Oldbury:
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 Oldbury 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

P J Sprague

P J Sprague, Site Director, Oldbury Power Station

Contents

0 Executive Summary

This report is the response from Oldbury power station to the ENSREG Stress Tests following the events at Fukushima, Japan in March 2011. Oldbury has two Magnox reactors (see next paragraph) that first went critical in 1967. Reactor 2 is now permanently shutdown and Reactor 1, which generates around 700 MW thermal, will be shutdown by the end of February 2012.

The Oldbury 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 Oldbury and light water reactor designs such as Fukushima are:

- fuel and clad will melt at lower temperatures;
- notwithstanding this, Magnox reactors 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 a water filled pond that is tolerant to very extended periods of loss of cooling.

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. The spent fuel storage pond is tolerant to very extended periods of loss of cooling.

The review against external hazards has confirmed that Oldbury is in an area of low seismic activity and, for off-site flooding, extreme tide and surge bounds tsunamis. With the possible exception of site flooding from tide and surge, it has been confirmed that the design basis hazard specifications remain appropriate and that the plant is qualified against them; the measures to enhance resilience described below take the potential off-site flood into account. 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 spent fuel storage pond.

1 General data about site/plant

1.1 Brief description of the site characteristics

- location (sea, river)[1]
- number of units;
- license holder

Oldbury is located on the East bank of the Severn river estuary in South Gloucestershire, England, United Kingdom. The estuary, which has a large tidal range, is used for the ultimate heat removal when operating at power; a reservoir ensures adequate water is available at all states of the tide.

The site contains two "Magnox" reactors. Reactor 1 is currently generating approximately 200 MW of electricity and is scheduled to be permanently shutdown by the end of February 2012. Reactor 2 is permanently shutdown. There are two turbo/generators, one per reactor although they can be cross coupled. There is a water filled spent fuel storage pond and radioactive waste storage facilities on site.

Magnox Limited is the Site Licence holder for the Oldbury 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).

Reactor 1

Reactor 1 is a Magnox reactor of a graphite moderated, gas cooled reactor design. It contains natural and slightly enriched metallic uranium fuel in magnesium alloy cans in a graphite core with a large number of vertical fuel channels.

The cylindrical graphite core consists of a central, active, region surrounded by a reflector region and is made up of alternate columns of square and octagonal graphite bricks, with each column comprising 12 layers. Overall the core is 14.2m diameter, 9.8m high and weighing 2061 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.

The reactor is normally cooled by forced circulation of pressurised Carbon Dioxide (CO_2) gas through the core which transfers the heat from the fuel to water fed boilers. The reactor is in a cylindrical pre-stressed concrete pressure vessel of 23.5m internal diameter and 28.1m external diameter with a height of 18.3m internally, 31.7m externally, which also

[1] 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.

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 can initially be cooled by either forced or natural circulation of pressurised CO_2 gas, with feed water to the boilers. As it is a large mass / low power density reactor, there are long timescales for establishing post trip core cooling.

Reactor 1 first went critical on 16th August 1967. It is currently at power, generating typically 700 MW thermal power; core gas temperatures are approximately 230ºC inlet and 360ºC outlet. It is expected to remain at power until the end of February 2012; after final shutdown, it will be defuelled.

Reactor 2

Reactor 2 is the same design as Reactor 1. It first went critical on 19th November 1967.

It has been permanently shutdown since 1st July 2011 and all core temperatures are below 100ºC. The reactor is held shutdown by full insertion of all control rods except the Safety Group, which is held in reserve. At shutdown it had a full core, in excess of 26,000 irradiated fuel elements. The reactor core is currently being cooled by forced circulation of air at atmospheric pressure with one gas circulator on pony motor drive and its associated boiler in service. The circulator/boiler in service is changed on a routine basis for plant preservation purposes. It has commenced defuelling by transfer of fuel to Reactor 1.

Irradiated Fuel Storage Pond

There is one, below ground level, water-filled reinforced concrete pond divided into five bays. It provides cooling and shielding of irradiated fuel elements routinely discharged from Reactors 1 and 2 before they are transferred to fuel flasks for transport to Sellafield, after a minimum 90 days cooling. The water is cooled by circulation of a proportion of the water through chillers, cooled by a secondary water circuit which in turn rejects the heat to atmosphere. This active cooling is only required to keep the ponds water in the target temperature, 9-13ºC, for long term corrosion control rather than to prevent the water boiling. Fuel elements cannot be returned to a reactor once they have been discharged to the ponds so the pond cannot be used to temporarily store fuel to allow access into the pressure vessel at shutdowns.

Radioactive Waste Facilities

Intermediate Level active Waste (ILW) and Low Level active Waste (LLW) is contained in purpose built storage facilities:

- Active Waste Vaults: These contain magnesium alloy can splitters, sludges and general waste.
- Low Level Waste Management Facilities: LLW is stored in ISO containers prior to transfer to the national LLW store for disposal.
- Reactor storage and disposal tubes, voids and cells: These contain non-combustible metallic items.

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 shutdown 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 planned or in a fault situation 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 Rods

Core reactivity is controlled by the movement of neutron-absorbing control rods inserted in 101 of the vertical interstitial channels in the graphite core. A bulk (or black) control rod consists of a stainless steel tube with boron steel inserts, which absorb virtually all incoming neutrons, a sector (or grey) control rod is a solid mild steel bar, both are approximately 7.9m long, suspended by a chain from an electrically driven actuator mechanism, mounted at the top of a control standpipe.

The actuating mechanism is designed to be "fail-safe" such that the associated rod will automatically drop into the reactor core under gravity should the drive mechanism fail, on loss of electrical supply, or on operation of the reactor trip system.

The 101 rods are arranged in groups for operational purposes:

- Regulating Group 26 Rods
- Trim Group 2 Rods
- Safety Group 8 Rods
- Bulk Group 65 Rods, subdivided into 4 groups.

The Regulating and Trim Groups are grey rods and allow control of the 9 reactor sectors, the former normally being automatically controlled on reactor temperatures.

The Safety and Bulk Groups are black rods. They are used for the bulk control of the reactor and to provide the majority of the shutdown and hold-down capability. The Safety rods have articulated joints which would facilitate rod entry and provide shutdown in the event of limited core disruption.

In normal operation the Safety Rods and three of the four Bulk rod groups are fully withdrawn from the core. The fourth Bulk Group is typically >60% withdrawn and manually adjusted to keep the Regulating rods in an optimum operating range.

Interlocks are provided to ensure the correct rod withdrawal sequence. Over-speed protection is provided to prevent an excessive rate of release of reactivity. The control rod data logger system records control rod heights as a function of time as they fall into the reactor following a reactor trip and monitors any slackness in the control rod suspension chain due to the rod fouling in its channel. Examination of the control rod insertion characteristics provides a means of monitoring the integrity of both the rod and the channel it is dropping into.

During normal steady state operation, entry of one or two Safety or Bulk Group rods in the central region of the core is adequate to shut the reactor down. In faults

involving a pre trip temperature transient, more are needed to terminate the transient rapidly and reduce the risk of fuel failure during the temperature excursion. Overall, there is massive redundancy for shutdown. There is also very large redundancy for hold-down.

Reactor 2 is permanently shutdown, with all the rods except the Safety Group fully inserted. The Safety Group are still connected to the reactor trip system and would insert in a fault. When conditions become appropriate, during defuelling, the Safety Group will also be fully and permanently inserted. Non-removable locking devices which prevent attachment of the handwind mechanism and connection of the electrical supply, have been fitted to each individual control rod assembly.

Boron Dust Injection Facility

This provides permanent hold-down of the reactor in the event that insufficient control rods enter the core to maintain the hold-down once the Xenon poison has decayed.

Four boron dust injection points are provided on each reactor.

The facility remains available for use on both reactors.

The Effect of Core Cooling

The Magnox core has a large positive moderator reactivity temperature coefficient of the order of +10milliNile/ºC. However due to the large mass of the core and resultant large thermal inertia this is associated with a long time constant. 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).

The shutdown reactor, Reactor 2, is maintained below 100ºC.

Criticality External to Core

The Magnox fuel used at Oldbury is natural or very low enrichment. Criticality in other than a designed regular array with suitable moderator is not possible. Operation of the new (dry) fuel route and wet (irradiated) fuel routes are covered by criticality certificates.

Criticality in the dry fuel route is not an issue as there are so few new fuel elements left on site.

Irradiated fuel cannot accumulate in the wet fuel route other than in the ponds. Irradiated fuel is stored in the ponds in skips and cannot go critical under any arrangement of skips with or without water present. The pond water does not have Boron added and there are no neutron absorbing materials added to the pond structure specifically for criticality control.

1.3.2 Heat transfer from reactor to the ultimate heat sink

1.3.2.1 Existing Reactor heat transfer chains

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 shutdown conditions: hot shutdown, cooling from hot to cold shutdown, cold shutdown with closed primary circuit, and cold shutdown with open primary circuit.

The Oldbury reactors consist of a cylindrical graphite core within a concrete pressure vessel. The fuel elements are located within a large number of vertical channels within the graphite core. The four boilers are internal to the pressure vessel and consist of tubes on platens suspended in an annular space between the core and the vessel.

Removal of the heat from the fuel is by forced circulation of pressurised (365psig) CO_2 gas up through the fuel channels and down through the boilers combined with forced flow of water up through the boiler tubes.

Gas Circulation

Each reactor is provided with four, (one per boiler) horizontally mounted variable speed gas circulators driven by their own steam turbine taking steam from its associated boiler. During normal full power operation, all four will be operating at 2000 to 2300 rpm. Their function is to drive the flow of CO_2 gas up through the fuel channels and down through the boilers. They draw gas from a plenum chamber below the boilers and deliver it to a common chamber below the reactor core.

When a reactor is shut down and steam is no longer available, the circulators can be driven by either a low speed (420rpm) or high speed (950rpm) electric pony motor mounted on the same shaft as the steam turbine. The pony motors are fed by essential electrical supplies that are backed by the Gas Turbines (GTs). High speed can only be used at coolant pressures below 20psig. The circulator auxiliaries, such as lubricating and seal oil systems, are also on the essential electrical supplies. The oil coolers reject heat to the reactor cooling water system which uses river water extracted directly from the culverts. The oil coolers have fire hose connections so that any other water source can be used, such as pumped town mains, town mains direct, mobile fire pump or fire engine

The drive shaft connecting the steam turbine/pony motor to the impeller passes through a steel lined penetration into the pressure vessel and is provided with two shaft seals to complete 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 either in or out of service. The running seal is a mild steel sleeve having a white metalled bearing face which bears against a rotating collar on the main drive shaft. The sleeve is free to move axially and contact on the bearing face is maintained by springs which bear against the seal housing. Seal oil is supplied to the space between the sleeve and the seal housing and assists the springs in maintaining contact between the sealing faces. Seal oil is provided at approximately 15 psi above reactor gas pressure, to form an oil film that prevents the escape of reactor gas. The seal oil system consists of one AC motor driven pump and two DC motor driven pumps; in normal operation, the AC motor driven pump and one of the two DC motor driven pumps are used with the other DC motor driven pump on standby; the DC pumps are battery backed to provide continuous provision of seal oil in any loss of electrical power event.

The second drive shaft seal is called the standstill seal and can only be used when the gas circulator is stationary. A sealing face is machined onto the back of the impeller, which mates with a face on the stationary part of the gas circulator housing. When required, the drive shaft is hydraulically moved (using seal oil

pressure) in an axial direction to pull the impeller sealing face into contact with the housing. A secondary seal called the spring standstill seal acts as a back-up. This spring seal is a thin, flexible metal ring attached to the gas circulator housing and bears against the impeller (on a different diameter to the main standstill seal) when the shaft is in the standstill seal position. In the event of seal oil system failure, the standstill seal can be applied manually using a mobile, air driven, oil pump; air pressure is supplied by readily available Breathing Apparatus (BA) air cylinders.

Boiler feed

During power operation and immediately after shutdown, boiler feed water is recovered from the turbine condenser by the condensate extraction pumps and is then pumped to the boilers by one of the two 100% duty main boiler feed pumps per reactor. A Reserve Feed Tank (RFT) on the turbine hall roof acts as a head tank to the system and is only used if there is a need to make up water that is being lost from the system. Only the top half of the reserve feed tank contents is available to the main boiler feed pumps. The pumps are driven by 11kV motors from the reactor/turbine unit or from grid supplies. Steam generated in the boilers is condensed in the turbine condenser, which is in turn cooled by circulating water drawn from the river (the primary ultimate heat sink).

On loss of pressure in the feed main at shutdown, boiler feed water is pumped to the boilers by one of the two emergency boiler feed pumps per reactor. The pumps can be started manually and can be cross-connected via an installed connection to the other reactor. Water is taken from the RFT on the turbine hall roof; all the water in the RFT is available to the emergency boiler feed pumps. The pump's sealing glands are normally cooled via the general service water system which is in turn cooled by river water drawn from the main cooling water culverts providing water to the main condensers. They can also be cooled using RFT or deaerator water, or through a fire hose connection. The pumps are driven by 415V electric motors that are on essential electrical supplies backed up by Gas Turbine generators (GTs). Steam generated in the boilers is initially condensed in the turbine condenser and subsequently when established in a dedicated shut down cooling loop both of which are in turn cooled by circulating water drawn from the river. If condenser cooling is unavailable, the steam can be vented to atmosphere (the alternate ultimate heat sink).

A manually aligned and operated back-up feed system comprising six diesel-driven pumps is available in the event of unavailability of main and emergency feed. The two facilities each have a dedicated feed water tank. Connections between the tanks, pumps and boilers are made with fire hoses. Each pump unit has a diesel day tank and there is a local bulk tank serving the three units. To be able to inject back-up feed, the boilers need to be depressurised. Steam generated is vented to atmosphere (the alternate ultimate heat sink).

All on-site tanks that contain significant quantities of feed water (reserve feed tanks, deaerators and condensers) or town mains (two concrete tanks) are fitted with outlet points that allow connection to mobile fire pumps or fire engines (of which there are three on site). In an emergency these can be used as a source of boiler feed which is pumped into the boilers in a similar manner to the back-up feed system.

Cooling Under Shutdown Conditions

Natural circulation of gas, driven by cool water in the boilers, is sufficient to cool the reactor under most shutdown conditions, as discussed below.

During hot shutdown and cooling to cold shutdown (at around four days post trip), forced or natural circulation of the pressurised CO_2 with any of the above feed systems is adequate to provide post-trip cooling.

After 96 hours post trip the reactor may be depressurised and the CO_2 coolant replaced with air to permit vessel entry or open standpipe working. Natural circulation of the air is sufficient to cool the core provided the boilers are fed with water as above.

Therefore, if the reactor is still at pressure or has been shut down for a significant period, natural circulation alone is sufficient to control reactor temperatures (with the application of boiler feed).

Minimum post trip cooling requirements have been calculated on a conservative design basis and a best estimate basis for both forced circulation and natural circulation as shown in Tables A and B below.

Table A: Post Trip Minimum Cooling Requirements – Forced Circulation

99% confidence data used for limiting depressurisation

Fault Type	**Number of Gas Circuits Required**
Pressurised &Very Slow Depressurisation	1
Slow Depressurisation	2
Limiting Depressurisation	2

Table B: Post Trip Minimum Cooling Requirements – Natural Circulation

Best estimate data used

Fault Type	Number of Gas Circuits Required
Pressurised	2
Very Slow Depressurisation	2
	3
Slow Depressurisation	3
Limiting Depressurisation	Not viable

1.3.2.2 Layout of reactor 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 gas circulator turbine, pony motors, control cubicles and associated ancillary plant are located in the annular circulator hall. No specific segregation or protection from hazards is employed.

Main Boiler Feed

The Condensers, condensate extraction pumps and Main Boiler Feed Pumps (MBFP) are all located in the Turbine hall. Apart from a system that trips the main cooling water pumps and closes the main cooling water discharge valves if water is detected in the turbine hall basement, no specific segregation or protection from hazards is employed.

Emergency Boiler Feed Pumps

The Emergency Boiler Feed Pumps (EBFP) are situated in the turbine hall and normally take their water supply from the RFT on the turbine hall annex roof. In the event water cannot be recirculated through the condenser or shutdown cooling loop then steam can be vented to atmosphere via valves in the reactor building. Non-return valves in the feed lines and ring main ensure that three out of four boilers can be fed regardless of where a single failure in a feed main occurs.

Back Up Feed System

In the event of failure of both Main and Emergency Boiler Feed Pumps there are diesel driven Back Up Feed System (BUFS) pumps. Each pump house has its own water tank. These pumps can operate totally independently of any other site electric supplies. Both would be vulnerable to ~30 to 50 cm water above site ground level, affecting either the starting electrics or the air intakes. The pumps are connected to dedicated pumping in points using standard fire hoses that are run out after the event. This arrangement is designed such that the pipe work would not be damaged in the initiating event and the hoses can

be run out over any debris/rubble resulting from the event. Furthermore any standard fire pump or fire engine, either one held on site or brought in from off-site, post event, could be used to pump water in from any available source if necessary.

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).

During a normal trip or shutdown, the MBFP would be expected to continue running until it was shut down by operators. Post trip cooling normally has to be reduced to stay within maximum permitted cool down rates.

In the event the MBFPs fail, the EBFP would start automatically on loss of feed main pressure with no interruption of cooling. Note the EBFPs are for post trip cooling only and are not sufficient to allow a reactor to continue to operate at power.

On failure of the EBFPs, feed would be established to a pressurised reactor using the Back-Up Feed System (BUFS) pumps to establish cooling by natural circulation of the CO_2 gas and keep the core within normal temperature limits. There are up to 24 hours to establish some cooling before core damage occurs. Systems are designed to provide 24 hours cooling before replenishment of fuel/water supplies is required. Plant modifications have previously been implemented to allow recovery of boiler feed water for use by the BUFS in an emergency, from the condenser or RFT. Alternatively, town mains water either direct or from storage tanks could be used. Water could be brought to site in tankers or could be extracted directly from the river.

Alternative means of venting the boilers to allow discharge of steam direct to atmosphere are identified in the Plant Operating Instructions in the event the preferred route is not 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 main boiler feed system can only be driven by 11kV supplies from the reactor/turbine unit or from the electricity grid. The emergency boiler feed system and the gas circulators can be driven from the electricity grid or from the Gas Turbine backed on-site essential electrical supply system; these also support the other AC and battery backed DC systems necessary for their operation. The back-up feed system does not require any electrical input.

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).

The BUFS was installed to provide diversity of post-trip cooling, which also addressed the potential for some common mode failures in the installed post-trip cooling system. It provides a diverse source of water, diverse routes and connections to the boilers. It was not possible to provide a diverse boiler, however there are 4 separate boilers, only 2 are required immediately post trip if it is associated with depressurisation and one is sufficient if the reactor remains pressurised.

Due to the low power density of the Magnox reactors (<700kWm^{-3}), there is a long period before cooling is required, which gives the opportunity to provide ad hoc solutions.

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

The pond tank, which is set below site ground level, serves both reactors and comprises a single reinforced concrete structure divided into five bays, the Reactor 1 and Reactor 2 storage and handling bays and the dispatch bay. The separate bays can be isolated from one another by the installation of stop log gates. These stop logs would only normally be used if a bay had to be isolated and drained for maintenance. Installing the stop logs requires the skip crane to lift them in to position.

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)

Pond water temperature is maintained within the target range of 9-13°C by circulating a proportion of the water through heat exchangers in the pond chilling plant, cooled by a secondary water circuit which in turn rejects the heat to atmosphere. This active cooling is only required to keep the ponds water in the target temperature range for long term corrosion control rather than to prevent the water boiling.

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 heat burden in the ponds is low (<200kW) as it derives from relatively low rating fuel that is routinely discharged from the reactors, and thus represents a spectrum of fuel from a few hours discharged to hundreds of days. Experience shows that, on unavailability of the chilling system, pond water temperatures increase at less than 1ºC per day. Due to the large surface area and low heat load, there is sufficient time to take alternative actions before pond water temperatures rise and significant loss of pond water, due to evaporation occurs.

Due to the limited consequences of loss of cooling, the pond chilling plant is not specifically protected from hazards. It derives it supply from the 415Vac Reactor Services Board.

Pond water can be replenished from the deionised water tank or through the use of the fire hydrant system. Section 1.3.2 above identifies further sources of water that could be used in an emergency.

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

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).

The reactor buildings only provide a weatherproof barrier to the massive reinforced concrete pressure vessel and the refuelling and other ancillary equipment. Normal heat transfer / ventilation of this building via windows and louvre vents would ensure there is no significant heat build-up. There are specific hot gas release paths in the buildings to ensure hot gas is vented in the event of a hot gas/steam release incident within the building. These hot gas/steam release routes are defined by fire barriers and fire doors. Louvres in

ventilation ducts are designed to close on detection of local excess temperature to prevent back flow of hot gas. The primary aim is to facilitate release to atmosphere and to prevent hot gas reaching heat sensitive equipment.

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 Oldbury, as discussed in Section 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.

National Grid provides an annual review report of the performance and reliability of the electrical grid connections to Oldbury. The most recent report, dated September 2010, concludes that the fault statistics do not show a deteriorating trend in the reliability of supply since April 1981.

An event occurred leading to a loss of site supply on 12th September 1968 due to a line fault combined with a design fault leading to the trip of a second line.

Due to the effects of heavy snow on 26th April 1981, faults on the grid led to several interconnecting lines disconnecting from the grid substation leaving Oldbury as the only connected generating unit supplying local loads at reduced output for approximately 6.5 hours. There was no loss of on-site power.

On 13th December 1981, high levels of faults were experienced due to snow. In all 63 faults are recorded for 1981 including 37 double circuit faults. Since this time faults have been significantly fewer with a peak of 8 during 1989 with the last double circuit fault occurring during 1999. Consideration of the statistics suggest a frequency of about 1 fault every 2 years. None of these faults resulted in the loss of off site supplies to the Oldbury site.

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.

Oldbury Grid electrical supplies are supplied by four 132kV overhead line connections run on two sets of high voltage towers. Diverse routes across country are taken by the two tower sets.

Oldbury substation is an indoor switchroom containing busbars, airblast switchgear, compressors, batteries, Low Voltage (LV) switchgear, telecommunications equipment and protection relay panels. External to the building is a dedicated standby diesel generator. The site addressable fire detection system extends into the Oldbury substation and is monitored within the central control room. Controls and indications for operation of the substation airblast circuit breakers are also located within the central control room.

Incoming 132kV lines connect to the building via four sets of through wall bushings and exit the building to the site via three similar sets of connections. Three sets of overhead lines cross from the Oldbury substation to the external bushings on the Station transformer and the two Generator Transformers.

There is a degree of separation in the 132kV connections to site in that for Generator Transformer 1, line 1 approaches the site on the Southerly tower set and line 4 approaches on the Northerly tower set. Busbar arrangements prevent these connections being used for the Station Transformer and Generator Transformer 2 which are both connected to line 2 approaching on the Southerly tower set and line 3 approaching on the Northerly tower set. Other than the robustness of the tower construction and the aforementioned separation, there are no specific design claims with regard to external and internal hazards. The on-site grid substation is a fully enclosed building containing compressors, batteries, LV switchgear, Air blast circuit breakers, protection relays and the main distribution busbars. The 50 year operational period and the reliability statistics give confidence in the design aspects but, for a beyond design basis situation, there are obvious vulnerabilities.

A seismic event may cause damage to rigid insulation bushings causing a loss of one or more lines through operation of the protection systems which may not be immediately recoverable. This is more likely on through wall bushings or transformer bushings as tower bushings are not so rigidly held. Such an event may also cause one or more transformers to trip due to disturbances in the Buchholz protection relays. The transformers were not designed against seismic events.

Fire or flood in the on-site 132kV substation relay protection room may cause loss of any grid connection. However, recent discussions with National Grid suggest there is a possibility that temporary arrangements could be made at the Oldbury substation, to bypass the switchgear and operate switchgear remotely.

1.3.5.2 Power distribution inside the plant

1.3.5.2.1 Main cable routings and power distribution switchboards.

<u>132kV distribution arrangements to provide 11kV supplies</u>

132kV overhead line connections from the on-site Oldbury substation to Generator Transformer 1 and 2 and the Station Transformer cross the site south road for a distance of approximately 100m. The connection at the substation is from horizontal oil filled through wall bushing with a cable tension arrangement attached to the substation steel structure. The transformers have vertical oil filled bushings which the overhead lines connect to with similar cable tension attachments to the turbine hall steel structure.

The Station Transformer 11kV connection to the Station Board is a cable running through the west side of the turbine hall on steelwork suspended below the ground level floor. On the north side of the turbine hall the cable enters the 11kV Station Board.

132kV/16.5kV Generator Transformer connections are normally configured as an outgoing supply to the 132kV system with a 16.5kV tee connection to supply a dedicated 16.5kV/11kV Unit Transformer. Once shutdown, the 16.5kV connection can be reconfigured, by rearranging the solid copper busbar connections, providing an incoming supply as described below.

Generator Transformer 2 16.5kV connection is via solid busbars from the transformer terminals, through the turbine hall reinforced concrete wall into the basement. The busbars are supported on the turbine hall wall by insulating porcelain bushings and the whole structure is enclosed within a large galvanised sheet steel enclosure. From the busbars within the enclosure, a cable connects to an earthing transformer located in the basement. A second cable connection, via horizontal porcelain bushings, runs through the east side of the turbine hall on steelwork suspended from below the ground level floor. On the north side of the turbine hall the cable rises to enter into the first floor east cable gallery, it is then routed through the turbine hall annex corridor before exiting the building in underground concrete ducting to Unit Transformer 2. An 11kV cable from Unit Transformer 2 runs to the 11kV Unit Board 2.

Generator transformer 1 connections are similar.

The 11kV Station and Unit Boards 1 and 2 can be interconnected by cables.

11kV distribution arrangements

There are three 11kV distribution boards, 11kV Unit Board 1, 11kV Unit Board 2 and the 11kV Station Board. The 11kV Station Board is normally supported from the 132kV/11kV Station Transformer through one 11kV air circuit breaker (ACB) with a further ACB either side to connect to the 11kV Station Board section 1 and 11kV Station Board section 2.

11kV Unit Boards 1 and 2 each support a Cooling Water Pump motor, a Condensate Extraction Pump motor and a Main Boiler Feed Pump motor. Each Unit Board also supports associated 11kV/415V Reactor Unit and Turbine Unit Transformers. The Unit Boards can also be interconnected to support the Station Board.

Each 11kV Station board section supports an associated Cooling Water Pump motor, Condensate Extraction Pump motor and Main Boiler Feed Pump motor. Each section also supports associated 11kV/415V Turbine and Reactor Services Transformers. Station Board section 1 also supports a General Services Transformer and a feeder circuit to the offsite Technical Centre. All of the above supplies generally support generation and general site services.

Also, each section of the Station Board supports a 11kV/3.3kV Essential Transformer. These provide the grid supported electrical connection to the 3.3kV Essential supply systems which supports plant claimed for reactor post trip cooling duty.

3.3kV Essential supplies distribution

There are three 3.3kV distribution boards, Board 1, Board 2 and a Standby Board. 11kV/3.3kV Essential Transformer 1 supports Board 1 which supports Gas Circulator Pony motors 1 to 4 associated with Reactor 1, 3.3kV/415V AC Essentials Transformer 1A and 1B and 3.3kV/475Vdc Essential Transformer/Rectifier 1. 11kV/3.3kV Essential Transformer 2 supports Board 2 which supports Gas Circulator Pony motors 5 to 8 associated with the permanently shutdown Reactor 2, 3.3kV/415V AC Essentials Transformer 2A and 2B and 3.3kV/475Vdc Essential Transformer/Rectifier 2. The Standby Board is supported by either Board 1 or Board 2 and supports 3.3kV/475Vdc Essential Transformer/Rectifier Standby. All three boards can be interconnected and supported by either 11kV/3.3kV Essential Transformer. In addition, each Board is supported by an associated Gas Turbine which will start and connect automatically if any board loses supplies.

All three Gas Turbines are located in the Gas Turbine house. The Gas Turbine House includes individual Gas Turbine engine cells and a common Gas Turbine generator hall. The three Gas Turbine generators are located within the generator hall mounted on concrete plinths. 3.3kV cables from the generators are routed out of the Gas Turbine generator hall on diverse routes to the 3.3kV switch rooms.

3.3kV/475V dc transformers are located on the ground floor external to the reactor block. Any one transformer is cable of supporting the 475Vdc loads.

415V Essential supplies distribution

There are four 3.3kV/415V AC Essentials Transformers 1A and1B are associated with Reactor 1, 2A and 2B with Reactor 2. Each transformer supports an associated 415V Turbine House AC Essential board which can be interconnected to its reactor associated board, allowing one transformer to support two boards. Each 415V Turbine House AC Essential board supports one Emergency Boiler Feed Pump, one Pressure Vessel Cooling Pump and an associated Reactor AC Essential Board supporting Gas Circulator auxiliaries. (Other loads distributed between the boards include Gas Turbine auxiliaries and 240Vdc, 110Vdc and 50Vdc battery chargers.)

3.3kV /415V Essential supplies transformers 2A and 2B are located at ground level. 1A and 1B are similarly located. 415V Turbine House AC Essentials boards 1A and 1B are located in two separate fire compartments. 415V Turbine House AC Essentials boards 2A and 2B are located in two separate fire compartments. 415V Reactor AC Essentials boards are located in a switchroom in a separate fire compartment to the 3.3kV Essential supplies switch boards.

There are four emergency boiler feed pumps, each supported by a 415V supply from an associated 415V Turbine House AC Essentials supplies board. Emergency boiler feed pump 415V supply cables are routed from the associated 415V Turbine House AC Essentials switchboard.

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

Following an incident circa 2006, when Generator Transformer 2 bushing catastrophically failed, permanent barriers have been erected around each Generator Transformer compound to ensure a similar failure cannot lead to damage of adjacent plant.

Each distribution transformer on site is enclosed in a dedicated concrete walled compound with durasteel fire barrier access doors which protect adjacent buildings in the event of a transformer fire.

All transformers have dedicated automatic deluge fire protection systems which activate deluge valves to release water sprays if frangible bulbs in air filled pipework rupture through heat releasing air pressure.

Distribution transformers are vulnerable from seismic disturbances activating Buchholz protection relays leading to a trip. The transformer may be immediately operational following cessation of the seismic disturbance.

Distribution cables through the turbine hall are separated at opposite ends of the turbine hall which provides a degree of tolerance to fire. However a major fire that engulfs the turbine hall is likely to lead to a complete loss of grid connection.

Flooding of the turbine hall does not present a risk to the Station transformer supplies derived from the grid connection however each Generator transformer if reconfigured as an incoming grid supply is vulnerable from a turbine hall basement flood due to the location of cooling water pumps and busbars.

Cables running through cable tunnels are protected by fast acting sprinkler systems and previous hazard tolerance considerations ensure that redundancy for plant is provided by running cables on diverse routes through segregated tunnels. Cables for post trip cooling plant operation that are routed external to cable tunnels through areas of the turbine hall or reactor block building have been sprayed with fire retardant coatings.

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.

In the event of a complete loss of offsite grid electrical supplies, all supplies from the incoming 132kV grid connections will be lost resulting in the complete loss of the 11kV supply system and all 415V unit and service supplies. None of these supply systems have any on site source of back up supply and will not be immediately recoverable without the return of a grid supply connection. The 3.3kV and 415V Essential electrical Systems will initially be lost but are automatically recoverable from on-site Gas Turbines as described below. Until Essential Electrical systems are recovered all battery chargers will become unavailable and station batteries will support emergency lighting, gas circulator oil pumps, instrument motor-generator sets, generator hydrogen seal oil pumps, alarm systems, circuit breaker tripping/closing supplies, telephone systems and 50V control supplies.

In the event of a complete loss of Grid electrical supplies, the 3.3kV Essential Electrical supplies are supported by the automatic starting and connection of Gas Turbines onto the dead 3.3kV boards. There are 3 Gas Turbines and normally 2 would start and connect automatically and the third would start and be available for manual connection. As a pre-condition to an automatic connection to a dead bar, a series of interlocks ensure the Gas Turbine is running at the appropriate speed and an adequate selection of interconnecting circuit breakers have opened to ensure the two automatically connecting Gas Turbines do not attempt a parallel connection. (The Gas Turbines are not designed to run in parallel with each other). A manual connection bypasses the series of interlocks and relies on the Operator to ensure the 3.3kV dead board is appropriately configured.

During each Statutory outage, the operation of the automatic sequence to open interconnecting 3.3kV circuit breakers, start Gas Turbines and automatically connect a Gas Turbine onto a dead 3.3kV board is routinely demonstrated (Ref: procedures ORTP 218 and ORTP 219).

Weekly test starts and monthly load runs of each Gas Turbine give confidence in reliability. During the monthly load runs, the Gas Turbines are synchronised with the Grid electrical supply (they are not closed onto a dead board).

Availability of the 3.3kV Essential electrical supplies on Gas Turbines leads to the automatic re-start of Gas Circulator Pony Motors, automatic restoration of 415V Essential electrical supplies to support reactor coolant pumps, critical oil pumps and emergency boiler feedpumps, automatic restoration of battery chargers to support critical oil pumps, telephone systems and emergency lighting. It does not support general site services such as heating, lighting, computer networks or workshop facilities.

Electrical supplies to the Remote Emergency Indication centre (REIC) are normally fed from one of two Grid derived supplies. When the grid supplies are lost, a UPS supply provides an interim supply and a dedicated diesel Generator provides a longer term supply.

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

There are three Gas Turbines and any one Gas Turbine has sufficient power capability to support the Post Trip cooling electrical requirements of both reactors at the same time. All three Gas Turbines are located in the Gas Turbine house. Each individual GT is located in a dedicated concrete walled engine cell with a dedicated engine external exhaust stack. The GT mounting places the closely coupled gearbox within the GT Generator hall through a fire resistant durasteel fire barrier which also provides a seal between the engine cell and Generator Hall. The three generators are located within the Generator Hall. Fuel control valves and gearbox casings of each engine are provided with additional durasteel fire barriers in mitigation of a fuel spill event and a potential fire. Each engine cell is provided with an automatic CO_2 fire suppression system and each gearbox/fuel control valve area is provided with a ‘double knock’ (2 out of 2) fire sensing system which automatically releases a water deluge via the installed Mulsifyre fire fighting system. The Generators, dedicated control

panels (including electronic governor system) and dedicated 24V control batteries are all located within the Generator Hall with spatial separation only, aligning with the associated engine position. Bulk fuel tanks are located in bunded areas. Each GT has its own supply tank. Dedicated 110V GT starter batteries are located in a dedicated battery house. Each GT 110V starter battery and charger is located in a dedicated room of the battery house. From the GT Generator hall, 3.3kV and control cables run on diverse underground routes to the reactor block switchgear room and the reactor block central control room. The switchroom is separated into two areas for fire protection reasons, one room houses switchgear for GT 2 and the other room houses switchgear for GT 1 and GT Standby.

There is no specific protection provided for other internal or external hazards although the GTs are remote from most sources of hot gas, steam or water derived from plant failures and not they are at risk from rotating plant failures. As part of the latest update to the Periodic Safety Review the snow loading and seismic capability of the Gas Turbine house were reviewed. While the snow loading capability was assessed as satisfactory the seismic review identified the need for seismic strengthening of some of the Mulsifyre pipe work and additional supports have been installed.

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).

One GT has sufficient power capability to support the post trip cooling electrical requirements of both reactors at the same time.

Forced cooling utilising Gas Circulators and Emergency Boiler Feed Pumps is dependent on the availability of the 3.3kV supply system supported by at least one GT. There is a POI requirement for a minimum fuel stock level sufficient, with a 10% contingency, to run 2 GTs at a nominal 2MWe each for 24 hours. (These durations are all based on having two operational reactors shutting down from full power and are pessimistic for Oldbury given that in June 2011 Reactor 2 ceased generation.)

Station POI 2.12 describes the required operator actions in the event of a loss of 11kV supplies and restricted 3.3kV supplies. The rehearsal of various aspects of this has recently taken place for Oldbury Operations staff during routine simulator training.

For a complete loss of all supplies, including GTs, POI 2.12 instructs the Operations staff on key measures including:

- Shutdown Safety Motor Generator (MG) sets to conserve 475Vdc battery power.
- Isolate one 475Vdc, one 240Vdc and one 110Vdc battery to allow a rapid restoration of forced cooling if ac supplies are restored.
- Turn off unnecessary emergency lighting to conserve 240Vdc battery power.
- Turn off Turbine flushing oil and stator coolant pumps to conserve 240Vdc battery power.
- Put all Gas Circulators onto standstill seal.

- Shutdown unnecessary Gas Circulator seal and lube oil pumps to conserve 475Vdc battery power.
- Purge Turbine Generator frame of hydrogen with CO_2.

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 purpose (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)

In the event of a loss of all on-site electrical supplies there are several diesel generators installed or available for immediate use.

The Remote Emergency Indication Centre (REIC) includes an installed diesel generator that can support all the required supplies to maintain the REIC as functional. This diesel is subject to routine testing and demonstration of its capability.

A mobile diesel generator is maintained and available on site to connect by installed plug and socket to the access control point buildings required to operate the on site emergency scheme arrangements.

Low voltage supplies to the on site 132kV substation can be maintained by an installed diesel generator operated and maintained by National Grid.

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

The REIC diesel generator is installed in a dedicated steel-framed structure mounted on a concrete cast slab at ground level. The diesel itself is internally installed within a bund. The building has, as far as is reasonably practicable, been sited where it would be unaffected by any single event that imperils the CCR or any essential services to it. A fire detection system is fitted within the REIC diesel generator building. The REIC UPS is adequately rated to support full system load for at least 2 hours and the diesel generator would be available to support the REIC within one hour. Additional to the dedicated REIC diesel tank, adequate supplies for continued running of the REIC are available from the permanently stored diesel bowsers.

The mobile diesel generator is located in the Fire Station building. The building also houses the site fire engine. There is no physical barrier around the diesel generator when it is sited in its normal storage location. The diesel generator has its own fire detection system installed with an auto shutdown function. No time constraints are placed on the diesel with regard to the time it would take to connect and start the diesel generator. A prudent estimate would be that it would be available within one hour. Adequate supplies for 24 hours continuous running are held within the internal, double skinned diesel storage tank.

The 132kV diesel generator is sited in a dedicated brick built building. A fire detection system is linked in to an automatic shutdown system. The 132kV diesel generator has an automatic start facility that does not rely on operator intervention. Additional to the dedicated 132kV diesel tank,

adequate supplies for continued running of the 132kV diesel generator are available from the permanently stored diesel bowsers.

Whilst it would be considered a last resort, in the event the Gas Turbines are disabled but their bulk kerosene fuel tanks remain in tact, short term operation of any of the station diesels, using this kerosene is considered to be possible. No data is available to confirm this; however, informed opinion suggests that this would be a viable alternative if there were no other supplies available.

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.

None identified.

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

There are no specifically designed installation points for the hook-up of transportable power sources to supply safety systems.

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

Not applicable as no sources identified. Further consideration to be given to identifying possible sources as discussed in Section 5.1.2.

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.

Not applicable as no sources identified. Further consideration to be given to identifying possible sources as discussed in Section 5.1.2. This will include any necessary arrangements and training.

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.

Oldbury Power Station has the following d.c. electrical supply systems:

The 475Vdc system provides ‘no break’ supplies to gas circulator auxiliaries, instrument MG sets and reactor safety circuits MG sets.

The 475Vdc system consists of two Reactor DC Essential Supplies Boards and one Reactor DC Essential Supplies Standby Board, which can be interconnected. Each of these three boards is supplied from a Transformer/Rectifier Unit (TRU) rated to provide normal system loads whilst maintaining a ‘float’ charge on its associated 1200Ah battery. The TRUs are supplied from the 3.3kV AC Essential Supplies System.

In the event of a loss of grid supplies, 475Vdc supplies are maintained by the battery connected to each DC Essential Supplies Board. Each of the three batteries is capable of carrying out this emergency duty for 90 minutes.

However, under normal circumstances, supplies to the 475Vdc TRUs would be returned to service in 90 seconds and maintained by the GTs on the 3.3kV AC Essential Supplies System. If only one TRU re-energised, then automatic closure of the reactor DC Essential Supplies Boards interconnectors would be initiated.

The 240Vdc system provides 'no break' supplies to emergency lighting, turbine essentials auxiliaries and auxiliary equipment on boilers and gas circulators. It also provides power to close 11kV switchgear.

The system consists of one 240Vdc switchboard, powered from the 415Vac Essential Supplies System via two transformer/rectifier units and supported by two 900Ahr batteries. Each of the two TRUs is capable of supplying the system load of 600 amps whilst maintaining a 'float charge' on the battery. Under normal operating conditions, both TRUs are in service such that one unit supplies the system load with the other unit available to automatically pick up load if required.

In the event of a loss of grid supplies, 240Vdc supplies are maintained by the battery supplying the connected loads. One battery is capable of carrying out this emergency duty for at least 60 minutes.

Under normal circumstances, supplies to the TRUs would be returned to service in 90 seconds and maintained by the GTs on the 3.3kV AC Essential Supplies System.

Diverse manual means have been established for all safety functions carried out by the 240Vdc system.

The 110Vdc system provides supplies necessary for the operation of the majority of plant items associated with the Essential Supplies, including rectifier controls, Safety MG sets, Instrument MG sets and closing and tripping coils for 11kV & 3.3kV Air Circuit Breakers (ACBs).

The system consists of two 110Vdc distribution boards, each supported by a 400Ahr battery and its own charger. A standby battery and charger, both rated for full duty, are incorporated in the system and can be connected via interconnectors to each distribution board. The chargers are powered from the 415Vac Essential Supplies System. The system is normally operated with three batteries and chargers in service. However, maintenance allows a minimum number of two batteries and chargers in service.

In the event of a loss of grid supplies, 110Vdc supplies are maintained to each distribution board by the battery. One battery is capable of supporting the station system emergency load for at least 120 minutes.

Under normal circumstances, supplies to the chargers would be returned to service in 90 seconds and maintained by the GTs on the 3.3kV AC Essential Supplies System.

The 50Vdc system provides supplies for the operation of major items of plant from the Central Control Room (CCR) and alarms.

The system consists of the 50Vdc Centralised Control Distribution Board, providing supplies for the operation of the major items of plant from the CCR,

and the 50Vdc Alarms Distribution Board, which provides supplies for the alarm fascias. Each distribution board is supported by two 200Ah batteries and two chargers, with an interconnector between the two boards. The distribution boards are normally operated with both batteries and chargers in service but each battery and charger can be disconnected for maintenance or boost charging. The chargers are powered from the 415Vac Essential Supplies System.

In the event of a loss of grid supplies, dc supplies are maintained to each distribution board by the batteries. Discharge tests have confirmed that with only one battery in service on each distribution board the system would function satisfactorily for 5 hours under normal load conditions.

Under normal circumstances, supplies to the chargers would be returned to service in 90 seconds and maintained by the GTs on the 3.3kV AC Essential Supplies System.

If the 50Vdc control supplies are lost, plant can be controlled locally.

There are 110Vdc and 24Vdc battery and charger systems dedicated to each GT to provide starting, ignition and control supplies. The battery design/rating is based on the requirement to support a minimum of three start attempts on the associated GT. In practice the installed capacity of each battery is well in excess of the minimum claimed design and several more start attempts are likely to be possible.

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

475Vdc systems provide 'no break' supplies to gas circulator auxiliaries, instrument MG sets and reactor safety circuits MG sets.

110Vdc systems provide supplies necessary for the operation of the majority of plant items associated with the Essential Supplies, including rectifier controls, safety MG sets, instrument MG sets, closing and tripping coils for 3.3kV ACB's and tripping coils of 11kV ACBs.

240Vdc systems provide 'no break' supplies to emergency lighting, turbine essentials auxiliaries and auxiliary equipment on boilers and gas circulators. It also provides power to close 11kV switchgear.

50Vdc systems provide supplies for the operation of major items of plant from the CCR and alarms.

110Vdc and 24Vdc battery and charger systems dedicated to each GT provide starting, ignition and control supplies.

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

475Vdc batteries and switchboards are located in fire segregated zones. The battery stands have been upgraded to include restraints against seismic disturbance and consideration of the risk of flooding due to internal plant damage have resulted in a degree of flood diversion features being installed. TRUs (Transformer/Rectifer Units) are located at ground level and each of the

three units is individually located in concrete walled berths with fire resistant durasteel access doors.

The two 240V dc batteries and switchboards are housed in individual rooms. TRU's are located at ground level external to the turbine hall and each of the two units are individually located in concrete walled berths with fire resistant durasteel access doors.

110V dc batteries and switchboards are located in fire segregated zones, two in one zone and one in a separate zone. The battery in the separate zone includes an electronic battery charger in an adjacent room. The two in the single zone feed onto, effectively, one switchboard in an adjacent room and each of these units is supported by a TRU located at ground level. The battery stands have been upgraded to include restraints against seismic disturbance and consideration of the risk of flooding due to internal plant damage have resulted in a degree of flood diversion features being installed. These consist of low (~50cm) bund walls with removable, drop in stop log gates across corridors where wheel equipment access is required.

50V dc alarm batteries, chargers and switchboard are located in a single fire zone. 50V dc Control batteries and chargers are located in the control block switchroom.

1.3.6.4 Alternative possibilities for recharging each battery bank.

The 475Vdc system consists of two Reactor DC Essential Supplies Boards and one Reactor DC Essential Supplies Standby Board, which can be interconnected. Each of these three boards is supplied from a TRU rated to provide normal system loads whilst maintaining a 'float' charge on its associated 1200Ah battery. The TRUs are supplied from the 3.3kV AC Essential Supplies System. In the event of a loss of grid supplies, 475Vdc supplies are maintained by the battery connected to each DC Essential Supplies Board. Each of the three batteries is capable of carrying out this emergency duty for 90 minutes. However, under normal circumstances, supplies to the 475Vdc TRU's would be returned to service in 90 seconds and maintained by the GT's on the 3.3kV AC Essential Supplies System. If only one TRU re-energised, then automatic closure of the reactor DC Essential Supplies Boards interconnectors would be initiated.

All three 475V dc batteries can be supported and charged from any one TRU.

The 240V dc consists of one Switchboard, powered from the 415Vac Essential Supplies System via two TRUs and supported by two batteries. Each of the two TRUs is capable of supplying the system load whilst maintaining a 'float charge' on the battery. Under normal operating conditions, both TRUs are in service such that one unit supplies the system load with the other unit available to automatically pick up load if required. In the event of a loss of grid supplies, 240Vdc supplies are maintained by the battery supplying the connected loads. Under normal circumstances, supplies to the TRUs would be returned to service in 90 seconds and maintained by the GTs on the 3.3kV AC Essential Supplies System.

Either of the two 240Vdc chargers can support and charge both batteries.

The 50Vdc system consists of the 50Vdc Centralised Control Distribution Board and the 50Vdc Alarms Distribution Board. Each distribution board is supported by two batteries and two chargers, with an interconnector between the two boards. The distribution boards are normally operated with both batteries and chargers in service but each battery and charger can be disconnected for maintenance or boost charging. The chargers are powered from the 415Vac Essential Supplies System. In the event of a loss of grid supplies, 50V dc supplies are maintained to each distribution board by the batteries. Under normal circumstances, supplies to the chargers would be returned to service in 90 seconds and maintained by the GTs on the 3.3kV AC Essential Supplies System.

Any of the four battery chargers can support and charge all four batteries.

110Vdc and 24Vdc battery and charger systems are dedicated to individual GTs and are not provided with interconnections.

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.

Plant: Reactor 1 and 2 are essentially identical plants.

Operation: This is discussed in Section 1.2. Reactor 1 is currently at power, generating typically 700 MW thermal power and apart from one further planned outage, it is expected to remain at power until the end of February 2012. Then, after final shutdown, it will be defuelled. Reactor 2 has been permanently shutdown since 1st July 2011 and has commenced defueling as a result of transfer of partially irradiated fuel to Reactor 1.

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 shutdown.

A detailed Level 2 Probabilistic Safety Assessment (PSA), incorporating the results of a human factors analysis, was undertaken in support of the periodic safety review to March 2008. For the generating reactors, it addressed shutdown, start-up and at-power faults, maintenance states and 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 is predominantly from large releases derived from failure to trip, shutdown and post trip cool.

It concluded that the frequency of failure of the reactor trip and shutdown function was 1.01×10^{-5} per reactor year, which was dominated by assumed common cause failure cut-offs for trip thermocouple and control rods. However, these are multiple redundant systems and the common cause failures assumed are deemed to be conservative; in particular, the diversity of the control rod system was increased through the use of articulated control rods in the Safety Rod group.

The PSA frequency of failure of post-trip cooling is 3.21×10^{-6} per reactor year. There are no dominating risk factors. 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.

The deterministic safety cases for hazards were addressed separately in the PSA. It demonstrated that the risk from hazards was less than that from plant faults, the majority of risk from hazards being derived from a turbine missile causing a depressurisation (see discussion below).

During the production of the PSA, two significant enhancements were identified and undertaken. The PSA identified a further five enhancements, of which one was implemented; the other potential enhancements were shown not to be reasonably practicable. Three of the four other potential enhancements have been specifically considered in the plant vulnerability workshops. The remaining potential enhancement, which relates to turbine missiles, has been mitigated since the PSA, by targeted inspections and modification of the turbines to ensure risk remains as low as is reasonably practicable.

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 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 design basis. The capability of the station to withstand seismic events was first evaluated as part of the Long Term Safety Review carried out during the late 1980s, with a more detailed assessment being carried out as part of the periodic safety review to March 2008.

The current design basis earthquake for the Oldbury site is defined by the envelope of the Principia Mechanica Limited (PML) hard site United Kingdom (UK) design response spectrum anchored to a horizontal zero period acceleration of 0.1g and a UK generic 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 0.16g.

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

No site specific seismic hazard study has been undertaken for the Oldbury site.

The uniform risk spectrum component of the design basis earthquake for the Oldbury site was derived from a probabilistic seismic hazard assessment whose input seismic source parameter distributions (b-value, activity rate, maximum magnitude, depth etc) represent the characteristics of seismicity within the UK region as a whole. The seismic source is taken to be a 500km square zone centred around a generic site. 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 response spectrum used in the definition of the design basis event is that assessed to have a uniform probability of exceedance of 10^{-4} per annum.

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,

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 Oldbury design basis event (average maximum magnitude $6.5M_S$) are credible. Examination of the pattern of historical UK seismicity indicates that Oldbury is situated in a region of low to moderate earthquake activity by UK standards. The use of a UK generic uniform risk spectrum within the definition of the design basis event is, therefore, considered reasonable in lieu of a site-specific hazard assessment.

Knowledge of UK seismicity has increased somewhat since the design basis was established and methods for seismic hazard analysis continue to advance. Nevertheless, it is considered that the design basis earthquake is an adequate representation of the prevailing seismic hazard for the Oldbury site at a 10^{-4} per annum exceedance frequency.

2.1.2 Provisions to protect the plant against the design basis earthquake

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

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 2.1.1 are as follows:

<u>Key Structures</u>

- reactor concrete pressure vessel, pressure vessel liner and internal structures (including the reactor graphite core, and its support and restraint structures, and the boilers)
- reactor drum building
- central block
- control block
- back-up boiler feed pump houses
- remote emergency indication centre building
- cooling pond and pond building
- waste vaults and facilities.

<u>Key Systems and Components</u>

- 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 pressurised coolant gas within the reactor pressure vessel;
- Back-up boiler feed system (including water tanks, pumps and fixed low pressure boiler feed pipework);
- Remote emergency indication system (including instrumentation and cabling);

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 (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 stand still seal using the local Standstill Seal Portable Air-Driven Pump, if this cannot be achieved remotely. Instructions for this are given in POI 2.4 Circulator Faults and repeated on special labels attached to the pump. 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;

If the Main and Emergency boiler feed has been disabled by the event, commission the back-up boiler feed system. Recommended minimum flow rates and maximum delay times, dependent on state of pressurisation and availability of boilers, are given in POI 2.7. Procedure for commissioning the BUFS is in POI 2.14 Stage 3.

- Establish monitoring of key reactor parameters

Reactor monitoring will normally be carried out in the CCR using the installed temperature scanner and alarm analyser. In the event the CCR is untenable CCR staff will redeploy, this will include 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 becoming untenable are given in POI 2.19. The REIC provides indication only, manual local control of plant would be required in the event 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 POI 2.17. These state that if a reactor has been shutdown as a result of a seismic event it may not be restarted without the advice of the Nuclear Safety Committee and permission of ONR (Office for Nuclear Regulation). 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 (BA) with CO_2 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_2 pressure in the vessel to exclude any air from entering 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 amounts 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 identified. Such items include the nuclear island buildings, cranes, charge machine support structures 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 retro-fitted 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 detail. 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 boiler feed system has dedicated diesel 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. On longer timescales, it is assumed that necessary supplies and personnel will be available from off-site sources.

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

The potential for consequential fire or explosions affecting the plant following a design basis earthquake has not been explicitly evaluated. It is not considered that either of these hazards poses a substantive risk to the key structures, systems and components required to maintain safety functions following a design basis event.

Threats from failures of structures, systems and components that have not been explicitly qualified to withstand the design basis event have been identified through a systematic programme of plant walkdowns. Where

necessary, follow-up assessments have been carried out and strengthening or protection measures implemented to mitigate such threats.

Failure of internal tanks and pipework has already been considered in the context of the hazard from site generated flooding. Water leaking from internal sources is directed out of the building or from the reactor building basement, through the cable or pipe tunnels to the turbine hall basement. Essential plant that could possible be affected is protected by bunds.

Water treatment plant bulk chemical storage tanks are situated close to the end of the turbine hall where the Gas Turbine generators are situated. It is considered unlikely that liquid chemicals will enter the Gas Turbine house itself.

The risk to the integrity of the exhaust stacks from corrosive chemicals in the short term (hours) is small and failure of the stack would not prevent the Gas Turbines being operated in an emergency.

The Gas Turbine air intakes are high off the ground and the amount of corrosive atmosphere ingestion would be dependant of the prevailing weather condition and how quickly it can be dispersed. Although detrimental to the engine internals and lubricating oil, if the quantity was small and for a short duration the engines would probably still run although there may be long term damage. Performance may well deteriorate.

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.

The Site Licence requires that ‘The Licensee shall make and implement adequate arrangements for the regular and systematic examination, inspection, maintenance and testing of all plant which may affect safety.’ It further requires that the arrangements provide for the preparation of a plant maintenance schedule, known as the Maintenance Schedule (MS), for each plant. Failure to complete maintenance as specified in the MS is a breach of a Site Licence condition. Plant is therefore 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 MCP 19 “Management of Maintenance Work” and MCP 13 “Surveillance and Routine Testing of Plant Items and Systems”. Specific procedures include S-268 "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-021 "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 have been implemented.

Plant walkdowns have been undertaken, covering the following plant;

- back-up feed system
- boron dust injection equipment
- circulator standstill seal equipment
- remote emergency indication centre
- portable fire pumps (two off)
- site fire engine

These walkdowns have 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.

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):-

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

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

A targeted programme of walkdowns is in progress to verify the capability of the claims on 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 (SQUG) 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.

On site equipment for use in an emergency, that is not routinely proven by use for generation, is inspected, tested and maintained as specified in the Maintenance Schedule (see 2.1.3.1). This includes fire fighting equipment, Boron Dust Injection equipment, Iodine Adsorption Plant, emergency lighting, communication equipment and emergency equipment.

Equipment that would be called in from off site post event is controlled by the CESC (Central Emergency Support Centre).

2.1.3.3 Potential deviations from licensing basis

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

The only deviations with respect to the seismic safety case are derived from the routine S-268 "Inspection and Assessment of Nuclear Safety Related Civil Structures to Comply with Site Licence Condition 28" inspections. These have identified cracks in 5 masonry walls that are required to be seismically qualified; 3 have been repaired and the remaining two are programmed for completion by December 2011. It is anticipated that further cracks will be detected and repaired during the ongoing inspection programme.

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.

No estimate of the peak ground acceleration that could threaten the integrity of nuclear safety significant structures at Oldbury has been made. Damage caused by a Beyond Design Basis earthquake has not therefore been specifically assessed. However, to cause severe fuel damage, the event would have to cause a breach in the primary pressure circuit and prevent all the gas circulators from operating or prevent any water being fed to the boilers.

The essential reactor safety functions that must be maintained are the ability to trip, shutdown and hold down the reactor, the ability to provide adequate post-trip reactor cooling, and maintenance of the integrity of the reactor primary cooling gas circuit. 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 and shielding of radioactive wastes is also essential.

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

<u>Reactor Trip</u>

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 of sufficient 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 safe. 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 rapidly lead to fuel damage. Reactor shutdown and hold down is achieved by insertion, under gravity, of sufficient control rods into channels within the graphite core. During normal steady state operation, entry of one or two Safety or Bulk Group rods in the central region of the core is adequate to shut the reactor down; more are needed to terminate the transient rapidly and reduce the risk of fuel failure during the temperature excursion, or to 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.

Based on the outcome of existing assessments, it is judged that scenario b) is the limiting scenario (i.e. that which is likely to occur at the lowest beyond design basis earthquake severity).

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, given the relatively modest structural displacements induced by the design basis event, it is judged that an event substantially more severe than the design basis would be required to cause damage sufficient to prevent safe 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 primary cooling gas 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 the boilers by the 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 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. This might occur as a consequence of overstressing of pressure boundary pipework or equipment external to the reactor pressure vessel or as a result of unrelated structural or plant failures damaging such pipework.

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.

Primary Pressure Circuit Integrity

Primary coolant containment is provided by the pre-stressed concrete reactor pressure vessel, associated penetration closures and connected plant and equipment that collectively form the reactor primary coolant gas circuit pressure boundary. The integrity of the concrete pressure vessel itself would not be threatened by credible seismic loading. The limiting components of the gas circuit pressure 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.

The reactor primary coolant gas circuit pressure boundary is not an essential safety function for Reactor 2 as it is already maintained in an air atmosphere at atmospheric pressure.

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 uninterruptable 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, therefore, highly desirable.

Monitoring capability could be lost in the following scenarios:

a) Damage to primary instrumentation (including pressure gauge piping etc);

b) Damage to data transmission cabling;

c) Damage to the REIC;

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 or damage to equipment. In particular cabling would be vulnerable to significant failures within the reactor buildings 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 the irradiated fuel storage pond. The pond water provides shielding and cooling. Under normal circumstances, the pond water is actively cooled but the heat loading from discharged fuel is sufficiently low that pond water cooling is not considered to be an essential safety function following a severe earthquake. If active cooling capability was to be lost, then the pond is tolerant to very extended periods of loss of cooling and passive cooling alone may be sufficient. A reducing water level would result in an increased dose level for personnel working in the ponds area. Fuel damage by overheating would not be an issue until it became uncovered.

A substantial reduction of pond water level resulting from failure of the pond structure would lead to loss of shielding and may cause fuel damage. It is notable that the Oldbury pond is mainly below ground level and any loss of pond water caused by cracking of pond walls would be slow. Loss of pond water following failure of the pond wall would also require the water to escape through the surrounding ground. The radiological release potential in such an event may be enhanced if coupled with mechanical damage to the fuel caused by objects falling into the pond during the earthquake.

The existing design basis assessment suggests that the reinforced concrete pond walls may be susceptible to cracking for events marginally more severe than the

design basis. However, a much more severe event would be required to cause damage leading to rapid water loss.

Containment and Shielding of Radioactive Waste

Intermediate Level active Waste is stored on site in purpose built facilities. These are above ground massive concrete structures where the structure was designed primarily for shielding purposes. The five Magnox waste vaults contain magnesium alloy can splitters directly in the concrete vault. Sludges, resins and other potentially mobile waste is contained in steel tanks within the concrete vault. Access to the vaults is from the top and both would require at least five meters of water on site before overtopping occurred. These structures themselves are considered robust against seismic, wind or wave damage.

Low Level Waste is stored in ISO containers prior to transfer to the national Low Level; Waste repository for disposal.

Non-combustible metallic items are stored in storage and disposal tubes, cells and voids with in the reactor building.

None of the waste facilities require active cooling.

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.

As detailed in section 1.3.4.1, there is no secondary reactor containment included in the Magnox design.

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 Oldbury 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 Oldbury 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.

There are no nearby bodies of stored water or water-retaining structures that are above the level of the Oldbury site. There are, therefore, no bodies of water that could be breached leading to site flooding following a design basis earthquake.

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 detail. 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.

2.2.4 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.

Considerable work to enhance the robustness of the site to an earthquake has already been undertaken following the seismic assessments carried out as part of the periodic safety review. However following the Fukushima event a series of workshops have been held to further review the robustness of the site to external and internal events, especially beyond design basis scenarios, and to consider 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 topic are:

Consideration OLD 1. Consideration will be given to enhancing the methods and equipment for primary pressure circuit sealing.

Consideration OLD 4. 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.

The potential for flooding from external sources to affect the Oldbury site with an exceedance frequency greater than, or equal to, 10^{-4} per annum has been assessed.

The site is located on the east bank of the River Severn. In the vicinity of the site, the river is tidal and the river still water level is determined by a combination of fluvial flow, tidal variation and surge. The 10^{-4} per annum exceedance frequency still water level at the site has been determined to be +9.2m above Ordnance Datum (OD), comprising +8.1m highest astronomical tide level combined with +1.1m surge contribution. The site sea defence has a minimum height of +10.2m OD giving a freeboard of 1.0m against over-topping by the 10^{-4} per annum exceedance frequency still water level.

The height of wind waves on the river adjacent to the Oldbury site is limited by fetch length and river depth. The conditional probability of the significant wave height (given the extreme still water level described above) being sufficient to cause over-topping of the sea defence is estimated to be less than 10^{-6}. It is concluded that wave overtopping of the sea defence will not occur at the 10^{-4} per annum exceedance frequency.

A limited amount of water ingress onto site in the form of spray cannot be discounted. However, in general, site levels behind the sea defence are such that water would drain back towards the river. It is recognised that spray water could accumulate in the cooling water pump house as a consequence of site road system topography.

It is also noteworthy in this respect, that the Severn estuary has the second highest tidal range in the world and, as a consequence, around high tide, the still water level falls by about 10% of its range (~1.5m around highest astronomical tides) within the first hour following high water. The period over which water ingress onto site could occur is, therefore, very limited.

The 10^{-4} per annum exceedance frequency extreme rainfall event is assessed to be a total of 138mm of rain within 2 hours. Flooding from snow melting has also been considered but the extreme assessed snow melting rate (42mm/day of melt water) is bounded with a large margin by the extreme rainfall event.

In defining the design basis river levels for the Oldbury 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 river levels considering extreme tide and surge combinations.

There are no off-site water retaining structures (dams, reservoirs etc) whose failure could credibly lead to site flooding.

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 River Levels

Extreme tidal levels (highest astronomical tide) are based on long term observations at the nearest standard port, the Port of Bristol (Avonmouth), transformed to provide tide predictions at river locations adjacent to the Oldbury site. The extreme combined tide and surge level has been derived from statistical analysis of long term observations of surge levels coincident with high tide at Avonmouth.

Significant wave heights and periods have been estimated by wind wave modelling assuming relevant water depths, fetch length and limiting wind direction. When combining wave heights with still water levels, it has been assumed that the wave shape is such that the wave crest is two-thirds of the wave height above still water level.

Water levels in the River Severn around the location of the Oldbury site are the product of a complex interaction of tidal processes, surge, river flow and surface wind waves. The detailed of analysis of tide and surge levels and significant wave heights, appropriate to the Oldbury site, was carried out in the late 1980s. Since that time, much research has been undertaken and, combined with the availability of greater computing power, the understanding of the contributing processes and their interaction has improved.

The underlying tide height estimates used to define the design basis extreme water levels are expected to be accurate because tides are reliably predictable based on the available observation records. The basis for estimating extreme combined tide and surge levels is less certain. It is credible that the 10^{-4} per annum exceedance frequency still water level (tide + surge) may be under-estimated. Furthermore, the design basis still water level does not include an allowance for climate change-induced sea level rise.

Design Basis Rainfall

Short duration rainfall amounts for given return periods are derived from formulae based on statistical analysis of long term extreme rainfall data gathered from locations across the UK.

Methods and data supporting the estimation of extreme rainfall events have, in common with those to determine extreme river levels discussed above, improved since the Oldbury design basis rainfall event was derived.

3.1.1.3 Conclusion on the adequacy of protection against external flooding

It is concluded that the design basis (10^{-4} per annum exceedance frequency) river levels may be under-estimated. A consequence of allowing for this under-

estimate would be an increase in the estimated likelihood of wave over-topping of the sea defence, with a consequent increase in the volume of water potentially discharged onto site under extreme high water conditions. Significant wave heights may also be under-estimated.

Notwithstanding the above conclusion, it remains true that the duration of any wave over-topping and discharge onto site would be limited by the rapid drop in water level following the time of high tide as a result of the high tidal range at the Oldbury site.

It is credible that the 10^{-4} per annum exceedance frequency rainfall rates are also under-estimated relative to those that would be predicted using more modern data and methods.

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

The flooding risk is currently being reviewed as part of our response to Fukushima.

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 (SSC) that are required for achieving and maintaining safe shutdown state and are most endangered when flood is increasing.

The emphasis within the safety case against external flooding hazards (from the river or precipitation) is on prevention of significant water ingress onto site and/or into buildings or other facilities.

<u>Key Structures Providing Protection against Flood Water Ingress</u>

- Sea wall;
- Building envelopes and thresholds.

<u>Key Systems Providing Protection against Flood Water Ingress or Accumulation</u>

- Site storm water drainage system.

If water ingress onto site was to occur from external sources, then the key structures, systems and components providing ultimate protection against loss of essential safety functions are identical with those listed in Section 2.2.1 that provide protection against the design basis seismic event.

During construction, the general level of the Oldbury site was raised several metres above that of the surrounding land. Within the site, roads are then slightly below that of the building thresholds, so water on site would drain away from buildings, via roads and site drains. If the drains could not cope with the quantity of water entering the site, then it would simply drain off onto the surrounding land. Over-topping would only create a significant hazard if the rate of water entering the site exceeded that at which it could drain away to an extent that the standing water level on the site roads exceeded the level of the

building thresholds. At this point, water would then start to enter the reactor/ turbine hall basements. Assuming total loss of on-site power coincident with this level of over topping, such that sump pumps would not operate, then this would become a problem once the water level in the basements rose to the level of the emergency batteries, the pony motor vent fans and circulator oil systems.

Note that the sea wall is only a facing to the raised site, there is no 'behind' for water to be trapped except near the Cooling Water outfall and sewage discharge plant.

The consequences of total loss of the cooling water system, as a result of flooding, have been considered. In such circumstances adequate, protection against loss of essential safety functions has been demonstrated to remain available.

The coincidence of extreme rainfall combined with an extreme tide and surge event have also been considered. It is considered that the ability of the site drainage system will not be impaired under such conditions.

3.1.2.2 Main design and construction provisions

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

During construction, the general level of the Oldbury site was raised several metres above that of the surrounding land. Within the site, roads are then slightly below that of the building thresholds so water on site would drain away from buildings, via roads and site drains.

3.1.2.3 Main operating provisions

Main operating provisions to prevent flood impact to the plant.

Many hours notice of extreme tides and surges would be expected. Precautionary actions could, therefore, be taken to mitigate the risk of flooding.

Plant Operating Instruction 2.8 specifies actions to be taken in the event of severe weather (including anticipated high tide and storm surge combinations). This includes provisions to mitigate the risk of flooding such as:

- closing external doors and windows;
- checking and clearing roof drains to avoid effects from drain blockages;
- deploying sand bags at entrances to the cooling water pump house;
- inspect cooling water forebay area hourly (the area most vulnerable to flooding);
- carrying out weather tightness checks on buildings.

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.

Coincident loss of external power supplies has not been explicitly considered within the Oldbury external flooding safety case nor has post-event availability of personnel and supplies from off-site. Ultimately, 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 boiler feed system has dedicated diesel pumps with their own starter batteries. The REIC system has its own dedicated diesel generator. 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. On longer timescales, it is assumed that necessary supplies and personnel will be available from off-site sources.

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 shutdown state, as well as systems and structures designed for flood protection remain in faultless condition.

The plant is subject to routine maintenance, inspection and testing as required by the nuclear MS, which lists those ongoing activities that are necessary to support the site safety case. This is implemented in accordance with MCP 19 “Management of Maintenance Work” and MCP 13 “Surveillance and Routine Testing of Plant Items and Systems”. Specific procedures include S-268 "Inspection and Assessment of Nuclear Safety Related Civil Structures to Comply with Site Licence Condition 28", whose scope specifically includes "sea and river flood defences that protect the licensed site from flooding".

As necessary, the plant and safety case is modified or updated in accord with MCP-021 "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 response to operating experience elsewhere have been implemented.

A plant walkdown specifically to consider flooding vulnerability has been carried out, covering Cooling Water plant, EBFPs, turbine hall basement, GT house, circulator hall and basement and fuel storage ponds.

A review of the Plant Operating Instructions (POIs) for dealing with a flooding event has also been completed.

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.

Equipment for use in an emergency that, is not routinely proven by use for generation, is inspected, tested and maintained as specified in the MS. This includes fire fighting equipment, Boron Dust Injection equipment, Iodine Adsorption Plant, emergency lighting, communication equipment and emergency equipment.

3.1.3.3 Potential deviations from licensing basis

Potential deviations from licensing basis and actions to address those deviations

There are no known shortfalls against the DBF from external sources.

A consideration of the cast iron pipework safety case highlighted the possibility for a main cooling water pipe failure in the turbine hall basement. Under the previous protection scheme, which held the main cooling water valves open to provide a source of cooling water for reactor auxiliaries this could lead to flooding of the turbine hall basement dependent on the state of the tide. At the highest tides this could extend to the reactor building basements through pipe and cable tunnels and hence affect station batteries. To overcome this, a modification has been completed to trip the main cooling water pumps and close the cooling water valves on detection of 10 to 15 cm of water on the turbine hall basement floor.

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.

During construction, the general level of the site was raised several metres above that of the surrounding land. The site roads are also slightly below that of the building thresholds so water on site would drain away from buildings and via roads and site drains.

Building/Facility	**Height in metres above Ordnance Datum**	**Comment**
10^{-4} per annum exceedance frequency still water level	9.2	
Ground/road adjacent to sewage plant	9.296	
Sea Wall	10.210	
CW Pump Pit Entrance	10.363	
Turbine Hall	10.516	
Reactor Circulator Halls	10.516	
Reactor Control Block	10.516	
Gas Turbine House	10.516	
BUFS Pump Houses	10.516	
Turbine Hall Basement level	1.54	
Reactor Block basement level	6.6	~ 1m in these rooms would submerge batteries.
Boron Dust Plant Building	10.820	Level taken to be the same as the adjacent 132kv Switch House
Civil workshop (west end of site)	10.820	

If the water level exceeds the turbine hall/reactor building ground floor level building thresholds sufficiently to flood their basements, that is a water level approximately 1.3m above the predicted 1 in 10,000 year event level, then all on-site electrical supplies will be lost. If there is a further increase in water level across the site of between a 0.3m and 0.5m then the gas turbines including fuel pumps, bulk to day storage tank transfer pumps and the control cubicles, circulator pony motors and back-up feed system motors would be submerged rendering them unavailable without significant work even when the water receded and power could be made available again.

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.

Any internal water leak within the reactor building is directed out of the building or to the turbine hall via the pipe or cable tunnels. Batteries and switch boards in the reactor building basement are protected by bunds from water flowing to these tunnels.

The turbine hall basement is at risk from a major cooling water pipe failure especially at high tide. A trip scheme has been installed to stop the cooling water pumps and close the main cooling water valves on detection of 10 to 15cm of water on the turbine hall floor which would occur if the leak exceeded the capability of the sump pumps.

3.2.2 Potential need to increase robustness of the plant against flooding

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

Given the number of doors, windows and ventilation louvres near ground level and the interconnectivity via pipe/cable tunnels, it is not considered practical to protect buildings individually. Constructing a wall all around the site would be possible but not within the remaining generating life of the station. As water would soak through the ground, any such scheme would have to include active pumping to keep the water out.

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.

Extreme weather conditions against which safety-related structures, systems and components have been assessed as part of the Periodic Safety Review process are summarised below.

High Winds

Nuclear safety-related structures have been assessed against naturally occurring high winds having maximum gust speeds between 36m/s and 52m/s, depending on assumed wind direction. These compare with a maximum regionally recorded gust speed of 43m/s. The assessment wind speeds are based on guidance given in British Standards adjusted to the desired return period (see Section 4.1.1.3).

Extreme Ambient Temperatures

The range of ambient temperature against which the performance of nuclear safety-related plant has been assessed is -20°C to +40°C. The range of temperatures recorded in the region is -20.1°C to +34.3°C. It should be noted that while a range of temperatures is assumed for assessment purposes the safety case does not, in general depend on precise ambient temperature values. The primary protection against such events is via pre-emptive actions taken in anticipation of extreme conditions.

Heavy Rainfall

See Section 3.1.1.1.

Snow

A uniform (undrifted) extreme building roof snow load of 0.6kN/m^2 has been assumed for assessment purposes based on guidance in British Standards. This corresponds to an approximate 0.4m snow covering (although this depends on snow density). Where necessitated by roof geometry, snow drift loading has been considered. In the worst case the drifted snow load is 6.6kN/m^2.

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.

The extreme weather conditions described in Section 4.1.1.1 above form the basis of the current Oldbury safety case established through the 10 year Periodic Safety Review process.

4.1.1.3 Assessment of frequency

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

With the exception of minimum ambient temperature, all extreme weather conditions (maximum ambient temperature, high winds, rainfall and snow loading) correspond to an exceedance frequency of 10^{-4} per annum. The exceedance frequency for the assumed minimum ambient temperature has not been estimated (see discussion in Section 4.1.1.1 for safety case basis).

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;

- extreme winds, extreme precipitation, lightning
- extreme winds, driven snow and snow loadings on buildings;
- extreme low temperatures plus snow and ice.

It was confirmed that the combined hazards did not present any significant additional threats to nuclear safety more onerous than when considering the hazards 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.

The existing safety case assesses that extreme weather conditions present very little threat to nuclear safety at Oldbury. Reactor trip, shutdown and hold down safety functions cannot be credibly threatened by extreme weather.

The most significant risk from beyond design basis extreme weather events is associated with structural damage caused by extreme winds. It is conceivable that sufficiently severe consequential damage could cause a breach of the reactor containment by secondary missile impact against reactor pressure boundary components. Such damage could also undermine post-trip cooling capability. The scenarios are similar to those identified in Section 2.2.1.

For reasons similar to those discussed in Section 2.2.1, it is not possible to estimate, on the basis of existing assessments, severe weather event severities at which limiting damage scenarios would occur. However, it is judged that a substantial margin exists beyond the design basis.

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 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

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 Nuclear power reactors

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 Oldbury off site power supply is given in sections 1.3.5 and 1.3.6

In the event of a complete loss of Grid electrical supplies, the 3.3kV Essential Electrical supplies are supported by the automatic starting and connection of GTs onto the dead 3.3kV boards. There are three GTs and normally two would start and connect automatically and the third would start and be available for manual connection.

A single GT is capable of supporting the required post-trip cooling plant loads for both reactors with one reactor having a depressurising fault.

On loss of Grid supply, the automatic starting and connection of the GTs takes approximately 90 seconds. During this period when the 3.3kV and associated 415V ac supplies will be dead, station batteries provide no-break support. Each GT is supported by a dedicated 110V starting and 24V control battery.

475Vdc systems support Safety MG sets for the operation of Guardlines, Instrument MG sets for essential indications, Computer MG sets for alarm systems and Gas Circulator Seal and Lubricating oil pumps. There are three 475Vdc boards which can be interconnected. Each board has a dedicated battery and charger and any one battery can support all three boards if required. Each battery is capable of carrying out this emergency duty for 90 minutes.

The 240Vdc system supports emergency lighting, turbine essential auxiliaries and auxiliary equipment on boilers and gas circulators. It also provides power to close 11kV switchgear and thus, re-establish supplies from the grid following loss of grid. There is one 240Vdc switchboard supported by two batteries, each battery is capable of supporting the system for 60 minutes.

The 110Vdc system provides supplies necessary for the operation of the majority of plant items associated with the Essential Supplies, including rectifier controls, MG sets and closing and tripping coils for ACBs (Air Circuit Breakers).

The system consists of two distribution boards which can be interconnected, each supported by a dedicated battery and charger. Each battery is capable of supporting the station emergency load for at least 2 hours.

The 50Vdc system consists of a centralised Control Distribution Board providing remote operation of the major items of plant from the CCR and an Alarms Distribution Board which provides for the alarm fascias. Each distribution board has two batteries and two chargers with an interconnector between the two boards. In the event of a failure of supplies from the Centralised Control Distribution, local operation of the plant is possible.

Loss of Grid supplies and subsequent loss of 11kV supplies represents an initiating event as this would result in a Reactor trip and a subsequent demand on plant claimed for protection.

Forced cooling utilising Gas Circulators and Emergency Boiler Feed Pumps is dependent on the availability of the 3.3kV supply system supported by at least one Gas Turbine. There is a POI requirement for a minimum fuel stock sufficient, with a 10% contingency, to run two GTs at a nominal 2MWe each, for 24 hours.

Grid derived electrical supplies are not required to establish a satisfactory minimum level of post trip cooling at Oldbury.

If Grid supplies and GT supplies fail, Reactor cooling is achieved by use of the back up feed system to provide feedwater to the boilers.

(These durations are all based on having two Operational Reactors shutting down from full power and are pessimistic for Oldbury given that in June 2011, Reactor 2 was permanently shutdown.)

5.1.1.1.2 Autonomy of the on-site power sources and provisions taken to prolong the time of on-site AC power supply.

In the event of an extended loss of grid supplies at Oldbury, POI 2.12 describes operator actions necessary to preserve fuel stocks for the Gas Turbines. This includes shutting down to minimum plant requirements and isolating one battery from each system to avoid undue discharge and to assist in the recovery of normal plant conditions on restoration of grid supplies.

Additional kerosene fuel stocks for Gas Turbines would be sourced on an urgent basis, possibly from the nearby Bristol International airport. In an emergency, if kerosene fuel is not available the GTs could be run on ordinary diesel.

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.

In the event of a loss of off-site power (grid) and loss of the GTs as back up supplies, there are no permanently installed AC power sources available that could support decay heat removal or cooling of spent fuel. There are

also no arrangements in place to facilitate the procurement of an alternative AC power source and its connection into the system.

A load bank has previously been connected to the standby GT for testing purposes. This connection point still exists and could be used to connect a standby generator

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

With no source of AC power, there are no provisions for recharging batteries once discharged. For the support of decay heat removal, the 475Vdc batteries are key, as they provide supplies to Gas Circulator lubrication and seal oil pumps; however, with no AC power the Gas Circulators will not be available, so the support from the DC systems is irrelevant.

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

As there are no permanently installed diverse back-up AC power sources. This situation is the same as that described in 5.1.1.2.

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

Currently there are no plans in place to procure and connect AC power supplies from transportable or dedicated off-site sources. The possibility of connecting to dedicated off-site sources in such extreme circumstances is considered an unlikely option given the location of the site. Procurement of transportable diesel generators on a hire basis is the most likely option if AC power cannot be restored on site otherwise. There are a number of national companies with diesel generators available and Oldbury does hire from external companies for small applications when maintenance outages of service supplies is planned.

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.

With no dedicated connection points, the competence of shift staff to make the necessary electrical connections into the system of transportable AC power sources would be limited. The most likely arrangement is for a small team of electricians and engineers to be on site and, once the transportable AC power source is arranged, the connection requirements would be developed and implemented. In the extreme, the connections would involve a degree of innovation and would be coarsely applied such that supplies could be available within 24 hours following delivery of the transportable AC power source.

5.1.1.3.4 Time available to provide AC power and to restore core cooling before fuel damage: consideration of various examples of time delay from reactor shutdown and loss of normal reactor core cooling condition (e.g., start of water loss from the primary circuit).

For an intact reactor circuit adequate cooling to prevent fuel damage can be achieved by natural circulation of the pressurised CO_2 with water feed to the boilers. Boiler feed can be achieved using BUFS which has its own

independent diesel driven motors so no AC supplies are required. There would be up to 24 hours to restore boiler feed.

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

Electrical power is not required to cool a reactor with an intact primary pressure boundary. However consideration will be given to increasing the resilience of the on-site electrical system and to the availability of Gas Turbine fuel stocks as detailed in section 6.1.4.

Consideration OLD 3. 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.

Water is drawn from the river by four cooling water pumps which force water through culverts in the turbine hall basement, the condensers if they are in service and ultimately back to the river through the cooling water out fall. Each has a fixed coarse screen and finer rotating drum screen with back wash arrangements to prevent ingress of debris. The pump pits and drum screen chambers are independent allowing any one to be individually taken out of service and drained, if necessary, for maintenance/repair. The culvert is below river level and would remain flooded without any pumps operating thereby retaining adequate water for post trip cooing purposes.

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

In the event of loss of access to the primary ultimate heat sink it would be necessary to trip the reactor. Once shutdown sufficient water can be drawn from the cooling water culverts to meet post trip cooling requirements. Also a shutdown reactor can be satisfactorily cooled without access to cooling water from the river. For a reactor with an intact primary pressure circuit, adequate cooling to prevent fuel damage can be achieved by natural circulation of the pressurised CO_2 with water feed to the boilers. Forced circulation of air or CO_2 at atmospheric pressure would also provide adequate core cooling with the boilers fed. Boiler feed can be achieved using the Back Up Feed System which has its own independent diesel driven motors so no AC supplies are required. Adequate cooling can be achieved with the water/steam being discharged direct to the atmosphere as the alternate heat sink.

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

For a pressurised reactor boiler feed, including a route for discharge to atmosphere, has to be established within 24 hours to prevent fuel damage. If there is advanced warning of the problem, such that the reactor can be shut down before loss of access to the primary ultimate heat sink occurs, then cooling the core rapidly and as far as possible would extend the time before fuel damage would occur as the graphite core has a large thermal capacity and would take time to be reheated to a temperature of concern.

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.

Water from any available source as discussed above would be pumped in to the boilers using any standard fire pump or equivalent. Connecting in points are installed on external walls of the reactor building. Water/steam is then discharged direct to atmosphere from the boilers.

5.1.3.3.2 Time available to recover one of the lost heat sinks or to initiate external actions and to restore core cooling before fuel damage: consideration of situations with various time delays from reactor shutdown to loss of normal reactor core cooling state (e.g., start of water loss from the primary circuit).

There would be from 4 to 24 hours in which to establish some feed to the boilers depending on the state of pressurisation of the primary cooling circuit.

5.1.3.4 Loss of the primary ultimate heat sink, combined with station black out (i.e., loss of off-site power and ordinary on-site back-up power source).

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

Water loss from the primary circuit is not an issue for a gas cooled reactor. The equivalent is loss of the pressurised CO_2 primary coolant. This will occur if the pressure circuit is breached physically or if the primary circuit pressure increases to more than the Gas Safety Relief Valve set pressure and the valves lift and stick open and cannot subsequently be re-seated or isolated manually. The most likely cause of an over pressurisation is the failure of a boiler tube internal to the pressure vessel. Physical damage could occur as a direct result of the earthquake

5.1.3.4.2 External actions foreseen to prevent fuel degradation

The principle action required is to establish a supply of feed water to the boilers. This can be on a once through basis, with discharge of the steam/water direct to atmosphere until the shut down cooling loop can be established to enable the water to be re-circulated. Re-establishing a shutdown cooling loop would allow high quality water to be retained in the boilers.

There would be from 4 to 24 hours in which to establish some feed to the boilers depending on the state of pressurisation of the primary cooling circuit.

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

The principle action required is to establish a supply of feed water to the boilers. The most vulnerable aspect of this is the Back Up Feed System pumps themselves and the supply of good quality water for use in the boilers.

Consideration OLD 2. Consideration will be given to increasing the resilience of the Back-Up Feed System.

The availability of feed water stocks is being considered as part of the review of consumables proposed in section 6.1.4.

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

The fuel storage ponds are not at an immediate risk in the event of a loss of electrical supplies. On occasions when the pond chiller plant has been switched out for maintenance/refurbishment, the pond temperature was observed to increase by <1^{o}C per day. Current pond stocks, and hence heat burden, are very low and, with one reactor permanently shut down, unlikely to approach previous levels again. The pond is tolerant to very extended periods of loss of cooling and passive cooling alone may be sufficient, many weeks are therefore available to establish alternative electrical supplies, cooling arrangements or to provide pond make-up.

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

Not considered necessary in light of timescales available to re-establish supplies post event.

5.2.3 Loss of the ultimate heat sink

The pond water cooling plant rejects heat to the atmosphere; loss of ultimate heat sink is not therefore an issue.

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

Any loss of pond water due to evaporation could easily be made up from a water tanker parked nearby with a hose running in to feed water to the pond under gravity. As the top of the pond wall is below the surrounding site ground level simply pumping water in to the ponds building, in the event access is not possible would eventually result in refilling the ponds once the surrounding voids and plant rooms were full. A simple rigid pipe pushed in from out side the building over the pond wall would allow the pond to be topped up from any ground level water source while allowing personnel to remain at a greater distance from the pond itself if the radiation levels in the immediate vicinity were elevated.

Consideration OLD 12. Consideration will be given to enhancing the resilience of spent fuel pond equipment 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 shift staffing requirements for normal site running are defined in OLD/PODI/11/032. The site operates a 5 shift pattern. The requirements for a normal shift compliment are made up of 22 members. A minimum number of 18 members of staff will always be maintained. As well as having the correct number of staff, they have to also be able to cover certain roles and responsibilities and therefore need to be suitably qualified and experienced (SQEP) in the role they are brought onto site to cover.

6.1.1.2 Plans for strengthening the site organisation for accident management

During an incident, a number of additional staff can be called upon to assist shift emergency teams both during normal working hours and outside normal hours. Eleven roles are identified and groups have been set up to provide 24 hour cover. In total, 65 staff are on a rota covering these positions. Further additional roles such as the “Muster Coordinator” and “Damage Repair Advisors” have been identified but are not on a fixed 24/7 rota; however, identified staff receive training in these emergency scheme positions and can be called if necessary. Systems are in place to call staff using pagers, with pre-defined messages, as well as mobile and fixed phones. Documents listing stand-by staff together with their contact details are readily available for shift personnel to use. A document, OLD/MCP/26/002, providing guidance for stand-by staff, is available. This covers their responsibilities when on call.
Consideration has also been given to operating long term with reduced availability of shift staff, in the context of a flu pandemic, for which a 4 and a 3 shift rota pattern was drawn up.

6.1.1.3 Measures taken to enable optimum intervention by personnel

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 attendance at the alternative off-site Emergency Control Centre (ECC). Arrangements include for authorising increased personal dose limits under REPPIR, provision of specialist equipment and Personal Protective Equipment (PPE).

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.

(iii) Provide the requisite technical advice on off-site issues to all stakeholders in the Strategy Coordination Centre (SCC) 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 system 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 co-operation from other nuclear companies.

6.1.1.5 Procedures, training and exercises

Procedures

The plant is normally operated under the Plant Operating Instructions (POIs) and supporting lower tier documentation. POI part 2 gives advice on operations in design basis fault conditions, including responses to hazards. The sections of POI 2 include:

- POI 2.5: Loss of Coolant.
- POI 2.7: Natural Circulation (action in the event of loss of forced circulation).
- POI 2.8: Severe Weather (flood, wind, extreme temperatures, etc).
- POI 2.11: Grid Disconnection.
- POI 2.12: Loss of 11kV/Restricted 3.3kV Supplies.
- POI 2.14: Loss of Feed.

- POI 2.17: Seismic Event.
- POI 2.19: CCR Untenable.

If an event is not adequately controlled through use of POIs, 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 POIs 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, this includes pre-defined training found in emergency scheme training specs.

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 attendance at the alternative off-site ECC.

6.1.2 Possibility of using 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 shares a Beyond Design Basis Accident Container set in a central location in the UK that can be transported to any affected site. These containers are equipped with Command and Control, fire fighting, reactor cooling and contamination control materials.

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

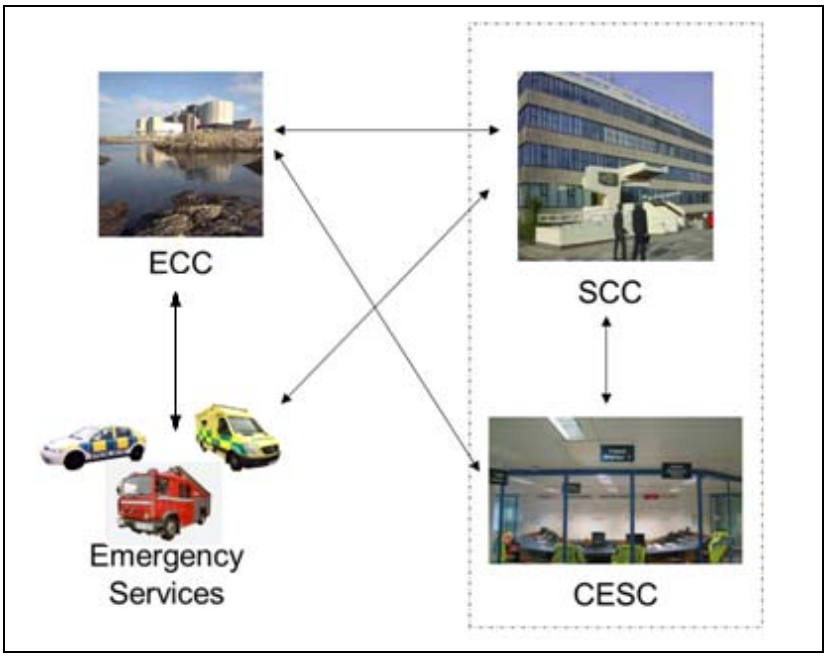
No special on-site arrangements for the provisions of supplies are in place; normal procurement arrangements would be employed. In an emergency, procurement of materials would be dealt with by the CESC.

6.1.2.3 Management of radioactive releases, provisions to limit them

Limiting any radioactive release will be a high priority during any incident. Particular attention has been paid to penetrations emanating directly from the reactor primary pressure circuit and a document has been produced listing all penetrations that do not have a direct means of isolation. This document, “Pressure Vessel Containment Techniques” also includes suggested tools and equipment required to seal such penetrations. The size of potential holes in specific areas and floors of each reactor has been matched to repair equipment e.g. bungs, pipe clamps, sealing compounds etc which have then been placed close to said penetrations. Checks are made periodically to make sure all the correct equipment remains in place and fit for use. Other general damage repair equipment is available and stand-by staff have been trained in its use. Deployment is practised during annual shift emergency exercises.

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 SCC, the CESC and the responding emergency services (see diagram).



Magnox Communications Systems

The Magnox telephone system for operating sites is designed to be resilient and function through any single point failure. Operating sites have two telephone exchanges, physically separated and connect to the Public Switched Telephone Network (PSTN) via diverse routes[2]. Telephones in the key response centres are divided between the two exchanges so that failure of an exchange will not leave the room without at least some working telephones. The telephone exchanges are connected to robust electrical supplies and have battery backup with a design period of not less than 300 minutes.

The exchanges at operating sites are connected to the PSTN using a Secure+ link which provides each exchange with duel separated routes to the public network.

A link is provided to the Government Telephone Network (GTN).

Communications in a Crisis: Declaration and Promulgation

Oldbury would declare a Site Incident or Off-site Nuclear Emergency and promulgate 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. Back-up systems exist in the event of any component of the system failing.

[2] BT offer three types of links from site to the national network infrastructure.

Standard	Single link provided
Secure	Dual fibre routed from a single POP. (Point of Presence)
Secure+	Dual fibre routed from separate POPs and separation of routes guaranteed end to end (unless specified during survey)

The minimum infrastructure required to alert company responders is a single working phone on site, the PSTN and the pager system to be running.

Alerting of other organisations requires a functioning telephone 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

Oldbury would communicate 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 Oldbury can communicate with the police and other emergency services:

- Emergency Services are alerted and informed using the 999 system via the Magnox telephone system and the PSTN.
- Further information is provided by FAX.
- The Emergency Services each send an Officer to the site's ECC. These officers will be able to communicate with their Headquarters by:

1. Telephone
2. Fax
3. Service mobile phone
4. Service Airwave radio

- There are also many mobile telephones on 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 telephones used within Magnox are registered on the Mobile Telephone Privileged Access System (MTPAS)

Communications in a Crisis: CESC to/from Oldbury

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 6hr back-up.

Cabling between the PABXs and the CESC telephones follow separate routes as far as practicable. Separate routes are provided such that any single fault will not affect more than 50% of the connections.

CESC DDI service is provided to CESC telephones which are separate from the normal site DDT service, both in numbering range, lines and carrier (PTOs). Each PABX has CESC 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 carriers (PTO's).

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 terminating network node is not 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 EDF 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 telephones 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 by the CESC, SCCs, 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, Food Standards Agency (FSA.)

Tiims runs on a dedicated server with a back-up available.

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

- A basic rate 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 to improve the resilience of Critical National Infrastructure (CNI) to disruption from natural hazards.

Critical National Infrastructure (CNI)

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 in this programme and within the programme were 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.

Land immediately surrounding the site, including the access road, is below the level of the site and the sea wall and would be flooded before the site. As the site is higher than the surrounding area this could result in the site being islanded. There is only a single approach road for the last km to the site, and the only alternatives for the last ~5km are narrow lanes. There are no major bridges or other structures likely to collapse between the site and the main road network. The road does cross two small drainage culverts and there are many trees along the route. The ability of responding staff, Emergency Services and essential supplies and equipment to reach the site in a timely manner could be affected until the roads are cleared.

Oldbury has sufficient people on site at all times to initiate a response to an emergency, see section 6.1.1 Personnel on shift include a person authorised to act as Emergency Controller with authority to respond as they deem necessary; casualty rescue/first aid capability and damage assessment/repair capability.

The site relies on support from personnel off-site at the time of the incident and Emergency Services for medical support, casualty rescue and fire fighting. It would present difficulties if this aid could not be sent in by road.

Oldbury has damage assessment and repair teams, made up from shift staff, able to fight fires and effect repairs in hostile environments under BA but these people would quickly become exhausted if relief teams could not reach the site.

There is a designated helicopter landing site adjacent to the power station boundary and on the same raised level as the site.

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.
- 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.
- Two telephones to the National Grid telephone system located in the CCR.
- A direct link to the local (Thornbury) police station.

A total failure is highly unlikely.

<u>Potential Impact of widespread disruption and mitigation</u>

- Loss of mains electricity for prolonged period

  Should be able to promulgate alert before the battery back-up fails.

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

- Loss of masts for mobile telephones and Airwave

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

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

  Use of mobile telephones (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 two of these on operating sites with the design intent that it is unlikely that they would both be damaged in any reasonably foreseeable event.

A mobile PABX is available for deployment if both PABXs fail.

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 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 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 doserate, 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. The function of the ECC could be transferred to other locations on site 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, an alternative facility would be nominated and 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 is in the control block which is connected to the two reactor buildings and the centre block. The control block building would be subject to structural collapse at a magnitude of earthquake below that necessary to damage the more massive reactor buildings and centre block structure. Whilst there is no secondary control room at Oldbury, there are indications in the REIC, which can support local plant operations.

The minimum actions required would be:

- To cut the electrical supplies to the guardlines or the control rods. In all probability this would have already occurred as a result of the initiating fault.
- To establish boiler feed using the Back Up Feed System. This is all done manually and external to the reactor building.
- To open a vent path to atmosphere from the boilers for the water/steam prior to establishing a re-circulating shut down cooling loop

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). An alternative for each facility is available on-site should the primary facility be unavailable. In addition, there is an off-site ECC from which the Emergency Controller and his team could coordinate the response to an incident.

The CCR provides centralised control and monitoring of the plant. Alternative monitoring facilities only are available in the event the CCR becomes untenable. All plant can be operated local to the plant provided access is possible. Access could therefore be required to any area of the reactor building depending on the location(s) of the fault. In the event of a significant hot gas/steam release, it is not envisaged that an entry would be attempted until the reactor had fully depressurised. BA and protective clothing is provided to address the issues of gas and contamination but not for working at excessively elevated temperatures.

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. In the event neither of the on site Emergency Control Centres are tenable, the emergency team can function from an alternative facility.

6.1.3.7 Unavailability of power supply

Oldbury has diverse and redundant systems providing a resilient electrical system. A stand-alone back-up generator can be used to power the ECC/ACP/AACP if necessary.

6.1.3.8 Potential failure of instrumentation

Instrument readings and alarms are primarily displayed in the CCR. A selected sub-set of reactor parameters are also available to the Duty Standby Physicist in the ECC. A specified set of essential instrumentation provides input to the REIC via hardened and diverse routes.

6.1.3.9 Potential effects from the other neighbouring installations at site

The nearest neighbouring site to Oldbury is Berkeley Power Station, some 5km up river, which is shutdown and defueled. All the fuel has been removed from the Berkeley site so it poses a negligible risk to Oldbury. There are no other nearby facilities that threaten post-event recovery.

Aircraft impact is also addressed in the Safety Case with the overall frequency of an aircraft impact estimated to be less than 10^{-6} per year, with the frequency of a crash resulting in a radiological release being even less. There is no reactor protection claimed specifically for this hazard as the risk from an aircraft impact is considered to be sufficiently low. Reactor protection would depend on the plant affected. However, vulnerability of the station has been reduced substantially by the installation of the Back Up Feed System and the Remote Emergency Indication Centre.

6.1.4 Measures which can be envisaged to enhance accident management capabilities

Measures that might be taken to enhance accident management capabilities can be considered under three headings:

- More people
- More training
- More equipment

Consideration OLD 5. Consideration will be given to enhancing the resilience of plant monitoring systems.

Consideration OLD 6. Consideration will be given to enhancing the availability of beyond design basis equipment.

Consideration OLD 7. Consideration will be given to providing further equipment to facilitate operator access around the site.

Consideration OLD 8. Consideration will be given to reinforcing the training for staff who may be required to respond to extreme events

Consideration OLD 9. Consideration will be given to enhancing on site arrangements for Command, control and communications.

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

Consideration OLD 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

The reactor core is contained within a massive, reinforced concrete pressure vessel on solid foundations. The flat vessel top is 6.7m thick, the cylindrical sides 4.6m thick and the flat base 6.1m thick. 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 system (PVCS). There are penetrations through the top and sides of the vessel for access to the fuel, water and steam pipes, circulators and other ancillary gas and instrumentation connections. There are no penetrations through the base, but there is a narrow 2.9m long tube from the inside of the vessel.

The Severe Accident Guidelines (SAGs), see Section 6.1.1.10, give detailed advice on the performance and potential mitigating measures for the pressure vessel in the event of a core meltdown. There are no voids below the vessel to allow activity release.

There is no separate secondary containment.

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 (<700kWm^{-3}), such that significant fuel damage or meltdown is very unlikely. Individual channel damage / melt was experienced at Magnox designs in other countries, but the Oldbury 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 melt is given in the plant operating instructions (POIs), Symptom Based Emergency Response Guidelines (SBERGs) and the Severe Accident Guidelines (SAGs), see 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. The normal vessel blowdown route and the gas safety relief valves discharge to atmosphere outside the building and would not result in a build up of Hydrogen.

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 gas and/or steam to atmosphere via particulate filters. The filters on Reactor 1 (the at-power reactor) have bursting discs which will ensure adequate steam/gas relief in the event the filters block.

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 adsorption plant if there was any failed fuel in the core. Advice on preventing reactor over-pressurisation is given in POIs, 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.

In the event insufficient control rods have entered the core to ensure long term hold down then the Boron dust system can be deployed. This requires the reactor to be depressurised and a circulator to be available to operate on pony motor drive. The Boron dust would ensure the permanent hold down of a reactor on which it is deployed.

Reactor 2 re-criticality is no longer an issue as all rods except the safety group, are fully inserted.

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

As described in Section 6.1.5, the massive pressure vessel is part of the concrete pressure vessel Magnox design, which assists in the prevention of molten fuel reaching the environment.

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

This is not applicable to Oldbury 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 turn over 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 depressurised 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 Oldbury as there is no containment area outside of the concrete pressure vessel.

6.2.6.2 Operational provisions

This is not applicable to Oldbury 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 Oldbury 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 Oldbury 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

In common with other gas cooled reactor designs, Oldbury does not have a secondary gas tight containment. In the event of a failure of the primary gas circuit, the design objective is to vent the gas to atmosphere to prevent over-pressurisation of the reactor building and access of hot gas to temperature sensitive plant. To achieve this, various vents, louvres and blow-out panels open or close on detection of local high temperatures or pressures.

In the unlikely event of a slow leak in or anticipated failure of the reactor primary coolant gas pressure boundary, coincident with failed fuel cans leaking fission products into the coolant gas there is an Iodine adsorption plant through which the reactor gas can be vented to reduce the quantity of radioactive Iodine being discharged to the atmosphere.

6.3.1.2 Operational provisions

Operating Rules ensure that reactors are operated in a safe manner.

The Maintenance Schedule ensures that the reactors and support equipment are well maintained.

The Safety Case and Modification processes ensure that any proposed changes to the design and operation are carefully considered.

SBERGs provide advice about dealing with events that are outside or not controlled by the normal Plant Operating Instructions. SAGs provide advice on preventing or terminating releases in the event of a degraded core incident.

An emergency scheme exists to provide a prompt and appropriate response to any emergency.

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

6.3.2.1 Hydrogen management

No specific hydrogen management equipment is provided as it is not credible to uncover fuel due to nuclear heating, see Section 1.3.3.2. It is unlikely that water would be lost by other means, eg. loss of pond integrity, as the pond is set below ground level. The ponds building is served by a contaminated ventilation system and is sufficiently air tight that it normally operates at a slight negative pressure. However if the ponds hatch cover is opened to allow ponding of a irradiated fuel transport flask this negative pressure cannot be maintained. Any hydrogen build-up would therefore be removed from the ponds building by this ventilation system.

In the event of loss of power supplies to the ventilation system the ponds hatch cover could be manually opened or the large maintenance access doors opened to allow natural ventilation to remove the Hydrogen.

6.3.2.2 Providing adequate shielding against radiation

As discussed under Section 6.2.2.1, it is not credible to uncover fuel due to nuclear heating. It is unlikely that water would be lost by other means, eg. loss of pond integrity, as the pond is set below ground level. If water were lost, measures would be taken to restore water cover in the ponds, see Section 1.3.3.2. Loss of water and hence shielding would be indicated by gamma alarms in which case personnel access to the building would be restricted.

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

Damage to the spent fuel in the ponds by overheating due to evaporation of the water is extremely unlikely. Physical damage to the spent fuel following collapse of the structures above the ponds in a beyond design basis event could not be discounted. Provided the fuel remained submerged, the radioactivity release rates would not pose a significant problem.

Used Magnox fuel does require cooling but not necessarily to the extent of other fuel designs.

Response would be dominated by a desire to keep the fuel wet to cool it and, ideally, covered in water to provide shielding. There are diverse sources of water on-site and a variety of methods of pumping it into the ponds.

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

There is no specific monitoring of the temperature of the fuel as it is not credible that it could be exposed. Pond water temperature is monitored in the pond water cooling circuit and displayed local to, but out side, the ponds building. In the event electrical supplies are lost the pond water cooling pumps will shutdown, and with no flow, these would not indicate actual pond water temperature.

There are high and low pond water level alarms that display in the CCR. There is also a trip on all pond water treatment pumps on low pond water level.

Monitoring of any increased activity in the ponds building is provided by an EBERLINE situated outside the ponds building but sampling from inside it. There are also gamma monitors that would alarm on low pond water. Neither system would work on loss of electrical supplies.

Due to the very long timescales for the water to increase in temperature (weeks), ad hoc temperature monitoring could readily be deployed.

6.3.2.5 Availability and habitability of the control room

The Central Control Room (CCR) is manned 24 hours a day. Essential operations can be performed from here during an emergency which can limit the need for intervention by personnel in hazardous areas, e.g.

shutting/opening of valves. Safe shut down of the reactors and checks that all rods have entered the reactor can take some time and if possible, checks should be completed before leaving the CCR. To enable CCR staff to do this with the potential for CO_2 to enter the control room, installed breathing apparatus is available. This equipment also features the ability to double up as an escape set when evacuation is required. The system comprises two banks of three air cylinders (one being a spare), six hose reel air feed lines and six portable BA sets. The BA sets are initially connected to the fixed air system for longer duration use. There is potential for six operators to stay in the CCR under air for over an hour.

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

It is not considered practical to attempt to terminate a release from a non-isolatable breach of the pressurised CO_2 coolant gas circuit. Temperatures in the vicinity of the escaping gas would prevent access. Provided no fuel is physically damaged in the initial event, the radioactivity released by discharging the coolant gas is minimal.

Once a reactor has fully depressurised, an attempt would be made to seal the breach. This would firstly exclude air and secondly allow a small re-pressurisation in order to enhance cooling by either forced or natural circulation.

If cooling cannot be restored, the fuel will eventually overheat and once the Magnox can fails, activity will be released to the gas circuit. Cooling the boiler and pressure vessel liner will encourage some activity to plate out. If water is leaking in to the circuit from failed boiler tubes, then the circuit will re-pressurise or continue to discharge gas/steam. In this scenario the SAGs contain suggestions on the construction of ad-hoc filters through which reactor gas could be allowed to escape to minimise release of activity.

7 Glossary

AACP	Alternative Access Control Point
ACB	Air Circuit Breakers
ACP	Access Control Point
ALARP	As Low As Reasonably Practicable
BA	Breathing Apparatus
BUFS	Back Up Feed System
CCR	Central Control Room
CESC	Central Emergency Support Centre
CNI	Critical National Infrastructure
CO_2	Carbon Dioxide
DDI	Direct Dialling In
DECC	Department of Energy and Climate Change
DfT	Department for Transport
EBFP	Emergency Boiler Feed Pump
ECC	Emergency Control Centre
FSA	Food Standards Agency
GT	Gas Turbine generator
GTN	Government Telephone Network
HPA	Health Protection Agency
ILW	Intermediate Level active Waste
ISDN	Integrated services digital network
LAN	Local Area Network
LLW	Low Level active Waste
LV	Low Voltage
MBFP	Main Boiler Feed Pump
MTPAS	Mobile Telephone Privileged Access System
MG	Motor Generator
MS	Maintenance Schedule
NIAS	Nuclear Industry Airwave Service
OD	Ordnance Datum
ONR	Office for Nuclear Regulation
PABX	Private Automatic Branch Exchange
POI	Plant Operating Instruction
PPE	Personal Protective Equipment
PSA	Probabilistic Safety Assessment
PSTN	Public Switched Telephone Network
PTO	Public Telephone Operators
REIC	Remote Emergency Indication Centre
REPPIR	Radiation Emergency Preparedness and Public Information Regulations
RFT	Reserve Feed Tank
SAG	Severe Accident Guidelines
SBERG	Symptom Based Emergency Response Guidelines
SCC	Strategic Coordination Centre
SERS	Site Event Reporting System
SQUG	Seismic Qualification Utility Group
Tiims	The Incident Information Management System
TRU	Transformer/Rectifier Unit
UK	United Kingdom
UPS	Uninterruptable Power Supply
WAN	Wide Area Network

TABLE 1 List of Considerations Identified for Oldbury Site

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

Reference	Section No.	Consideration
OLD 1	2.2.4	Consideration will be given to enhancing the methods and equipment for primary pressure circuit sealing.
OLD 2	5.1.4	Consideration will be given to increasing the resilience of the Back-Up Feed System.
OLD 3	5.1.2	Consideration will be given to increasing the resilience of the on-site electrical system.
OLD 4	2.2.4	Consideration will be given to providing a facility for the injection of Nitrogen to support reactor hold down.
OLD 5	6.1.4	Consideration will be given to enhancing the resilience of plant monitoring systems.
OLD 6	6.1.4	Consideration will be given to enhancing the availability of beyond design basis equipment.
OLD 7	6.1.4	Consideration will be given to providing further equipment to facilitate operator access around the Site
OLD 8	6.1.4	Consideration will be given to reinforcing the training for staff who may be required to respond to extreme events
OLD 9	6.1.4	Consideration will be given to enhancing on site arrangements for command, control and communications.
OLD 10	6.1.4	Consideration will be given to providing additional stocks of consumables for plant and personnel.
OLD 11	6.1.4	Consideration will be given to updating and enhancing severe accident management guidance.
OLD 12	5.2.4	Consideration will be given to enhancing the resilience of spent fuel pond equipment to severe events.