
- During shutdown, boiler feed is normally supplied by recirculating feedwater which has been cooled by the seawater fed condensers. Non recirculating boiler feed can also be supplied from three back-up feed system water tanks and the resulting steam is simply vented to atmosphere.
- There is an additional system which provides cooling water to essential items of plant. This system is either cooled by seawater fed condensers using the main cooling water system or by using a back-up cooling water system which takes water from a large lagoon located close to the station. This additional cooling system also provides the heat sink for fuel route cooling plant.

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

Cooling water is taken directly from the sea via twin intakes and then via a single tunnel which discharges into the pump house forebay. Intake grilles prevent large debris entering the forebay and four self-cleaning rotating drum screens, each one serving a main cooling water pump and a seawater cooling water system pump, provide additional debris protection. The drum screens prevent fish, seaweed and marine debris from entering the systems. In addition, chemical control is employed to inhibit biological growth on the drum screens and in the cooling water systems.

A cooling water pump house contains all of the pumps associated with these two cooling systems. The pump house is divided into two halves to provide some segregation, with pumps in each half. This arrangement enables sufficient main cooling water supplies to be maintained for both reactors to allow a controlled shutdown in the event of loss of either chamber.

The operators are trained to protect the cooling water system and the operators would take preventative action such as shutting the reactors down and reducing cooling water flow to ensure that sufficient seawater is available to meet requirements. An alarm in the central control room will indicate that the seawater levels in the forebay have been reduced below a set level.

Conclusion DNB 5.13: Several robust and redundant means of preventing the loss of main and additional cooling water by blockage of the water intakes are employed 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 and the seawater cooling water supplies described above. This is a loss only of the seawater heat-sink.

The loss of main and seawater cooling water flow is within the station safety case and design basis.

Loss of the main cooling water system is considered to be a frequent event as the main pumps are grid supplied. At power, loss of main cooling water would result in the loss of turbine condenser vacuum and lead to both turbines tripping and the inter-tripping of both reactors. With loss of flow the main condenser would be unavailable for boiler feedwater recovery and boiler feed would need to be supplied on a once through basis with venting to atmosphere.

Loss of the seawater cooling water system, including loss of electrical supplies and loss of seawater flow to the pumps, is considered to be an infrequent event. As mentioned previously, owing to the nuclear safety duty of the cooling water system, there is a need for the operators to trip the main cooling water pumps if the drum screens become heavily fouled, in order to ensure that a screened supply of water remains available to the cooling water system.

On loss of the seawater cooling system there would be insufficient cooling of the recirculating water system which in turn provides cooling for the gas circulator oil systems, the pressure vessel cooling systems and reactor seal oil systems. However, as described below an alternative heat sink exists which ensures the availability of these essential items of plant, so they would continue to be operable.

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

Boiler feed and heatsink

On loss of boiler feedwater and subsequent recovery and recirculation, once through boiler feed with venting to atmosphere is sufficient for post-trip cooling. Feedwater can be obtained from various on-site tanks and supplied to the boilers using one of a number of feed systems.

There are three separate systems, each with their own dedicated tanks of water which can provide a minimum of 24 hours cooling to both reactors for each of the systems. In addition to this there is the potential to top up these tanks with an alternative (low quality) water supply which could be used if required in extreme circumstances. These connections are not permanently installed, however operator instructions exist and the operators are trained in the necessary actions.

Seawater equipment cooling

The seawater cooling water system provides cooling for most of the plant and equipment with a nuclear safety duty including:

- Vessel cooling systems which ensure the integrity of the reactor pressure vessel
- Gas circulator lubricating oil and seal oil cooling which are needed for forced gas circulation
- Cooling pond water coolers.

On loss of cooling from the seawater cooling water system using the seawater fed system, sufficient cooling can be provided by connecting a back-up cooling system. This back-up cooling system is started manually, and normally shut

motorised valves are opened to allow the flow of water into the recirculating water reactor ringmain. The reactor ringmain however does not serve cooling ponds or other fuel route heat loads.

The back-up cooling system is a once through system and takes water from two interconnected disused gravel pits which are now filled with brackish water forming lagoons. These are situated close to the station site. The lagoons have a large capacity which is sufficient for the cooling demands of the equipment for a 24 hour mission time provided that the flow is managed by the operators.

Conclusion DNB 5.14: Diverse alternative heat sinks for primary circuit cooling (boiler feed) and essential equipment cooling exist in case of loss of the primary ultimate heat sink (the sea) – this scenario is covered by the existing safety case.

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

Boiler Feed and Heat-sink

The boiler feed systems described previously are permanently installed and connected systems, each with sufficient capacity to ensure adequate post trip feed for at least 24 hours. The feedwater stock levels are monitored and station technical specifications set minimum levels that must be maintained with stated actions if the minimum levels are not met.

Additional time can be achieved by using the back-up cooling system to top up the tanks associated with the three cooling systems described above or by transferring stocks between tanks.

After a maximum of 24 hours, essential stocks are assumed to be available from off-site sources and capable of being delivered to site. The EDF Energy safety cases and emergency arrangements (see Chapter 6) have been developed to achieve this. In extreme circumstances seawater could be introduced to the boilers but this would only be enacted once all possible freshwater stocks had been exhausted and would require provision of mobile pumps from off-site. It can be seen that if the feedwater tanks remain intact there are many days worth of boiler feed on site which will prevent significant reactor fuel or structural degradation.

Seawater Equipment Cooling

As previously mentioned, the back-up cooling water system has access to sufficient lagoon water for the 24 hour mission time. After the 24 hour mission time it is assumed that supplies would be available from off-site sources and delivered to site.

Although there is an extract licence which limits the quantity of water than can be extracted from the lagoons in a short period of time, during a potential incident a decision would need to be made on whether more water could be extracted if needed to ensure nuclear safety.

Conclusion DNB 5.15: In the event of a loss of the ultimate heat sink, there are sufficient stocks of cooling water for a minimum period of 24 hour.

Consideration DNB 5.7: Consideration should be given to the practicability of extending the availability of essential stocks of cooling water, by either providing additional on-site storage facilities or additional means to replenish stocks to allow an extended operating period.

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

This event proposes the loss of all seawater and all alternate cooling systems through failure or unavailability. This is a total loss of all otherwise available cooling via any systems available.

The loss of both the primary ultimate heat sink (access to seawater cooling) and the alternative heat sink (essential equipment cooling from back-up systems) is not covered in the existing safety case as it is considered to be a beyond design basis event owing to the number of different back-up cooling systems available. This scenario involves the loss of two independent and segregated essential equipment cooling systems as well as the loss of three independent feed systems to all four boilers on each reactor. Trip and shutdown would not be affected but with loss of all boiler feed there would be no means of removing the decay heat from the primary circuit and the fuel and reactor internal structures would begin to overheat. The timescales to loss of integrity and potential actions to prevent any failure are discussed below.

5.1.3.3.1 External actions foreseen to prevent fuel degradation

In this total loss of cooling scenario, the key action required would be to restore feedwater to at least one boiler on each reactor if they were pressurised. For a depressurised reactor the operators would first need to reseal and repressurise the reactor and then restore boiler feed to establish natural circulation of the primary cooling circuit gas. Alternatively, restoring essential equipment cooling and boiler feed would allow forced gas circulation, without the need to reseal and repressurise the reactor. Whilst pressure vessel cooling is desirable, in these unlikely scenarios, it is not essential as adequate integrity of the pressure vessel has been demonstrated without this cooling being available.

There is a set of emergency equipment that would support essential safety functions with additional special items to enable forced cooling to be restored. This equipment is located remotely off-site and centrally within the UK on trailers to be transported to the affected site and deployed within an appropriate timescale following the declaration of an off-site nuclear emergency (Chapter 6).

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

Pressurised Reactor

If the ultimate and alternative heat sinks are lost then boiler feed and forced gas circulation would be lost. On a pressurised reactor the high natural circulation coolant gas 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, although the relevant timescales are many hours even under the most pessimistic conditions.

For this total loss of cooling scenario if a viable boiler feed can be restored within several hours, the situation is recoverable and severe core degradation should not occur. The timescale to loss of integrity would be extended if a controlled blow down of the reactor were to be initiated. This would assist in allowing time to deploy the off-site emergency equipment referred to in the previous section. A sensitivity study has been carried out which indicates that if the boilers are fed for a time following shutdown before then being lost, then the timescale on which feed needs to be restored is increased accordingly. Each additional period of initial boiler cooling gives further extension to the time available to restore longer term cooling.

Shutdown and Depressurised Reactor

If the reactor is depressurised then natural circulation is not possible. Loss of equipment cooling would also result in the loss of forced gas circulation and therefore there would be very little heat transfer from the fuel to the structures.

In this scenario a reactor would not be in a depressurised state unless it had been shutdown for many days and the decay heat was below clearly specified limits. In this scenario there would be longer to recover and it is judged that the timescales would be similar to those discussed in Section 5.1.1.3.4 which looked at loss of forced gas circulation with boiler feed remaining from the direct diesel driven feed system.

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 (seawater cooling) as well as a complete station blackout comprising loss of off-site power supply as well as loss of all back-up power supplies.

If loss of primary ultimate heat sink coincided with station blackout but the alternative heat sink was still available, an alternative cooling system could provide boiler feed on a once through basis, venting to air. This is the same as the station blackout scenario addressed in Section 5.1.1.3 above.

A further scenario in this report is for the unlikely event of complete station blackout on a pressurised reactor and a loss of all heat sinks, including all direct diesel driven pump systems. In this case, the estimate is that important structural failures would occur after several hours, implying that if boiler feed can be restored before then, the situation is recoverable and severe core degradation should not occur. This scenario is the same as the loss of 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

Advanced Gas-Cooled Reactors do not use water in the primary cooling circuits of its reactors. The cooling medium is pressurised CO₂ gas.

The loss of the CO₂ gas, which is used as the primary circuit 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 following the unlikely event of a station blackout and loss of primary ultimate heat sink will be focused on providing additional means to cool the reactor and the fuel.

The provision of external sources of boiler feed is required, combined with both the reseal and repressurisation of the primary circuit or forced circulation for the depressurised case. Hence there is a requirement for power and boiler feed.

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

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

The preceding sections have shown that there are robust provisions for design basis loss of heat sink scenarios. The reactor design is generally tolerant to the loss of the primary ultimate heat sink as a result of the inherent capacity to transfer heat to atmosphere. Hence, fewer specific issues have been identified when compared with the loss of electric supplies scenarios.

It should be noted that a consideration to extend the availability of essential stocks for severe accident scenarios has been raised.

Conclusion DNB 5.16: The current robustness and maintenance of the plant is compliant with its design basis for loss of the ultimate heat sink. However, steps to improve the resilience of the plant following a beyond design basis event should be considered.

5.1.5 Licensee Review of Robustness

The Licensee Board required a number of reviews to be carried out in the days immediately following the events in Fukushima.

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 the 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, it was noted that enhancements to the 24 hours mission time for essential stocks could be beneficial.

Disabling reactor cooling while shutdown in air at the advanced gas-cooled reactors would be a particular challenge: there is no identified cooling arrangement for a reactor in air in the event of loss of all electrics. Cooling requires either forced gas circulation, or the reactor to be resealed and repressurised, both of which require electrical supplies.

Loss of non-essential equipment will provide additional challenges for longer term events and various locations have local fire fighting air compressors that will not be resupplied and eventually will lead to deluge valve trips and wetting of equipment and additional demands of water/fuel stocks plus operator action to terminate.

Access issues will be created by loss of supplies at most sites, requiring manual breaching of fences/turnstiles around certain plant areas.

Conclusion DNB 5.17: The current robustness and maintenance of the plant is compliant with its design basis against loss of electrical supplies and ultimate heat sink. However, steps can be made to improve the resilience of the plant for a beyond design basis event.

Consideration DNB 5.8: Consideration should be given to increasing the provision of off-site back-up equipment including: equipment to enable boiler feed; a supply of suitable inert gas for primary circuit cooling; electrical supplies for lighting, control and instrumentation.

5.2 Spent fuel storage pools

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

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

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

5.2.1 Loss of electrical power

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

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	Cooling lost, timescales to recover as per Chapter 1. Note that diesel driven pumps can top up water level.
Effect of loss of grid and on-site generation	Manual operation available for movement of fuel, adequate passive cooling available.	Cooling lost, timescales to recover as per Chapter 1.	Cooling lost but passive cooling acceptable (see Chapter 1)	Cooling lost, timescales to recover as per Chapter 1. Note that alternative means could be set up to top up water level using e.g. diesel driven pumps.

Conclusion DNB 5.18: In either the event of both loss of grid or station blackout, sufficient cooling can be maintained to the station fuel route areas for a 72 hour mission time.

5.2.2 Measures which can be envisaged to increase robustness of the plant in case of loss of electrical power

The preceding sections have shown that there are robust provisions for design basis loss of power scenarios. Furthermore, there are also arrangements for mitigation of the effect of loss of power faults beyond design basis.

Generic measures set out in Section 5.1.2 to increase robustness of the plant in case of loss of electrical power would also increase robustness of the fuel route plant areas

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

Conclusion DNB 5.19: Whilst there are no vulnerabilities identified in the current design basis for the fuel route against loss of electrical power, further resilience enhancements can be envisaged.

Consideration DNB 5.9: To improve resilience of decay store cooling against loss of electrical power, consider possible enhancement options in respect to guidance to operators, fault recovery techniques, and improved understanding of credible consequences.

Consideration DNB 5.10: To improve resilience of pond cooling and make up against loss of electrical power, consider possible enhancement options in respect to guidance to operators, replenishment of lost pond water, and standalone pond cooling facilities having no dependence on any other station supplies or systems.

5.2.3 Loss of the ultimate heat sink

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

Stage of fuel storage and	Handling with	Buffer storage	Dismantling	Storage in ponds
---------------------------	---------------	----------------	-------------	------------------

handling	fuelling machine			
Primary heat sink	Ambient air - loss not credible	Sea	Sea- loss is tolerable as per Chapter 1	Sea
Secondary heat sink	-	Fresh water from lagoon	-	-
Tertiary heat sink	-	-	-	-

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

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

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

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

Conclusion DNB 5.20: Whilst there are no vulnerabilities identified in the current design basis for the fuel route against loss of ultimate heat sink, further resilience enhancements can be envisaged.

Consideration DNB 5.11: To improve resilience of decay store cooling against the loss of the ultimate heat sink, consider possible enhancement options in respect to guidance to operators, fault recovery techniques, and improved understanding of credible consequences.

Consideration DNB 5.12: To improve resilience of pond cooling and make up against the loss of the ultimate heat sink, consider possible enhancement options in respect to guidance to operators, replenishment of lost pond water, and standalone pond cooling facilities having no dependence on any other station supplies or systems.

Chapter 6 – Severe Accident Management

Dungeness 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 company's generic approach to emergency planning each EDF Energy Nuclear Generation power station adopts the emergency organisation depicted below in Figure 6.1:

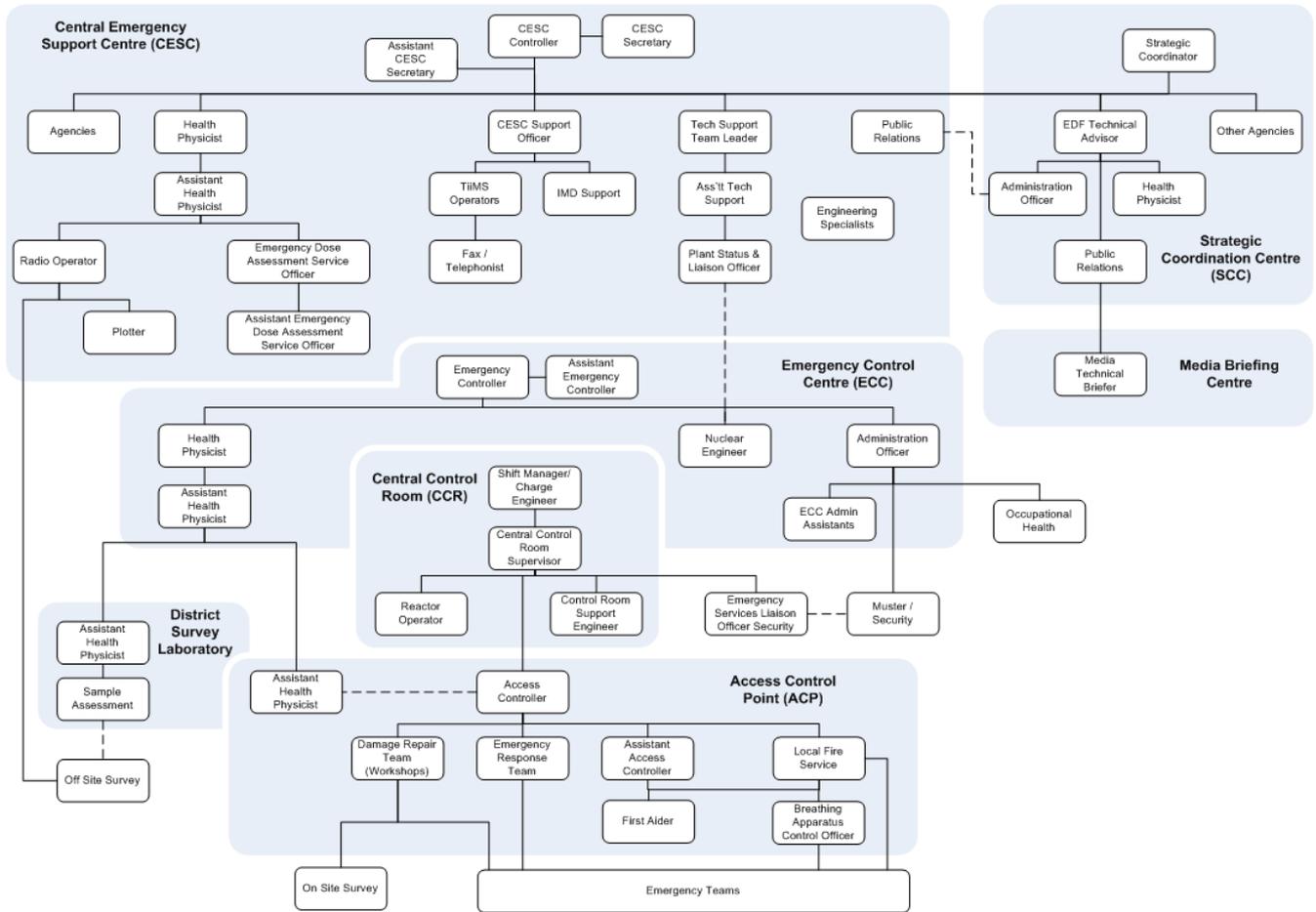


Figure 6.1: EDF Energy Generic Emergency Response Organisation

EDF Energy Nuclear Generation has adopted two declaration states which are as follows:

Site Incident is a hazardous condition which is confined within the boundary of a Nuclear Licensed Site. A site incident could be an accident that is not necessarily nuclear in nature, but possibly a fire or a chemical incident. It may involve the plant becoming hazardous in some way but with no release of radioactivity to an area outside the site boundary.

Off-site Nuclear Emergency is a hazardous condition which results in or is likely to result in the need to consider urgent countermeasures to protect the public outside the site security fence from a radiological hazard. A site incident will usually need a more limited response than an off-site nuclear emergency.

During an emergency of either type, the following centres operate on the station site, working together to provide a co-ordinated and focused response. The centres are detailed below:

Central Control Room

Within the central control room there are dedicated facilities to enable the initial management of the site, take command of the response organisation and interface with external support during an emergency. Once the duty Emergency Controller takes responsibility, the central control room will be used to manage and co-ordinate the ongoing activities in the damaged area of the site and to make the plant safe. The facilities include maps, station procedures, drawings, communications equipment, tenability monitoring equipment, wind speed and direction indicators, plotting equipment, log sheets and general stationery. The initial location will normally be the central control room, however should the need arise an alternative indication centre is available and is similarly equipped.

Emergency Control Centre

The emergency control centre at Dungeness B is a dedicated facility to enable the site to be managed, command of the internal response and interface with external support during an emergency. Should the need arise an alternative emergency control centre is available.

The basic equipment provided in the emergency control centre includes maps, station procedures, drawings, communications equipment, tenability monitoring equipment, wind speed and direction indicators, plotting equipment, log sheets and general stationery.

The staff will include the following key personnel available on a 24 hour standby rota to become operational as part of emergency arrangements:

- Emergency Controller.
- Emergency Health Physicist.
- Emergency Reactor Physicist.
- Assistant Emergency Controller.
- Emergency Administrative Officer.
- Emergency Control Centre Communication Co-ordinator.
- Emergency Control Centre Support Staff.
- Security Liaison

Access Control Point

For any event which creates an uncontrolled hazardous area, an entry and egress point will be established to enable command and control activities to be carried out safely in the area. The control point will be located as appropriate for the event, taking into account the prevailing conditions. In its simplest form this may be a single barrier, e.g. in a road for minor fires.

For all events a dedicated access control point facility is available and will be established to provide safe, controlled and rapid access to the affected area. Should the primary access control point be untenable an alternative access control point is available. All access to the affected area will be made through an access control point. Exceptionally other routes may be used but only with the agreement of the access controller.

The access control point and its alternative are equipped with means of communicating directly with Emergency Teams and the central control room. There is adequate space, equipment and facilities for the contamination, radiation dose and breathing apparatus control necessary for the safe and effective dispatch and reception of emergency teams, including emergency services, and for the initial treatment of casualties.

Site Access and Egress Control

Within the security lodge there are dedicated facilities to enable the site to be secured, initiate the roll call and manage access and egress from the site including the emergency services. The facilities include: maps, emergency procedures, communications equipment and tenability monitoring equipment.

The initial location will normally be the main security gatehouse controlling site access but, depending on the location of the emergency and the prevailing environmental conditions, an alternative site access facility is available and can be similarly equipped.

Declaration of an event

The central control room is manned at all times and has access to detailed information on the state of the plant. In the event of this information indicating abnormal conditions, the shift manager will carry out an immediate investigation and assessment. If the situation demands, the shift manager will initiate actions in accordance with the conditions for declaring a site incident or an off-site nuclear emergency.

Depending upon the nature and duration of an accident the emergency organisation may evolve in three stages:

Stage 1 begins with the declaration of a site incident or off-site nuclear emergency. Trained staff from the nuclear power station forms a site emergency response organisation under the command of the Emergency Controller. The Emergency Controller is responsible for initiating the emergency actions to be taken by EDF Energy staff, and for alerting the off-site organisations which have responsibility for countermeasures to protect the public.

Stage 2 occurs when EDF Energy Nuclear Generation establish a central emergency support centre at the EDF Energy offices located in Barnwood, Gloucestershire. For an off-site nuclear emergency a Strategic Co-ordination Centre and associated Media Briefing Centre will be activated by the Police.

During a Site Incident, the central emergency support centre will provide technical support to the nuclear power station as necessary and, at the appropriate time agreed with the Emergency Controller, take over responsibility for off-site monitoring for radioactive release to continuously assess the possibility of the site incident developing into an off-site nuclear emergency.

During an off-site nuclear emergency, the central emergency support centre, staffed by EDF Energy staff, together with other relevant organisations, will at the appropriate time as agreed with the Emergency Controller, take over control of the deployment of the off-site monitoring resources, assessment of the need for countermeasures and provision of expert advice to the Strategic Co-ordination Centre. The central emergency support centre will also co-ordinate the technical support to the station.

Stage 3 occurs in an off-site nuclear emergency only, when the Department for Energy and Climate Change appoints a Government Technical Adviser who, after briefing, will assume the responsibility for giving authoritative advice to Police, Local and Health Authorities, and other off-site organisations on any actions necessary to protect the public. The EDF Energy Nuclear Generation Company Technical Adviser and team will support the Government Technical Adviser in this role and continue to liaise with the central emergency support centre Controller. The Government Technical Adviser will be the principal Government spokesperson for briefing the media.

Emergency Response Staffing

EDF Energy Nuclear Generation emergency arrangements have been developed, embedded and tested against minimum staffing levels for emergency response roles for each nuclear power station in the EDF Energy nuclear generation fleet.

The basis for the current emergency scheme staffing levels was established through systematic analysis. This analysis used an assessment of risks and hazards to identify emergency task requirements. These emergency task requirements were, in turn, used to identify emergency scheme staffing levels and enhancements required for equipment and training.

Emergency plan actions and guidelines have been designed against a minimum staffing resource and with the objective for emergency response to be effective using staff from the power station for the initial 60 minutes of an emergency. The staffing resources are derived for a reasonable foreseeable accident involving a reactor event and release of radioactivity. For other events the resources will be managed to provide additional expertise or staffing levels as required. The emergency roles are staffed from both 'Shift Staff' who would be on-site at the time of an emergency and from 'Standby Staff' who may not be on-site at the time of emergency, but who can attend site within a 60 minute timeframe.

Shift Staff: A record of the current shift staffing is available from the central control room indicating cover for emergency roles which will meet or exceed the minimum manning levels defined. The operations team leader maintains the staffing level for the next 24 hour shift cycle. Any changes in staffing levels during this period will be communicated to the central control room. Part of the shift handover procedure is to ensure that the emergency role responsibility has being passed on effectively.

Dungeness B Incident Response Team is made up of a Fire Team and Intervention Team. The Fire Team consists of staff trained in Breathing Apparatus, First Aid, Casualty Handling and Rescue, Rescue from Confined Spaces, on-site monitoring, Chemical and Fire Response. The intervention team are breathing apparatus wearers that are trained to provide an initial assessment of the damage area, carry out emergency plant operations, complete monitoring and damage control activities.

The Damage Repair Team consists of Maintenance shift personnel who are trained breathing apparatus wearers. Their key objective is the engineering of permanent damage repairs, with an additional role of carrying out on-site surveys.

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 time scale 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. Dungeness B are in the process of aligning with the company process associated with emergency scheme training.

Dungeness B has evaluated the exercising and training associated with beyond design basis events and concluded the frequency and content should be altered to reflect the needs of role holders more accurately.

Exercising

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

The following describes the types of exercises, personnel involved and frequency of exercise type:

Table 6.1: Emergency Exercising Arrangements

Exercise Type	Description	Frequency
Assessment and Training Drill	An exercise limited in content to test/demonstrate one or two defined areas of the emergency arrangements, e.g. access control points, off-site survey and District Survey Lab, muster roll-call and site security for training purposes or test/develop skill base of participants.	As required
Shift Exercise	An exercise focused on the activities of the whole shift staff complement to demonstrate their ability to deal with the consequence of a simulated event. Areas of activity are limited to the central control room, Access Control Point and Emergency Teams. Any support staff from days that could assist in these areas may be included for training purposes.	Annually
Desk Top Exercise	Focused on an emergency facility in operation and driven by simulating realistic inputs to the facility	As required
Full Scope Exercise	An exercise involving the whole of the nuclear power station. It may extend to full station roll-call and may include external agencies such as emergency services for training purposes. These exercises are not witnessed by the Office for Nuclear Regulation. These exercises are used to ensure any training or new procedures associated with the emergency arrangements can be evaluated as part of internal regulation of standards.	Annually
Level 1	An exercise – usually annually- involving all nuclear power station staff, visitors and contractors, to demonstrate the adequacy of the current approved emergency arrangements to the Office for Nuclear Regulation. These exercises may involve emergency services and other external organisations. The extent to which the interface with the Strategic Coordination Centre and central emergency support centre in dealing with off-site implications is tested will be decided by EDF Energy Nuclear Generation or as required by Office for Nuclear Regulation	Annually

Exercise Type	Description	Frequency
Level 2 (off-site plan)	These exercises are aimed specifically at demonstrating the functions of the Strategic Coordination Centre and central emergency support centre in dealing with off-site implications of an emergency on the basis of a defined input from the site. The Office for Nuclear Regulation will provide a Government Technical Adviser. EDF Energy Nuclear Generation, the Local Authority and Emergency Services will normally be involved to test the interactions between various parties and the decision making process. The aim will be to demonstrate the function of the central emergency support centre and Strategic Coordination Centre once every three years.	Every 3 years
Level 2 (support station)	A team from the dedicated support station consisting of Emergency Controller, Health Physicist, Admin Officer and Communications Co-ordinator will respond to the Strategic Coordination Centre in the event of an off-site nuclear emergency being declared at the affected power station. This is tested on a three yearly basis and involves the aforementioned personnel responding and operating within the designate Strategic Coordination Centre facility.	Every 3 years
Level 3	A Level 2 exercise, nominated by Department for Energy and Climate Change and the Scottish Executive, will be enhanced to become the relevant Level 3 exercise and the aim will be to have one such exercise within the nuclear industry each year. As per a Level 2 exercise, but additionally includes Central Government response and interactions between Government Departments and Ministers.	One such exercise within the nuclear industry each year
Counter Terrorism (CT) Exercise	An exercise – usually annually- involving all station staff, visitors and contractors, to test the adequacy of the site and company Counter Terrorism plan arrangements to the Office for Nuclear Regulation. These exercises may involve emergency services and other external organisations.	Annually
RADSAFE Exercise	An exercise, usually conducted annually, involving nuclear power station and other EDF Energy staff, to test the adequacy of the site and company arrangements for accidents involving the transport of radioactive materials, attended by the Department for Transport. These exercises may involve emergency services and other external organisations	Annually

The exercising regime aligns with the requirements of The Radiation Emergency Preparedness and Public Information Regulations.

In order to ensure that the full breadth of the arrangements is adequately exercised, EDF Energy Nuclear Generation manages a rolling programme of exercising to include the alternative response centres and back-up contingencies.

In addition to annual exercise drills, the management team at the nuclear power stations aim to undertake at least 6 full site emergency exercises per year. One of these exercises is formally witnessed by the Office for Nuclear Regulation as the annual Level 1 exercise. In addition to the Level 1 exercise, the station is required to complete a Level 2 demonstration exercise every three years.

For all the witnessed exercises the team of inspectors from the ONR and assessors from EDF Energy will review the adequacy of the emergency arrangements and highlight any identified areas for improvement. A timetable of improvements is established in consultation with the Office for Nuclear Regulation and EDF Energy. This is subject to review at an annual emergency arrangements review meeting between the Office for Nuclear Regulation and Station. This rigorous annual review process ensures the station emergency arrangements satisfy the site licensing requirements.

The emergency exercise planning and administration documentation contains information regarding the processes defining the activities that take place when planning and reviewing emergency exercises and defining the activities for modular exercises. This includes timescales, activities, tasks, responsible personnel and completion dates. Following an

exercise thorough debriefs take place to ensure lessons and improvements are identified, captured and any resulting actions recorded.

Conclusion DNB 6.1: EDF has detailed robust arrangements for Emergency Response which are subject to a programme of continuous improvement and exercised as required by standard procedures and regulatory demand.

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

Consideration DNB 6.1: Alignment of Dungeness B with generic role profile for responding ACP teams would enhance their resilience due to an increase in skills available.

Consideration DNB 6.2: EDF energy will consider how lessons identified from Japan and credible beyond design basis events can be reflected in our facilities, procedures, training and exercise programmes. Utilising experience from other emergency response organisations and the military, EDF will consider enhancement of its staff welfare, human factors and emotional aspects associated with emergency response.

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

Consideration DNB 6.3: EDF Energy will consider further resilience enhancements to its equipment and critical supplies which take onboard lessons of extendibility and issues that prolonged events could present. Extensive work has already begun to highlight updates to equipment, its location and deployment.

6.1.2.3 Management of radioactive releases, provisions to limit them

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

At Dungeness B there is a system that allows the reactor gas coolant to be blown down for operational reasons. All contaminated gases discharged from the reactor, the bypass plant, the circulators, the fuelling machine and other fuel handling facilities, must pass through the blowdown system so that the activity is reduced to a safe level. Blowdown occurs via the various blowdown routes and may pass through particulate filters and the main iodine adsorption plant, before being discharged to atmosphere via the main exhaust.

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

Management advice to minimise release of activity to the environment can be found in symptom based emergency response guidelines and severe accident guidelines.

A Detailed Emergency Planning Zone is provided around a nuclear installation, where there is the potential for an off-site release of radioactivity that would require implementation of countermeasures.

The Detailed Emergency Planning Zone is defined on the basis of the most significant release of radioactive material from an accident, which can be reasonably foreseen. In the event of an accident being larger than the reasonably foreseeable event, arrangements are in place for extending the Detailed Emergency Planning Zone consistent with the concept of 'extendability'.

A number of emergency preparedness activities take place within the Detailed Emergency Planning Zone around EDF Energy Nuclear Generation sites. As part of the company's responsibility under Radiation (Emergency Preparedness & Public Information) Regulations, prior information in the form of a calendar is produced and distributed to residents within the zone, these contain information about what to do in the event of an emergency event and other factual information regarding the radiation. Potassium iodate tablets are also distributed to residents within the area. Residents are also given the option to be added to a Public Emergency Telephone Information System, which would notify them of what action to take in the event of an emergency at their local power station.

6.1.2.4 Communication and information systems (internal and external)

The station has substantial diversity of communications media to ensure requirements are met during a response situation. The on-site links include the use of the station's routine telephone networks - Private Automatic and Branch exchange lines, and a number of BT telephone lines together with dedicated direct wire telephones linking the on site response centres. Across the nuclear power station, the 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 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 DNB 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.

The primary use of the Dungeness B Power Station’s site radio system is for day-to-day operations. There is not a dedicated emergency channel; however emergency calls have priority. The system comprises of four channels, hence the loss of a channel would reduce the through put of radio traffic (no loss of site coverage). Only if all four channels were lost would radio communication cease on site. Three of the four trunk controllers have telephone cards fitted enabling calls to be made from a radio to a site telephone and vice versa.

Potential enhancements have been identified in the 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 DNB 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 DNB 6.4: EDF Energy should 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 Dungeness B 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.

In general, the equipment in the control room has not been functionally qualified to withstand a bottom line seismic event, and is not claimed as essential plant, although it is expected to remain habitable. Should for any reason the control room need to be evacuated, an alternative indication centre provides a single area from which the status of the trip, shutdown and post-trip cooling of the two reactors can be monitored.

This alternative indication centre provides the operator with post-trip indications and has been designed to withstand the infrequent level event. The facility has an uninterruptible power supply and is powered by an electrical supply (which is also seismically qualified). Local plant indications may also be available.

6.1.3.5 Impact on the different premises used by the crisis teams or for which access would be necessary for management of the accident.

EDF Energy conducted a recent review of access control points and emergency control centres during or after external events, and on operators' actions following the events. This detailed review outlined the impacts on the existing facilities from a range of external hazards.

These facilities are generally qualified for the full range of external hazards and where they are not alternatives have been identified. The central emergency support centre which is responsible for management of the accident is remotely located from all nuclear power sites.

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

Consideration DNB 6.5: EDF Energy will consider a review of its mobile facilities and the resilience of equipment contained within.

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

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

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

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

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

Off-site monitoring - there is an established process for providing off-site countermeasures advice to protect the public during a release of radiation from a site involving mobile sampling vehicles. One of the lessons identified from the

Japanese Earthquake was the inability of off-site monitoring vehicles to access pre-determined monitoring locations and determine the levels of radiation that were being discharged off-site.

Conclusion DNB 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 DNB 6.6: EDF Energy should consider reviewing existing arrangements to ensure the principles of extendibility are adhered to.

6.1.3.7 Unavailability of power supply

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

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

6.1.3.8 Potential failure of instrumentation

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

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

6.1.3.9 Potential effects from the other neighbouring installations at the site

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.

Dungeness B power Station is situated next to the Magnox owned Dungeness A site. Dungeness A ceased to generate power at the end of 2006 and is working through a decommissioning process. The radiological hazard from Dungeness 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 DNB 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 DNB 6.7: Further mitigation against the effects of beyond design basis accidents could be provided by additional emergency back-up equipment. This equipment could be located at an appropriate off-site location close to the station to provide a range of capability to be deployed in line with initial post-event assessment. This equipment may include the following capabilities:

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

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

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

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

1. The fuel matrix.
2. The fuel clad and
3. The primary circuit (pressure vessel / containment).

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

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

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

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

If severe fuel damage has occurred, or is anticipated, or if applying symptom based emergency response guidelines advice has not controlled fission product release, the Emergency Controller would consult the severe accident guidelines for advice on limiting the release. The severe accident guidelines advice is broadly based, to deal with unanticipated

situations, and uses existing plant in standard and innovative techniques. In addition, some advice calls for equipment and material not normally held on site.

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 DNB 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 DNB 6.8: EDF Energy to review the adequacy of training in the use of the severe accident guidelines and the feasibility of implementing the advice in real scenarios

6.2.1 Elimination of fuel damage/meltdown in high pressure

6.2.1.1 Design provisions

The power density of the advanced gas-cooled reactor is lower than that in light water reactors. For loss of post-trip cooling, this leads to much longer times before any significant fuel damage, in particular the fuel matrix and clad remain intact for a longer period. This means that high pressure ejection of the corium (fuel containing materials) from the vessel is not possible.

6.2.1.2 Operational provisions

There are no specific operational provisions for this scenario as it is not possible in an advanced gas-cooled reactor.

6.2.2 Management of hydrogen risks inside the containment

The extensive damage to essential plant at Fukushima led to oxidation of the Zircaloy fuel clad and hydrogen formation. When this was vented into upper containment buildings it formed an explosive mixture with oxygen in the ambient air. The resulting explosions destroyed the building causing further damage and challenging the accident management.

In his consideration of the implications for the UK Nuclear Industry, the Chief Nuclear Inspector concluded that hydrogen formation was not a hazard for advanced gas-cooled reactors.

Therefore for the advanced gas-cooled reactor design this section addresses the carbon monoxide risks identified rather than discussing hydrogen.

6.2.2.1 Design provisions, including consideration of adequacy in view of hydrogen production rate and amount

Within the design basis there is no carbon monoxide hazard in an advanced gas-cooled reactor and as such there is no requirement for design provisions to be made.

6.2.2.2 Operational provisions

The severe accident guidelines warn of the gas flammability hazard associated with vessel failure and molten-fuel-concrete interactions. It is considered that the existing advice on containing fission products would minimise the flammable-gas threat to damage control teams and to accident management. Ducting off-gas through a filter, to remove radioactive aerosols, requires that the filter be cooled to remove decay heat. This would also remove any tendency for the gas to auto-ignite. It might, however, be necessary to arrange for the gas to be flared.

6.2.3 Prevention of overpressure of the containment

6.2.3.1 Design provisions, including means to restrict radioactive releases if prevention of overpressure requires steam/gas relief from containment

The final containment barrier on an advanced gas-cooled reactor is the Pre-stressed Concrete Pressure Vessel. The normal operating pressure within this structure is 30 bar, as it is the main pressure retaining part of the reactor.

The design of the advanced gas-cooled 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.

Although the control rods are an extremely reliable system, a secondary system incorporating nitrogen injection provides defence in depth. A tertiary system involving water injection provides further means to controlling criticality over a longer period of time.

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

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

6.2.4.2 Operational provisions

It can be seen from the description of the various plant items available that the primary documents relating to hold-down of the reactor are the normal operating instructions. These are, then supplemented by the symptom based emergency response guidelines and the severe accident guidelines should the plant move in to a beyond design basis scenario.

There is guidance presented in these documents on how to protect against an increase in reactivity that would lead to the potential for re-criticality.

6.2.5 Prevention of basemat melt through

6.2.5.1 Potential design arrangements for retention of the corium in the pressure vessel

This situation is considered to be beyond the design basis for an advanced gas-cooled reactor due to the low power density and other design provisions of the reactor. Nonetheless there are arrangements in place for the severe accident scenario.

The pressure vessel, due to its construction, provides the best means of long term containment of a degraded core. For the prevention of basemat melt through the critical safety function is containment and advice and recommendations are given in severe accident guidelines.

6.2.5.2 Potential arrangements to cool the corium inside the containment after reactor pressure vessel rupture

The possible arrangements to cool the corium inside the containment after reactor pressure vessel rupture would involve the use of the installed pressure vessel cooling water pipework system for the concrete pressure vessel or direct injection of water, as advised in severe accident guidelines.

A potential alternate strategy to cool the vessel is by passing water along the pre stress tendon ducts which pass through the concrete.

Advice and recommendations for alternate cooling strategies are also found in severe accident guidelines.

6.2.5.3 Cliff edge effects related to time delay between reactor shutdown and core meltdown

In an extremely unlikely scenario of inadequate cooling for a prolonged period, it is inevitable that fuel will melt and the core start to fail. The timescales for this to happen in an advanced gas-cooled reactor are considerably larger than for a pressurised water reactor allowing arrangements for the severe accident management plan to be implemented.

This time delay should leave sufficient scope for the adoption of cooling, utilising improvised methods as advised in the severe accident guidelines, to mitigate against any possible cliff edge effects.

6.2.6 Need for and supply of electrical AC and DC power and compressed air to equipment used for protecting containment integrity

6.2.6.1 Design provisions

The vessel is the third layer of containment after the fuel matrix and clad. The concrete structure and the steel penetrations provide a barrier to fission products. It would, though, be desirable to seal the breach which caused the depressurisation. To meet design basis standards, the vessel is reliant on its own cooling system and other core cooling systems which in themselves may be reliant on AC power supplies when pressurised.

If depressurised and without cooling, the vessel would still function as a passive containment. Studies have shown that, without cooling, the concrete structure would withstand self-weight loads for at least 14 days after excessively high internal temperatures

6.2.6.2 Operational provisions

The severe accident guidelines advise on protecting the containment provided by the vessel after 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 DNB 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 DNB 6.9: EDF Energy should consider a review, extension and retraining for the sbergs.

Consideration DNB 6.10: Consideration should be given to providing further mitigation against the effects of beyond design basis accidents, by additional emergency back-up equipment. This equipment should provide additional diverse means of ensuring robust, long-term, independent supplies to the sites. This equipment should be located at an appropriate off-site location close to the station to provide a range of capability to be deployed in line with initial post-event assessment. This equipment may include the following capabilities:

- **Equipment to enable pressure vessel cooling.**
- **Supply of suitable inert gas for primary circuit cooling.**
- **Equipment to enable boiler feed.**
- **Compressed air supply for decay tube cooling.**
- **Electrical supplies for primary circuit coolant circulation.**
- **Equipment to enable fuel pond cooling.**
- **Emergency command and control facilities including communications equipment.**
- **Emergency response/recovery equipment.**
- **Electrical supplies for lighting, control and instrumentation.**
- **Water supplies for cooling from non-potable sources.**
- **Robust means for transportation of above equipment and personnel to the site post-event.**

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 DNB 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 advanced gas-cooled reactor design there are additional fuel route plant areas, measures to enhance robustness in these areas have been considered in Chapter 5.

Consideration DNB 6.11: Consideration should be given to providing further mitigation against the effects of beyond design basis accidents by the provision of additional emergency back-up equipment. This equipment could provide additional diverse means of ensuring robust, long-term, independent supplies to the ponds. This equipment could be located at an appropriate off-site location close to the station to provide a range of capability to be deployed in line with initial post-event assessment. This equipment may include the following capabilities:

- Equipment to enable fuel pond cooling.
- Emergency command and control facilities including communications equipment.
- Emergency response/recovery equipment.
- Electrical supplies for lighting, control and instrumentation.
- Water supplies for cooling from non-potable sources.
- Robust means for transportation of above equipment and personnel to the site post-event.

It would be appropriate, if this equipment was developed and in any case to capture learning from events in Japan to review and where necessary revise the documentation and training provided for severe accident management in the fuel route plant areas.