

## Wylfa: Response to EU Stress Tests following the Events at Fukushima, Japan



Following the nuclear accident at Fukushima in Japan, the European Union agreed on assessments for all of its 143 nuclear power plants, based on a set of common criteria. These criteria have been developed by ENSREG (the European Nuclear Safety Regulators Group) and have become known as 'Stress Tests'.

In response to the Stress Tests, operators of UK nuclear power plants have reviewed the resilience of their plants to extreme situations, in particular the loss of safety functions however caused, including the loss of electrical power or loss of ultimate heat sink for heat removal from the reactor or spent fuel storage areas.

This report details the results of the Stress Tests for Wylfa Power Station. It has been submitted to the Office for Nuclear Regulation (an agency of the Health and Safety Executive) who will review all UK submissions and prepare a summary national report. This will be reviewed by ENSREG who will report to the European Council in June 2012.

Issued by.....*D. S. Law*.....

pp N Gore, Site Director, Wylfa Power Station

## Contents

0	Executive Summary .....	5
1	General data about site/plant .....	7
1.1	Brief description of the site characteristics .....	7
1.2	Main characteristics of the unit.....	7
1.3	Systems for providing or supporting main safety functions .....	9
1.4	Significant differences between units .....	27
1.5	Scope and main results of Probabilistic Safety Assessments.....	27
2	Earthquakes .....	29
2.1	Design basis.....	29
2.2	Evaluation of safety margins .....	36
3	Flooding.....	42
3.1	Design basis.....	42
3.2	Evaluation of safety margins .....	47
4	Extreme weather conditions .....	49
4.1	Design basis.....	49
4.2	Evaluation of safety margins .....	50
5	Loss of electrical power and loss of ultimate heat sink .....	54
5.1	Nuclear power reactors .....	54
5.2	Spent fuel storage pools.....	60
6	Severe accident management.....	62
6.1	Organisation and arrangements of the licensee to manage accidents .....	62
6.2	Maintaining the containment integrity after occurrence of significant fuel damage (up to core meltdown) in the reactor core.....	76
6.3	Accident management measures to restrict the radioactive releases .....	79
7	Glossary.....	82

Table 1: Considerations Identified for Wylfa Site.

This page has been left blank intentionally.

## Executive Summary

This report is the response from Wylfa power station to the ENSREG Stress Tests following the events at Fukushima, Japan in March 2011. Wylfa has two Magnox reactors (see next paragraph) each generating around 1600 MW thermal. They first went critical in 1971 and will be shutdown by the end of 2014.

The Wylfa reactor cores comprise metallic uranium fuel, some slightly enriched, within magnesium alloy cans in a graphite moderator. The cores are cooled by forced circulation of pressurised carbon dioxide gas, which transfers heat to water in boilers to generate steam. The reactor core and boilers are in a pre-stressed concrete pressure vessel. The key differences between Wylfa and light water reactor designs such as Fukushima are:

- fuel and clad will melt at lower temperatures;
- notwithstanding this, Magnox have much lower power densities and a high thermal inertia, which leads to longer timescales for establishing reactor post-trip cooling;
- if the pressure circuit remains essentially pressurised, no off-site or on-site electrical supplies are required for reactor post-trip cooling;
- there is no further containment outside of the primary pressure boundary;
- the ultimate heat sink for reactor post-trip cooling is water fed to the boilers with steam rejected to the atmosphere;
- the reactors are continuously refuelled; spent fuel is stored in carbon dioxide filled dry cells that are passively cooled.

The review has confirmed that the essential function of reactor trip (which is fail-safe) is secure. Reactor shut-down and hold-down, which are also fail-safe, could be affected if significant disruption of in-core components occurred. Post-trip cooling of fuel in the reactor may be threatened by significant disruption of in-core components or significant damage to the reactor pressure boundary or post-trip cooling plant. Spent fuel is passively cooled in massive structures.

The review against external hazards has confirmed that Wylfa is in an area of low seismic activity and that safety related plant is not threatened by off-site flooding or tsunamis. It has been confirmed that the design basis hazard specifications remain appropriate and that the plant is qualified against them. Reactor in-core components have a substantial margin against the design basis earthquake, supporting reactor shut-down and hold-down in beyond design basis events. The margin beyond the seismic design basis is discussed and is judged to be at least 50%.

Off-site electrical supplies are not required for reactor safety. On-site electrical supplies, including batteries, are only necessary for reactor post-trip cooling in the unlikely event of significant pressure vessel depressurisation. The ultimate heat sink for reactor post-trip cooling is independent of other on-site or off-site systems, and will be available for extended periods. There are diverse means of plant monitoring with dedicated supplies that are independent of other on-site or off-site systems.

The on and off-site management of severe accidents has been reviewed, including the resilience of the site following loss of local and national infrastructure and communications and the long-term unavailability of consumables.

A series of workshops has been held to identify potential measures to enhance resilience in the event of external hazards or severe accidents, and those being considered for

implementation are listed in Table 1. The site will also be supported by enhancements proposed for central emergency support. The potential measures address pressure circuit sealing, feed systems, on-site electrical system, reactor hold-down, plant monitoring, beyond design basis equipment, access, staff capability, command/control/communications, consumables, severe accident guidance and the dry cells.

## 1 General data about site/plant

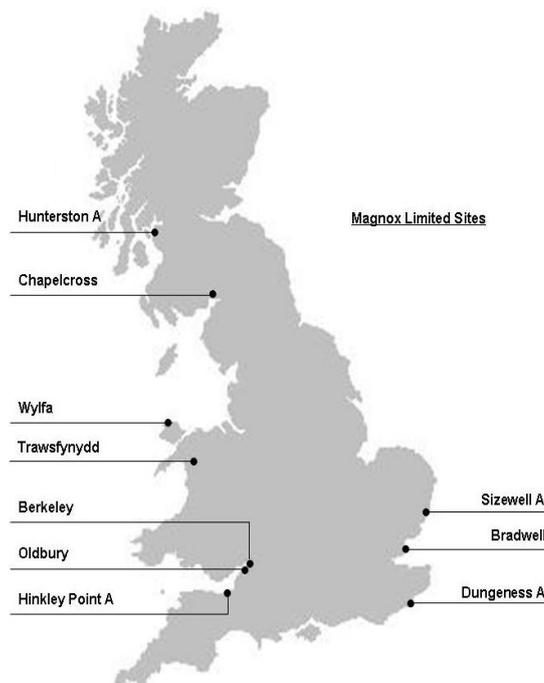
### 1.1 Brief description of the site characteristics

- location (sea, river)<sup>1</sup>
- number of units;
- license holder

Wylfa is located on the North coast of the island of Anglesey in North Wales, United Kingdom. The adjacent Irish Sea provides the ultimate heat removal when operating at power.

The site contains two "Magnox" reactors, both currently generating electricity. There are four turbo/generators (two per reactor) giving the station a total electrical output of around 840 MW. The reactors are due for permanent shutdown in 2012 (Reactor 2) and 2014<sup>2</sup> (Reactor 1). There is spent fuel storage in dry cells, and also radioactive waste storage on site.

Magnox Limited is the Site Licence holder for the Wylfa nuclear licensed site.



### 1.2 Main characteristics of the unit

- reactor type;
- thermal power;
- date of first criticality;
- existing spent fuel storage (or shared storage).

#### Reactors

The Magnox reactors are of a gas cooled design. They contain natural and slightly enriched metallic uranium fuel in magnesium alloy (Magnox) cans. The reactor is normally cooled by forced circulation of pressurised CO<sub>2</sub> gas (at a nominal absolute pressure of 27.5 bar (400 psia)) through the core which transfers the heat from the fuel to water fed boilers.

The 16 sided graphite core consists of a central active region, surrounded by a reflector region and is made up of alternate vertical columns of octagonal and square graphite bricks, with each column comprising 13 bricks. Overall the core is 18.6 m across, 10.2 m high and weighs 3,740 tonnes. The columns making up the active region each have a hollow central fuel channel. There are also interstitial channels centred at the junction between four adjacent columns which are used for control rods, absorber bars and neutron sources.

<sup>1</sup> Text and headings which are in a smaller font are relevant extracts from the ENSREG Stress Test documentation and not part of the Stress Test response.

<sup>2</sup> 2014 is the latest possible shutdown date for Reactor 1. The date is currently unconfirmed and is subject to operational constraints.

Each reactor is in a pre-stressed concrete pressure vessel, 29m in internal diameter, which also contains the four boilers. There is a non pressure retaining structure covering the pressure vessel and the reactor plant, but no hardened secondary containment. Reactivity is controlled by control rods; on reactor trip they drop by gravity into the core. Following trip and shutdown, the reactor core is initially cooled by either forced or natural circulation of CO<sub>2</sub> gas, with feed water to the boilers. As it is a high mass/low power density reactor, there are long timescales for establishing core cooling.

Reactor 1 first went critical on 16<sup>th</sup> January 1971.

Reactor 2 first went critical on 29<sup>th</sup> June 1971.

Each reactor operates typically at around 1600 MW thermal power. Core gas temperatures are approximately 230°C inlet and 365°C outlet.

### Irradiated Fuel Storage

There are no irradiated fuel storage ponds at Wylfa:

Irradiated fuel is normally stored in a CO<sub>2</sub> atmosphere in one of three Primary Dry Store Cells (PDSC). Irradiated fuel elements (IFE) can be loaded to the PDSC, and removed for transferring to fuel flasks and transport to Sellafield using the normal reactor fuelling equipment.

During the 1980s two additional secondary dry store cells (SDSC) were added. These were each designed to store cooled IFE in an air atmosphere at slightly negative pressure and with forced circulation. These SDSC are both currently empty of all IFE and would be subject to a full safety case justification if it were intended to reuse either store in the future.

### Radioactive Waste Facilities

There is very little intermediate level waste (ILW) or low level waste (LLW) stored on site. Excluding the non-combustible metallic items stored in the reactor disposal voids the remaining ILW on site consists mainly of desiccant from the reactor gas driers and old vacuum cleaner bags from cleaners used in contaminated areas. The ILW is stored in the following areas:-

- Intermediate Level Waste Store: Desiccant in drums and vacuum cleaner bags in drums. Active Incinerator Building: High Beta/Low Gamma intermediate level waste in drums. Loading Bay/ex Decontamination Shop: Desiccant in one ductile cast iron container.
- Waste Transit Store: Redundant burst can detection coolers.

The majority of LLW on site is stored in drums in the Active Incinerator Building prior to despatch to the Low Level Waste Repository in Cumbria. All drums have lids fitted with a steel band.

There is also slightly active liquid effluent which is stored in a dedicated Active Effluent Treatment Plant (AETP). This effluent is allowed to decay and settle before being diluted and discharged into the Irish Sea. The AETP is located in the reactor equipment building below ground level.

### 1.3 Systems for providing or supporting main safety functions

In this chapter, all relevant systems should be identified and described, whether they are classified and accordingly qualified as safety systems, or designed for normal operation and classified to non-nuclear safety category. The systems description should include also fixed hook-up points for transportable external power or water supply systems that are planned to be used as last resort during emergencies.

#### 1.3.1 Reactivity control

Systems that are planned to ensure sub-criticality of the reactor core in all shut down conditions, and sub-criticality of spent fuel in all potential storage conditions. Report should give a thorough understanding of available means to ensure that there is adequate amount of boron or other respective neutron absorber in the coolant in all circumstances, also including the situations after a severe damage of the reactor or the spent fuel.

Reactivity control during normal operation is by the movement of control rods in the graphite core. Reactor shutdown is by insertion of control rods. Reactor hold-down is normally provided by control rods, but can be provided by blowing boron dust into the core. Core cooling can also be used to reduce reactivity.

##### Control Rod system

Core reactivity is controlled by the movement of 185 neutron absorbing control rods inserted in vertical core interstitial channels. As well as providing the mechanism for shutting down the reactor in the short term, sufficient worth is also vested in the control rods to ensure long-term hold-down.

The control rod system is an inherently failsafe design with the control rods suspended at the top of the reactor core by energised control rod motors. A trip of the system by the main guardlines, diverse guardlines or reactor trip button, or a complete loss of electrical supplies, removes power from the control rod motors and the rods fall by gravity into the core at a speed limited by regenerative breaking of the motors but taking less than 10 seconds.

The control rods are divided into groups according to their neutron absorption cross section, and their method of use. The primary division is into zone or sector (grey) rods and coarse or bulk (black) rods.

There are 32 zone rods, divided into eight groups of four. Each rod is a hollow cylindrical tube 7.9m long and made of silicon killed mild steel. The rods in each group cover a defined zone of the core. These rods are used primarily for on-load temperature control but do fall into the core on a reactor trip as discussed above.

Of the 153 coarse rods, 137 are similar in construction to the zone rods, but have additional inserts of 4% boron steel and the remaining 16 are of articulated construction capable of entering the core should it suffer control rod channel axial misalignment. The primary function of the coarse rods is to shutdown and hold down a reactor when required, but they are also used for bulk reactivity control during start-up and shutdown, and to compensate for long term changes in reactivity. The coarse rods are divided into four Lifts and under normal operating conditions, Lifts 1 to 3 are more than 90% withdrawn and Lift 4 normally acts as the controlling lift, and is adjusted to maintain the zone rods between 35% and 65% withdrawn.

Interlocks are provided to ensure the correct rod withdrawal sequence. Rod withdrawal speed is limited to prevent excessive rate of release of reactivity. Control rod position information for each rod is given on the Data Processing System (DPS) along with out-of-limit alarms and slack chain alarms that would indicate slackness of rod suspension chains caused by fouling of the rod in the channel. The control rod data logger system records control rod heights as they fall into the reactor following a reactor trip providing rod insertion profiles which are compared after each shutdown.

There is massive redundancy in the number of control rods required for shutdown or hold-down. Just a small number of rods entering the core will cause the reactor to shut down and provided three lifts are inserted long term hold-down is assured.

#### Boron Dust Injection Facility

A Boron Dust Injection System is provided, which is designed to bring about permanent, irrevocable hold-down of the reactor and can be deployed within 8 hours if required. The dust is transported in mobile units which can be deployed in an emergency. The dust is blown into a depressurised reactor by a fan system on the mobile units. For this to be effective forced reactor gas circulation needs to be available to distribute the dust around the core.

There are four boron dust injection points, two serving each reactor located separately.

#### Core cooling

The Magnox reactors have an overall positive temperature coefficient of reactivity of the order of  $+10\text{mN}/^\circ\text{C}$ . Thus cooling the core below normal operating temperatures can be used to significantly reduce core reactivity such that reactor hold-down is credible by core cooling alone (see Section 1.3.2 for discussion of core cooling).

#### Criticality External to the Core

The Magnox fuel used at Wylfa is either natural uranium or has very low enrichment. Criticality in other than a designed regular array with suitable moderator is not possible. Operation of the fuel route for new fuel and irradiated fuel are covered by criticality certificates.

Irradiated fuel is stored in steel tubes in the Primary Dry Store Cells prior to its discharge and cannot go critical with or without water present. There are no additional neutron absorbing materials within the Dry Store Cell structure specifically for criticality control.

### 1.3.2 Heat transfer from reactor to the ultimate heat sink<sup>3</sup>

#### 1.3.2.1 Existing reactor heat transfer trains

All existing heat transfer means / chains from the reactor to the primary heat sink (e.g., sea water) and to the secondary heat sinks (e.g., atmosphere or district heating system) in different reactor shut down conditions: hot shut down, cooling from hot to cold shut down, cold shut down with closed primary circuit, and cold shut down with open primary circuit.

The Wylfa reactors consist of a cylindrical graphite core within a concrete pressure vessel and a spherical steel liner. The fuel elements are located within a large number of fuel channels within the core. The four boilers are internal to the pressure vessel and consist of interleaved tube platens located in the annulus between the core and the spherical steel liner and concrete pressure vessel.

Removal of heat from the fuel is by circulation of CO<sub>2</sub> gas up through the fuel channels and down through the boilers, combined with the forced flow of feed water up through the boiler tubes. Each of these two processes is discussed in detail below, and a discussion of the minimum post trip cooling requirements follows at the end of the section.

#### Gas Circulation

Each reactor is provided with four horizontally mounted electric motor driven gas circulators which are single stage, axial flow machines. Under normal operating conditions they are driven at a constant speed of 1000 rpm with the gas mass flow controlled by adjustable inlet guide vanes. Their function is to drive the flow of CO<sub>2</sub> through the reactor in order to control the temperature of the reactor and effect heat transfer to the boilers.

Each circulator is provided with:-

- Main Motor (11kV AC from the main station supplies)
- AC Pony Motor (3.3kV from the Essential Supplies System)
- DC Pony Motor (440V from the Guaranteed Supplies System)
- Two AC Pony Motors per reactor can also be supplied from the Electrical Overlay System (EOS). (See Section 1.3.5.4.1).

The motors of each circulator are all connected in line, with the main motor directly connected to the circulator impellor and the pony motors on a separate drive shaft with a self synchronising clutch. The clutch will only engage when the speed of the pony motors exceeds that of the drive shaft on which the main motor and circulator fan are mounted.

---

<sup>3</sup> During normal, at-power operation the Ultimate Heat Sink (UHS) for Wylfa is the sea. However, if the reactor was shut down in an emergency situation then the Circulating Water (CW) system (ie the sea) is no longer available for cooling and boiler feed water would be used on a “once through” basis and discharged to the atmosphere as steam/water through safety relief valves or Tertiary Feed vents. For the purposes of this report the Primary UHS is therefore defined as “the sea” (ie the Circulating Water system) and the Alternate UHS is defined as “the feedwater in the boilers venting to atmosphere”.

The drive shaft connecting the motors to the impeller passes through a lined penetration in the pressure vessel and is provided with two shaft seals to maintain the reactor pressure boundary.

The first of these seals is called the running seal and is used to prevent gas leakage through the shaft penetration when the circulator is running or with the shaft stationary. It consists of a stationary white metal thrust pad held against a collar on the shaft. Oil is pumped into the space between the seal faces at about 0.69 bar (10 psi) above the gas pressure, to form an oil film which prevents the escape of reactor gas. The oil is supplied by the seal oil system which consists of one AC pump which is normally in service and one AC and one DC pump which are normally on standby.

The second rotor shaft seal is called the static seal and can only be used when the circulator is stationary. It is normally applied by an externally mounted DC motor but in an emergency it can be applied either by hand or by utilising an additional AC motor which is supplied from a portable diesel generator unit with connection points external to the building.

Ancillary plant associated with the circulators is mostly accommodated in a basement room below the circulator motor room.

In normal operation, with the reactor at full power, all four Main Motors would be in service. Should more than two main motors fail the reactor will automatically trip on guardline protection. Should all four main motors fail the two selected DC pony motors would auto start.

With the reactor shut down any motor can be used to provide gas circulation (pressurised or de-pressurised) but the speed of rotation and gas mass flow depend upon the drive motor used and the reactor gas density (pressure).

### Feed Water to Boilers

#### Main Boiler Feed Pumps

During normal power operation feedwater is supplied to the boilers by two of the four Main Boiler Feed Pumps (MBFP) per reactor. The motors for these pumps are supplied from the station 11kV system. The steam/feed system works as a closed loop with steam from the boilers going directly to the two turbines, through the condensers and the feed water being returned to the MBFPs. Make up is from the Reserve Feedwater Tanks (RFT). There are two RFTs per turbine (eight in total) each with a nominal capacity of 336,000 litres. The condensers are cooled by seawater (the Primary UHS).

The MBFP can also be used after reactor shutdown provided that the turbine condensate system is still in service. In this situation the water is fed to the boilers but the steam is released to the atmosphere via the boiler safety relief valves (the Alternate UHS).

### Emergency Boiler Feed Pumps

If the MBFP are unavailable, water can be supplied to the boilers by any one of three Emergency Boiler Feed Pumps (EBFP) per reactor. The motors for these pumps are supplied from the 440V DC Guaranteed Supplies System. Water supply is direct from the RFTs, and each pump can provide from 0 to 15kgs<sup>-1</sup> to the boilers. The steam is again released to the atmosphere via the boiler safety relief valves (the Alternate UHS).

The permanently connected delivery lines from the 3 EBFP connect to a common header with sectioning valves, and a link to the other reactor. It is possible to use one of the three pumps from the other reactor to feed the boilers.

### Backup Feed System

A further diverse means of post trip cooling the boilers is provided by the Backup Feed System (BUFS). This was specifically designed for the seismic event but can also operate for other faults where main and emergency boiler feed pumps are unavailable.

This system consists of two proprietary diesel driven pumps located in a single, fire segregated pumphouse. Each pump is designed to supply both reactors at 8kgs<sup>-1</sup> through either of two ring mains, each of which feeds into 2 of the 4 boilers per reactor (Note: feed to only one boiler is sufficient to cool the reactor). The BUFS is a high pressure system; the boilers do not need to be depressurised before use and it would normally be used in preference to the TFS with the steam discharging to atmosphere through the boiler safety relief valves (the Alternate UHS). However cooling is enhanced if the boilers are depressurised in which case water/steam is discharged to atmosphere through the tertiary feed vents.

Water for the BUFS is provided from the tertiary feed tanks (see below). The pumps discharge through permanently installed pipework to the tertiary feed ring mains.

The BUFS is designed to be operated from the pumphouse without need to access the reactor building to confirm/alter valve states or check flow rates. A 415V AC generator is driven from each BUFS engine to provide electrical supplies for operating valves, local indications and lighting. The BUFS pumps are started from the dedicated starter batteries and the system will operate independently of any external electrical supplies.

### Tertiary Feed System

To provide an independent and diverse means of supplying post trip cooling to the boilers in the event of failure of both the MBFP and EBFP systems a Tertiary Feed System (TFS) was installed. This system is designed, as far as practicable, to be unaffected by any single event that affects operational availability of the main and emergency feed pumps.

The TFS consists of four proprietary diesel pumps, together with dedicated feed water tanks, fuel tank, permanent suction pipework and flexible delivery

hoses to link to either of 2 ring mains (as described above for the BUFS). The system requires no external electrical supplies for operation in an emergency.

The TFS is designed as a low pressure system, requiring the boilers to be depressurised before use. After passing through the boilers the water/steam is discharged through the tertiary feed vent valves to the atmosphere (the Alternate UHS). Each pump is designed to provide  $8\text{kg s}^{-1}$  of cooling water to one reactor.

The delivery hoses are of standard fire fighting design and are stored at a number of locations on site. Fixed pumping-in points are provided which connect to two dedicated tertiary feed ring mains per reactor.

Water for the Tertiary Feed system is provided from two seismically qualified tanks.

#### Other fixed or portable pumps

The Wylfa Severe Accident Guidelines (SAGs) list the following fixed or portable pumps available on site, any one of which is capable of supplying at least as much water as one tertiary feed pump (ie  $8\text{kg s}^{-1}$  - sufficient for one reactor):-

- Station Fire Engine Pump (1 off – portable)
- Portable Fire Pumps (4 off – portable)
- Fire Hydrant Pump (2 off – fixed)
- Diesel Fire Hydrant Pump (1 off – fixed)
- Fixed Jet Fire Pumps (3 off – fixed)

These pumps would require flexible hoses to connect to the tertiary feed pumping in points and would require depressurised boilers (other possible pumping in points are identified in the SAGs).

#### Minimum Post Trip Cooling Requirements

Following any reactor trip there are requirements for gas circulation and supply of feed to the boilers. However, due to the low power density of Magnox reactors there can be a long period before cooling is required. There are numerous factors affecting how much forced gas circulation is required (if any), how much feed is required for the boilers and how soon these must be delivered. The main factor is whether the reactor is pressurised or is depressurising and a summary of some typical scenarios is given below:-

#### Reactor pressurised (Gas circulator running seals or static seals effective).

- Natural circulation of the reactor gas is adequate. No gas circulators required.
- Feedwater to a boiler pair from a single MBFP or EBFP or BUFS pump or TFS pump.

Small depressurisation fault (Gas circulator seals not effective).

- Natural circulation of the reactor gas.
- Feedwater to a boiler pair from a single MBFP or EBFP or from a single BUFS pump or TFS pump.

OR

- One gas circulator driven by main, AC or DC pony motors.
- Feedwater to a boiler pair from a single MBFP or EBFP or BUFS pump or TFS pump.

Large depressurisation fault

- One gas circulator main motors or two DC pony motors subsequently replaced by two AC pony motors.
- Feedwater to a boiler pair from an EBFP.

- 1.3.2.2 Lay out information on the heat transfer chains: routing of redundant and diverse heat transfer piping and location of the main equipment. Physical protection of equipment from the internal and external threats.

Gas Circulators

The four gas circulators are located in separate circulator halls and they and their auxiliaries are segregated from hot gas or steam escape routes. Electrical supplies to main motor, AC pony motor and DC pony motor are from diverse supplies but cables are not specifically segregated. The Electrical Overlay System (EOS), which can provide alternate supplies to two AC pony motors on each reactor, is diverse from the other supply systems and cabling is segregated as far as practical.

Main Boiler Feed Pumps

The four main boiler feed pumps associated with a reactor are located in the same general area within the turbine hall basement. No specific segregation or protection from hazards is employed.

Emergency Boiler Feed Pumps

The three emergency boiler feed pumps associated with a reactor are located in a raised area in the turbine hall basement. Some protection is provided to protect the pumps from spray that could result from a joint or pipe failure in the vicinity of the motors and their position provides some protection against flooding of the basement. There is large physical separation between the sets of EBFP for the two reactors and the pipework arrangement allows any pump to feed either reactor. Pipework from the pump discharge to the reactors is also segregated such that feed to one pair of boilers is via a pipe bridge whilst feed to the other pair of boilers is via a tunnel. The EBFPs of each set are fed from two downcomers, each supplied from two separate pairs of RFTs. All eight

RFTs are normally interconnected. In the event of the failure of one tank or pipework operator action would be taken to isolate the failure.

### Tertiary Feed System

The tertiary feed system is designed, as far as practicable, to be diverse and separated geographically from the main and emergency feed systems such that it will be unaffected by any single event that could affect the other systems. It is qualified against the design basis seismic and wind hazard demands. The flexible hoses on the delivery side of the pumps allow any convenient route to the fixed pumping-in points on the exterior of the reactor buildings to be used after an initiating event avoiding, for example, any site civil damage. The fixed pumping-in points are connected to two tertiary feed ring mains which are physically separated. Each ring main is connected to a pair of boilers.

### Back-up Feed System

The BUFS provides a further independent and diverse means of supplying post trip cooling in the event of both the main and emergency feed systems being unavailable. It was installed specifically in support of the seismic safety case and is designed to withstand the design basis seismic and wind hazard demands. The two BUFS pumps are located in a purpose built building which is segregated internally by fire barriers and is situated away from the main reactor building to prevent damage by falling masonry.

- 1.3.2.3 Possible time constraints for availability of different heat transfer chains, and possibilities to extend the respective times by external measures (e.g., running out of a water storage and possibilities to refill this storage).

Water supply for the MBFP and EBFP is gravity fed from the RFTs and on-site townswater reservoir. If no make up was available from off-site, and all RFT tanks and the reservoir were at the minimum level allowed in the station procedures, then the available water supply would support one EBFP on each reactor for approximately 32 hours. With the RFT tanks and reservoir at normal operating levels this time would increase to around 65 hours.

The tertiary feed/BUFS tanks are designed to hold 24 hours of supply for either the BUFS or TFS systems feeding both reactors. By running out temporary hoses it is possible to top these tanks up from the water treatment plant/townswater reservoir.

Both the BUFS and TFS have installed diesel tanks with a minimum of 24 hours capacity for each pump. The fuel used on site for the gas turbine engines is of a similar specification and could be used to top up these tanks if no other supplies were available.

- 1.3.2.4 AC power sources and batteries that could provide the necessary power to each chain (e.g., for driving of pumps and valves, for controlling the systems operation).

The available power supplies are described in Sections 1.3.5 and 1.3.6.

The gas circulator main motors and main boiler feed system can only be driven by 11kV supplies from the reactor/turbines or from grid supplies. The gas

circulator AC pony motors are supplied from the Essential Supplies system which is supported by the grid or the on site gas turbines; these also support the other AC and battery backed DC systems necessary for their operation.

Two gas circulator AC pony motors on each reactor and their auxiliaries can also be supplied from the diesel generator backed Electrical Overlay System

The emergency boiler feed system and gas circulator DC pony motors are supplied from the battery backed Guaranteed Supplies system which is supported by the gas turbines or grid when available.

The BUFS and TFS systems are self contained and require no external electrical supplies for emergency operation.

- 1.3.2.5 Need and method of cooling equipment that belong to a certain heat transfer chain; special emphasis should be given to verifying true diversity of alternative heat transfer chains (e.g., air cooling, cooling with water from separate sources, potential constraints for providing respective coolant).

All of the heat transfer chains used for emergency cooling of the reactors are designed to be operated “once through” with the steam/water venting from the top of the boilers. There are no requirements for any heat exchangers in the feed/boiler circuit although there are options for conserving water by using the boiler drums as a recirculation route if normal station electrical supplies are available.

There are requirements for cooling water derived from the Seawater Cooling system<sup>4</sup>, via intermediate closed loop cooling water systems, for the following items of equipment in the heat transfer chains:-

- Main Boiler Feed Pumps (Bearing cooling water)
- GC main motors (Motor Air, Lub oil, bearing cooling)
- GC AC pony motors (not EOS) (Lub oil, Liquid controller, bearings)

The two gas circulator AC pony motors per reactor that are backed up by EOS supplies have alternative cooling systems for lubricating oil coolers, liquid controller coolers etc. which circulate the cooling water through radiators and require no external water supplies.

The TFS and BUFS require no external cooling water supplies.

---

<sup>4</sup> The Seawater Cooling System is supported by the Essential Supplies system and supports selected MSRP. The system may be vulnerable to seismic and severe flooding events.

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

- 1.3.3.1 All existing heat transfer means / chains from the spent fuel pools to the primary heat sink (e.g., sea water) and to the secondary heat sinks (e.g., atmosphere or district heating system).

There are no irradiated fuel storage ponds at Wylfa; irradiated fuel is stored in a CO<sub>2</sub> atmosphere in one of three Primary Dry Store Cells (PDSC). The PDSC are totally passive with no requirement for electrical supplies or water supplies for cooling of the irradiated fuel elements (IFE). The CO<sub>2</sub> within the tubes is at a slightly positive pressure and heat is removed from the IFE by radiation/conduction to the tube wall and some natural circulation of the CO<sub>2</sub>. The outside of the tubes are cooled by a natural thermal siphon air circulation system to a ventilation stack. The air circulation system is supplied by three massive underground ducts (one to each cell), each approximately 5m<sup>2</sup> in section. It has been shown that these ducts would have to be blocked by more than 99% for cell temperatures to rise significantly. In the event of total blockage of the ducts fuel clad melt would not occur for about 58 hours even for a recently loaded, peak rated fuel element.

Also provided are two Secondary Dry Store Cells (SDSC). These were designed to store cooled IFE in an air atmosphere at slightly negative pressure and with forced circulation and utilising one of the auxiliary cooling water systems. These SDSC are both currently empty of all IFE and would be subject to a full safety case justification if it were intended to reuse either store in the future.

- 1.3.3.2 Respective information on lay out, physical protection, time constraints of use, power sources, and cooling of equipment as explained under 1.3.2.

The three PDSC are located between the two reactors with the substantial concrete structure providing the necessary shielding and are qualified against the design basis seismic event. There are no forced cooling systems and hence no requirements for power supplies. There are no time constraints of use; fuel can be transferred directly from the reactor and remain in the store as long as is required. Fuel can be removed from the PDSC after cooling for a minimum of 90 days for onward transport to Sellafield for reprocessing.

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

In the Magnox design, the reactor vessel provides the reactor containment (the covering reactor building providing protection of plant from the environment). Cooling of the reactor internals and the pressure vessel is addressed in Section 1.3.2.

- 1.3.4.1 All existing heat transfer means / chains from the containment to the primary heat sink (e.g., sea water) and to the secondary heat sinks (e.g., atmosphere or district heating system).

Not applicable for Wylfa. The reactor buildings only provide a weatherproof barrier to the massive reinforced concrete reactor pressure vessels and PDSC, and heat transfer/ventilation through this barrier would ensure there is no significant heat build-up. There are specific hot gas release paths in the buildings to ensure that, in the event of a fault, hot gas and steam are vented to their exterior.

- 1.3.4.2 Respective information on lay out, physical protection, time constraints of use, power sources, and cooling of equipment as explained under 1.3.2.

Not applicable for Wylfa as discussed in 1.3.4.1.

### 1.3.5 AC power supply

#### 1.3.5.1 Off-site power supply

- 1.3.5.1.1 Information on reliability of off-site power supply: historical data at least from power cuts and their durations during the plant lifetime.

The arrangement of the off-site electrical supply is discussed in detail in the next section. Loss of the twin circuit 400kV line from Wylfa leaves the station “islanded” with only local load to supply. This represents a significant load rejection for Wylfa and can result in loss of one or both reactors. If both reactors trip when the 400kV circuits are unavailable this constitutes a “loss of off-site supplies” situation as all incoming supplies to the station are lost.

This fault is considered within the Wylfa Fault Schedule and is classed as a “Frequent Fault” with a frequency of  $5 \times 10^{-1}$  per annum.

In practice there have been 14 occasions in the life of the station where both 400kV lines have been lost. On two occasions one reactor tripped and on three occasions both reactors tripped. There have, therefore, been three “loss of off-site supplies” events in the life of the station. This represents an actual fault frequency of less than  $1 \times 10^{-1}$  per annum.

The most significant of these disconnections occurred during a severe storm in December 1990 when, although the 400kV lines were restored several times during the event, the station was without off-site supplies for over 5 hours. On this occasion three gas turbines were manually started prior to the trip of the second reactor in anticipation of the total loss of off-site supplies.

- 1.3.5.1.2 Connections of the plant with external power grids: transmission line and potential earth cable routings with their connection points, physical protection, and design against internal and external hazards.

The four Generator Transformers are connected via a 400kV substation and a single twin circuit 400kV overhead transmission line, to the North Wales section of the 400 kV national supergrid system. The 400kV substation is connected also to four 400/132kV supergrid transformers which supply an adjacent 132kV substation which supplies the local distribution system for the island of Anglesey and supplies three 132/11kV Station Transformers which feed grid supplies back to Wylfa power station.

Although the local distribution system has another connection to the supergrid, to prevent overloading of this system, there is an “intertrip” system which isolates this local distribution system from the supergrid, if the main 400kV connection is lost. In this situation Wylfa generation is left supplying the local load of Anglesey plus the station house load (a total of

around 170MW) which represents a significant load rejection for Wylfa, and can result in the trip of one or both reactors.

If both reactors trip and both 400kV lines are unavailable, this represents a total loss of external electrical supplies for Wylfa.

Both the 132kV and the 400kV substations are of an enclosed design giving protection against wind and weather, are located on high ground and have installed fire protection systems, but neither is formally qualified against any hazards.

The station earthing system consists of various interconnected earth grids within the main site buildings. These grids provide earthing for structural and cladding metalwork as well as providing star point connections for transformers and alternators. The main turbine hall earth grid is connected to the reactor building earth grid by four PVC insulated cables run underground in separate cable trenches.

The reactor building earth grid is connected via two underground PVC insulated cables to two cast iron earth electrodes which are immersed at all states of the tide in the Circulating Water intake chambers. The routes for these cables are diverse; one being from Reactor 1 building and one from Reactor 2 building, and the earth electrodes are physically separated.

### 1.3.5.2 Power distribution inside the plant

#### 1.3.5.2.1 Main cable routings and power distribution switchboards.

There are seven 11kV switchboards at Wylfa, all located in one long switchroom which is located at the 21.5m OD level. Three of these switchboards are supplied from the 132/11kV Station Transformers and are designated 11kV Station Boards. The remaining four are Unit Boards and are normally supplied through dedicated 17.5/11kV Unit Transformers from the output of each of the four main generators. When a generator is not in service the associated Unit Board is interconnected to the Station Boards.

The main items of plant supplied directly from these 11kV switchboards are gas circulator main motors, main boiler feed pumps and main circulating water pumps. These items of plant are distributed between the switchboards for maximum diversity of supply.

Also supplied from these 11kV switchboards are transformers that supply numerous 3.3kV auxiliary switchboards at various locations around site, which in turn supply 415V lighting and services switchboards.

Plant which is important for post trip heat removal from the reactors is fed from a 3.3kV Essential Supplies System. This is a short-break (< 15 minutes) system that is normally supplied, through transformers, from 11kV Station Boards 1 & 2 but can be supplied by five gas turbine generators (see below). This system consists of a 3.3kV Gas Turbine Board which is in two sections (A & B), and two 3.3kV Essential Auxiliary

Boards, both arranged as two half boards with an interconnecting bus section.

Two gas circulator 3.3kV AC pony motors are normally supplied from each of the Essential Auxiliary Boards and two AC pony motors are supplied from each of the 3.3kV Essential Overlay Gas Circulator Boards. These Essential Overlay Gas Circulator Boards are in turn supplied either from the Essential Auxiliary Boards or from the Electrical Overlay System diesel generators (see 1.3.5.4.1 below).

#### 1.3.5.2.2 Lay-out, location, and physical protection against internal and external hazards.

The 11kV system is distributed around plant with the main switchboards located in a switchroom at 21.5m OD. This system is not specifically qualified against internal or external hazards.

Gas Turbine Boards A & B are located in an annex to the main gas turbine building. They are not qualified against a design basis seismic demand.

The 3.3kV Essential Auxiliary Boards are located in the main reactor building switchgear room at ground level. The switchboards have canopies to protect against water ingress from above. They are not qualified against a design basis seismic demand.

The Guaranteed Supplies switchboards and transformer rectifier units are located at either end of a switchroom at 21.5m OD. The switchboards have canopies to protect against water ingress from above. They are not qualified against a design basis seismic demand.

The Guaranteed Supplies Batteries are located at ground level in two battery rooms. The batteries have canopies to protect against water ingress from above, and they are mounted in seismically qualified stands but the system is not fully qualified against a design basis seismic demand.

#### 1.3.5.3 Main ordinary on-site source for back-up power supply

##### 1.3.5.3.1 On-site sources that serve as first back-up if offsite power is lost.

Back-up power in the event of loss of grid supplies is provided by five gas turbine driven generators. Each of the generators has a nett electrical output of nominally 2.5MW.

Four of the gas turbines are located in one building located at ground level. These all generate at 3.3kV and two connect to the A half of the Gas Turbine Board and two connect to the B half of the board.

The fifth gas turbine was added more recently and generates at 11kV. This unit has an 11/3.3kV transformer and can be configured to connect to either half of the Gas Turbine Board.

On a loss of incoming supplies, a Selective Tripping Scheme (STS) automatically clears all running plant from the Gas Turbine Board and the

Essential Auxiliary Boards. The STS then automatically starts all five gas turbines and synchronises four to the Gas Turbine Board. The operator can then manually re-start essential post trip cooling plant and restore supplies to the battery systems. Any gas turbines not required can be shut down.

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

Normally, three gas turbines are run to provide sufficient electrical output to support the essential post trip cooling plant requirement. However, with just one gas turbine available, it is possible to support the Guaranteed Supplies system and run one Gas Circulator DC Pony Motor on each reactor and one Emergency Boiler Feed Pump on each reactor (plus supporting plant) and hence maintain emergency cooling to both reactors.

Four of the gas turbines are located in one building, and, although the gas turbine engines are in individual brick built cells, there is little segregation between the generators. The fifth gas turbine is located in a separate building but utilises common fuel supplies and connects electrically to the Gas Turbine Board which is located in an annex to the main gas turbine house.

Fire protection is provided for all of the gas turbine engines and generators. There is no specific protection provided for other internal hazards although the plant is remote from most sources of hot gas, steam or water and from other rotating plant. The plant is not qualified against design basis seismic or wind demands.

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

If off-site fuel supplies were unavailable, and in the unlikely event that the station was at the minimum stock level allowed by the Operating Rules, then the on-site supplies would last around 48 hours with four gas turbines in service.

These mission times quoted are very pessimistic and assume four gas turbines are running at full load. If fuel was in short supply essential reactor cooling could still be maintained with a considerably reduced electrical load which could be provided by two, or when cooling requirements are further reduced, one gas turbine. This would extend the mission time to in excess of 72 hours.

Minimal operator intervention is required to support the system.

#### 1.3.5.4 Diverse permanently installed on-site sources for back-up power supply

- 1.3.5.4.1 All diverse sources that can be used for the same tasks as the main back-up sources, or for more limited dedicated purposes (e.g., for decay heat removal from reactor when the primary system is intact, for operation of systems that protect containment integrity after core meltdown).

The diesel driven EOS system (see Section 1.3.2.4) is designed to provide electrical supplies to up to two GC AC pony motors on each reactor including associated lubricating and seal oil systems. Supplies are also provided for the seal oil systems on the remaining gas circulators to prevent slow depressurisation of the reactors through the gas seals on the circulator shafts.

The switchboard arrangement allows any of the diesel generators to supply one pony motor on each reactor. (One pony motor is sufficient to provide adequate forced CO<sub>2</sub> circulation for a shutdown reactor).

Upon loss of all incoming grid supplies, all three diesel generators auto-start ready for manual synchronisation to the switchboards if required. These EOS diesel generators are only to support forced circulation of CO<sub>2</sub> in the reactors and do not provide back up electrical supplies to other station plant.

A further small dedicated diesel generator is provided to support the Remote Emergency Indication Centre (REIC). The REIC is located at ground level in a separate building and provides a small subset of reactor instrumentation completely diverse from the main instrumentation systems. It is primarily intended for an event that makes the control room untenable but would provide a useful indication of reactor conditions in a total station blackout situation. The REIC is qualified against the design basis seismic demand.

- 1.3.5.4.2 Respective information on location, physical protection and time constraints as explained under 1.3.5.3.

The EOS diesel generators and switchboards are located at ground level and are physically remote from the gas turbine equipment.

Each EOS diesel generator has a day fuel tank with a nominal 8 hours worth of fuel. In addition, a single bulk fuel oil tank is maintained with more than a specified minimum quantity of oil. With minimum fuel stocks the claimed mission time is 24 hours for one diesel generator at full load.

Normal fuel supplies for the REIC diesel generator are sufficient for at least two days of operation.

- 1.3.5.5 Other power sources that are planned and kept in preparedness for use as last resort means to prevent a serious accident damaging reactor or spent fuel.

- 1.3.5.5.1 Potential dedicated connections to neighbouring units or to nearby other power plants.

Wylfa is a two reactor station with an interconnected electrical supply system which allows many supplies to be configured to be supported by the

other reactor's systems. However, there are no other nearby power plants and no dedicated facilities for supplies from any other source.

1.3.5.5.2 Possibilities to hook-up transportable power sources to supply certain safety systems.

Two small portable 415V AC diesel generator units are provided specifically to enable the gas circulator static seals to be applied in the event of loss of all other electrical supplies following a seismic event. The static seal provides a gas seal on the gas circulator shaft when the circulator is stationary and hence prevents the slow depressurisation of the reactor via this route.

1.3.5.5.3 Information on each power source: power capacity, voltage level and other relevant constraints.

The Static Seal Diesel Generators are small 415V AC units for use with the static seal motors only and are not suitable for large scale backup power generation.

1.3.5.5.4 Preparedness to take the source in use: need for special personnel, procedures and training, connection time, contract arrangements if not in ownership of the Licensee, vulnerability of source and its connection to external hazards and weather conditions.

Following a seismic event it could be necessary to connect the static seal generator to the installed connection points external to the reactor building. The connection points and static seal equipment are seismically qualified but it may be necessary to clear access routes of debris before the generator can be connected. The seals can be applied by hand if access to the inside of the circulator halls is available. Staff are trained for applying static seals in an emergency situation and this is practiced regularly as part of emergency exercise demonstrations.

### 1.3.6 Batteries for DC power supply

1.3.6.1 Description of separate battery banks that could be used to supply safety relevant consumers: capacity and time to exhaust batteries in different operational situations.

Plant that must have supplies available at all times (no-break) is fed from the Guaranteed Supplies System. This is a 440V DC battery backed system consisting of one switchboard on each reactor, each arranged as two half boards with a bus section. Normal supplies to the Guaranteed Supplies System come from the 3.3kV Essential Auxiliary Boards via four Transformer Rectifier Units. The four batteries (two per reactor) each have a capacity of 2000Ah.

Gas circulator DC pony motors and emergency boiler feed pumps are supplied from the Guaranteed Supplies System along with four General Instrumentation Motor Alternator (GIMA) sets that provide 110V AC supplies for station instrumentation equipment.

In normal operation all batteries are in service and each is capable of supporting the total load for one reactor for 15 minutes. This is sufficient time for the gas turbines to run up and synchronise and supplies to be restored to the transformer rectifier units. However, if grid supplies are lost the auto-

starting of Emergency Boiler Feed Pumps is delayed until supplies are restored to support the Guaranteed Supplies System. In this situation, even with one battery unavailable, the Guaranteed Supplies System is capable of supplying loads for more than 30 minutes.

Other major battery backed supply systems include:-

- 110V DC Switchgear Supplies System: This system provides control and protection supplies for all major items of plant on site. It comprises two switchboards supplied by four battery chargers and supported by four 250Ah batteries. The batteries will support the load for a minimum of 2 hours.
- 110V DC Gas Turbine Switchgear Supplies System: This system provides control and protection supplies for switchgear associated with the five gas turbine generators. Gas Turbines 1 to 4 are supplied by four battery sections and four switchboards located in two segregated rooms and Gas Turbine 5 has a dedicated battery and switchboard in a diverse location. Each of the five batteries is of 262Ah rating and will support the load for a minimum of 2 hours.
- 50V DC C & I System: This system provides supervisory control and protection supplies, Group 1 alarms and GC DC pony motor auto start circuits. (It does not supply the main data processing system, Group 2 alarm system or main station instrumentation; these are fed from the GIMA sets off the Guaranteed Supplies System). It comprises two switchboards supplied by four battery chargers and supported by four 1200Ah batteries. The batteries will support the load for a minimum of 2 hours.
- 50V DC Telecommunications System: This system provides support for the station telephone system and fire and emergency alarms. It comprises two distribution boards each fed by a battery charger and supported by a 400Ah battery. The batteries will support the load for a minimum of 12 hours.
- 240V AC/DC Emergency Lighting System: This system provides lighting to allow essential operations and safe egress until restoration of Essential Supplies. It comprises one switchboard normally supplied from the 415V Essential Supplies System and one 700Ah battery. The battery will support the load for a minimum of 15 minutes.

None of the systems described in this sub-section are qualified against the design basis seismic demand.

1.3.6.2 Consumers served by each battery bank: driving of valve motors, control systems, measuring devices, etc.

440V DC Guaranteed Supplies System serves:-

- 4 x Gas Circulator DC Pony Motors per reactor.
- 3 x Emergency Boiler Feed Pumps per reactor.
- 4 x General Instrumentation Motor Alternator (GIMA) sets total.

4 x Gas Circulator Lubricating/Seal Oil pumps per reactor.  
4 x Gas Circulator Static Seal Actuators per reactor.  
4 x Gas Circulator Inlet Guide Vane Actuators per reactor.  
Various Feedwater valves.

Note: These 440V DC supplies are duplicated by EOS batteries for gas circulators and auxiliaries backed up by the EOS system.

110V DC Switchgear Supplies System serves:-

Closing and tripping supplies to switchgear for most major items of plant on site. (Including operation of 440V DC Guaranteed Supplies system and GIMA Sets).

Note: These 110V DC supplies are duplicated by EOS batteries for gas circulators and auxiliaries backed up by the EOS system.

110V DC Gas Turbine Switchgear Supplies System serves:-

Closing and tripping supplies to switchgear for gas turbines and gas turbine switchboards, and supplies to the gas turbine Selective Tripping Scheme.

50V DC C & I System serves:-

Relays directly initiated by control room switches.  
Control room and panel indication lamps.  
Hard wired Group 1 Alarm system.  
Gas Circulator DC Pony Motor auto-start circuits.

Note: These 50V DC supplies are duplicated by EOS batteries for gas circulators and auxiliaries backed up by the EOS system.

Other battery systems are as discussed in Section 1.3.6.1.

1.3.6.3 Physical location and separation of battery banks and their protection from internal and external hazards.

440V DC Guaranteed Supplies Batteries:-

Batteries 1A and 1B are located at ground level.

Batteries 2A and 2B are located at ground level.

Batteries are protected by canopies from water from above.

110V DC Switchgear Batteries:-

Batteries 1B and 2A are located at ground level.

Batteries 1A and 2B are located at ground level.

110V DC Gas Turbine Switchgear Batteries:-

Batteries 1 – 4 are in two battery rooms approximately 1m above ground level.

Battery 5 in gas turbine 5 building.

50V DC C & I Batteries:-

Batteries 1 and 2 are in the reactor building at 25.5m OD level.

Batteries 3 and 4 are in the reactor building at 32.5m OD level.

50V DC Telecommunications Batteries:-

Batteries 1 and 2 are in the reactor building at 25.5m OD level.

240V DC Emergency Lighting Battery:-

The battery is located at ground level.

None of the above battery systems are qualified against external hazards.

1.3.6.4 Alternative possibilities for recharging each battery bank.

If the Main Station Electrical Supplies and the Essential Supplies systems are unavailable there are no alternative methods of recharging any of the safety related batteries.

## 1.4 Significant differences between units

This chapter is relevant only for sites with multiple NPP units of similar type. In case some site has units of completely different design (e.g., PWR's and BWR's or plants of different generation), design information of each unit is presented separately.

Reactor 1 and Reactor 2 are essentially identical units. However, it should be noted that Reactor 2 will be shutdown permanently in Spring 2012 but will remain essentially full of irradiated fuel until Reactor 1 is shutdown permanently.

## 1.5 Scope and main results of Probabilistic Safety Assessments

Scope of the PSA is explained both for level 1 addressing core meltdown frequency and for level 2 addressing frequency of large radioactive release as consequence of containment failure. At each level, and depending on the scope of the existing PSA, the results and respective risk contributions are presented for different initiating events such as random internal equipment failures, fires, internal and external floods, extreme weather conditions, seismic hazards. Information is presented also on PSA's conducted for different initiating conditions: full power, small power, or shut down.

A detailed Level 2 probabilistic safety analysis (PSA), incorporating the results of a human factors analysis, was undertaken in support of the periodic safety review to September 2014. For the generating reactors, it addressed shutdown, start-up and at-power faults, maintenance states, the risk to the public and workers. A PSA is considered to have two purposes:

- to quantify risk, allowing demonstration that risk is acceptable

- to identify where further consideration of risk reduction should be targeted.

The PSA used standard analysis techniques (such as failure effects analysis, fault tree analysis, hazard analysis, common cause failure analysis), and comprised three main elements:

- initiating faults and frequencies;
- reactor trip and shutdown reliability model;
- post-trip cooling reliability model.

The PSA showed that risk from faults and hazards is predominantly from large releases derived from failure to trip, shutdown or post-trip cool.

It concluded that the frequency of failure of the reactor trip function was  $2.18 \times 10^{-5}$  per reactor year. This was dominated by assumed common cause failure cut-offs for the main and diverse guardline trip contactors which, although of diverse designs, are in the same vicinity; it was shown not to be reasonably practicable to further modify the contactors.

The frequency of failure of the shutdown and hold-down function was  $5.27 \times 10^{-6}$  per reactor year. This was dominated by assumed common cause failure cut-offs for control rods; however, this is a multiply redundant system and the common cause failure assumed was shown to be conservative. The diversity of the control rod system was increased through the use of articulated control rods at some locations and measures were implemented to minimise the potential for common cause failure of control rod actuators.

For both the trip and shutdown/hold-down function, the contribution to failures from hazards is small, of the order of 1%.

The frequency of failure of post-trip cooling was  $1.12 \times 10^{-5}$  per reactor year, approximately half of which is derived from plant faults and half from hazards. There is no single dominating event, although both the extreme wind and frequent seismic hazards were shown to be significant. The extreme wind hazard was subsequently addressed by qualifying the Back-up Feed system for a  $10^{-4}$  pa event. The frequent seismic hazard was addressed by providing a further diverse feed system (the back-up feed system, not modelled in the PSA). In addition, several further ALARP safety measures were subsequently implemented to mitigate the effects of seismic hazards (both frequent and extreme).

Subsequent to the periodic safety review PSA, a focussed fire PSA was undertaken to consider the effect of fires on post-trip cooling. It identified that the frequency of failure of post-trip cooling due to fires was conservatively  $6.4 \times 10^{-6}$  per reactor year, and led to a series of enhancements to plant.

Changes to the safety case subsequent to the PSA have been tested against the probabilistic risk criteria to confirm that site risk remains Tolerable and ALARP.

In support of the post generation phase, and reflecting the reduced complexity of the safety case for a shutdown reactor, the probabilistic risk has been derived directly from a shutdown fault schedule. This shows that the level of risk significantly reduces with time from that at power, reflecting the lower hazard; however, this lower level of risk is partly negated by the increased reliance on operator action.

## 2 Earthquakes

### 2.1 Design basis

#### 2.1.1 Earthquake against which the plant is designed

##### 2.1.1.1 Characteristics of the design basis earthquake (DBE)

Level of DBE expressed in terms of maximum horizontal peak ground acceleration (PGA). If no DBE was specified in the original design due to the very low seismicity of the site, PGA that was used to demonstrate the robustness of the as built design.

Seismic hazards were not included within the original basis of design for Wylfa Power Station. The capability of the station to withstand seismic events was first evaluated as part of the Long Term Safety Review carried out during the early 1990s, with a more detailed assessment being carried out as part of the periodic safety review that concluded in 2004.

The current design basis earthquake for the Wylfa site is defined by the envelope of the Principia Mechanical Limited (PML) hard site UK design response spectrum anchored to a horizontal zero period acceleration of 0.1g and a site-specific uniform risk spectrum with a probability of exceedance of  $10^{-4}$  per annum. The PML spectrum determines the overall spectral magnitude at low frequencies. The uniform risk spectrum dominates at higher frequencies. The horizontal free-field peak ground acceleration associated with the design basis event is approximately 0.18g.

This design basis seismic event was selected to bound the expected  $10^{-4}$  per annum exceedance frequency event at the Wylfa site.

##### 2.1.1.2 Methodology used to evaluate the design basis earthquake

Expected frequency of DBE, statistical analysis of historical data, geological information on site, safety margin.

The uniform risk spectrum component of the design basis earthquake for the Wylfa site is derived from a site-specific probabilistic seismic hazard assessment. That assessment is based on detailed seismological and geological reviews of the region surrounding the site. The seismic hazard is calculated using a logic-tree formulation based on a zonal hazard model and source parameter (b-value, activity rate, maximum magnitude, depth etc) distributions that reflect the pattern of historical seismicity in the region. In the absence of sufficient UK-specific strong motion records, ground motion spectral attenuation relationships were derived by regression analysis of earthquake records from regions elsewhere in the world considered to share tectonic similarity with the UK. The ground response spectra used in the definition of the design basis event are those assessed to have a uniform probability of exceedance of  $10^{-4}$  per annum. Extensive sensitivity analyses have been undertaken to demonstrate that the predicted hazard is robust against input parameter variation. These have included investigations employing an alternative zone-free hazard assessment methodology. Furthermore, a second, fully independent, probabilistic seismic hazard study for the Wylfa site was undertaken concurrently with the primary study. That

secondary study confirmed the robustness of the hazard predictions derived from the primary study.

The PML UK design response spectra are piece-wise linear (on a standard tripartite plot) response spectra derived by statistical analysis of strong motion earthquake records from elsewhere in the world conforming to the profile of expected UK events. This is again necessitated by a lack of suitable UK-specific strong motion records. These design spectra may be anchored to any zero period acceleration. For the purpose of defining the design basis event for Wylfa, the spectrum has been anchored to a zero period acceleration of 0.1g in recognition of the international regulatory significance of that value.

The design basis earthquake is defined as the upper envelope of these two spectral components.

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

Reassessment of the validity of earlier information taking into account the current state-of-the-art knowledge.

The UK as a whole is a region of relatively low-level and diffuse seismic activity. No specific geological or tectonic features have been identified that would suggest that earthquakes larger than those considered in the studies underpinning the Wylfa design basis event (average maximum magnitude 6.5) are credible. Examination of the pattern of historical UK seismicity indicates that Wylfa is situated in a region of slightly above average earthquake activity by UK standards.

The causes and distribution of seismicity in the Wylfa region are subject to a variety of interpretations. However, it is considered that the two independent site-specific probabilistic hazard assessments together with the range of supporting sensitivity analyses that have been completed encompass the range of expert opinion and credible parameter variations. Moreover, those studies have been undertaken in accordance with modern standards in the field. It is concluded that the design basis earthquake is a pessimistic and robust representation of the prevailing seismic hazard for the Wylfa site at the  $10^{-4}$  per annum exceedance frequency.

### 2.1.2 Provisions to protect the plant against the design basis earthquake

#### 2.1.2.1 Systems Structures and Components (SSCs)

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

This report primarily addresses the design basis event and beyond design basis events. For less severe events, a second, diverse line of protection is provided.

The key structures systems and components required to achieve a safe shutdown state and claimed to remain available following an earthquake consistent with the design basis event described in Section 2.1 are as follows:

### Key Structures

- reactor pressure vessels and internal structures (including boilers, the reactor graphite core, and its support and restraint structures);
- reactor buildings;
- reactor equipment building;
- tertiary and back-up boiler feed pump houses;
- remote emergency indication centre building;
- primary dry store cells
- waste vaults and facilities

### Key Systems and Components

- reactor tripping function (failsafe operation of safety circuits and guardlines or manual operator trip);
- control rod system;
- reactor pressure vessel penetrations and primary pressure circuit pipework (including fuelling machinery if attached to the reactor) – sufficient integrity to allow primary cooling by natural circulation of coolant gas within the reactor pressure vessel;
- boilers and boiler venting system;
- gas circulator static seal application system;
- tertiary and back-up boiler feed systems (including water tanks, pumps and boiler feed pipework);
- remote emergency indication system (including instrumentation and cabling);
- primary dry store cell ventilation.

The key structures, systems and components identified above were not designed to withstand the design basis earthquake. Rather, they have been subject to retrospective qualification. The approach taken to demonstrate seismic robustness has been to carry out deterministic performance assessments of each key structure, system and component against the design basis seismic demand using conservative assessment methods and failure criteria.

Wide ranging modifications have been made to plant and structures to harden pre-existing key structures, systems and components against the design basis seismic demand. Additional diverse and redundant systems, explicitly designed to withstand seismic loading, have been installed specifically to enhance the security of provisions for post-event reactor cooling and post-event reactor monitoring.

It has been demonstrated that each required safety function will be maintained with high confidence following earthquakes consistent with the defined design basis event.

Best-estimate failure margins beyond the design basis have not been evaluated and deterministic seismic withstand capabilities have not been calculated on a common basis. Therefore, it is not possible, on the basis of existing information, to provide rigorously quantified consistent safety margins. However, conservative approaches have been taken to assessment and

design of the key structures systems and components, and substantial diversity and redundancy of safety-related plant provisions have been developed. On this basis it is judged that a best-estimate margin of at least 50% beyond the design basis exists before substantive loss of safety functions would occur as a result of seismically induced plant damage.

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.

Operations to be carried out following an earthquake consistent with the design basis event would be determined by the reactor operators/shift charge engineer/site emergency controller in accordance with station operating procedures. Actions will depend upon the state of the plant and system availability.

Assuming failure of all systems that are not explicitly qualified to withstand the design basis event, the following key operating provisions would be invoked:

- Establish command and control of the event

The Shift Charge Engineer assumes the role of Emergency Controller until he is relieved by standby personnel who are on a duty rota on 24/7 call out basis. The duty Emergency Controller would attend site and establish the Emergency Control room or designated alternative on site unless both are untenable, in which case an alternative off site facility is available.

- Secure safe reactor shutdown

Trip the reactor if not already tripped. Station Operating Instructions require that the reactor is manually tripped if there is evidence of a seismic event/seismic alarm (at this level of earthquake it would be expected that failures of non-qualified plant would trip the reactors via safety circuits and guardlines (which are failsafe) without the need for a manual trip intervention);

- Establish effective post-trip reactor cooling

If they are not running, put the gas circulators on static seal using the normal DC motor or manually. If this cannot be achieved use the emergency static seal application system (diesel generator and AC motor). Instructions for this are given in Station Operating Instructions. Ensure primary pressure boundary integrity by closure of valves to isolate a breach in any external part of the pressure circuit, to prevent rapid primary pressure circuit depressurisation (Procedure in SOI).

If the Main and Emergency boiler feed have been disabled by the event, commission the back-up boiler feed system to provide secondary reactor cooling. Recommended minimum flow rates and maximum delay times, dependent on state of pressurisation and availability of boilers, are given in the SOI.

- Establish monitoring of key reactor parameters

Reactor monitoring will normally be carried out from the Central Control Room (CCR) using the installed temperature scanner and alarm analyser. In the event that the CCR is untenable, staff will redeploy including manning the Remote Emergency Indication Centre (REIC) to confirm reactor shutdown, hold-down and adequacy of cooling provisions. Instructions in the event of the CCR being untenable are in SOIs. The REIC is for indication only; manual local control of plant would be required in the event that control from the CCR is not possible.

- Carry out plant inspections and prioritised repair of damaged systems

Instructions following a seismic event are given in SOIs. These state that if a reactor has been shutdown as a result of a seismic event it may not be restarted without the permission of the Nuclear Safety Committee and ONR. Instructions are given for carrying out plant checks to ascertain the extent of any plant damage to determine if it is safe to keep operating, if the reactor has not already tripped, or to instigate action to protect post trip functions if it has.

Emergency arrangements (see Section 6) include provision for sending out an assessment team in Breathing Apparatus with CO<sub>2</sub> and radiation monitoring instruments to assess the state of the plant. Damage repair teams can then deploy various pre-determined and rehearsed techniques for sealing the pressure circuit. The aim of this would be to achieve a sufficient seal to maintain a slight positive CO<sub>2</sub> pressure in the vessel to prevent significant air exchange within the circuit. Such repair techniques are not designed to hold normal operating pressure.

### 2.1.2.3 Protection against indirect effects of the earthquake

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

Structures and components that are not required to function during or following an earthquake but whose failure could present a potential threat to safety-related structures, systems and components have been systematically identified. Such items include the reactor buildings, cranes, pressurised steam pipework and masonry walls. These items have been assessed and capability consistent with the design basis seismic demand has been demonstrated. Where necessary, items have been modified to secure the required withstand capability.

Localised flooding following a design basis earthquake could arise from failures of on-site tanks or pipework that are not qualified against the design basis seismic demand. The potential for, and consequences of, such flooding (including the effects of spray) have been considered. In all cases it has been determined that key structures, systems and components required to provide safety functions following the design basis seismic event (Section 2.1.1.1) will remain available.

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

The seismic safety case for the design basis earthquake assumes that the earthquake causes an immediate loss of all incoming electrical power supplies to the site. No reliance is placed on restoration of those supplies for maintenance of essential safety functions. Post-trip primary cooling by natural circulation of coolant gas within an essentially intact reactor pressure boundary does not require electrical supplies. The back-up and tertiary boiler feed systems have dedicated diesel driven pumps with their own starter batteries. The REIC system has its own dedicated diesel generator.

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

Availability of personnel and supplies from off-site has not been explicitly considered within the seismic safety case. Sufficient stocks of diesel fuel and water are maintained available on-site for the claimed safety systems to function for a minimum of 24 hours.

Access of personnel and equipment to site is considered in Section 6.

- 2.1.2.3.4 Other indirect effects (e.g. fire, explosion).

The potential for consequential fire, explosions or other hazards (e.g. gas clouds or spilt chemicals) affecting the plant following a design basis earthquake has not been explicitly evaluated. It is not considered that any of these hazards pose a substantive risk to the key structures, systems and components required to maintain safety functions following a design basis event. Operator actions would take account of local conditions and utilise redundancy in the various claimed systems.

### **2.1.3 Compliance of the plant with its current licensing basis**

- 2.1.3.1 Processes to ensure SSCs remain in faultless condition

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.

Operating Rules and Station Operating Instructions define minimum plant availability requirements and ensure that only certain combinations of plant are allowed to be unavailable at the same time. Failure to meet these minimum availability levels can result in the requirement to shut one or both reactors down.

The plant is subject to routine maintenance, inspection and testing as required by the nuclear Maintenance Schedule, which lists those ongoing activities that are necessary to support the site safety case. This is implemented in accordance with Management Control Procedures (MCPs) for "Management of Maintenance Work" and "Surveillance and Routine Testing of Plant Items and Systems". Specific procedures include "Inspection and Assessment of Nuclear Safety Related Civil Structures to Comply with Site Licence Condition 28", whose scope specifically includes all significant civil structures and specifically includes structures claimed for seismic support.

As necessary, the plant and safety case is modified or updated in accord with MCP "Control of Modifications and Experiments".

At 10-yearly intervals, and in response to significant operating events, the safety of the plant is reviewed in a periodic safety review. This reviews the plant against modern standards, operating experience and the effect of ageing. Enhancements identified in the periodic safety reviews carried out to date have been implemented.

Immediately following the Fukushima event a series of plant walkdowns was carried out on the following plant:-

- back-up feed system
- boron dust injection equipment
- circulator static seal equipment
- remote emergency indication centre
- portable fire pump
- site fire engine

These walkdowns included a general review of the equipment, an assessment for defects, a review of the availability and storage of portable equipment and the ease of deployment of the equipment. No major shortfalls that would have compromised the deployment of the equipment have been identified. Minor defects identified have already been addressed or are planned to be addressed.

In addition to the walkdowns, active testing (as far as practical without risk to operating plant) of the following plant has been carried out. (Note this testing is in addition to that normally undertaken on a routine basis as part of Maintenance Schedule activities):-

- Tertiary Feed System / Back up Feed Systems
- Boron Dust Equipment
- Gas Circulator Static Seal Equipment
- Station Fire Tender
- Portable Fire Pumps

The ability of the above plant / equipment to operate successfully was tested, and it was confirmed available for use.

A targeted programme of walkdowns is currently in progress to verify the capability of the claimed safety-related systems (external to the reactor pressure vessel) to fulfil their safety function following the design basis event and to improve the understanding of vulnerability to events beyond the design basis. The walkdowns have been carried out by engineers trained in the US Electrical Power Research Institute-led Seismic Qualification Utility Group evaluation procedures for seismic verification of nuclear plant.

#### 2.1.3.2 Processes for mobile equipment and supplies

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.

The maintenance of mobile equipment is covered by the same processes as detailed in Section 2.1.3.1. The routine testing and maintenance of fire pumps, fire engines and gas circulator static seal generators are all on the maintenance schedule.

#### 2.1.3.3 Potential deviations from licensing basis

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

A review of maintenance and operation procedures for these SSC was carried out following the Fukushima event and minor improvements were implemented at that time. No other deviations have been identified.

## 2.2 Evaluation of safety margins

### 2.2.1 Range of earthquake leading to severe fuel damage

Weak points and cliff edge effects: estimation of PGA that would result in damage to the weakest part of heat transfer chain, and consequently cause a situation where the reactor integrity or spent fuel integrity would be seriously challenged.

A robust and conservative demonstration has been made of the capability to meet the design basis requirements (Section 2.1.2.1). The remainder of this section considers the potential for cliff edge effects.

The essential reactor safety functions that must be maintained to prevent fuel damage and radiological release are the ability to trip, shutdown and hold down the reactor, the ability to provide adequate post-trip reactor cooling, and maintenance of reactor containment (primary cooling gas circuit integrity). Assurance that these functions are being met is obtained via post-trip monitoring of reactor conditions. Containment, shielding and cooling of discharged fuel and containment of radioactive waste material are also essential.

Damage scenarios that could result in loss of each essential safety functions are considered below.

#### Reactor Trip

Reactor trip would be achieved via operation of safety circuits and guard lines. These systems are not qualified to withstand seismic events but are designed to be failsafe. In particular, the rods are held out of the reactor by electrical actuators. De-energisation of these actuators will lead to the control rods being released. The control rods then drop under gravity into the core to achieve shutdown and hold down. Similarly the guard lines require power and healthy signals from all inputs, loss a signals or power would cause a trip.

If significant plant damage were to result from a beyond design basis earthquake then the safety circuits and guard lines would either function normally or would fail safely. Either response would lead to reactor trip. Given the failsafe nature of the trip systems, failure to trip following a beyond design basis event sufficient to cause safety-significant plant damage is considered highly unlikely regardless of earthquake severity.

#### Reactor Shutdown and Hold Down

Inability to shutdown or hold down the reactor coupled with reduced reactor cooling would lead rapidly to fuel damage. Reactor shutdown and hold down is achieved by insertion, under gravity, of sufficient control rods into channels within the graphite core. Very few rods are required to actually shut a reactor down, more are needed to terminate a fault temperature transient or provide hold down long term. Control rods may be prevented from entering the core in the following eventualities:

- a) damage leading to widespread jamming of control rod mechanisms.
- b) excessive irrecoverable core movement causing rigid and/or articulated control rods to foul by 3-point contact during entry.
- c) widespread disruption of the graphite brick structure or integrity causing dislocation or blockage of control rod entry paths.
- d) failure of graphite core support and restraint structures causing collapse of the core and dislocation of control rod entry paths. This could also lead to effective withdrawal of the control rods.

Based on the outcome of existing assessments, it is judged that scenario d) would be likely to occur at a lower beyond design basis earthquake severity than the other scenarios.

The reactor core and its support and restraint structures have high mass and relatively low stiffness. As a consequence their fundamental natural frequency is predicted to be very low (~1Hz). These structures are, therefore, most sensitive to earthquakes having large spectral displacements at low frequencies, rather than to high peak ground accelerations.

There is limited correlation between peak ground acceleration and low frequency spectral displacement. Additionally, as noted in Section 2.1.2.1, explicit margins beyond the design basis earthquake have not been evaluated. Furthermore, structural responses would become non-linear before the above damage scenarios are realised.

As a consequence it is not possible to specify a peak ground acceleration, or other measure of earthquake severity, at which the limiting damage scenario would occur. However, assessments have demonstrated that the reactor pressure vessel internal structures are able to maintain essential safety functions following an event defined by a generic United Kingdom hard site uniform risk spectrum anchored to a zero period acceleration of 0.25g. This enhanced seismic demand level (~38% greater than the design basis) is considered to represent a minimum capability for the pressure vessel internal structures. At that earthquake level some inelastic behaviour of the core support structures is predicted. However, it is judged, on a best-estimate basis, that a seismic demand of severity at least 50% greater than the design basis (see Section 2.1.2.1) would be required to cause damage that would prevent reactor shutdown and hold down.

#### Post-trip Cooling

Following a design basis event, that is anticipated to cause loss of forced coolant gas circulation capability, primary cooling of the fuel would be by natural circulation of pressurised coolant gas within an essentially intact reactor coolant circuit. Secondary

heat removal is via low pressure feed water to the boilers with steam being vented to the atmosphere.

Effective post-trip cooling of the fuel would be undermined if any of the following were to occur:

- a) disruption of the graphite core structure causing blockage of coolant gas flow paths through the core.
- b) a large breach of the reactor pressure boundary leading to substantial depressurisation of the reactor gas circuit and inadequate heat transfer from fuel to coolant gas.
- c) damage to boilers preventing effective secondary heat removal.
- d) inability to provide sufficient feed water to the boilers as a result of damage to feed pipework, loss of all pumps or suitable water supplies.
- e) inability to complete operator actions necessary to initiate low pressure boiler feed as a result of access difficulties or plant and equipment damage.

Relatively long timescales of the order of 24 hours are available within which to establish boiler feed provided that the reactor has shutdown and the reactor remains substantially pressurised. On such timescales it should be possible to overcome access difficulties (e) and repair external feed pipework (d), if necessary, to enable feed water injection to the boilers. The most limiting of the remaining scenarios is judged to be (b): breach of the reactor pressure boundary leading to reactor coolant circuit depressurisation.

For the reasons stated above, within the discussion of reactor shutdown and hold down, it is not possible to quantify rigorously a peak ground acceleration, or other measure of earthquake severity, at which a limiting damage scenario would occur. The most likely limiting cause of pressure boundary damage is judged to be secondary damage to primary pressure circuit pipework external to the reactor pressure vessel resulting from failures of the adjacent equipment or structures having lesser resilience. For reasons discussed in Section 2.1.2.1, on a best-estimate basis, it is judged that a margin of at least 50% beyond the design basis exists before irrecoverable pressure boundary breaches could occur of a size preventing adequate post-trip cooling.

#### Reactor Containment

See Section 2.2.2 below.

#### Post-trip Reactor Condition Monitoring

Post-trip monitoring of reactor conditions following an event consistent with the design basis would be via the REIC. The REIC is located in a separate building outside the reactor controlled area and receives data through cables from dedicated reactor instrumentation. This system has a battery-backed uninterruptible power supply supported by a dedicated diesel generator. While loss of reactor monitoring would not of itself lead directly to fuel damage, a lack of monitoring information (temperature,

pressure, neutron flux) could hamper the capability of operators to take appropriate post-event remedial actions. Maintenance of monitoring is, thus, highly desirable.

Monitoring capability could be lost in the following scenarios:

- a) damage to primary instrumentation (including pressure gauge piping etc) within or external to the reactor pressure vessel.
- b) damage to data transmission cabling between the instrumentation and REIC.
- c) damage to the REIC including loss of electrical supplies.
- d) inability to complete operator actions necessary to access and operate the REIC.

It is judged that the most likely limiting scenarios are those (b and c) associated with damage to data transmission cabling within the reactor buildings or damage to equipment within the REIC. In particular cabling would be vulnerable to significant failures within the reactor buildings (as discussed above for the reactor pressure boundary) and electrical cabinets may topple. Again it is not possible to quantify rigorously a peak ground acceleration, or other measure of earthquake severity, at which the limiting damage scenario would occur. However, for reasons discussed in Section 2.1.2.1, on a best-estimate basis, it is judged that a margin of at least 50% beyond the design basis exists before damage could occur preventing adequate post-trip monitoring.

#### Containment, Shielding and Cooling of Discharged Fuel

Containment for fuel discharged from the reactors is provided by primary dry store cells. Discharged fuel is located in vertical storage tube bundles that are hung from surrounding reinforced concrete shielding structures. Cooling of the fuel is achieved by once-through natural circulation of air external to the storage tube bundles. Substantial blockage of the external air cooling paths can be tolerated before fuel would overheat. Existing assessments have shown that both the reinforced concrete shielding structures and storage tube structures can withstand loading consistent with at least twice the 0.25g uniform risk spectrum seismic demand (which is itself ~38% greater than the design basis demand). Containment, shielding and cooling for discharged fuel is, thus, immensely robust with a very large margin against the design basis before fuel damage could credibly occur.

#### Containment and Shielding of Radioactive Waste

Radioactive waste materials are mainly located below ground within the basements of the reinforced concrete reactor buildings or in massive concrete vault structures. The parts of the buildings containing the waste are considered to be robust against even very severe earthquakes. Although the primary plant containing waste (settling tanks etc) may fail during a seismic event, the material will remain confined within the building structure. Large margins against a significant short to medium term release of waste material to the environment as a result of a seismic event would be expected.

### **2.2.2 Range of earthquake leading to loss of containment integrity**

Estimation of PGA that would result in loss of integrity of the reactor containment.

Reactor containment is provided by the pre-stressed concrete reactor pressure vessel and steel liner, associated penetration closures and connected plant and equipment that collectively form the reactor pressure boundary. The integrity of the concrete pressure vessel itself would not be threatened by credible seismic loading. The limiting components of the containment boundary are the pressure vessel penetrations together with attached plant and equipment. The vulnerability of these components is discussed in the context of post-trip cooling within Section 2.2.1, identical considerations apply from the perspective of containment.

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

Possibility of external floods caused by an earthquake and potential impacts on the safety of the plant. Evaluation of the geographical factors and the physical possibility of an earthquake to cause an external flood on site, e.g. a dam failure upstream of the river that flows past the site.

The relatively low magnitudes together with the anticipated mechanisms of UK earthquakes indicate that the potential for a significant tsunami resulting from a local earthquake is very low. Furthermore, the potential for local land-slips into water or slippage of the river/sea bed leading to a local tsunami affecting the Wylfa site is also considered to be negligible. A more significant tsunami could credibly result from a distant earthquake. In that case, however, the ground motion at the Wylfa site resulting from the earthquake would not be damaging. Thus, the potential for significant earthquake damage combined with significant tsunami-induced damage can be discounted.

The only nearby body of stored water above the level of the Wylfa site that could conceivably be breached by a design basis earthquake is the water storage reservoir which is located slightly uphill of the main site. Failure of that reservoir could lead to loss of off-site electrical supplies and limited flooding of the Turbine Hall basement. Neither of these potential consequential flooding events would affect the key structures, systems and components required to provide safety functions following the design basis seismic event.

Localised flooding following a design basis earthquake could arise from failures of on-site tanks or pipework that are not qualified against the design basis seismic demand. Again such consequential flooding would not affect the key structures, systems and components required to provide safety functions following the design basis seismic event.

### **2.2.4 Potential need to increase robustness of the plant against earthquakes**

Consideration of measures, which could be envisaged to increase plant robustness against seismic phenomena and would enhance plant safety.

Following the Fukushima event a series of workshops has been held to consider the robustness of the site (reactors and primary/secondary dry store cells) against internal and external hazards, and to look at the site's emergency preparedness arrangements. Some areas for consideration were identified and these are currently being assessed. The areas for consideration relevant to this section are given below:-

Consideration WYA 01: Consideration will be given to enhancing the methods and equipment for primary pressure circuit sealing.

Consideration WYA 04: Consideration will be given to providing a facility for the injection of nitrogen to support reactor hold-down.

## 3 Flooding

### 3.1 Design basis

#### 3.1.1 Flooding against which the plant is designed

##### 3.1.1.1 Characteristics of the design basis flood (DBF)

Maximum height of flood postulated in design of the plant and maximum postulated rate of water level rising. If no DBF was postulated, evaluation of flood height that would seriously challenge the function of electrical power systems or the heat transfer to the ultimate heat sink.

##### Design Basis Sea Levels

Wylfa Power Station is located on the north coast of the island of Anglesey facing onto the Irish Sea. The site is bounded to the north and west by a rocky coastline comprising irregular rock outcrops intersected by narrow gullies. The land rises to the south and east.

The central part of the site, occupied by the turbine house and reactor buildings, is relatively flat at an elevation of approximately +12.5m Ordnance Datum (OD). Towards the western edge of the site, in the vicinity of the circulating water pump house, ground level reduces to between +7.5m and +10m OD. An intermittent mass concrete sea wall with a crest level of +6.1m OD exists coinciding with breaks in the rocky headland at the shore line. The north-west tip of Anglesey protects the site from Atlantic swell waves from the south-west. There is limited protection from waves generated more locally across the length of the Irish Sea. A shallow rocky area extending a few hundred metres offshore reduces the energy of the most severe sea conditions in the final approaches to the sea defences.

The primary threat of flooding arises from combined tidal, surge and wave effects (including swell and wind wave). The highest astronomical tide level is +3.7m OD with a mean spring tidal range in the vicinity of Wylfa of approximately 5.7m, slightly above the UK average. The maximum still (tide + surge) water level at an exceedance frequency of  $10^{-4}$  per annum is predicted to be +5.2m OD (including an estimate of +0.18m for climate change induced regional mean sea level rise by the year 2030).

The predicted maximum wave crest elevation (including tide, surge, swell and wind wave effects) at an exceedance frequency of  $10^{-4}$  per annum is +9.41m OD (again including +0.18m allowance for climate change induced mean sea level rise). The extreme sea state giving that maximum crest elevation comprises +3.35m OD still water level (tide, surge and mean sea level rise) and a significant wave height (peak-to-trough) of approximately 9m. The maximum crest elevation quoted is a wave crest level exceeded by only one or two percent of wave crests in the extreme sea state.

An extreme wave crest elevation of +9.41m OD would cause flooding of the circulating water pump house potentially resulting in loss of the circulating water and sea water cooling system and consequential unavailability of reactor ancillaries cooling water and pressure vessel cooling water systems. However, there is a large margin against flooding of the main buildings and surrounding

facilities that are located at, or above, +12m OD. Thus two lines of protection against loss of essential safety functions (provided by the key structures, systems and components identified in Section 2.1.2.1) will remain unaffected by flooding.

In defining the design basis flood levels for the Wylfa site no explicit account has been taken of potential tsunami risk. The tsunami threat is considered to arise primarily from large distant earthquakes. Any residual tsunami wave affecting the site is expected to be small. At the  $10^{-4}$  per annum exceedance frequency the risk from tsunamis will be bounded by the existing design basis sea levels considering extreme tide, surge and wave combinations.

#### Design Basis Rainfall and Snow Melt

The flooding risk presented by extreme rainfall events having  $10^{-4}$  per annum exceedance frequency has also been considered. Specifically, the capability of the site surface water drainage system to prevent flooding during and following extreme storms having durations between 15 minutes (49mm of rain) and 2 hours (126mm of rain) has been assessed. It is concluded that the maximum flood water level will not exceed the ground floor levels of the reactor buildings or turbine house. Although some water could enter the turbine house basement via an external pipe trench the depth of flooding would not threaten safety-related plant in the turbine house. The circulating water pump house could be flooded but the consequences of this are acceptable (see above).

The coincidence of extreme rainfall with the extreme sea flooding event has been addressed. In such circumstances the site drainage system would remain functional with a favourable hydraulic gradient and the consequences of such a combined event would be no worse than the impact of extreme rainfall alone.

The estimated  $10^{-4}$  per annum snow melt rate is a modest 83mm of water per day. Although unmelted snow could impair free drainage of melt-water causing localised flooding, clearance would be possible well in advance of significant safety-related consequences.

#### Offsite Water Sources

The only nearby body of stored water above the level of the Wylfa site whose failure could conceivably lead to flooding of the site is the water storage (“million gallon”) reservoir which is located to the east and slightly uphill of the main site. Failure of that reservoir could lead to loss of off-site electrical supplies and limited flooding of the turbine hall basement. Neither of these potential consequential flooding events would affect the key structures, systems and components required to protect nuclear safety functions.

#### 3.1.1.2 Methodology used to evaluate the design basis flood.

Reassessment of the maximum height of flood considered possible on site, in view of the historical data and the best available knowledge on the physical phenomena that have a potential to increase the height of flood. Expected frequency of the DBF and the information used as basis for reassessment.

#### Design Basis Sea Levels

Basic extreme tide levels have been derived from harmonic analysis of tide gauge data collected over a 12 month period at the site circulating water intake location during 1985 and 1986. Longer time series tide gauge data from the nearby port of Holyhead have been used to synthesise 24 years of hourly surge and tide level data adjacent to the site.

23 years of hourly synthetic wave hindcasts for a location offshore from the site over a period corresponding to that of the synthetic tide and surge data have been derived numerically based on hourly averaged wind velocity measurements from Blackpool Airport adjusted to represent conditions over the Irish Sea. The numerical modelling included wave generation in deep water, taking account of fetch lengths wind direction and wind duration. The numerical wave modelling also simulated the effects of wave refraction and shoaling as the deep water waves travel towards the shoreline. For this purpose detailed local bathymetry data was utilised.

The numerical wave hindcasts were calibrated against 12 months of measured wave data. The measurements were taken from a buoy located in deep enough water offshore of the site such that the predicted extreme waves would not have broken but near enough to the coast to represent the protective effects of nearby headlands and local bathymetry. Predicted wind wave heights were enhanced to include the effects of background swell.

Based on the resulting synthesised wave climate data, extreme significant wave heights for exceedance frequencies greater than or equal to  $10^{-4}$  per annum were estimated by extreme value analysis.

To estimate  $10^{-4}$  per annum exceedance frequency wave crest heights, a joint probability analysis of tide, surge and wave heights has been carried out. This demonstrates that the highest positive surges occur at low tide levels and vice-versa. Furthermore, the average still water level associated with the highest wind wave conditions is slightly higher than the average still water level. Maximum wave crest heights (including tide, surge, swell and wind waves) at the  $10^{-4}$  per annum exceedance frequency were then predicted taking account of these correlations.

#### Design Basis Precipitation

Predicted extreme rainfall quantities relating to the location of the Wylfa site for storms of various durations and exceedance frequencies up to  $10^{-3}$  per annum (and theoretical maxima) were obtained from the United Kingdom Meteorological Office. These are based on statistical analysis of long term regional rainfall records. These predictions have been interpolated to the  $10^{-4}$  per annum exceedance frequency using factors defined in the United Kingdom flood estimation methodology prevailing at the time (1990).

For assessing the capability of the drainage system and over-ground spillways the variation of rainfall intensity with time has been assumed based on the typical profile of a summer storm. Summer storm profiles exhibit a greater relative intensity of rainfall in the central period of the storm than do winter storm profiles. The summer storm profile, therefore, represents a more onerous case for a small catchment area of the kind presented by the Wylfa site.

The  $10^{-4}$  per annum uniform building snow load for the Wylfa site was derived from British Standards. That load was converted to an equivalent depth of water and complete melting was pessimistically assumed to occur over a period of 12 hours.

#### 3.1.1.3 Conclusion on the adequacy of protection against external flooding

The methodology employed to estimate the design basis sea levels is comprehensive and rigorous making best use of available site-specific and regional data. The numerical modelling has been undertaken by experts in the field based on validated computer codes. It is concluded that the design basis maximum wave crest level is a robust estimate of an extreme sea state consistent with the  $10^{-4}$  per annum exceedance frequency. There is also a large margin (>3m) against inundation of key structures, systems and components under the design basis flood condition. This margin is ample to accommodate any uncertainties in data and methodology used in defining that extreme condition.

The omission of tsunami contributions from the design basis sea levels is not judged to be significant. At the  $10^{-4}$  per annum exceedance frequency the contribution of tsunami to the overall flood risk is considered to be substantially bounded by that of extreme tide, surge and wind wave combinations.

The adequacy of the methodology and underlying data utilised to estimate the design basis extreme precipitation and consequent flood levels is less certain. The assessment of precipitation rates is now 20 years old and further data on extreme UK weather events will have been accumulated since that time. Similarly the methodology for predicting and evaluating such events will have improved. Notwithstanding such advances, the design basis flooding assessment exhibits significant margins against levels that could credibly threaten key structures, systems and components. It is judged that those margins are adequate to accommodate potential increases in flood levels from precipitation events resulting from uncertainty in the design basis.

Failure of offsite water sources cannot pose a significant threat to nuclear safety.

Overall it is concluded that the assessed consequences of flooding as a result of extreme sea levels or precipitation consistent with a  $10^{-4}$  per annum exceedance frequency, or failure of offsite water sources, have not been significantly underestimated. Therefore, it is considered that the evaluation of the design basis flooding conditions remains adequate.

### 3.1.2 Provisions to protect the plant against the design basis flood

#### 3.1.2.1 Systems Structures and Components (SSCs)

Identification of systems, structures and components (SSCs) that are required for achieving and maintaining safe shut down state and are most endangered when flood is increasing.

Many of the SSC essential for safety (identified in Section 3.2.1) are located at (or slightly above) ground level. Plant in basement levels would not be affected by external flooding until overtopping occurred from ground level.

The absolute water levels where plant would be affected are discussed below in Section 3.2.1.

#### 3.1.2.2 Main design and construction provisions

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

The Wylfa site is located on a rocky headland with the main buildings, roadways etc. at a level that is 9.2m above the highest astronomical tide level for the area, and 3m above the  $1 \times 10^{-4}$  pa extreme high tide/storm surge level. The ground level of the site is predominantly flat with the land falling to the sea along the full length of the westerly side. There are generally small gradients away from buildings.

Site storm drains exist to remove water from the site but even if these did not function it is unlikely that water level would build up significantly in an extreme rainfall event.

#### 3.1.2.3 Main operating provisions

Main operating provisions to prevent flood impact to the plant.

None.

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

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

The local topography around the Wylfa site is not particularly low-lying. Local roads are unlikely to be blocked by extreme high tides or tsunamis but some roads may be susceptible to localised flooding from severe storms. Access for large vehicles and 4 x 4 vehicles should be possible even in a severe flooding situation.

### 3.1.3 Plant compliance with its current licensing basis

#### 3.1.3.1 Processes to ensure SSCs remain in faultless condition

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

There are no systems or structures specifically for flood *protection* at Wylfa.

Systems that would be required for heat removal from the core in a flooding (or any other) event are all classified as Minimum Safety Related Plant. These are

subject to Operating Rule based limits on how much equipment can be released from service at any one time, and have a rigorous maintenance and testing regime defined by the station Maintenance Schedule.

### 3.1.3.2 Processes for mobile equipment and supplies

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 on site specifically for flooding events. Mobile fire pumps, which could be used for removing floodwater, are on the station Maintenance Schedule and are tested at a monthly frequency and maintained annually.

### 3.1.3.3 Potential deviations from licensing basis

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

A review of maintenance and operation procedures for this plant was carried out immediately following the Fukushima event and minor improvements were implemented at that time. No other deviations have been identified.

## 3.2 Evaluation of safety margins

### 3.2.1 Estimation of safety margin against flooding

Estimation of difference between maximum height of flood considered possible on site and the height of flood that would seriously challenge the safety systems, which are essential for heat transfer from the reactor and the spent fuel to ultimate heat sink.

The tables below give heights of sensitive plant above the  $1 \times 10^{-4}$  pa extreme high tide/storm surge level of 9.41m OD.

Equipment required for ultimate heat removal for design basis event:-

Tertiary Feed Pumps	3.6m
BUFS Pumps	3.5m

Other safety related equipment not essential for design basis event:-

Gas Turbines	3.4m
Essential Auxiliary Switchboard	3.5m
EOS Diesel Generators	3.3m
Guaranteed Supplies System	3.5m
110V Switchgear Batteries	3.5m
50V C & I Batteries	16.1m
50V Telecommunication Batteries	16.1m
240V Emergency Lighting Batteries	3.5m

Emergency Boiler Feed Pumps	3.0m (to flood turbine hall basement)
Fire Station	3.5m (Fire tender + portable pumps)
Fixed Jet Fire Pumps	3.0m (to flood turbine hall basement)
Fire Hydrant Pumps	3.0m (to flood turbine hall basement)
Diesel Fire Pump	3.5m
Gas Circulators	3.0m (to flood reactor building basement)
Gas Circulator Static Seal Equip.	3.9m
Boron Dust Equipment	3.3m
REIC	3.2m

Other significant plant:-

PDSC Air Inlet Ducts	3.2m
Seawater Cooling Pumps	-3.7m*

\*Seawater Cooling Pumps are located below the  $1 \times 10^{-4}$  pa flood height but are not claimed for design basis flooding or seismic events.

As site flooding was not within the design basis, no assessment has been made of hydrodynamic or debris loads on structures and equipment. These will be addressed in the assessment of the measures being considered to increase the resilience to flood.

### **3.2.2 Potential need to increase robustness of the plant against flooding**

Following the Fukushima event a series of workshops has been held to consider the robustness of the site (reactors and primary/secondary dry store cells) against internal and external hazards, and to look at the site's emergency preparedness arrangements. Some areas for consideration were identified and these are currently being assessed. Any enhancements relevant to this section are addressed within the areas for consideration discussed elsewhere in this document.

## 4 Extreme weather conditions

### 4.1 Design basis

#### 4.1.1 Reassessment of weather conditions used as design basis

##### 4.1.1.1 Characteristics of design basis extreme weather conditions

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.

The weather conditions incorporated into the design basis safety case are extremes of winds, ambient temperatures, snow and rain. The potential impact of these weather conditions on all safety related structures were considered and where appropriate modifications were implemented. The weather conditions of concern are recognised within the SOIs, namely Actions to be taken in the Event of Severe Weather Conditions. Four procedures are included:

- Procedure A: High Wind Conditions;
- Procedure B: Low Temperatures (-5°C or lower for 2 days or more);
- Procedure C: Heavy snowfall (2cm per hour for 2 hours or more)
- Procedure D: Persistent Rain (25cm per hour for 2 hours or more).

##### 4.1.1.2 Postulation of design basis characteristics

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

It is considered that the Periodic Safety Review process which has been employed twice at Wylfa has ensured that design standards and ageing effects have been kept under surveillance. This process has led to either justification that existing structures continue to meet modern standards adequately or to buildings having been strengthened to ensure that they meet their design duty. This applies particularly to buildings and plant associated with the EBFS, BUFS and TFS.

##### 4.1.1.3 Assessment of frequency

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

The return frequencies of the design basis weather conditions considered are:

- |      |              |  |
|------|--------------|--|
| i)   | Wind:        | $10^{-4}$ per annum;                       |
| ii)  | Temperature: | Deterministic bound of local temperatures; |
| iii) | Snow:        | $10^{-4}$ per annum;                       |
| iv)  | Rain:        | $10^{-4}$ per annum.                       |

The frequencies for wind, rain and snow are consistent with the safety case assessments carried out for external hazards and for which at least one engineered line of reactor cooling has been justified. With respect to temperatures, a bounding of experienced temperatures is a justifiable

approach, given the location of the site, which is adjacent to the sea. Seawater temperature varies by only around 10°C throughout the year, never being colder than about 5°C nor warmer than about 15°C. This range of seawater temperatures leads to air temperatures never being lower than 0°C for long periods.

#### 4.1.1.4 Potential combinations of weather conditions

Consideration of potential combination of weather conditions.

Within the most recent PSR, credible (rather than random) combinations of weather conditions were considered, namely:

- i) extreme winds, extreme precipitation, lightning (and high sea levels);
- ii) extreme winds, driven snow and snow loadings on buildings;
- iii) extreme low temperatures plus snow and ice.

In all cases it is acknowledged that disconnection from the grid could occur (e.g. due to excess wind or snow loadings on transmission lines) and hence the availability of on-site systems was considered. In no case was the ability to trip and shutdown challenged. The PSR confirmed that there was no instance in which the combined hazards gave rise to more onerous conditions than when the hazards were considered individually.

## 4.2 Evaluation of safety margins

### 4.2.1 Estimation of safety margin against extreme weather conditions

Analysis of potential impact of different extreme weather conditions to the reliable operation of the safety systems, which are essential for heat transfer from the reactor and the spent fuel to ultimate heat sink. Estimation of difference between the design basis conditions and the cliff edge type limits, i.e. limits that would seriously challenge the reliability of heat transfer.

Considering each weather condition in turn:

#### i) Wind

The current safety case relies on the outer envelope of the reactor buildings remaining intact. The envelope comprises concrete panels at the lower levels and steel sheet cladding on the upper sections. Within the most recent PSR, and subsequently, the fixings of all panels have been confirmed to meet appropriate standards and where necessary fixings have been either repaired or strengthened to ensure that the panels would not be compromised by a  $10^{-4}$  pa return frequency wind. The buildings remote from the reactor buildings associated with the EBFS and BUFS/TFS have been confirmed or strengthened to withstand appropriate levels of hazard, namely  $10^{-3}$  and  $10^{-4}$  pa return frequency events, respectively.

The formal assessments assume little permeability through the building envelope. Hence 'dominant' openings which form due to the loss of cladding theoretically could lead to significant challenges to the buildings structures and internal masonry walls. However, there are already large openings in the envelope formed by ventilation louvres and apertures where the boiler steam and feed pipes pass through the

envelope. It is therefore judged that there are considerable margins inherent in the current buildings relative to the loadings from the events considered.

There are no challenges to the cooling of the PDSCs from wind loading because the air inlet louvres are so large and the flow path is insensitive to large fractions of blockage.

In the case of the BUFS and TFS pump houses, there could be potential vulnerability to winds beyond the  $10^{-4}$  pa events against which they have been justified. However, the cladding on the buildings is lightweight, which reduces the likelihood of any damage to the plant housed and the buildings are of totally different designs and hence loss of BUFS and TFS simultaneously is judged very unlikely.

There is a further potential weakness due to wind that is already identified in current procedures, namely the ingress of seaweed to the main cooling water system. This could not compromise either EBFS or BUFS/TFS. The potential for the ingress of seaweed is a recognised feature of the Site and methods for clearing the blockage have been employed on a number of occasions in the past.

All of the above challenges can be forecast and appropriate measures taken to make the buildings and plant as well prepared as is practicable.

#### ii) Low Temperatures

The identified potential effects of low temperatures are:

- freezing of seawater;
- freezing of feedwater stocks;
- waxing of fuel oil;
- embrittlement of steel structures, including cranes.

At the seawater temperatures experienced at Wylfa the bulk freezing of seawater is not considered credible and in particular, the intake is from below surface levels and therefore loss of cooling water flow is judged to be extremely unlikely. Moreover, seawater is not claimed as the UHS once the reactor is shutdown.

Feed water stocks for the EBFS are held warm in the RFT. Pipes from the RFT to the EBFP pass through the turbine house which is very warm when the reactors are operating at power and for a substantial period post trip. The RFT are backed up from the Townswater Tank. This is a very large volume and its outlet pipework is trace heated. Hence, should the EBFS be required, even in very low air temperature conditions and with a delay of several hours, it is judged that there is no potential for loss of feed due to freezing. Water for the BUFS and TFS is in the TFS tanks at ambient temperature. However, the large volume (1,400,000 litres) and the take off for the pumps being at the bottom of the tanks mean that there is minimal potential for these water stocks being frozen. In addition, external pipework between the tanks and the BUFS and TFS pump houses are trace heated (This trace heating may be lost if station electrical supplies are lost but the pipework should remain warm long enough to establish flow).

Excessively low temperatures for long periods could lead to waxing of fuel oil. The EBFS, BUFS and TFS all rely on diesel oil supplies. Trace heating is used to prevent waxing and hence filter blocking. Also, the fuel oil used has a Cold Filter Plugging

Point of -15°C, which is colder than temperatures experienced at Site and significantly colder than the lowest sea temperatures (+5°C) experienced and which prevent protracted periods of low temperatures in coastal areas.

There are no challenges to cooling of the PDSCs due to low (or in fact high) ambient temperatures.

iii) Snow

Snow can have a number of effects (setting aside the effects of low temperatures which may accompany it), namely

- impairment of operator movements around site;
- impairment of the effectiveness of drainage systems with the potential for localised flooding;
- loading on the flat roofs of buildings;
- ingress of snow to buildings through louvres so that internal plant is affected.

Of these effects, it is only the building loading issue that could have some impact on damage to EBFS, BUFS or TFS plant or on plant that could challenge radiological containment.

A  $10^{-4}$  pa return frequency snowfall vent was considered in the most recent PSR and no issues which could challenge reactor cooling plant were identified. Current operating procedures restrict use of the pile cap crane in the reactor building when snow could generate an additional load on the structure that supports both the roof and crane.

Although there are no on-site issues identified, if grid connection continued to be lost for a long period and eventually on-site water or oil stocks needed to be replenished, then local road conditions could impede deliveries. Severe snow and low temperatures are very uncommon on the island and therefore local authorities do not make arrangements to deal with the effects of extremely cold weather. In addition, replacement water may need to be shipped a considerable distance on mainland roads even before local conditions are encountered.

iv) Rain

The range of rain storms considered is described in Section 3.1.1.2.

In the unlikely event that the water removal systems were inadequate then 2 areas were identified as potentially vulnerable:

- Turbine hall basement;
- CW/SWC pumphouse.

In both cases only the EBFS could be affected, although this is highly unlikely because of the heights of the relevant pumps above the floor level. In either case there would not be any impact on the BUFS or TFS which is at or slightly above site ground level and the reactor pressure boundary would be totally unaffected.

The air intakes to the PDSCs would also not be vulnerable to flooding from precipitation because the lower edges of them are approximately 20cm above the general site ground level.

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

Consideration of measures, which could be envisaged to increase plant robustness against extreme weather conditions and would enhance plant safety.

Following the Fukushima event a series of workshops has been held to consider the robustness of the site (reactors and primary/secondary dry store cells) against internal and external hazards, and to look at the site's emergency preparedness arrangements. Some areas for consideration were identified and these are currently being assessed. Any enhancements relevant to this section are addressed within the areas for consideration discussed elsewhere in this document.

## 5 Loss of electrical power and loss of ultimate heat sink

### 5.1 Nuclear power reactors

For writing chapter 5, it is suggested that detailed systems information given in chapter 1.3 is used as reference and the emphasis is in consecutive measures that could be attempted to provide necessary power supply and decay heat removal from the reactor and from the spent fuel.

Chapter 5 should focus on prevention of severe damage of the reactor and of the spent fuel, including all last resort means and evaluation of time available to prevent severe damage in various circumstances. As opposite, the chapter 6 should focus on mitigation, i.e. the actions to be taken after severe reactor or spent fuel damage as needed to prevent large radioactive releases. Main focus in chapter 6 should thus be in protection of containment integrity.

#### 5.1.1 Loss of electrical power

##### 5.1.1.1 Loss of off-site power

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

A detailed description of the offsite and onsite electrical supplies systems at Wylfa is given in Sections 1.3.5 and 1.3.6.

In the event of loss of all offsite supplies the time for the automatic starting and synchronising of gas turbines, and the manual restoration of essential AC plant is less than 15 minutes. During this time post trip cooling is provided by DC plant supported by the battery backed Guaranteed Supplies system provided this equipment has not been affected by the hazard.

Station procedures exist for restoration of these supplies and returning essential plant to service. Operators are trained and are familiar with these procedures.

Once the gas turbine system has been established and essential plant switched back into service the battery systems and DC plant and batteries will be supported. Minimal operator intervention is required to support the system and provided that fuel supplies are available the system could support the stations electrical requirements indefinitely. If only on-site fuel supplies are available the mission time would still be in excess of 72 hours (see Section 1.3.5.3.3).

- 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.

Four of the gas turbines are in the same building with the fifth being located in a separate, but nearby building. The three gas turbine fuel oil tanks are common to all five gas turbines and are located close to the two gas turbine buildings.

Operation of the Essential Supplies system requires the availability of control supplies from both the 110V DC Switchgear Supplies System and the 110V DC Gas Turbine Switchgear Supplies system. Both of these

systems are segregated and separated to prevent a single fault making the total system unavailable.

Station Operating Instructions (SOIs) give guidance for the operator for the situation of extended periods of grid disconnection.

Additional fuel stocks for the gas turbines would be sourced on an urgent basis.

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

- 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 in operation.

The Electrical Overlay System is designed to provide a diverse electrical supply to two gas circulator AC pony motors (and their auxiliaries) on each reactor in the event of total loss of station AC supplies or more localised loss of electrical supplies due to, for example, fire damage. Details of the EOS are given in Section 1.3.5.4.

In the event of loss of incoming electrical supplies all three EOS diesel generators auto-start ready for manual synchronisation to the switchboards if required.

Station procedures exist for operation of this equipment. Operators are trained and are familiar with these procedures.

Additional fuel stocks for the EOS would be sourced on an urgent basis either from other on site supplies or from off site.

- 5.1.1.2.2 Battery capacity, duration and possibilities to recharge batteries.

Battery capacity is discussed in Section 1.3.6 and associated sub-sections.

There is no facility to recharge station safety related batteries from EOS supplies although the EOS system does have dedicated 440V, 110V and 50V batteries for operation and control of essential auxiliaries for the backed up AC pony motors.

#### 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

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

Battery capacity is discussed in Section 1.3.6 and associated sub-sections.

There are no installed facilities for recharging any safety related batteries in this situation.

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

There are no specific arrangements or procedures for the connection of temporary AC power sources.

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

Any connection of temporary AC power supplies would require specialist support and would take several days.

- 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 shut down and loss of normal reactor core cooling condition (e.g., start of water loss from the primary circuit).

Electrical power is not claimed for protection against design basis seismic, flooding or extreme weather faults.

Fault scenarios, claimed protection and timescales for implementation are discussed in Section 1.3.2.1.

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

Following the Fukushima event a series of workshops has been held to consider the robustness of the site (reactors and primary/secondary dry store cells) against internal and external hazards, and to look at the site's emergency preparedness arrangements. Some areas for consideration were identified and these are currently being assessed. The areas for consideration relevant to this section are given below or are included in Section 6.1.4 considerations:-

Consideration WYA 03: Consideration will be given to increasing the resilience of the on-site electrical system.
--

### **5.1.3 Loss of the ultimate heat sink**

- 5.1.3.1 Design provisions to prevent the loss of the primary ultimate heat sink

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

The primary UHS is not available for long term reactor cooling once the reactors have tripped.

- 5.1.3.2 Effects of loss of the primary ultimate heat sink

Loss of the primary ultimate heat sink (e.g., loss of access to cooling water from the river, lake or sea, or loss of the main cooling tower).

- 5.1.3.2.1 Availability of an alternate heat sink

EBFS. BUFS and TFS are available along with systems to discharge boiler steam to atmosphere in the form of the high pressure boiler safety relief valves and the tertiary feed vent valves.

Loss of that element of the alternate heat sink involving the EBFS can arise from a variety of challenges:

- (i) loss of electrical supplies to the EBFPs or failure of the pumps themselves (see Section 5.1.1 above);
- (ii) loss of the RFTs or Townswater Tank or depletion of their water stocks
- (iii) failure of pipework or valve closures between the RFTs and the EBFPs and between the EBFPs and the boilers. This item also includes non-closure of non-return valves in pipe branches such that flow can be diverted away from the boilers;
- (iv) blockage of boiler tubes;
- (v) failure of the boiler safety relief valves to open;
- (vi) failure of the boiler structures.

Taking each in turn, design provisions to avoid each of these failure modes are:

- (i) See Section 5.1.1.
- (ii) The RFTs comprise 4 tanks per reactor. There are sectionalising valves which enable each tank to be isolated from the others. The RFTs are seismically qualified against weak seismic events ( $10^{-2}$  pa return frequency) and not vulnerable to any building collapse challenges.
- (iii) The pipework is robust and flexible. There are diverse routes between the tanks and the pumps and the pumps and the reactors (Section 1.3.2.2). All valves can be operated manually so if closed they can be opened. Non-return valves in the feed system are tested periodically.
- (iv) All on-site water stocks used to feed the boilers is of very high purity to avoid any potential for corrosion or blockage of the boiler tubes. The stocks are stored in the RFTs, deaerators and TFS tanks.
- (v) Each of the 4 boiler sections has 7 safety relief valves which are designed to open when pressure within the boilers reaches the set pressure of the valves. In the extremely unlikely event that none of the valves opened then the tertiary feed vent valves could be opened to complete the alternate UHS. Heat removal from the reactors is most efficient with the boilers depressurised.
- (vi) The boilers are divided into 4 sections. They and their support structures are extremely robust and can withstand reactor temperatures in excess of 500°C. In addition, the boilers can withstand at least a  $10^{-4}$  pa return frequency seismic demand.

The effectiveness of the alternate UHS incorporating the BUFS and TFS could be lost through items (iv) and (vi) above. There are also analogous items to (i) and (ii) above for the BUFS and TFS in that they are both reliant on their dedicated diesel oil and water stocks. It is judged that there

is sufficient redundancy in the relief and vent valves that item (v) would not present a challenge.

The EOS (Section 1.3.2.4) would be available after a number of hazard events to support forced circulation of the reactor primary coolant. However, it is not formally qualified against hazards, particularly earthquakes, and therefore while it could be of value in transferring heat from the reactor cores to the boilers if it and all the systems it supports remained available, no formal claim will be placed on it in the context of this review.

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

The EBFS can be available immediately because its power supply is battery backed and the boiler safety relief valves will open without intervention. The batteries have a limited capacity (of order 30 minutes) but the system is designed to be supplied from the GT system. The BUFS can be commissioned within 1 hour or the TFS within 3 hours. The systems are designed to operate for 24 hours in total, the limitations being the water and fuel oil stocks. Operator actions required are simple and there is redundancy in the systems to aid avoidance of potential obstructions.

A capability exists to pipe water from the RFTs or the Townswater reservoir to the TFS tank and this would provide around 60 hours of boiler feed to both reactors (at  $8\text{gks}^{-1}$  per reactor). Also, as stated in Section 1.3.2.3, the fuel oil for the gas turbines could also be used for the BUFS and TFS diesel engines, providing an additional 6 months of running for both reactors (assuming that no gas turbines had run since the start of the event).

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

5.1.3.3.1 External actions foreseen to prevent fuel degradation.

To avoid fuel degradation, feed to boilers must be re-established and maintained in order that reactor heat can be transferred to the atmosphere via the boilers. Hence, alternative water stocks and a pumping facility are required (see proposals in Section 6.1.4 – Consideration WYA10). Because the boilers can be readily depressurised, the pumping system can be relatively low pressure. The possible alternatives are presented in Section 1.3.2.1. Forced circulation of the primary coolant is essential only if the reactor pressure circuit has experienced a significant breach. It is important with a reactor incorporating graphite to prevent the exothermic air-graphite oxidation reaction taking place because this could lead to a run-away transient that would be very difficult to control once initiated. At high temperatures the air-graphite reaction becomes uncontrollable if the supply of free oxygen is unlimited (i.e. the reactor pressure circuit is breached permanently). It is more effective to prevent air ingress rather than to re-establish forced circulation, which requires quite complex and extensive plant systems. Covers for the types of openings created during outages

exist on-site already, as does the facility for feeding CO<sub>2</sub> directly to the reactors from the CO<sub>2</sub> storage tanks, without using the vaporiser plant.

- 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 shut down to loss of normal reactor core cooling state (e.g., start of water loss from the primary circuit).

It has been shown that so long as the reactor primary pressure boundary remains essentially intact, then connecting the boilers to the atmosphere (i.e. establishing the alternate UHS) can be delayed for 24 hours. Similarly, if boiler feed was established relatively quickly after the initiating event, then a delay of order 24 hours could be accommodated at a later time before off-site alternatives need be implemented to maintain access to the alternate UHS.

- 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).

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

The primary UHS is not available for long term cooling once a reactor has tripped regardless of whether or not site electrical supplies are available. Water loss from the primary circuit is not an issue for gas cooled reactors. The equivalent is loss of the pressurised CO<sub>2</sub> primary coolant but total loss would lead to replacement of the primary coolant by air from the atmosphere and hence access to the alternate UHS would remain available. An uncontrolled air-graphite chemical reaction needs to be avoided by appropriate measures (see Section 5.1.3.3.1) to prevent a constantly replenished supply of air to the reactor core.

- 5.1.3.4.2 External actions foreseen to prevent fuel degradation.

The BUFS and TFS are totally independent of any off- or on-site power supplies but will require replenishment of their consumables (see Section 6.1.4 – Consideration WYA10). In addition, the REIC, which also has a dedicated diesel driven generator, could be utilised to provide indications of the state of the reactors under conditions of no available power supplies.

The principal action required is to secure a regular and frequent supply of good quality water for boiler feed until an on-site boiler re-circulation system can be re-established for the boiler feed water. In addition, a regular supply of diesel oil is required for the EBFS (for GTs), BUFS and TFS. The BUFS/TFS uses water at 8 kgs<sup>-1</sup> for each reactor. It is acknowledged that as time progresses the feed rate can be reduced. The EBFS can also use water at this low flow rate and be throttled to as low a flow rate as is required.

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

Following the Fukushima event a series of workshops has been held to consider the robustness of the site (reactors and primary/secondary dry store cells) against internal and external hazards, and to look at the site's emergency preparedness arrangements. Some areas for consideration were identified and these are currently being assessed. The areas for consideration relevant to this section are given below or are included in Section 6.1.4 considerations:-

Consideration WYA 02: Consideration will be given to increasing the resilience of the back-up feed systems and tertiary feed systems.

## **5.2 Spent fuel storage pools**

Where relevant, equivalent information is provided for the spent fuel storage pools as explained in chapter 5.1 for nuclear power reactors.

### **5.2.1 Loss of electrical power**

There are no irradiated fuel storage ponds at Wylfa. Irradiated fuel is stored in a CO<sub>2</sub> atmosphere in one of three Primary Dry Store Cells. These are discussed in detail in Sections 1.2 and 1.3.3. These PDSC are totally passive and do not require any electrical supplies to maintain the integrity of the fuel.

As stated in Section 1.2, Wylfa also has two Secondary Dry Store Cells but these are empty of all IFE and would be subject to a full safety case justification if it were intended to reuse either store in the future.

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

Not applicable. There are no electrical power requirements essential for storage of spent fuel at Wylfa.

### **5.2.3 Loss of the ultimate heat sink**

It has been assessed conservatively that newly discharged fuel in a dry store cell would take around 58 hours to reach fuel element clad melt temperature if the cooling air flow was 100% blocked. The cells are sealed and therefore there would be no immediate off-site release of radionuclides even if fuel damage occurred.

The cooling air flows to the cells through large underground reinforced concrete tunnels, driven by natural circulation promoted by decay heat in the spent fuel elements. It has been shown that a blockage of more than 99% of the cross-sectional area would be required to lead to fuel element damage temperatures being reached. It would be physically impossible to block a tunnel to that degree with any form of solid debris but flooding of the tunnels could achieve a complete blockage.

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

Following the Fukushima event a series of workshops has been held to consider the robustness of the site (reactors and primary/secondary dry store cells) against internal and external hazards, and to look at the site's emergency preparedness

arrangements. Some areas for consideration were identified and these are currently being assessed. The area for consideration relevant to this section is given below:-

Consideration WYA 12: Consideration will be given to enhancing the resilience of the primary dry store cells to severe events.
--

## **6 Severe accident management**

### **6.1 Organisation and arrangements of the licensee to manage accidents**

Chapter 6.1 should cover organization and management measures for all type of accidents, starting from design basis accidents where the plant can be brought to safe shut down without any significant nuclear fuel damage and up to severe accidents involving core meltdown or damage of the spent nuclear fuel in the storage pool.

#### **6.1.1 Organisation of the licensee to manage the accident**

##### **6.1.1.1 Staffing and shift management in normal operation**

The normal staffing of the Wylfa site is approximately 630 full time employees, supported by approximately 50 Agency Supplied Workers. In addition to this, contract partners support the operation of various aspects of the site, numbering approximately 150 people.

For those aspects of the site which operate on a 24/7 basis, a five shift cycle is used, with a complement of 30 people per shift (excluding Security). The minimum manning level for each shift is primarily determined by the number required to man the Emergency Scheme, which is currently 19 (excluding security).

Each of the shift teams are led by a Shift Charge Engineer, who reports to the Operations Manager. Each of the Shift Charge Engineers are appointed to act as initial Emergency Controllers, with the expectation that they will take control of any incident until the Duty Emergency Controller is able to attend site and establish a team to run the Event Management Centre.

##### **6.1.1.2 Plans for strengthening the site organisation for accident management**

Prior to the Fukushima event attention was focussed on two areas of improvement. As part of the ongoing programme of maintaining the numbers of people appointed to the Emergency Scheme, a conscious decision was made to increase the numbers of people appointed to each role within the Emergency Scheme. Each of these roles is filled by Suitably Qualified and Experienced Persons, who are on a Duty Emergency Scheme rota. In addition to reducing the imposition made to people on the Emergency Scheme rota, the appointment of additional people has the benefit of providing defence in depth for the emergency scheme. In the event of a protracted incident, a larger pool of people will be available to fulfil the identified roles.

Prior to 2011, the site had developed and operated a number of contingency plans for different types of events – Nuclear emergency, Security, Environmental event, Severe Weather, Flu Pandemic etc. Each of the various types of response plans was exercised in some capacity, with the Nuclear Emergency and Security responses being formally demonstrated to the appropriate Regulator on an annual basis. At the request of the Regulators, in 2011, the site was asked to develop arrangements for responding to a combined Nuclear Emergency and Security event. Work is progressing on this, with an intention to demonstrate the combined response to the Regulators in November 2011. In developing the combined response, a number of conflicts between the requirements for the two types of events have been revealed.

Developing arrangements to resolve these conflicts has led to a more responsive capability, which it is believed will be more effective in responding to events which are outside of the normal scope of incidents considered in the well established programme of Nuclear Emergency and Security exercise scenarios.

#### 6.1.1.3 Measures taken to enable optimum intervention by personnel

As described above, the development of arrangements for responding to a combined Nuclear Emergency and Security event should lead to an increased capability to respond to events of an unexpected nature.

Wylfa has an established programme of Command and Control training, provided by an external organisation with significant military experience. This programme is aimed at providing Emergency Scheme members with the knowledge, techniques and facilities to deploy effective Command and Control in non-routine situations. The techniques learned from the training are practised during a programme of training exercises, such that relevant people are familiar with this type of management, which is significantly different to that used in the day to day management of the Wylfa site. The site has also recognised the value in using such command and control techniques to manage significant abnormal occurrences during the day to day operation of the site, and hence uses the Event Management Centre and Emergency Scheme members to manage such situations e.g. abnormal weather, loss of towns water supply to the site. By using the available techniques at appropriate opportunities, the skills of the relevant people are developed to enable optimum intervention.

#### 6.1.1.4 Use of off-site technical support for accident management

In the event of a site incident or off-site nuclear emergency being declared the Central Emergency Support Centre (CESC) is set up in Gloucestershire.

This dedicated facility is manned by a Controller, a Health Physicist and a Technical Officer each with a support team on a one-hour call out rota.

The remit of the CESC is to:

- (i) 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.
- (ii) Take over for the affected site at an early stage the task of directing the off-site monitoring teams and assessing their results.
- (i) Provide the requisite technical advice on off-site issues to all stakeholders in the Strategy Coordination Centre and those agencies represented in the CESC.
- (iv) Provide regular authoritative company briefings for the media on all aspects of the emergency.
- (v) Co-ordinate advice and support from within the affected company and other parts of the nuclear industry to the affected station.

- (vi) Centrally manage the collation of all relevant information relating to the event (using appropriate means).

The CESC Controller has the full backing of the Company to take whatever steps are necessary, including using any resources required, to control the situation.

The Technical Support Team in the CESC has access to the Company Drawing Office so can obtain and print systems diagrams and a range of experts to help analyse the issues on-site and formulate recovery plans.

The CESC also has access to Procurement and the Supply Chain to obtain any goods or services required in the recovery.

The CESC manages the links to the local and national responding organisations.

The CESC takes over the management of the Off-site survey and the formulation of Company advice.

The CESC mobilises and coordinates the resources of the whole Company and cooperation from other nuclear companies.

#### 6.1.1.5 Procedures, training and exercises

##### Procedures

The plant is normally operated under the Station Operating Instructions (SOIs) and supporting lower tier documentation. These give advice on operations in design basis fault conditions, including responses to hazards. These include:

- Action following an abnormal event
- Action in the event of severe weather (flood, wind, extreme temperatures, etc)
- Action following loss of grid supplies
- Action following a possible seismic disturbance
- Operation of boron dust injection equipment
- Operation of the remote emergency indication centre
- Remote trip and control of reactor cooling

Plant item operating instructions are provided for the deployment of all significant items of emergency equipment.

If an event is not adequately controlled through use of SOIs, further guidance to the operator is provided in the Symptom Based Emergency Response Guidelines (SBERGs). Whilst the use of the guidelines in given situations is mandatory, the application of any particular item of advice is at the discretion of the operating team at the time of an incident; in this way, prevailing circumstances and operating constraints can be taken into account. The advice to the operator takes account of potential conflicts in requirements and gives guidance on how to achieve the best effect with minimum risk.

The SBERGs consist of: -

- a combined flowchart and entry checklist

- four individual SBERGs covering the four critical safety functions:
  - control of reactivity
  - maintenance of pressure circuit integrity
  - control of reactor heat removal
  - control of radiological release.
- a table summarising the limiting plant constraints for key reactor structures.

The detailed advice within each SBERG includes the following:

- a check on the state of relevant critical parameters
- recommended actions
- caution boxes highlighting the possibility of potentially disastrous plant states
- comments on reasons for the advice and further background information.

If application of the SOIs and SBERGs fails to prevent the onset of core degradation, or if a degraded core appears possible, then further management of the accident would be based on advice given in the Severe Accident Guidelines (SAGs). These provide advice to on-site and off-site technical support, to limit the escape of fission products to the environment in the event of an accident which is outside the design basis. The advice is broadly based since it is not possible to anticipate the detailed plant conditions which would exist in such low-frequency accidents.

The advice in the SAGs is based around the same four critical safety functions described above. The process comprises:

- a list of long lead time items that should be considered
- identification of the critical safety functions that are threatened
- identification and implementation of actions (via tabular advice statements)
- detailed supporting information on the above.

### Training

Emergency scheme training is set and controlled in the same manner as regular training. Predefined training is identified in emergency scheme training modules and includes familiarity of emergency equipment and associated operating procedures.

### Exercises

Emergency arrangements are routinely practised including a yearly demonstration exercise to the satisfaction of ONR. These exercises have included out of hours call in, and control of the event from both the onsite and the alternative off site ECC.

## **6.1.2 Possibility to use existing equipment**

6.1.2.1 Provisions to use mobile devices (availability of such devices, time to bring them on site and put them in operation)

The Company has joined with other Nuclear Site operators in establishing a number of Beyond Design Basis Accident Containers. Owing to its relatively remote location, a set of these containers are located near the Wylfa site. These containers are equipped with a range of equipment and materials which are intended to be utilised should a beyond design basis accident occur. The containers are located conveniently and could be deployed in a short period of time. The equipment stored in the containers is inspected and maintained on a routine basis.

Should it be necessary to bring other devices and equipment onto the site, there are two operational Helipads. Furthermore there is a military airfield located approximately 12 miles from the site. The site is also located a few miles from port of Holyhead.

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

Contracts are in place for the provision of supplies either through a Magnox Ltd Framework contract or directly from Wylfa. Where relevant, these contracts include provision for out of hours or urgent requirements. As part of the Wylfa Flu Pandemic preparations, the contingency arrangements for key suppliers were examined and found to be satisfactory. Out of hours contact details for urgent request for key suppliers are maintained in the Event Management Centre and the Wylfa Commercial Team will be available to support the Event Management Centre with any urgent requirements. The supply of towns water to the site is an exception to the contract arrangements, in that there is no specific contract for guarantee of supplies from Dwr Cymru (the local water utility). At the time of the pandemic preparations, availability of towns water was excluded from consideration, on the advice from the Department for Energy and Climate Change that these supplies should be taken as guaranteed. However, the site has recently (December 2010) had experience of managing a response to a significant interruption of townswater supplies. The event was successfully managed, with water supplies being imported by road tanker for a period of 3 – 4 days.

In addition to the arrangements described above, it should be recognised that the CESC is also available to assist the site in obtaining essential supplies.

6.1.2.3 Management of radioactive releases, provisions to limit them

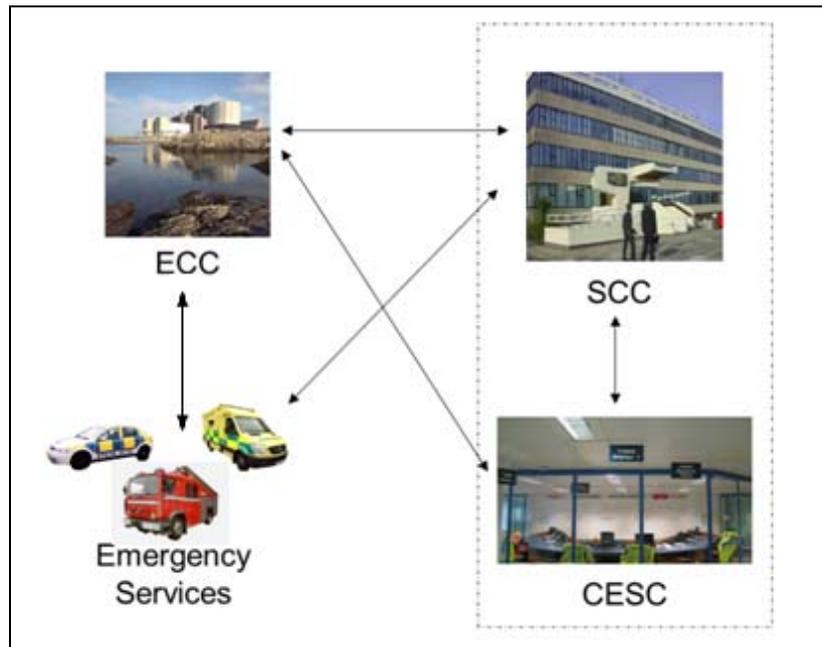
Robust arrangements are in place on the site for managing the radioactive discharges from the site during routine operations, in accordance with conditions attached to the various permits granted to the site by the Environment Agency. The conditions attached to the permits are still applicable during an abnormal situation. In terms of installed equipment to help mitigate a release during an event, the only significant item is the Iodine Absorption Plant which is fitted into the blowdown route. This can be used to remove radioactive iodine, provided that the gas is within certain temperature limits, and hence if it is possible to route any gaseous releases through this system, some form of mitigation is possible.

Depending on the location and nature of the radioactive release, it may also be possible to manoeuvre the plant, such that the particular item of plant is isolated, or the release is routed towards a discharge route which has some form of filtration installed, for use during routine operations.

As part of the emergency response arrangements, the site has a damage repair team on a standby rota. This team have a range of tools and equipment available to them, which can be used to temporarily seal a range of breaches, or reduce the magnitude of a release until a more permanent repair can be carried out.

#### 6.1.2.4 Communication and information systems (internal and external).

In the event of an accident or natural disaster at a power station there is a need to be able to promulgate an alert and then to pass information into and out of the site. Particularly important communications paths are those between the site, the Strategic Coordinating Centre (SCC), the Central Emergency Support Centre (CESC) and the responding emergency services (see diagram).



There are numerous communication systems available to perform these tasks and although none are formally qualified for seismic (or other) events it is envisaged that sufficient would survive to allow this off-site communication.

#### Magnox Communications Systems

The Magnox telephone system for operating sites is designed to be resilient and function through any single point failure. Wylfa has three telephone exchanges physically separated and connected to the Public Switched Telephone network (PSTN) via diverse routes. Phones in the key response centres are divided between two exchanges so that failure of an exchange will not leave the room without at least some working phones. The telephone

exchanges are connected to robust electrical supplies and have battery backup with a design period of not less than 12 hours, although these are not qualified seismically.

In addition Wylfa has a number of telephones connected directly to the public system without passing through the Company exchanges.

The Magnox Wide Area Network (WAN) (see diagram below) provides data and voice links between the sites and is designed with a degree of resilience.

Wylfa has physically diverse routes into the MPLS (Multiprotocol Label Switching) network. Both main WAN connections are routed to different BT Exchanges on the mainland.

#### Communications in a Crisis: Declaration and Promulgation

Wylfa would declare a Site Incident or Off-site Nuclear Emergency and promulgates the alert using the Site Event Reporting System (SERS). SERS is a resilient system based on two servers at two different locations within Magnox, giving a replicated service with no single point of failure.

SERS alerts a number of internal personnel and external personnel using telephones on Dial and Deliver, voice mail systems and pagers. Backup systems exist in the event of the failure of any component of the system.

The minimum infrastructure required to alert company responders is a single working phone on site.

Alerting of other organisations requires a functioning phone system at both ends.

Receiving the alert, which contains minimal information, is sufficient to trigger a multi-agency response to an Off-site Nuclear Emergency.

#### Communications in a Crisis: Site Communications with Emergency Services

The sites need to communicate with the emergency services to:

- Promulgate the alert
- Explain the severity and urgency of the situation
- To define the resources needed

There are a number of ways in which the site can communicate with the police and other emergency services:

- Emergency Services are alerted and informed using the 999 system using the Magnox telephone system and the PSTN.
- Direct line to Police Station/Headquarters at St. Asaph.
- Further information is provided by FAX.
- The Emergency Services each send an Officer to the affected site's ECC. These officers will be able to communicate with their Headquarters by:
  - Telephone
  - Fax
  - Service mobile phone

- Service Airwave radio
- There are many mobile phones on each Magnox site which provide another line of communications should it be needed.

Once the Emergency Services are deployed they can use their own communications infrastructure to communicate with their co-ordination functions and across the responding forces.

Key mobile phones used within Magnox are registered on the Mobile Telephone Privileged Access System (MTPAS).

#### Communications in a Crisis: CESC to/from Site

The CESC and site need to be able to communicate to:

- Raise the alarm.
- Discuss the situation.
- Discuss the recovery plans and equipment/supplies needs.
- Report progress and issues when recovery plans are implemented.

The CESC voice services consist of the following infrastructure and features:

The CESC provides telephones for each agreed CESC staff member. 50% of the telephones will be served from each of two PABXs. The two PABXs are located in separate buildings, with separate batteries and power supplies. At least one of the PABXs is generator backed as well as the batteries. Batteries will provide at least 12hr backup.

Cabling between the PABXs and the CESC telephones follow separate routes as far as practicable. Separate routes are provided through the EDF Energy network between the EDF-Magnox Ltd gateways and the PBXs serving the CESC, such that any single fault will not affect more than 50% of the connections.

Each CESC PABX has the Direct Dial Identifier (DDI) service arranged such that if one PABX is faulty, service will continue via the other PABX.

CESC telephones will have outgoing PSTN access to at least two Public Telecommunications Operators (PTOs).

In extremis the Airwave system NIAS (Nuclear Industry Airwave Service) can be used to communicate between the sites and the CESC. This is a national resilient system. In this system the voice capability is resilient against failures in the Company network although such failures can defeat the data pathways.

#### Communications with off-site survey vehicles

The Airwave system (NIAS) provides the means for communication with the mobile survey vehicles deployed in an emergency situation. Failure of the WAN would not affect voice communication between survey vehicles, the CESC and the affected site. Data communication would however be lost and it

would be necessary to relay results back by voice. This would result in some inconvenience in plotting the survey data but would not present a significant nuclear safety-related issue.

#### Communications: CESC to/from SCC

The CESC needs to be able to communicate with the SCC to:

- To communicate and discuss the situation
- To communicate the Company's view of off-site countermeasures required.

Key links are telephone (Voice and FAX)

Voice services to Strategic Coordinating Centres (SCCs) are provided under contract. They comprise:

- The means to enable six simultaneous voice or FAX telephone calls to be established to or from the contractor's telephone network without using the PSTN, consisting of two routes, each capable of three simultaneous calls.
- At the contractor's end of each route, the two routes terminate at separate private network nodes.
- Each of the private terminating network nodes is not to be on a site where the equipment, connectivity or access can be affected by a nuclear incident.
- At the SCC end of each route, the two routes are terminated on separate (Multiplexor) equipment. The equipment is located in separate rooms if possible. The equipment has separate power supplies as far as is practicable. The power supplies are taken from maintained (no break) supplies where locally available.
- If two SCC PABXs are available, one route is connected to each, approx. 50% of the telephones to each.
- Two routes are provided through the contractor's network between the contractor's end of each SCC route and the PBXs serving the CESC, such that any single fault on the contractor's network will not affect more than 3 voice channels between the CESC and any SCC.

In addition the PSTN can be used if available.

In addition mobile phones can be used if available.

In addition the SCCs are built in Police facilities and can benefit from the Police Service's communications systems.

#### Company communications with other organisations

The SCC and CESC are both communications hubs in which information is shared between the Company and external organisations.

In addition the Company operates the TiiMS (The Incident Information Management System) system which is available to key external agencies.

TiiMS is a Lotus Notes based information system, supporting data entry, validation and action tracking. The system may be used remotely between the CESC, SCC's, HPA (Health Protection Agency), FSA (Food Standards Agency), DfT (Department for Transport ) and the DECC (Department of

Energy and Climate Change) to display key information relating to a nuclear emergency.

The TiiMS service is provided on workstations located at the CESC, SCCs and various remote locations e.g. DECC, HPA DfT, FSA.

Tiims runs on a dedicated server with a backup available.

The following is provided at each SCC, to support delivery of the TiiMS service:

- A basic rate Integrated Services Digital Network (ISDN) line.
- A router.
- A local area network
- Two workstations
- Provision on the LAN for a further two workstations at the shared SCCs
- Provision on the LAN for four workstations at the Magnox Ltd SCCs.
- A fall back communications channel if the ISDN is unavailable.
- UPS.

Two mobile SCC workstations are provided as central equipment, which will be taken to SCCs as required.

ISDN connectivity is provided at the CESC, to support delivery of the TiiMS service to any one of the SCCs, along with a fallback communications channel if the ISDN is unavailable.

ONR, DECC, HPA, DfT, FSA have workstations which connect via ISDN.

#### Communications between the off-site responders

The Government has established a policy of improving the resilience of the Critical National Infrastructure (CNI) to disruption. Details are summarised below:-

#### Critical National Infrastructure.

The Government defines CNI as: “Those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life”. Communications is one of nine sectors considered. Within the communications sector are four strands:

Strand 1. Working with providers and responders to enhance the resilience of everyday commercially available telecommunications.

Strand 2. Improving the management, take-up and resilience of privileged telecommunications schemes that are only accessible to emergency responders.

Strand 3. Delivering a High Integrity Telecommunications System (HITS) providing connectivity and services between key responder sites at the national, regional and local level.

Strand 4. Delivering a means for securely sharing information between all local regional and national responders both in preparing for and in response to an emergency (National Resilience Extranet).

### **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.**

Wylfa currently has a single approach road, with a single gatehouse entrance to the site, and hence this is a potential vulnerability. In the vicinity of the gatehouse, there are two additional routes onto the site, intended for use by emergency vehicles, in the event that the gatehouse route is not usable. In the event that none of these are usable, equipment is available on site which could be used to cut through the perimeter fences. Whilst there is a single access road, there are a number of other potential routes to the site boundary fence, utilising farm tracks, or across farmland. In addition, the site has two registered helipads, one on site and the other off-site, adjacent to the site boundary.

In terms of access to the locality of the site, crossing the Menai Straits from the mainland to the Isle of Anglesey is a potential vulnerability. There are two bridges crossing the Straits, located a few hundred metres apart. Should these bridges not be available, there is no other means of road access to the locality.

The site is located close to the commercial port of Holyhead<sup>5</sup>, which has extensive facilities for loading and unloading of equipment and roll-on roll-off ferry facilities, which could potentially be utilised should the roads to the mainland not be available.

The potential vulnerabilities with road access would affect the ability of responding staff, Emergency Services and essential supplies and equipment to reach the site in a timely manner. In the short term, the site has sufficient people on site on a 24/7 basis to initiate a response to an emergency. The site is however reliant on support from personnel off-site at the time of an incident and Emergency Services for medical support, casualty rescue and fire fighting in order to respond to an event of significant magnitude.

#### **6.1.3.2 Loss of communication facilities / systems**

The Company has robust communications systems featuring diversity and redundancy, particularly at operating sites. These include:

- A resilient Company Wide Area Network
- For operating sites – diverse routes to the outside world communications cloud.
- Telephones that are independent of the Company exchanges with direct (copper) links to the PSTN.

---

<sup>5</sup> Holyhead is located on a separate island to Anglesey but is connected by three road causeways and a railway embankment. One of these causeways is of modern construction and it is considered unlikely that a seismic or flooding event would make all of these routes unavailable.

- The Nuclear Industry Airwave Service, designed to allow communication with off-site survey vehicles, can be used to make phone calls independent of the local PSTN.

A total failure is highly unlikely.

Potential Impact of widespread disruption:

- Loss of mains electricity for prolonged period

Should be able to promulgate alert before the battery backup fails.

Should have several hours of battery time to communicate initial information and to engineer communications routes.

- Loss of masts for mobile phones and Airwave

Can use voice function within airwave if sufficient infrastructure exists. Have mobile phones on different services (accidental rather than by design at the moment), can record readings and report back using land-land phones or by returning to site.

- Loss of telephone exchanges (Direct loss or loss of power)

Use of mobile phones (on MTPAS), NIAS radio, direct line or runners.

- Cabling damage

Real efforts have been made to avoid common mode failure with regard to cable routes for WAN and phone calls.

- Damage to PABXs

There are three of these at Wylfa with the design intent that it is unlikely that they would all be damaged in any reasonably foreseeable event.

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

In all exposure conditions including accident response, doses to personnel should be below dose limits (normally 20 mSv whole body dose) and must be As Low as Reasonably Practicable (ALARP). In the event of a major accident at a nuclear site the higher REPPiR Emergency Exposures can be applied to informed volunteers. The role of the Health Physicist in the Emergency Control Centre (ECC) is to ensure the safety of all people on site.

Staff that are not responding to an accident will be subject to controls based on dose rate, airborne contamination levels and other hazards, and may be evacuated from the site.

The ECC is positioned to minimise the likelihood that it would be damaged in an accident or affected by radiation. It would be subject to tenability checks,

the Initial Control Dose limit being 10 mSv over the first 10 hours. After this period the situation would be reassessed in the light of the radiological conditions, availability of replacement staff, etc. Arrangements are in place to transfer the functions of the ECC to the off-site alternative ECC should the primary facility be declared untenable, including destruction and blocked access.

On-site survey and emergency team staff controlled from the Access Control Point (ACP) are subject to the normal dose limits but in the event of a major accident the higher REPPiR Emergency Exposures (whole body doses of 100 mSv for operations and 500 mSv for life saving) can be applied to informed volunteers. Health Physics monitoring provides information on the local dose rates allowing response teams to ensure their doses are minimised and Electronic Personal Dosimeters are used to monitor doses and enforce dose limits. If necessary, the on-site Alternative ACP, or other suitable facility, would be used.

Training is given on the use of appropriate Personal Protective Equipment, including breathing apparatus, and undressing/decontamination processes, and use of these would not prevent appropriate remedial work being undertaken.

In some extreme instances high radiation levels could make access to the damage scene unachievable. If this were the case then remote access or the installation of the appropriate level of shielding would be required. If radiation levels remain high then working time would be limited, which could impair the recovery operation particularly if the operations required are time consuming. Under conditions of high local dose rates, contamination and destruction of some facilities the Company would be relying on the site Command and Control structures to manage the event making an accurate assessment of the situation and best use of available resource.

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 this situation

The Central Control Room at Wylfa is located in the heart of the Reactor Equipment Building, which is of robust design and construction, reflecting the nature of the nuclear safety related equipment located in this building. Breathing Apparatus is available to the staff who operate in the control room, such that the main control room is intended to be habitable at all times. In the unlikely event that the main control room is not tenable, there is no full-scope secondary control room. There is however a facility located outside the Reactor Equipment Building – the Remote Emergency Indication Centre – which was installed following the Long Term Safety Review to enable essential plant to be monitored on a shutdown reactor. It should be noted that the purpose of the facility is to monitor systems which are essential to maintain shutdown and post trip cooling, following the shutdown of the reactors from the Central Control Room. Local control of the plant would be carried out, based on the information from the REIC.

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.

Key emergency response centres on site are the Emergency Control Centre (ECC) and Access Control Point (ACP). Wylfa has fully functional alternative facilities should the primary facility be unavailable.

The REIC also provides a limited subset of essential indications should the Central Control Room become untenable.

For decontamination of returning teams there are a number of options including other shower facilities on site or, in the longer term, use of the emergency services mobile facilities.

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

The accident management measures provided at Magnox sites are intended to be flexible. Identified personnel have high levels of authority to utilise any resources available and technical advice is available from off-site facilities.

6.1.3.7 Unavailability of power supply

Wylfa is provided with diverse and redundant systems to ensure that essential electrical supplies are maintained for the site. In the event that the site is disconnected from the National Grid, the site is capable of maintaining electrical supplies to essential equipment for a significant period of time. This is achieved primarily by five gas turbines on the essential supplies system and in the event that these are also unavailable three diesel generators on the Electrical Overlay System, which can be used to supply the gas circulators in order to maintain circulation of the reactor coolant gas. The availability of fuel oil for the gas turbines and diesel generators is the limiting factor in maintaining electrical supplies.

6.1.3.8 Potential failure of instrumentation

Noting that the plant was constructed in the 1960s, Wylfa has a computerised data processing system, which has been upgraded on a number of occasions. In the event of failure of this system, battery backed instrumentation, which provides information essential to the monitoring of the state of the plant, is hard-wired to the Central Control Room. A totally diverse subset of essential indications is also available in the REIC.

6.1.3.9 Potential effects from the other neighbouring installations at site.

There are no other significant industrial premises in the vicinity of the Wylfa site and hence little likelihood of an impact from neighbouring facilities. The port of Holyhead is located approximately 9 miles from the site and it is possible that hazardous materials pass through the port. Ships passing by the Wylfa site may also potentially be carrying materials which could be hazardous to the operation of the site.

The RAF Valley military base is located approximately 12 miles from the site, which may also present a potential hazard to the site. The safety case for routine operation considers these potential hazards and concludes that the risk

posed is very low. There are no specific mitigation measures against aircraft crash but the measures described in Section 6 (in general) would be taken.

#### **6.1.4 Measures which can be envisaged to enhance accident management capabilities**

Following the Fukushima event a series of workshops has been held to consider the robustness of the site (reactors and primary/secondary dry store cells) against internal and external hazards, and to look at the site's emergency preparedness arrangements. Some areas for consideration were identified and these are currently being assessed. The areas for consideration relevant to this section are given below:-

Consideration WYA 05: Consideration will be given to enhancing the resilience of plant monitoring systems.

Consideration WYA 06: Consideration will be given to enhancing the availability of beyond design basis equipment.

Consideration WYA 07: Consideration will be given to providing further equipment to facilitate operator access around the site.

Consideration WYA 08: Consideration will be given to reinforcing the training for staff who may be required to respond to extreme events.

Consideration WYA 09: Consideration will be given to enhancing on site arrangements for command, control and communications.

Consideration WYA 10: Consideration will be given to providing additional stocks of consumables for plant and personnel.

Consideration WYA 11: Consideration will be given to updating and enhancing severe accident management guidance.

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

### **6.2.1 Elimination of fuel damage / meltdown in high pressure**

#### **6.2.1.1 Design provisions**

The Magnox reactor design has a very low power density, such that significant fuel damage or meltdown is very unlikely. Individual channel damage / melt was experienced at Magnox designs in other countries, but the Wylfa design and operating conditions are more tolerant to faults. Potential causes of channel melt include:

- channel blockage / channel flow bypass – potential threats have, where possible, been designed out; graphite core damage / debris is a credible cause, for which fuel failure protection systems are provided

- reactor faults – due to the Magnox design there is a wide spread of fuel channel powers; reactor protection is designed to protect the highest power channels such that a more severe fault than a design basis fault would only threaten a small proportion of channels.

#### 6.2.1.2 Operational provisions

Advice on preventing fuel damage and meltdown is given in the Station Operating Instructions (SOIs), Symptom Based Emergency Response Guidelines (SBERGs) and the Severe Accident Guidelines (SAGs) (Refer to Section 6.1.1.5). The advice primarily includes means of maintaining pressure circuit integrity, provision of boiler feed and reactor gas circulation, but also includes non design basis measures.

### 6.2.2 Management of hydrogen risks inside the containment

#### 6.2.2.1 Design provisions, including consideration of adequacy in view of hydrogen production rate and amount

There is no separate secondary containment.

The SAGs discuss the risk of hydrogen generation in water ingress or very high temperature faults in the reactor and highlights the risk of the hydrogen burning or explosion if it is released from the reactor into the reactor building. This in a non-pressure retaining structure, which protects auxiliary plant from the environment, and it is unlikely that hydrogen would build up within the building.

#### 6.2.2.2 Operational provisions

The SAGs provide advice on reducing water ingress and very high temperatures, which will reduce the rate of hydrogen generation.

### 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

There is no separate secondary containment.

The pressure circuit has safety relief valves which are adequate to vent steam and/or gas to atmosphere via particulate filters.

The reactor building is in a non-pressure retaining structure, which protects auxiliary plant from the environment. It could not over-pressurise as it is designed to relieve pressure in the event of a hot gas or steam release from the reactor.

#### 6.2.3.2 Operational and organisational provisions

If the pressure circuit was over-pressurising, the operator would either prevent further pressurisation, by altering feed flows for example, or would blow down some of the reactor gas, via the iodine filters if there was any failed fuel in the core. Advice on preventing reactor over-pressurisation is given in SOIs, SBERGs and SAGs.

#### **6.2.4 Prevention of re-criticality**

##### **6.2.4.1 Design provisions**

Section 1.3.1 describes the design means of reactivity control. It includes the potential to prevent re-criticality via core cooling, a feature of a graphite moderated reactor.

##### **6.2.4.2 Operational provisions**

The SAGs provide advice on mitigation in the event of failure of normal means of criticality control, which includes measures to ensure control rod insertion, core cooling and the injection of gaseous or powder absorber.

#### **6.2.5 Prevention of base-mat melt through**

##### **6.2.5.1 Potential design arrangements for retention of the corium in the pressure vessel**

The reactor core is contained within a massive, reinforced concrete pressure vessel on concrete foundation on the underlying rock. The inside of the pressure vessel is spherical whilst the outside is substantially cylindrical in shape with a minimum concrete thickness of 3.35m. The inside of the vessel is lined with a mild steel liner (to act as the pressure boundary) with insulation on the gas side. The liner and concrete is cooled by water from the Pressure Vessel Cooling Water (PVCW) system. There are penetrations through the top, sides and bottom of the vessel for access to the fuel, water and steam pipes, gas circulators and other ancillary gas and instrumentation connections. There are two penetrations through the base, at the centre and slightly offset from the centre. These penetrations lead to a tunnel containing reactor gas pipework. This tunnel is surrounded by thick concrete founded directly onto bedrock.

The design of the pressure vessel assists in the prevention of molten fuel reaching the environment. Any corium escaping from the bottom of the pressure vessel would be retained within the heavily shielded structure.

##### **6.2.5.2 Potential arrangements to cool the corium inside the containment after reactor pressure vessel rupture**

This is not applicable to Wylfa as there is no containment area outside of the concrete pressure vessel.

##### **6.2.5.3 Cliff edge effects related to time delay between reactor shut down and core meltdown**

Following a reactor shutdown it is necessary to provide post-trip cooling of the reactor core, using the plant described in Section 1.3.2. However, due to the low power density of the Magnox core and its large mass (and hence thermal inertia), best estimate analyses for a pressurised reactor indicate that there is up to 24 hours before any form of cooling (water feed to the boilers or gas circulation) is necessary. This analysis is based on a peak fuel channel, such that the number of fuel failures would initially be expected to increase only slowly thereafter. Implementing boiler feed would terminate the transient. Forced circulation at 24 hours would distribute heat more evenly in the massive core, giving a very extended period before feed was required.

The period available for initiation of core cooling is shorter for a depressurising reactor.

#### **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

This is not applicable to Wylfa as there is no containment area outside of the concrete pressure vessel.

##### 6.2.6.2 Operational provisions

This is not applicable to Wylfa as there is no containment area outside of the concrete pressure vessel.

#### **6.2.7 Measuring and control instrumentation needed for protecting containment integrity**

This is not applicable to Wylfa as there is no containment area outside of the concrete pressure vessel.

#### **6.2.8 Measures which can be envisaged to enhance capability to maintain containment integrity after occurrence of severe fuel damage**

This is not applicable to Wylfa as there is no containment area outside of the concrete pressure vessel.

### **6.3 Accident management measures to restrict the radioactive releases**

#### **6.3.1 Radioactive releases after loss of containment integrity**

##### 6.3.1.1 Design provisions

The plant is designed to provide defence in depth against the release of fission products or other radioactive material. In support of this a number of redundant and diverse systems are installed. In the unlikely event of a breach of the barriers preventing fission product release, the plant is fitted with an Iodine Absorption plant. If the location of the fission product release and the integrity of the primary circuit are such that it is possible to blowdown the reactor through the Iodine Adsorption plant, then this may be used to remove radioactive iodine from the discharge.

#### 6.3.1.2 Operational provisions

For normal operations, the reactors and associated plant are operated within a 'safety envelope' which ensures that the plant remains within any relevant safety limits. In order to ensure that the plant remains within the 'safety envelope' the Nuclear Site Licence requires arrangements to be made in a number of areas. The site has a well established management system to ensure compliance with the Site Licence, which includes: Operating Rules, Operating instructions, Maintenance Schedule, maintenance instructions etc.

In the event that deviations from normal operating parameters occur, the site has well established arrangements for responding to this. The overriding principle is that of conservative decision making. For deviations from normal operation that can be anticipated, operating instructions are in place to define the expected response. For unexpected deviations, the accepted practice would be to stabilise the situation and then use a defined Operational Decision Making process to arrive at a solution to the problem. The relatively benign nature of the Wylfa reactors enables this approach to be used.

In the unlikely event that the reactors suffer significant damage, leading to a significant radioactive release, again the site has SAGs and SBERGs, which provide advice on actions that can be taken to mitigate the release. In such circumstances, the site would deploy its emergency scheme arrangements to ensure effective control of the situation.

### 6.3.2 Accident management after uncovering of the top of fuel in the fuel pool

#### 6.3.2.1 Hydrogen management

Not applicable at Wylfa. As discussed in Section 1.3.3.1 there are no irradiated fuel storage ponds at Wylfa. Irradiated fuel is stored in a CO<sub>2</sub> atmosphere in one of three Primary Dry Store Cells.

#### 6.3.2.2 Providing adequate shielding against radiation

Not applicable at Wylfa – see 6.2.2.1 above.

#### 6.3.2.3 Restricting releases after severe damage of spent fuel in the fuel storage pools

Not applicable at Wylfa – see 6.2.2.1 above.

#### 6.3.2.4 Instrumentation needed to monitor the spent fuel state and to manage the accident

Not applicable at Wylfa – see 6.2.2.1 above.

#### 6.3.2.5 Availability and habitability of the control room

Not applicable at Wylfa – see 6.2.2.1 above.

**6.3.3 Measures which can be envisaged to enhance capability to restrict radioactive releases**

Nothing has been identified that is reasonably practicable.

## 7 Glossary

AC	Alternating Current
ACP	Access Control Point
AETP	Active Effluent Treatment Plant
ALARP	As Low as Reasonably Practicable
BCD	Burst Can (Fuel Element) Detection System
BUFS	Back-up Feed System
C & I	Control and Instrumentation
CESC	Central Emergency Support Centre
CNI	Critical National Infrastructure
CW	Circulating Water
DBE	Design Basis Earthquake
DBF	Design Basis Flood
DC	Direct Current
DDI	Direct Dial Identifier
DECC	Department of Energy and Climate Change
DfT	Department for Transport
DPS	Data Processing System
EBFP	Emergency Boiler Feed Pump
ECC	Emergency Control Centre
EDF	EDF Energy
EOS	Electrical Overlay System
FSA	Food Standards Agency
GC	Gas Circulator
GIMA	General Instrumentation Motor Alternator
GSRV	Gas Safety Relief Valve
GT	Gas Turbine
HPA	Health Protection Agency
IFE	Irradiated Fuel Element
ILW	Intermediate Level Waste
ISDN	Integrated Services Digital Network
LLW	Low Level Waste
MBFP	Main Boiler Feed Pump
MCP	Management Control Procedure
MPLS	Multiprotocol Label Switching
MTPAS	Mobile Telephone Privileged Access System
NIAS	Nuclear Industry Airwave Service
OD	Ordnance Datum (Mean Sea Level in Newlyn in Cornwall UK 1915 - 1921)

ONR	Office for Nuclear Regulation
pa	Per annum
PABX	Private Automated Branch Exchange
PAX	Private Automated Exchange
PDSC	Primary Dry Store Cell
PSA	Probabilistic Safety Analysis
PSR	Periodic Safety Review
PSTN	Public Switched Telephone Network
PTO	Public Telecommunications Operator
PVCW	Pressure Vessel Cooling Water
REIC	Remote Emergency Indication Centre
REPPiR	Radiation (Emergency Preparedness and Public Information) Regulations
RFT	Reserve Feedwater Tank
SAGs	Severe Accident Guidelines
SBERGs	Symptom Based Emergency Response Guidelines
SCC	Strategic Coordinating Centre
SDSC	Secondary Dry Store Cell
SERS	Site Event Reporting System
SOI	Station Operating Instruction
SQUG	Seismic Qualification Utility Group
SSC	Systems, Structures and Components
STS	Selective Tripping Scheme
SWC	Sea Water Cooling
TFS	Tertiary Feed System
TiiMS	The Incident Information Management System
UHS	Ultimate Heat Sink
WAN	Wide Area Network

**Table 1**

This is a consolidated list of the items to be considered arising from the Stress Test review.

<b>Reference</b>	<b>Section No.</b>	<b>Consideration</b>
WYA 01	2.2.4	Consideration will be given to enhancing the methods and equipment for primary pressure circuit sealing.
WYA 02	5.1.4	Consideration will be given to increasing the resilience of the back-up feed systems and tertiary feed systems.
WYA 03	5.1.2	Consideration will be given to increasing the resilience of the on-site electrical system.
WYA 04	2.2.4	Consideration will be given to providing a facility for the injection of nitrogen to support reactor hold-down.
WYA 05	6.1.4	Consideration will be given to enhancing the resilience of plant monitoring systems.
WYA 06	6.1.4	Consideration will be given to enhancing the availability of beyond design basis equipment.
WYA 07	6.1.4	Consideration will be given to providing further equipment to facilitate operator access around the site.
WYA 08	6.1.4	Consideration will be given to reinforcing the training for staff who may be required to respond to extreme events.
WYA 09	6.1.4	Consideration will be given to enhancing on site arrangements for command, control and communications.
WYA 10	5.1.2, 5.1.4, 6.1.4	Consideration will be given to providing additional stocks of consumables for plant and personnel.
WYA 11	6.1.4	Consideration will be given to updating and enhancing severe accident management guidance.
WYA 12	5.2.4	Consideration will be given to enhancing the resilience of the primary dry store cells to severe events.