

Public Report on the Generic Design Assessment of New Nuclear Reactor Designs

Westinghouse Electric Company LLC AP1000 Nuclear Reactor
Conclusions of the Fundamental Safety Overview of the AP1000 Nuclear Reactor
(Step 2 of the Generic Design Assessment Process)



Contents

Foreword	3
Executive summary	4
Background	5
Introduction	6
HSE expectations for modern reactors	7
HSE expectations from the GDA process	8
The safety standards and criteria used and links to WENRA reference levels and IAEA Standards	8
Assessment strategy	8
Main features of the design and safety systems	9
Reactor shutdown	10
Emergency cooling	10
Containment	10
Retention of molten core debris	10
Summary of HSE findings	11
Quality management and safety case development arrangements	11
Standards	12
The approach to ALARP	12
The design basis analysis/fault study approach	13
The probabilistic safety analysis (PSA) approach	14
Structural integrity	14
Waste and decommissioning	15
Civil engineering and external hazards	16
Internal hazards	17
Reactor protection and control	18
Novel features	18
Long-lead items	19
International Atomic Energy Agency technical review	19
Any matters that might be in conflict with UK Government policy	19
Security	19
Public involvement process	20
Overseas regulators' assessments	21
Conclusions	22
Abbreviations	23
Annex 1: Summary of HSE's expectations for Step 2 of the GDA process	24
References	25
Contacts	27

Foreword

Our job is about protecting people and society from the hazards presented by the nuclear industry. As new nuclear power stations are now being considered for the UK, it is right for us as regulators to start our work to examine the safety and security aspects associated with those power stations' design.

We are looking at the reactors within a new process called Generic Design Assessment (GDA), which seeks to get the nuclear regulators involved at an early stage in development of proposals for new nuclear power stations. GDA allows the technical assessments of the reactors to be conducted before any specific nuclear site licence assessments are undertaken, thus identifying and resolving any potential regulatory issues before commitments are made to construct the reactors. The assessment is in several steps and includes initial and then more detailed examinations of the safety and security of the proposed reactors.

I am really pleased to be able to publish this report today and to set out the conclusions of our initial assessment of the AP1000 reactor. In summary, at this stage, we have found no safety shortfalls that would rule out its eventual construction on licensed sites in the UK.

The GDA process is new both for us and for the industry and we have set out very clear guidance on how it will be conducted. This report provides real proof that we are moving forwards in our assessment work, with the rigour, quality, and openness expected by the public.

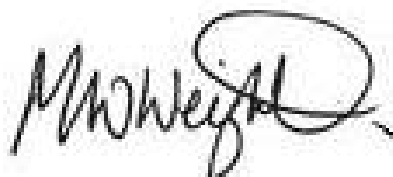
In doing this work we are setting new standards in efficiency. For example we have set up a Joint Programme Office with our colleagues at the Environment Agency so that the industry has a one-stop shop for nuclear regulatory issues.

We are also undertaking our assessment work in a more open manner than seen in the UK before. We have set up new reactor assessment information websites, put leaflets in libraries and set up an e-bulletin system. The industry has supported this open approach by putting GDA announcements in the press, making their safety documentation available on their websites, and inviting comments from the public. By acting in such an open manner, we aim to earn public confidence in our work.

We have also put ourselves up for independent scrutiny. In 2006 we underwent a review by the International Atomic Energy Agency (IAEA), and in the past few weeks, we have had an independent team look at how we have applied our GDA process. These reviews highlight that our regulation is effective and efficient, but they also help us identify areas for improvement and we will strive to learn from what they tell us.

There are challenges ahead. For example, we need more staff and we are actively recruiting to help us continue our assessment of new reactors and to ensure that people will continue to be properly protected if these reactors are eventually constructed.

If you have any comments on this report I will be pleased to hear from you, especially if you can help us in our drive for continuous improvement.



Mike Weightman
*HM Chief Inspector of Nuclear Installations and
Head of HSE's Nuclear Directorate*

Executive summary

The role of the Health and Safety Executive's (HSE's) Nuclear Directorate (ND) is to protect people and society from the hazards of the nuclear industry. To achieve this aim in the light of proposals for construction of new nuclear power stations in the United Kingdom, we have been assessing the nuclear safety and security aspects of four reactor* designs. We are examining these particular designs as they have been identified by the Department for Business, Enterprise and Regulatory Reform (BERR) as those most likely to be built in the UK, and which would thus be those that are most likely to present a hazard to the public.

The assessment being undertaken by HSE, along with the Environment Agency, is part of a new process called Generic Design Assessment (GDA). This report is an interim report on our GDA assessment and it summarises our findings to date. In parallel, the Environment Agency is publishing a separate report on its assessment of environmental aspects.

Progress through GDA does not guarantee that any of the designs will eventually be constructed in the UK. What it does do is allow us to examine the safety and security aspects at an early stage when we can have significant influence, and to make public reports about our opinions so that:

- the public can be informed about our independent review of the designs; and
- industry can have clarity on our opinions and thus take due account of them in developing new construction projects.

This new GDA process is being conducted with a high degree of openness. We have made information about our process and the reactor designs available to the public via our website www.hse.gov.uk/newreactors. Furthermore, the public have been encouraged to comment on the reactor designs and we are considering these comments, along with the responses from the designers, within our assessment.

A further advantage of the GDA process is that it has been designed to allow the nuclear regulators (HSE and the Environment Agency) to work closely together. In support of this we have set up a Joint Programme Office, which administers the GDA process on behalf of both Regulators, providing a 'one-stop shop' for this phase of the assessment of potential new nuclear power stations. We believe this is improving efficiency both for the Regulators and the Industry, and it helps to provide more effective regulation of potential hazards.

There are four steps to the GDA process. Step 1 of the GDA was devoted to preparatory work and we made a statement on our website in August 2007 that this was complete and that Step 2 was commencing.

This report is the first of our public statements for the AP1000 reactor designed by Westinghouse (WEC) and it comes at the end of GDA Step 2. The aim of Step 2 was to provide an overview of the fundamental acceptability of AP1000 within the UK regulatory regime. It was also intended that Step 2 would allow HSE inspectors to familiarise themselves with the design and provide a basis for planning subsequent assessment work.

* In this report, the word 'reactor' can be taken to cover all nuclear safety and security related areas of the proposed nuclear power station design.

To achieve these aims, HSE has undertaken a high-level review of WEC's claims for a number of different safety aspects of the AP1000 reactor, and we have considered the security aspects of the design.

In summary, we have not found any safety or security shortfalls that are so serious as to rule out at this stage eventual construction of the AP1000 on licensed sites in the UK.

As anticipated, our assessment has identified a number of topics that will need to be addressed in more detail during GDA Step 3 and Step 4, should the AP1000 proceed through to the next steps of the GDA process. In this event, we will summarise our progress on these topics in a public report at the end of Step 3 and in a final GDA report at the end of Step 4.

Background

In response to growing interest in nuclear power and in anticipation of possible applications for new build in the UK, HSE began development in 2005 of a progressive generic design assessment approach for new nuclear power stations. HSE outlined the proposed assessment process in its Expert Report on new energy technologies, which was submitted to DTI* in June 2006 to inform the Government's Energy Review. The Government subsequently asked HSE to fully develop its assessment proposals and this led to the production of guidance on HSE's GDA process for new nuclear power stations, which was published in January 2007 and updated in July 2007.

HSE considers that the GDA approach not only offers benefits to an expanding nuclear industry, but also strengthens HSE's position as an independent regulator with a focus on protecting workers, the public and society, by ensuring that it has sufficient time to address regulatory and technical issues relating to a design for a new nuclear power station, in advance of and separate from any public planning inquiries based on a site-specific proposal.

Following on from its Energy Review, the Government published an Energy White Paper in May 2007, alongside which DTI launched a public consultation on the future of nuclear power. At the same time, DTI invited interested parties to submit proposals to the Regulators for reactor designs to be subject to GDA. In the event, four designs were proposed which DTI (BERR) confirmed were suitable for the regulators to start GDA assessment. The four designs were:

- ACR-1000 (Atomic Energy of Canada Limited)
- AP1000 (Westinghouse)
- ESBWR (GE-Hitachi)
- UK EPR (EDF and AREVA)

Based on DTI's advice that there was potential support from industry for building these four designs, HSE formally started a dialogue with each 'Requesting Party' in July 2007. In parallel, the Environment Agency also began its regulatory assessment work. HSE and the Environment Agency's work on GDA has been co-ordinated by a Joint Programme Office, which has been set up specifically for this project and is based in HSE's Merseyside headquarters.

* At the time, the Department of Trade and Industry (DTI) was the lead department for UK Government energy policy. This role now falls to the Department for Business, Enterprise and Regulatory Reform (BERR).

Having considered the views expressed during its nuclear public consultation, the Government published a further White Paper on the future of nuclear power* on 10 January 2008. This concluded that it would be in the public interest to allow energy companies to invest in new nuclear power stations. To ensure that people and society are properly protected, HSE will continue to apply the GDA process to the designs which are most likely to be chosen for construction in the UK. In allocating resources to this ongoing GDA process, HSE will therefore take due account of advice from the Government and others about the designs that are considered most likely to be progressed for construction.

Introduction

The safety of nuclear installations is achieved by good design and operation, but it is assured by a system of regulatory control at the heart of which is the nuclear site licensing process. This requires a licence to be granted before any construction work can start. The licence is granted, after assessment of the application, to a corporate body (eg an operator) to use a site for specified activities. In doing this we look at the siting and organisational factors. Licensing and the licence conditions apply throughout the lifetime of an installation from manufacture, through construction, commissioning, operation, modification and on to eventual decommissioning.

Following renewed interest in nuclear power in the UK, HSE introduced a new procedure for assessing the safety of new nuclear power stations. The updated arrangements are based on a two-phase process which separates the design assessment from the site and again from specific licensing assessment (Phase 2).

Phase 1, termed Generic Design Assessment (GDA), is a review of the safety features and ultimate acceptability of nuclear reactor designs. It is undertaken independently from any specific site. The process will allow a rigorous and structured examination of detailed safety and security aspects of the reactor designs, and is likely to take around 3.5 years to complete.

If successful, we will issue a 'Design Acceptance Confirmation' – a statement that HSE finds the reactor design acceptable for nuclear safety and security. Guidance on the GDA process is provided in *Nuclear power station generic design assessment – Guidance to requesting parties*¹ and *Guidance document for generic design assessment activities*.²

Phase 2 will involve an applicant seeking a nuclear site licence to construct and operate such a reactor at a specific site (or sites). Phase 2 will take approximately one year and will enable HSE to carry out a site licence assessment, in which we will examine the proposed design, the site and the management organisation of the operating company. If the application is judged to be acceptable we will grant a Nuclear Site Licence. More information on the licensing process can be found in the HSE publication *The licensing of nuclear installations*.³

Phase 1 (the GDA process) consists of four steps:

- Step 1, which was completed for AP1000 in late August 2007, was for the preparatory part of the design assessment process. The majority of the work was undertaken by WEC, as the Requesting Party, in assembling the safety submissions for Step 2. It involved discussions between the Requesting Party

* *Meeting the Energy Challenge: A White Paper on Nuclear Power* CM 7296 The Stationery Office January 2008

and HSE to ensure a full understanding of the requirements and processes that would be applied, and to arrive at formal agreements to allow HSE to recover its costs associated with the assessment from the Requesting Party.

- Step 2, which is completed with the publication of this report, was an overview of the fundamental acceptability of the proposed reactor design concept within the UK regulatory regime. The aim was to identify any fundamental design aspects or safety shortfalls that could prevent the proposed design from being licensed in the UK. It also introduced HSE inspectors to the design and provided a basis for planning subsequent assessment. This report provides HSE's findings and the conclusions of the fundamental overview.
- Step 3 will be a system design safety and security review of the proposed reactor. The general intention will be to move from considering the fundamental safety claims of the previous step to an analysis of the design, primarily by examination at the system level and by analysing the Requesting Party's supporting arguments. From a security perspective, the foundations for developing the conceptual security plan will be laid through dialogue with the Requesting Party.
- Step 4 is designed to move from the system-level assessment of Step 3 to a detailed examination of the evidence given by the safety analyses, on a sampling basis. We will also seek to examine the proposed conceptual security plan for AP1000. If the design is considered acceptable, we will issue a 'Design Acceptance Confirmation' at the end of Step 4. There may be certain exceptions or exclusions attached to the Design Acceptance Confirmation, eg on any issues that are not fully resolved, or where the design is not sufficiently complete.

The Design Acceptance Confirmation could then be carried forward to support a site-specific nuclear site licence application. It is the intention that there will be no reassessment of aspects included in the Design Acceptance Confirmation except, of course, to address any of the exceptions or exclusions. The assessment of AP1000 during Phase 2 should therefore be limited to any site-specific aspects and any proposed design changes.

HSE expectations for modern reactors

HSE expects that any nuclear reactor that is built in the UK in the near future will be of a robust design that provides adequate protection against potential accidents to a degree that meets modern international good practice. In other words, reactors built in the UK should be at least as safe as modern reactors anywhere else in the world.

Potential accidents in a reactor could arise from failures of equipment, for example pipe leaks or pump breakdowns, or from hazards such as fires, floods, extreme winds, earthquakes, or aircraft crash. HSE expects the reactor to be designed to withstand all these scenarios. We expect to see a robust demonstration of three key features: the ability to shut down the reactor and stop the nuclear chain reaction; the ability to cool the shutdown reactor; and thirdly the ability to contain radioactivity.

The adequacy of protection provided should be demonstrated by a comprehensive safety analysis that examines all the faults and hazards that can threaten the reactor. This should show that the reactor design is sufficiently robust to withstand these faults and hazards and that it operates with large margins of safety. HSE expects an approach of defence-in-depth to be adopted. This means that if one part of the plant fails then another part is available to fulfil the same safety duty. To maximise protection, different backup systems and other safety features can be provided. This multi-barrier protection concept should be repeated until the risk of an accident is acceptably low.

In modern reactor design, these concepts are well understood and HSE therefore expects to see a comprehensive demonstration that an acceptably low level of risk has been achieved. The principles used by HSE in assessing whether the safety demonstration is adequate are set out in the document *Safety assessment principles for nuclear facilities*⁴ (SAPs). To help ensure HSE applies good international practice in its assessment, the SAPs have recently been revised and updated and this included benchmarking against the IAEA Safety Standards.

HSE expectations from the GDA process

Details of HSE's expectations for Step 2 of the GDA process can be found in the GDA guidance.¹ For the completeness of this report a key section of that document, which describes what HSE expects from a Requesting Party, is repeated in Annex 1.

Some of the items listed in Annex 1 (specifically items 1, 3, 4, 7 and 16) are generic and have been considered as an integral part of all the assessments described in this report. In the other cases, the items relate to the specific topic areas assessed and reported below.

Details of the expectations of the Office for Civil Nuclear Security (OCNS) for Step 2 can be found in the OCNS guidance.² In summary, the expectation was that a Requesting Party would provide sufficient information to allow an initial review of design submissions to enable OCNS to become familiar with the technology, and to form a view of the measures required to deliver appropriate security.

A key aim of this report is to provide a summary of the information HSE has gathered from WEC during Step 2 to address the points listed in Annex 1.

The safety standards and criteria used and links to WENRA reference levels and IAEA Standards

The main document used for the Step 2 assessment was the 2006 edition of HSE's *Safety assessment principles for nuclear facilities*⁴ (SAPs). We also benchmarked the relevant SAPs against the Western European Regulators' Association (WENRA) reference levels⁵ and the IAEA document *Safety of Nuclear Power Plants: Design – Requirements*.⁶

Assessment strategy

The aim of Step 2 was a high-level review of the fundamental safety issues. In particular we focused on the claims made by the Requesting Party in the safety documentation.

Throughout this report the words 'claims, arguments and evidence' are used. The concept behind these words is explained below by using a simple everyday analogy:

Many people purchase cars and one criterion for the purchase is often the claimed fuel economy, one important part of which is the urban cycle. So if the manufacturer states in the brochure that the urban cycle is 55 mpg, that is a **claim**. Responsible manufacturers do not leave it at that and often they give **arguments**, within the car's brochure, why the car can meet its urban cycle claim. Valid arguments might be the development of advanced engine

management systems, use of advanced lightweight construction materials, development of low rolling resistance tyres and many more. In addition, **evidence** can be provided by the manufacturer by publishing the results of independent tests on the car's performance under urban cycle conditions.

So, for the Step 2 assessment, we have focused on the claims. Our objective was to make sure that the claims were complete and that they were reasonable in the light of our current understanding of reactor technology. Examination of the detailed arguments and evidence will come in our assessment during Step 3 and Step 4 of GDA.

In our Step 2 assessment, we have made a judgement on the claims in WEC's safety, security and environmental report (SSER)⁷ when compared against the relevant parts of HSE's SAPs. To help us in this task, we developed a strategy to define both the technical areas to be covered and those SAPs most relevant for Step 2 of the GDA process.

Main features of the design and safety systems

The AP1000, as proposed to us by WEC, is described in the *UK AP1000 safety, security and environmental report*.⁷

WEC describes the AP1000 as a pressurised water reactor based closely on the AP600 design which, although it achieved US Nuclear Regulatory Commission (NRC) design certification, was never constructed. AP1000 maintains the AP600 configuration and the US licensing basis by limiting the design changes to as few as possible. It has a claimed 60-year design life and a nominal gross electrical output of 1117 MWe. In comparison to other pressurised water reactors the design includes novel passive safety features and extensive plant simplifications that WEC claim enhance the safety, construction, operation and maintenance of the plant.

The AP1000 reactor comprises a steel reactor pressure vessel and two heat transfer circuits, each with a single hot leg and two cold legs, a steam generator, and two reactor coolant pumps installed directly into the steam generator. The pressure vessel is cylindrical with a hemispherical bottom head and removable flanged hemispherical upper head. It is approximately 12 m long with an inner diameter of approximately 4 m, and is designed to withstand a pressure of 17.1 MPa and temperature of 343 °C for 60 years.

The reactor core is comprised of 157, 4.26 m 17 x 17 fuel assemblies containing 2.35–4.95% enriched U²³⁵. Refuelling is carried out off-load, and the core is designed for a fuel cycle of 18 months with a 93% capacity factor, and region average discharge burn-ups as high as 60 000 MWd/t.

WEC claims that the AP1000 safety systems are designed to mitigate the consequences of plant failures, ensuring reactor shutdown, removal of decay heat and prevention of radioactive releases. Key systems identified by WEC are:

Reactor shutdown

- The **reactivity control system**, which WEC claims provides the means to trip the reactor, maintain a safe shutdown condition, and to control reactivity in the event of certain anticipated events. It comprises the protection and safety monitoring system, plant control system, the diverse action system, the reactor control rods and boration of the reactor coolant.

Emergency cooling

- Passive safety-related systems operate in the unlikely event of an accident and consist of:
 - a **passive core cooling system**, which uses three passive sources of water that WEC claims will maintain core cooling through safety injection. The injection sources include the core make-up tanks, the accumulators and the in-containment refuelling water storage tank. In addition, after injection of these water supplies, WEC claims long-term containment recirculation can be provided by gravity-driven flow;
 - a **passive containment cooling system**, which provides the safety-related ultimate heat sink for the plant. This is a spray system connected to the passive containment cooling water storage tank mounted on the reactor building roof. WEC claims this system cools the containment so that the pressure is rapidly reduced and the design pressure is not exceeded. The steel containment vessel provides the heat transfer surface and heat would be removed from the containment vessel by continuous natural circulation of air;
 - the **main control room emergency habitability system**, which provides fresh air, cooling and pressurisation to the main control room.

WEC claims that the passive safety systems require no operator actions to mitigate design-basis accidents and, once activated, work using only natural forces (eg gravity, natural circulation or compressed gas). They are activated by the operation of a few valves and are designed to meet the single-failure criterion, and to support probabilistic risk assessment (PRA) safety goals.

Containment

- The reactor core and heat transport systems are housed within the AP1000 containment building, which consists of a steel containment vessel inside a pre-stressed concrete reactor building, enclosing them in a continuous, pressure-retaining envelope. WEC claims that a containment isolation system will ensure adequate isolation of the containment by ensuring relevant penetrations are closed.

Retention of molten core debris

- WEC claims that in a core damage event where the core has uncovered and overheated, water will flood the outside of the reactor vessel and prevent vessel failure, thus retaining any molten core debris. The water is sourced from the in-containment refuelling water storage tank, either through normal post-accident operation of the passive safety systems or operator-initiated draining of the tank.

Summary of HSE findings

This section summarises the findings of the fundamental safety overview which comprised Step 2 of the GDA process.

Quality management and safety case development arrangements

HSE considers that leadership and management for safety are key to achieving appropriate high levels of safety, and establishing and sustaining a positive safety culture.

HSE believes that good quality design and safety documentation is dependent on having in place an organised management system, effective procedures (especially for change control), and sufficiently appropriately trained and qualified staff. As part of the examination of WEC's claims in this area, HSE and the Environment Agency jointly undertook an inspection at WEC's USA offices. To assist us, we were joined by an inspector from the US nuclear regulatory body, the Nuclear Regulatory Commission (US NRC).

The inspection found that WEC operates a matrix organisation structure across its range of activities. The AP1000 design organisation, which is housed in their Nuclear Power Plants business, employs over 600 people in a variety of technical disciplines. These are supported by other technically qualified and experienced staff from other parts of WEC. We found clear evidence that WEC is committed to recruiting further significant resource to meet the growing and anticipated demand for nuclear reactors worldwide (particularly in the US and China). Training and placement of new recruits (both graduate and experienced) appeared to be professionally managed and we noted that succession planning is considered and core skill reviews are carried out periodically. Where external contractors are used, they are subjected to screening and selection processes that are appropriate to the nature of the work being undertaken. WEC has recently acquired some contractor support with experience of the UK regulatory process, and is considering employing additional resource to support the UK licensing project.

WEC operates a well-developed set of quality arrangements which include sub-tier procedures which are periodically reviewed and audited. Auditing processes are well established and a related Corrective Action Programme has been developed. We found that the arrangements for developing the Step 2 submission were adequate. We have confidence that the production and update of safety documentation is adequately controlled for this stage of the GDA process, and that arrangements are in place to deal with comments and queries in a satisfactory manner.

We noted that WEC has a quality programme for work performed for the AP1000 project that meets the US requirements, including control of the design process. WEC has also considered other national and international codes, has achieved certification to ISO 9001 and is aware of the requirements of the IAEA Quality Assurance codes and guides. WEC recognises that effective configuration control is an important factor for the Regulators to have confidence in the safety documentation.

The AP1000 design is based on the AP600 and as a consequence, continuous quality programme development has taken place over a number of years with the current Quality Management System now being well established. There has been a recent review of a number of procedures in the design control area in an attempt to

make them more user-friendly, with new recruits specifically in mind; we welcome these developments. WEC has developed the AP1000 design within the US regulatory framework and the US nuclear regulator has carried out significant assessment. WEC recognises that it needs to address the UK requirements for demonstration of 'as low as reasonably practicable' (ALARP) and 'Best Available Technology', but has yet to demonstrate that the AP Series design evolution has used these approaches.

Overall, we conclude that WEC's quality management arrangements provide a sound basis for this stage of the UK GDA process.

Standards

As noted above, HSE works on the basis of linking its SAPs to international standards, such as those of IAEA and WENRA. To evaluate detailed design information, we also use more detailed international standards such as International Electrotechnical Commission (IEC) standards, implemented by the British Standards Institution (BSI).

Our examination of WEC's documentation shows that it has used US standards, some from the 1980s and 1990s. HSE has therefore asked WEC to produce, as part of the future safety documentation submissions, a document demonstrating that the standards used are consistent with modern international good practice.

The approach to ALARP

In respect of 'as low as reasonably practicable' (ALARP), Step 2 of the GDA guidance¹ requires the Requesting Party to provide a description of the process being adopted to demonstrate compliance with the UK legal duty to reduce risks to workers and the public so far as is reasonably practicable (SFAIRP). The GDA guidance goes on to say that HSE will undertake 'an assessment directed at reviewing the design concepts and claims' and, specifically, 'the approach to ALARP'. Hence whether ALARP has been demonstrated has not been assessed in Step 2; rather we have looked at high-level claims on how ALARP will be shown to be met by WEC during Step 3 and Step 4.

WEC's case is outlined in the UK compliance document for the AP1000,⁸ to which a major reference is the UK AP1000 report.⁷ Section B of the UK compliance document addresses ALARP, describing a process of progressive safety improvement both through the evolution of WEC's pressurised water reactors in general and the specific evolution of the AP1000. This process has, for example, led to safety improvements to reduce the likelihood and impact of severe accidents such as the inclusion of in-vessel retention in the event of core melt and materials selection and equipment design to minimise radiation levels. As a result, WEC is able to claim a significant reduction in risk from previous plants. WEC goes on to report cost-benefit analyses for a number of severe accident mitigation design alternatives, which indicate that only trivial amounts of money would be worth spending on further risk reduction measures given the already low risks for both accidents and operational doses.

Overall we conclude that WEC has provided an adequate description of the approach to ALARP for Step 2. Our assessment for Step 3 and beyond will consider whether or not the approach described by WEC actually delivers a design for which the risks have been reduced ALARP.

The design basis analysis/fault study approach

For Step 2 of the GDA process, Section 2.5 of the GDA guidance¹ requires the Requesting Party to provide 'An overview statement of the approach, scope, criteria and output of the deterministic safety analysis'. The guidance goes on to say that HSE will undertake 'an assessment directed at reviewing the design concepts and claims' to include, among other things 'the design basis analysis/fault study approach'. Hence the detail of the deterministic safety case itself was not assessed in Step 2; rather the aim was to see that claims have been made in respect of the relevant SAPs, for example on the reactor core, design basis analysis and severe accidents. The arguments and evidence supporting these claims will be assessed in Step 3 and beyond.

The AP1000 is a design that has evolved making extensive use of the operating experience of existing generations of pressurised water reactors. New features include the use of passive systems for heat removal and emergency cooling to cope with design-basis accidents.

As part of the safety and fault analysis in support of the design of the AP1000, WEC has presented information on the following:

- Core stability – SSER⁷ Section 4.3
- Design basis analysis – SSER⁷ Chapter 15
- Severe accident evaluation – SSER⁷ Section 19.34

WEC claims that the core will be stable under normal operation and fault conditions, such that there will be no uncontrollably large or rapid increases in reactivity due to any changes in temperature, power, xenon distribution or coolant voiding.

In the design basis analysis, WEC claims to have carried out a comprehensive study to identify a complete set of faults (ie those things that could go 'wrong' on the reactor). The transients resulting from these faults have been modelled using validated codes embodying appropriate assumptions and data. This includes, for example, assuming the worst combination of plant temperature, pressure and power distribution that could exist just before a fault occurred, and the worst possible performance by the safety systems after the fault occurs. Even with such pessimistic assumptions, WEC claims that the plant has appropriate protection against these faults and that consequences such as, for example, melting of the fuel, are avoided. The methods used by WEC to arrive at these conclusions will form an important part of our assessment in future steps.

Severe accidents have been addressed to identify necessary actions and provisions to contain large-scale fuel melting and prevent a large activity release from the containment building. The philosophy is to apply external cooling to the vessel sufficient to contain the Corium (ie the mix of fuel and reactor internals resulting from any potential core meltdown). Should the Corium melt through the vessel, a cavity has been provided directly below it to spread and cool the molten material.

Overall, we conclude that WEC has carried out what appears to be an extensive study identifying all significant faults and analysing the effects on the core and where necessary making provision to contain severe accidents. In doing this they claim to meet the Fault Analysis SAPs covering Design Basis Analysis and Severe Accidents, identifying the relevant sections in the SSER. The quality of the submission leads us to be confident that they will be able to substantiate their claims in the later Step 3 and Step 4.

The probabilistic safety analysis (PSA) approach

For Step 2 of the GDA process, Section 2.6 of the guidance document¹ requires the Requesting Party to provide 'an overview statement of the approach, scope, criteria and output of the probabilistic safety analysis'. The guidance goes on to say that HSE will undertake 'an assessment directed at reviewing the design concepts and claims' and specifically in point 2.22 'the PSA approach'. Hence the PSA itself is not being assessed in Step 2; rather the aim is to see that appropriate claims have been made in respect of PSA SAPs and that there is a reasonable prospect of meeting the SAP's Basic Safety Objective numerical targets. The arguments and evidence supporting these claims will be assessed in Step 3 and beyond.

WEC addresses PSA in Sections A3.4 and C of the UK compliance document⁸ and claims to have carried out a comprehensive study and to systematically analyse the complete range of anticipated initiating faults, internal and external initiators, and all modes of operation. Section A3.4 discusses the various elements of the PSA covering PSA methodology and gives an overview of the results. The methodology section covers initiating faults, accident sequence analysis, systems analysis, human reliability analysis, data analysis (initiating fault frequencies, component reliability and common cause failure), quantification, containment performance and consequence analysis. Section C of the UK compliance document contains specific claims against each of our SAPs and numerical targets.

WEC's preliminary estimate of the AP1000 total core damage frequency is $5.09 \times 10^{-7}/\text{yr}$ which, in conjunction with the arguments presented, gives HSE a strong indication that the Basic Safety Objective numerical targets set out in our SAPs will be met.

HSE recognise that PSA provides **estimates** of the risks, not a precise measure of them, and that these cannot be readily compared between designs. The way in which uncertainty over input parameters and sensitivity to assumptions affects the results will feature in the more detailed assessment in Step 3 and beyond.

Overall, we conclude that WEC has provided an adequate overview of the approach, scope, criteria and output of the PSA. The argument given by WEC is that they have addressed non-core sources of radioactivity (such as resin tanks, the spent fuel pool) needs further support, and they will need to re-analyse the PSA consequences to demonstrate they meet SAPs numerical targets.

Structural integrity

For Step 2 of the GDA process, HSE's review of design concepts and claims for the integrity of metal components and structures includes aspects of:

- the safety philosophy, standards and criteria used;
- the design basis analysis/fault study approach;
- the overall safety case scope and extent;
- an overview of the claims in a wide range of areas of the safety analysis.

A fundamental aspect of the SAPs for integrity of significant safety-related metal components and structures (pressure vessels and piping, their supports and vessel internals) is the identification of those components where the claim is that gross failure is so unlikely that the consequences can be discounted from consideration in the design of the station and its safety case. For such components, the SAPs require an in-depth explanation of the measures over and above normal practice that support and justify the claim. In these circumstances, the emphasis falls on the

arguments and evidence to support the claim that gross failure is so unlikely it can be discounted. Similar claims have featured in safety cases for operating nuclear stations in the UK and the supporting arguments and evidence have been considered by HSE.

For the AP1000, WEC has implied (ie without explicit claims) in the submission that gross failure of the reactor pressure vessel (RPV), of any of the four steam generators, the pressuriser, the core make-up tanks or the accumulators is discounted. On the other hand, gross failure of certain piping is explicitly claimed to be discounted based on one of two sets of arguments and evidence, referred to as 'break exclusion zone' (piping in the vicinity of the containment wall) or 'leak before break evaluation procedure'.

The Step 2 review has not examined in detail the arguments and evidence to support claims on structural integrity of metal components and structures. Some of the items in question are long lead-time components and, to reduce their regulatory risk, WEC may wish to ask HSE to assess such items at an early stage, before any long-lead orders are placed.

Relevant general matters which are likely to arise in Step 3 and Step 4 assessments are:

- material specification for ferritic forgings and welds to be used in main vessels (reactor pressure vessel, steam generators, pressuriser);
- materials used for the reactor coolant pump bowl and the weld joining the bowl to the steam generator channel head;
- nature of the arguments and evidence to support integrity claims for some piping.

Overall, we conclude that WEC has provided an adequate overview of the claims made for structural integrity of metal components and structures. However, for Step 3 and Step 4 there will need to be an explicit listing of those components where gross failure is claimed to be so unlikely that it can be discounted. WEC has also provided some coverage of the type of arguments and evidence to support the claims.

Waste and decommissioning

The objective of HSE's Step 2 GDA radioactive waste and decommissioning assessment was to identify any fundamental aspects or safety shortfalls that could prevent the proposed design from being constructed on licensed sites in the UK. The Environment Agency have also assessed radioactive waste and decommissioning proposals and their findings are reported separately.

For Step 2 of GDA, Section 2.18 of the GDA guidance¹ requires the Requesting Party to provide 'Information on radioactive waste and decommissioning'. The GDA guidance goes on to say that HSE will undertake 'an assessment directed at reviewing the design concepts and claims', to include 'any matters that might be in conflict with UK Government policy'. The aim of the Step 2 assessment is to identify whether the strategies put forward for radioactive waste and decommissioning are likely to comply with Government policy, SAPs and existing HSE guidance on waste and decommissioning matters. The arguments and evidence supporting these claims will be assessed in Step 3 and beyond. It should be noted that the UK Government recently announced its intention to make it a legal requirement for funded decommissioning plans to be approved by the Government before construction of new reactors commences.

Chapter 11 of WEC's SSER⁷ details and quantifies the expected waste streams. It is WEC's intention that radioactive waste is to be packaged ready for shipment and disposal and spent fuel stored on site in a fuel pond. Measures which WEC claim will facilitate decommissioning include the omission of stellite from the primary circuit, which helps to reduce the level of radioactivity around the plant. Four decommissioning strategies ranging from prompt decommissioning, safe-store and entombment are identified in Chapter 20 of the SSER. The eventual choice of strategy will be assessed at a later stage of the licensing process.

There are no indications of any waste streams which would present particular difficulties, and this is sufficient for HSE for Step 2. However, there is no attempt to demonstrate that the waste streams would meet the appropriate criteria for disposal in a low level waste (LLW) facility or an intermediate level waste (ILW)/spent fuel repository. HSE will therefore be seeking further detail of the acceptability of waste for disposal during subsequent steps of the GDA process. Equally, there is no demonstration that facilities will be provided for through-life storage of wastes and spent fuel and we will be asking WEC for further information for GDA Step 3.

Civil engineering and external hazards

As noted above, for Step 2 of the GDA process the Requesting Parties were required to provide a Preliminary Safety Report (PSR) that included sufficient information for the HSE fundamental safety overview assessment, in particular:

- design philosophy and a description of the resulting conceptual design;
- overview of the approach, scope, criteria and output of the deterministic safety analyses;
- specification of the site characteristics used as the basis for the safety analysis (the 'generic siting envelope');
- reference to and justification of standards and design codes used.

A review of these aspects has been undertaken in the light of civil engineering, external hazards and siting. External hazards include potential challenges to the plant that arise from outside the site, such as extreme winds or earthquakes. Our assessment has found that WEC have clearly identified the design classification for structures and plant in what appears to be a systematic manner. This has been linked to design codes and standards. These standards for the most part are specifically intended for application to nuclear facilities and are primarily American in origin. It is noted that some of the standards applied have been superseded by more recent versions. The standard design incorporates a foundation which is primarily designed for siting on rock or firm strata. For some UK coastal sites, with deep soil profiles, including some existing nuclear sites, this standard design would not be applicable. Therefore, if the AP1000 is not to be limited to only certain UK sites, WEC will need to amend their design or carry out site remediation work. We will progress this issue through Step 3 and Step 4 of GDA.

We note that WEC has not reviewed the design against other HSE requirements, such as the requirements of the Construction (Design and Management) Regulations 2007. These Regulations apply during the design phase and so we expect them to be addressed later in the GDA process.

The design basis external hazards applied to the structures and plant have been clearly identified by WEC, as have the limitations on the standard design. WEC recognises that there are a number of hazards, such as external flooding, the magnitude of which cannot readily be determined until a site(s) has been identified.

There has not been an attempt to put the design basis hazards into a UK context at this stage. The standard design includes specific consideration of aircraft impact of a non-accidental nature. We will review the completeness of the external hazards considered by WEC in more detail in the next steps of the GDA process.

Overall, we conclude that the submission is sufficient at this stage to allow progression to Step 3 of the assessment process. WEC has acknowledged the need to place the design in a UK context, and to consider other UK-specific regulations which apply to the design of installations such as this.

Internal hazards

For Step 2 of the GDA process, Section 2.5 of the GDA guidance¹ requires the Requesting Party to provide 'an overview statement of the approach, scope, criteria and output of the deterministic safety analyses'. Deterministic analysis includes, among others, consideration of internal hazards. The guidance goes on to say that HSE will undertake 'an assessment directed at reviewing the design concepts and claims'. Hence the analysis of internal hazards itself is not being assessed in Step 2; rather the aim is to see if appropriate claims have been made against the internal hazard-related SAPs. The arguments and evidence supporting these claims will be assessed in Step 3 and beyond.

The overall objective of the hazard principles is to minimise the effects of internal hazards such as, for example, fires. In particular, we want to ensure that internal hazards do not adversely affect the reliability of safety systems. One of the threats posed by hazards such as fires is that they can, if not properly addressed, affect a range of different plant at the same time. This is called a 'common cause' effect and it is important to ensure that this is avoided. Safety systems and safety-related systems should therefore be qualified to withstand the effects of internal hazards or they should make appropriate use of redundancy, diversity, separation or segregation. The SAPs therefore require that a comprehensive and systematic approach be used to identify the internal hazards and protection provided. This should include combining the hazards with other potential simultaneous hazards and/or faults, and taking into account plant out for maintenance.

WEC has addressed its compliance with the internal hazard SAPs in its submission *UK Compliance Document for AP1000 Design, Section C – Safety Assessment Principles Roadmap for AP1000 Design*.⁸ Additional information was provided in *UK AP1000 safety, security and environmental report*.⁷

WEC has identified a range of potential internal hazards. Segregation/separation of redundant trains of safety-related equipment is principally achieved, outside primary containment, with three-hour fire-rated hazard barriers and within containment with a combination of structural walls, local fire barriers, distance and equipment qualification. The passive approach to ensuring segregation outside containment is the preferred approach and is consistent with IAEA recommendations.⁹

Overall we note that WEC claims compliance with the internal hazard SAPs. We conclude that they have provided an adequate overview of the concept and approach being adopted to address internal hazards within the deterministic safety analysis. This approach provides reasonable confidence that WEC will be able to substantiate its claim in Step 3 and Step 4.

Reactor protection and control

The objective of the Step 2 GDA Control and Instrumentation (C&I) assessment was to identify any fundamental design aspects or safety shortfalls that could prevent the proposed design from being constructed on licensed sites in the UK. In particular, to determine whether an adequate claim of compliance exists for those C&I SAPs which address fundamental design aspects.

WEC provided a number of submissions relevant to C&I including a specific response against the SAPs. The main submission⁷ describes the C&I. The C&I provisions claimed include those that would be expected of a modern nuclear reactor such as:

- safety systems (eg reactor shutdown systems such as the Plant Protection and Monitoring System (PMS) which initiates reactor trip and provides engineered safety features functions such as reactor core cooling via initiation of the passive residual heat removal system);
- plant control and monitoring systems (eg the plant control system that performs functions such as reactor power control);
- main control room with back-up via the remote shutdown workstation; and
- communications systems allowing information transfer both within and external to the plant.

An important aspect of the safety demonstration is the classification of systems important to safety and the application of appropriate design standards. The accepted practice is that the standards are more onerous for those systems that are more important to safety. In the UK the importance to safety is typically judged by a combination of deterministic and probabilistic criteria. The deterministic analysis considers the functions performed by the system, such as to shut down the reactor, and the probabilistic analysis considers the reliability required of the system. The WEC AP1000 C&I design concept reflects US custom and practice, and is largely based on US C&I standards (eg Institute of Electrical and Electronics Engineers (IEEE) standards) and US NRC requirements. Two system classifications are used, safety related and non-safety related.

During Step 3 and Step 4, WEC will address the issue of the use of international standards (IEC and IAEA), grading the importance to safety through the use of three system classifications (ie safety system, safety-related system and non-classified), and use of probabilistic criteria in the design of C&I systems important to safety.

WEC's submissions provide a satisfactory overview of the C&I provisions and adequate claims of compliance for all of the fundamental C&I Step 2 SAPs. In addition, the Step 2 C&I assessment has not identified any fundamental issues that would prevent the AP1000 from proceeding to Step 3.

Novel features

WEC claims that the AP1000 reactor concept contains a number of advanced passive features. 'Passive' features are those that operate independently from facility power sources, such as electrical supplies. For example, these might include cooling systems that operate by natural circulation, or water injection systems that operate through differential pressures. On the other hand, 'active' features are those that rely on external power sources. Safety systems on existing reactors are often active and require electric supplies to power pumps and valves.

In safety terms, passive systems are often simpler than active ones and so can be considered more reliable. HSE's own SAPs rate passive systems higher than active safety systems in the preference hierarchy of responses to hazards.

No nuclear power plant that has a significant dependence on passive safety systems has received a licence to operate anywhere in the world and therefore many aspects of the AP1000's cooling system are considered to be novel. This does not mean that there is no experience in the world of passive systems, as many existing reactors do use elements of passive safety in their designs, but their use on the AP1000 is more widespread.

The robust design of the AP1000 should avoid accidents that could damage the reactor core. Although such accidents would be extremely unlikely, we still require them to be considered in the safety analyses. Part of the protection designed into the AP1000 concept is the claim that the molten reactor core would be retained within the reactor pressure vessel, and this is a novel claim. There are significant merits to this claim. However, the arguments and evidence to support it will, in our view, be challenging to demonstrate with an appropriate degree of confidence. We will look at this further in Step 3 and Step 4.

Long-lead items

Large plant items such as the reactor pressure vessel and steam generators take a long time to manufacture and they are typically among the first items to be ordered. If there is a possibility that some of these orders will be placed while the GDA assessment is still ongoing then, to reduce their regulatory risk, WEC may wish to ask HSE to assess such items at an early stage.

Currently there is no specific request from WEC related to the assessment of long-lead items.

International Atomic Energy Agency technical review

As part of the Step 2 assessment, HSE requested that IAEA undertake a technical review of all four Requesting Parties' designs against the relevant IAEA standards. The reason for this is that IAEA has ready access to considerable expertise on a wide range of reactor types in operation and under construction throughout the world.

The findings from the IAEA technical review have been taken into account by HSE during our own assessment. IAEA did not reveal any fundamental safety problems with the AP1000. All of the findings in the report are recommendations for further assessment work, particularly in areas that are novel or technically complex, and we will take these into account in Step 3 and Step 4 as appropriate.

Any matters that might be in conflict with UK Government policy

HSE has found no matters in the WEC submission that are in conflict with UK Government policy.

Security

OCNS has begun familiarisation with the AP1000 design during Step 2. Initial discussions have been held with WEC and a review of the documentation provided to date has been carried out. It is concluded that the design appears to be sufficiently developed to give confidence that during Step 3 and Step 4 of the GDA process a conceptual security plan can be developed which will provide the

appropriate resistance to postulated threats. This outcome will of course depend on the detailed review of the design during Step 3 and Step 4 and adoption of any UK-specific design changes deemed necessary (eg UK-specific security furniture).

Discussions with the relevant US authorities are progressing to allow the transfer of sensitive nuclear information between countries to support the GDA process. A procedure is in place to allow vetting clearances to be granted by the Director of OCNS to facilitate the exchange of such information.

Public involvement process

HSE has emphasised the importance it attaches to openness in the GDA process, and the opportunity for public involvement at key stages is an important part of this. By this means, we aim to give the public confidence in the GDA process.

Members of the public have been able to view the design information provided by WEC for the GDA process. A comprehensive safety, security and environmental report for the AP1000 was made available on the company's website from 10 September 2007, www.ukap1000application.com. The same information was also made available upon request in CD-ROM format.

In addition, to help encourage public participation, WEC made announcements in the national press at that time to publicise the GDA openness arrangements. To supplement these, the Regulators (HSE and the Environment Agency) published a leaflet, *Designs for potential new nuclear power stations: Public involvement*, which was distributed to public libraries. We also set up a new-build e-bulletin system and wrote to all UK Members of Parliament, Peers, Scottish Members of Parliament and Welsh Assembly Members to inform them of the public involvement opportunity.

Members of the public were invited to view the design information and comment on it – either electronically or in writing. Comments relevant to the published design information were forwarded to WEC, to respond to the person who made the comment within 30 days of receipt. The Regulators monitored this process and where appropriate the issues raised have been considered as part of our assessment during Step 2. Only those comments made between 10 September 2007 and 4 January 2008 have been considered in Step 2; any issues raised in comments made after that date will be considered in our assessment during GDA Step 3.

The number of website hits recorded indicated a good level awareness of and interest in the public involvement process. However, only a small number of comments were received during GDA Step 2. Issues raised on the AP1000 included fault analysis (how were all potential faults and their consequences identified, and what evidence was there for this?), aircraft impact (can it be demonstrated that reactors can withstand deliberate high-speed aircraft impact?), and on-site storage of radioactive waste and spent fuel (how many years storage does the design provide for low level and intermediate level waste and spent fuel?).

The issues raised from the comments and their responses have been considered in the judgements made by HSE on the AP1000 as part of Step 2 of GDA. Where appropriate, these issues will be considered in more depth by assessors during Steps 3 and 4.

A number of the comments made by the public were not directly relevant to the AP1000 or the other designs being assessed; nevertheless these were considered by HSE and responded to as appropriate.

Overseas regulators' assessments

Design review in the US

The US NRC is the only other regulatory authority that has undertaken a formal review of the AP1000 design. The AP1000 was one of the first plants to use the new licensing process in the US, Title 10 of the US Code of Federal Regulations, Section 52, *Licenses, certifications, and approvals for nuclear power plants*. In addition, the AP1000 standard plant design is based closely on the AP600 design that US NRC certified in December 1999.

Following some initial US NRC pre-application review work, WEC submitted an application for standard design certification for the AP1000 in March 2002. US NRC's final design approval was based on Revision 14 of WEC's Design Control Document (DCD) and was issued in September 2004. This was subsequently amended to take account of Revision 15 to the AP1000 DCD. The final AP1000 design certification was completed in January 2006.

Revision 16 to the AP1000 DCD is the version that formed the basis for the *UK AP1000 safety, security and environmental report*.⁷ It includes a number of substantial design changes compared to Revision 15. Revision 16 has not received final design approval from US NRC as it is currently being evaluated, and it is expected that a final safety evaluation report will be issued in March 2010.

It should also be noted that US NRC design certification does not mean that the reactor design is complete. For the AP1000, at Revision 15 of the DCD, a number of technical areas remain outstanding. In addition, formal licence applications have to be made and assessed before any construction will be permitted. Several such applications for AP1000 are currently under US NRC review.

HSE collaboration with other regulators

HSE has an information exchange agreement with US NRC and has had a number of bilateral meetings to discuss new-build assessment collaboration and transfer of information. This process is ongoing for the AP1000 and HSE intends to continue this through the GDA timeframe.

HSE sees great value in being able to share information with other regulators who have carried out relevant assessments and we have published our views on how this information can be used in our GDA guidance.¹ However, because the UK legal and regulatory framework is UK specific, design approval by other regulators cannot be transferred automatically to the UK. Furthermore, under international conventions etc, nuclear safety regulation is a national responsibility and HSE must perform its duty to the UK public and workers. This has not prevented HSE from making appropriate use of overseas regulators' assessments, and it is HSE's intention that this practice will continue in future GDA Steps.

Conclusions

This report is our GDA Step 2 public statement for the AP1000 reactor.

The aim of Step 2 was to provide an overview of the fundamental acceptability of AP1000 within the UK regulatory regime. It was also intended that Step 2 would allow HSE inspectors to become familiar with the design and provide a basis for planning subsequent assessment work.

HSE has undertaken a high-level review of WEC's claims for a number of different safety aspects of the AP1000 reactor, and we have considered the security aspects of the design.

In summary, we have not found any safety or security shortfalls that are so serious as to rule out at this stage eventual construction of the AP1000 on licensed sites in the UK. As a result of our assessment, we see no reason why AP1000 should not progress to GDA Step 3.

As anticipated, our assessment has identified a number of topics that will need to be addressed in more detail during the GDA Step 3 and Step 4 assessment, should the AP1000 proceed through to the next steps of the GDA process. In this event, we will summarise our progress on these topics in a public report at the end of Step 3 and in a final GDA report at the end of Step 4.

Abbreviations

ALARP	As low as reasonably practicable
BERR	Department for Business, Enterprise and Regulatory Reform
BSI	British Standards Institution
C&I	Control and Instrumentation
DCD	Design control document
DTI	Department of Trade and Industry (now BERR)
GDA	Generic design assessment
HSE	Health and Safety Executive
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ILW	Intermediate level waste
LLW	Low level waste
ND	Nuclear Directorate
OCNS	Office for Civil Nuclear Security
PRA	Probabilistic risk assessment
PSA	Probabilistic safety analysis
PSR	Preliminary safety report
RPV	Reactor pressure vessel
SAPs	Safety assessment principles
SFAIRP	So far as is reasonably practicable
SSER	Safety, security and environmental report
US NRC	Nuclear Regulatory Commission (United States of America)
WEC	Westinghouse Electric Company LLC
WENRA	Western European Nuclear Regulators' Association

Annex 1: Summary of HSE's expectations for Step 2 of the GDA process

Details of HSE's expectations for Step 2 of the GDA process can be found in the GDA guidance.¹ From that document, the key expectations of Requesting Parties for Step 2 are:

Provide a Preliminary Safety Report that includes sufficient information for the Step 2 Fundamental Safety Overview, in particular:

1. A statement of the design philosophy and a description of the resultant conceptual design sufficient to allow identification of the main nuclear safety hazards, control measures and protection systems.
2. A description of the process being adopted by the applicant to demonstrate compliance with the UK legal duty to reduce risks to workers and the public so far as is reasonably practicable (SFAIRP).
3. Details of the safety principles and criteria that have been applied by the Requesting Party in its own assessment processes, including risks to workers and the public.
4. A broad demonstration that the principles and criteria are likely to be achieved.
5. An overview statement of the approach, scope, criteria and output of the deterministic safety analyses.
6. An overview statement of the approach, scope, criteria and output of the probabilistic safety analyses.
7. Specification of the site characteristics to be used as the basis for the safety analysis (the 'generic siting envelope').
8. Explicit references to standards and design codes used, justification of their applicability and a broad demonstration that they have been met (or exceptions justified).
9. Information on the quality management arrangements for the design, including design controls; control of standards; verification and validation; and interface between design and safety.
10. A statement giving details of the safety case development process, including peer review arrangements, and how this gives assurance that nuclear risks are identified and managed.
11. Information on the quality management system for the safety case production.
12. Identification and explanation of any novel features, including their importance to safety.
13. Identification and explanation of any deviations from modern international good practices.
14. Sufficient detail for HSE to satisfy itself that HSE's Safety Assessment Principles (SAPs) and that the Western European Nuclear Regulators' Association (WENRA) Reference Levels are likely to be satisfied.

15. Where appropriate, information about all the assessments completed by overseas regulators.

16. Identification of outstanding information that remains to be developed and its significance.

17. Information about any long lead items that may be manufactured in parallel with the Design Acceptance process.

18. Information on radioactive waste management and decommissioning.

The Requesting Party will also be required to respond to questions and points of clarification raised by HSE during its assessment, and to issues arising from public comments.

References

- 1 *Nuclear power station generic design assessment – guidance to requesting parties* (Version 2) HSE 16 July 2007 www.hse.gov.uk/nuclear/reactors/design.pdf
- 2 *Guidance document for generic design assessment activities* (Version 2) Office for Civil Nuclear Security 201206 January 2007 www.hse.gov.uk/nuclear/ocns/ocnsdesign.pdf
- 3 *The licensing of nuclear installations* HSE March 2007 www.hse.gov.uk/nuclear/notesforapplicants.pdf
- 4 *Safety assessment principles for nuclear facilities* (2006 Edition Version 1) HSE December 2006 www.hse.gov.uk/nuclear/saps/saps2006.pdf
- 5 *WENRA Reactor safety reference levels* Western European Nuclear Regulators' Association Reactor Harmonization Working Group January 2007 www.wenra.org
- 6 *Safety of Nuclear Power Plants: Design – Requirements* IAEA Safety Standards Series No. NS-R-1 IAEA 2000
- 7 *UK AP1000 safety, security and environmental report* (Revision 1) Westinghouse Electric Company LLC UKP-GW-GL-700 1 August 2007 www.ukap1000application.com
- 8 *UK compliance document for AP1000 design* (Revision 0) Westinghouse Electric Company LLC UKP-GW-GL-710 11 May 2007 www.ukap1000application.com
- 9 *Protection against internal fires and explosions in the design of nuclear power plants* IAEA Safety Standards Series No. NS-G-1.7 IAEA 2004

HSE priced and free publications are available by mail order from HSE Books, PO Box 1999, Sudbury, Suffolk CO10 2WA Tel: 01787 881165 FAX: 01787 313995 Website: www.hsebooks.co.uk (HSE priced publications are also available from bookshops and free leaflets can be downloaded from HSE's website: www.hse.gov.uk).

For information about health and safety ring HSE's Infoline Tel: 0845 345 0055 Fax: 0845 408 9566 Textphone: 0845 408 9577
e-mail: hse.infoline@natbrit.com or write to HSE Information Services, Caerphilly Business Park, Caerphilly CF83 3GG.

Contacts

The Joint Programme Office
Nuclear Directorate 4N.2
Health and Safety Executive
Redgrave Court
Merton Road
Bootle
Merseyside L20 7HS
www.hse.gov.uk

new.reactor.build@hse.gsi.gov.uk

© *Crown copyright* This publication may be freely reproduced, except for advertising, endorsement or commercial purposes.

First published March 2008. Please acknowledge the source as HSE.