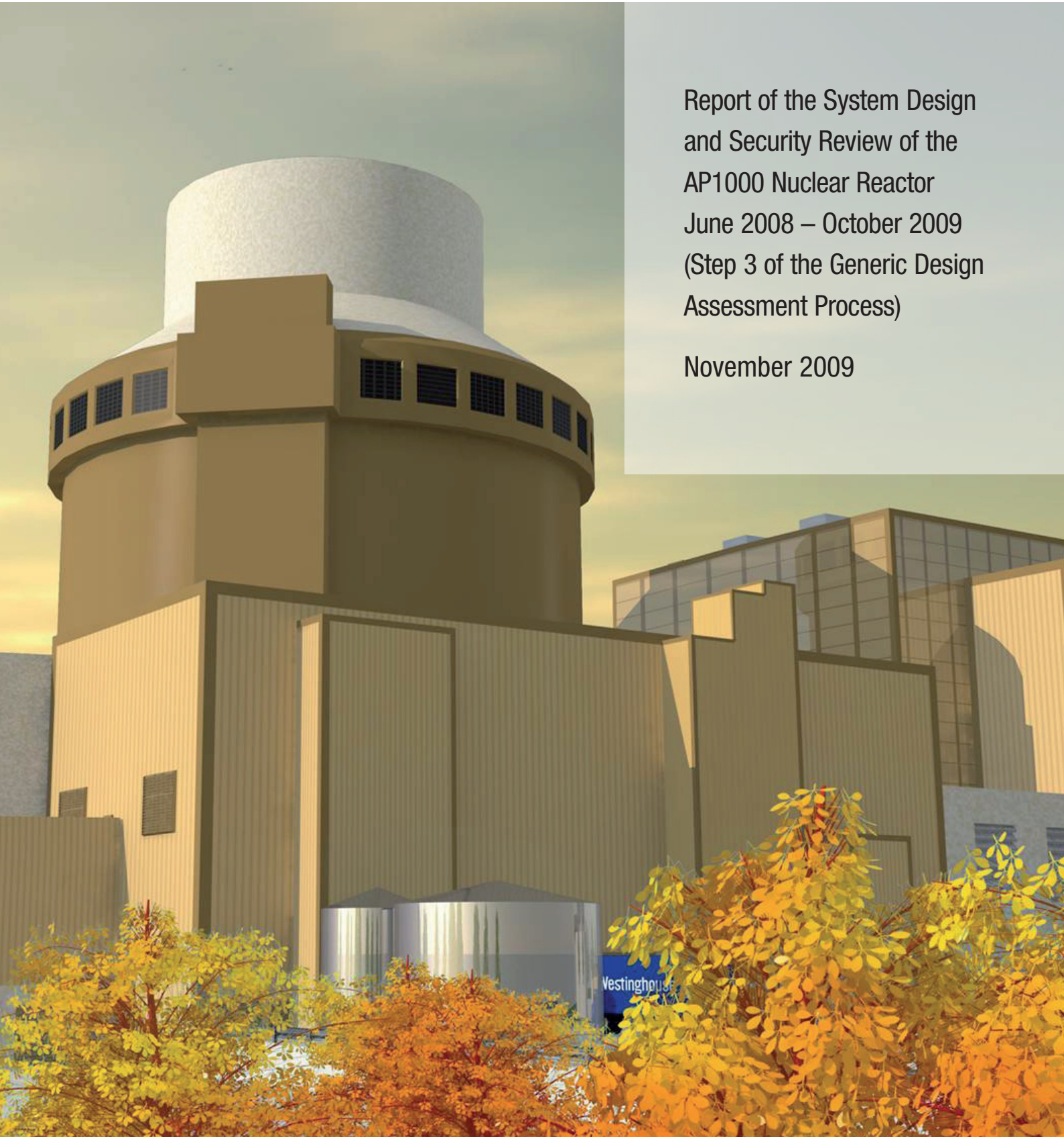


Public Report on the Generic Design Assessment of New Nuclear Reactor Designs

Westinghouse Electric Company LLC AP1000 Nuclear Reactor



Report of the System Design
and Security Review of the
AP1000 Nuclear Reactor
June 2008 – October 2009
(Step 3 of the Generic Design
Assessment Process)

November 2009

Contents

Foreword	3
Executive summary	5
Background	5
Introduction	8
HSE expectations for modern reactors	9
HSE expectations from the GDA process	9
The safety standards and criteria used	10
Assessment strategy	10
Technical Support Contractors	10
Main features of the design and safety systems	11
Summary of HSE findings	12
Internal hazards	12
Civil engineering	13
External hazards	14
Probabilistic Safety Analysis	15
Design basis analysis/fault studies	16
Reactor protection and control	18
Essential electrical power systems	19
Fuel design	20
Reactor chemistry	21
Radiological protection	22
Mechanical engineering	22
Structural integrity	24
Human factors	25
Quality management and safety case development arrangements	26
Radioactive waste and decommissioning	27
Security	28
Safeguards	28
Issues raised through the public involvement process	29
Working with overseas regulators	29
Cross cutting issues	30
The demonstration of as low as reasonably practicable	30
Submission configuration control and design reference point	31
Categorisation of structures, systems and components	32
Metrication of the AP1000 design	32
Summary of significant issues	33
Potential Exclusions	34
Conclusions	35
Abbreviations	36
Annex 1: Summary of HSE expectations for Step 3 of the GDA process	37
References	38
Contacts	39

Foreword

I am pleased to present in this Generic Design Assessment (GDA) Step 3 report, the developing findings of our assessment of the AP1000 reactor. This is in effect akin to a mid-point progress report on how our assessment is progressing through the GDA process that we started in 2007 and are planning to complete in mid 2011. We publish this report today, together with a series of more detailed supporting technical reports, as part of our commitment to be open and transparent about our work on GDA.

This current project is the first application of GDA, which is a new process for both us and the industry. GDA seeks to get the Nuclear Regulators involved at an early stage in development of proposals for new nuclear power stations and it allows the technical assessments of the reactors to be conducted before any specific nuclear site licence assessments are undertaken. In this way we are seeking to identify and address any potential regulatory questions and challenges before commitments are made to construct the reactors. We believe that we are being successful in this aim as is evidenced by the contents of this report.

The GDA assessment is in several steps and includes initial and then more detailed examinations of the safety and security of the proposed reactors. We are undertaking our GDA assessment jointly with the Environment Agency and in parallel with our work on safety and security aspects the Environment Agency is examining the potential environmental impact. The step-wise assessment approach was planned to allow us to look in increasing detail at the safety and security issues as we progress through the various Steps, and also it allowed us to start with a fairly small assessment team and to grow this as we progressed through the project. After a slow start we have made excellent progress in deploying more resource, and we have also set-up a technical support framework within which we have placed over 40 support contracts to further bolster the analytical resources available to us. The result of this has been that, whilst our GDA programme suffered some delay against the original plan during 2008, over the last year there has been an acceleration in our technical work and I am therefore confident in our assessment plan for the remainder of GDA.

We published a set of reports on the outcome of GDA Step 2, the initial assessment, in March 2008. More recently we have reported on our progress through a series of Quarterly Reports. These are available on our website. This report, that we are publishing today, is on the subject of our GDA Step 3 assessment, the overall design safety and security review, and it covers the period from June 2008 to the end of October 2009. In some areas we did not have sufficient resource in place at the beginning of GDA Step 3, and in others we have had insufficient information from Westinghouse, and this has limited the extent of assessment sampling that we have been able to do. In this report, we have identified where this has been the case and where we intend to significantly accelerate our assessment during GDA Step 4.

The reports that we are publishing today reflect progress up to about October 2009, as since then we have concentrated on report writing. There have been some recent developments that are not therefore captured in these reports, but we will provide updates on these within our quarterly progress reports and in our reports at the end of GDA Step 4.

As is normal for complex assessment projects of this type, we are identifying technical questions and issues that we are requesting Westinghouse to address. It is making progress in doing so, but at this stage, as we are only part-way through

GDA, many remain open and require further work. The fact that we have identified these issues should not in all cases be interpreted as us being critical of the AP1000 design, rather, they should be seen as evidence of an independent and robust regulatory process. They are also evidence that GDA is working as intended and allowing us to have influence on the design and safety case well in advance of construction in the UK.

We have identified the more significant of the issues within this report, and we anticipate that progress on them will continue through Step 4 of GDA, the detailed design assessment. This will require an ongoing active dialogue with additional detailed assessment by us, and high quality and timely safety submissions from Westinghouse. In view of the significant amount of issues identified as requiring attention by Westinghouse, I am encouraged that it has recently both reorganised its project management arrangements and also committed to increase its presence in the UK. This is essential if Westinghouse is to interact with us effectively and provide the necessary information to allow us to complete a meaningful GDA Step 4 assessment.

If you have any comments on this report I will be pleased to hear from you. To assist in this we have extended the existing GDA public involvement process to invite comment on any of our GDA Step 3 reports.



Kevin Allars
Director for New Nuclear Build Generic Design Assessment
Nuclear Directorate
Health and Safety Executive

Executive summary

This is an interim report on the Health and Safety Executive's (HSE) GDA work and it summarises our findings to date.

This report is the second of our major public reports for the AP1000 reactor and it covers our GDA Step 3 work. The aim of GDA Step 3 was to provide an overall design safety and security review of the AP1000 reactor, and specifically to:

- improve our knowledge of the design;
- identify significant issues;
- identify whether any significant design or safety case changes may be needed.
- identify major issues that may affect design acceptance and attempt to resolve them; and
- achieve a significant reduction in regulatory uncertainty. (By this we mean that we are seeking to identify and address any potential regulatory questions and challenges before commitments are made to construct the AP1000 reactor in the UK).

A further aim for GDA Step 3 was that it would allow HSE Inspectors to further familiarise themselves with the design and safety case and provide a basis for planning subsequent assessment work.

To achieve these aims, HSE's Nuclear Directorate has undertaken an examination of the AP1000 reactor at the system level and analysed Westinghouse's supporting arguments. From a security perspective, the foundations for developing the conceptual security plan have been laid through dialogue with Westinghouse.

The summary of our assessment is given in this report. We continue to believe that the AP1000 could be suitable for construction on licensed sites in the UK. However, we have identified a significant number of issues with the safety features of the design that would first have to be progressed. If these are not progressed satisfactorily then we would not issue a 'Design Acceptance Confirmation' at the end of GDA Step 4. We will progress our assessment of these issues, in dialogue with Westinghouse during GDA Step 4, but at this stage it is too early to say whether they can be resolved solely with additional safety case changes or whether they may result in design modifications. We will summarise our progress on these in our Quarterly Reports, which we will continue to place on our website, and in a final GDA report at the end of GDA Step 4 which is presently scheduled for June 2011.

Background

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 and permission given before any significant construction work can start (defined as: the placement of the first structural concrete for buildings with nuclear safety significance). 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 also 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.

In response to growing interest in nuclear power and in anticipation of possible applications for new build in the UK, the Nuclear Regulators (HSE and the

Environment Agency) developed revised assessment proposals for new nuclear power stations and this led to the production of guidance on the GDA process, which was originally published in January 2007¹.

The updated arrangements are based on a two-phase process which separates the GDA from the site-specific HSE licensing assessment and Environment Agency permitting process.

Phase 1, GDA, is a review of the safety features and acceptability of the proposed nuclear reactor design. 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.

GDA consists of four steps.

- GDA Step 1 is the preparatory part of the design assessment process. It involves discussions between the Requesting Party 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 from the Requesting Party.
- GDA Step 2 is an overview of the fundamental acceptability of the proposed reactor design concept within the UK regulatory regime. The aim is to identify any fundamental design aspects or safety shortfalls that could prevent the proposed design from being acceptable for construction in the UK.
- GDA Step 3 is a system design safety and security review of the proposed reactor. The general intention is 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 analysing the supporting arguments made by the Requesting Party. From a security perspective, the foundations for developing the conceptual security plan are laid through dialogue with the Requesting Party.
- GDA Step 4 is designed to move from the system-level assessment of GDA Step 3 to a detailed examination of the evidence provided within the safety analyses, on a sampling basis. It will also seek to examine the proposed conceptual security plan. If the generic design is considered acceptable, we would issue a 'Design Acceptance Confirmation' at the end of GDA Step 4.

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). Before a reactor is constructed, two things are required: (i) a licence has to be granted by HSE; and (ii) subsequently, under the conditions attached to the site licence, permission to start the construction needs to be obtained from HSE. Phase 2 will enable HSE to carry out a site licence assessment, in which we will examine the proposed site, the management organisation of the operating company and the proposed type of facility to be installed on the site. 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

The intention is that the 'Design Acceptance Confirmation' would be carried forward from GDA to support the Phase 2 site-specific work and, in particular, HSE's assessment of whether to permit construction. It is our intention that there will be no reassessment of aspects included in the 'Design Acceptance Confirmation' except, of course, to address any Exclusions, new developments, site-specific elements, or any design changes proposed by the operator.

The 'Design Acceptance Confirmation' will therefore be required before permission to construct can be issued, but not necessarily before a site licence is granted. Ultimately the 'Design Acceptance Confirmation' can be used to underpin the permissions to construct a fleet of identical reactors, except for site or operator specific changes.

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 in advance of any significant construction activity.

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 where 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.

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 the assessment of potential new nuclear power stations. We believe this is improving efficiency both for the Nuclear Regulators and the Requesting Parties, and it helps to provide more effective regulation of potential hazards.

Following on from its Energy Review, the Government published an Energy White Paper in May 2007 (see www.decc.gov.uk), and at the same time, DTI (now the Department of Energy and Climate Change (DECC)) invited interested parties to submit proposals to the Nuclear Regulators for reactor designs to be subject to GDA. In the event, four designs were proposed.

- 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 and the Environment Agency formally started a dialogue with each Requesting Party and launched GDA in July 2007.

In April 2008 Atomic Energy of Canada Limited withdrew the ACR-1000 from GDA and in June 2008 we made a statement on our website that GDA Step 3 was commencing for the remaining three designs.

In September 2008, GE-Hitachi requested that assessment work on the ESBWR be suspended and we therefore continued to progress GDA Step 3 on the UK EPR and AP1000 reactor designs only.

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.

This new GDA process is being conducted in an open and transparent way. 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.

Introduction

The role of the HSE's Nuclear Directorate 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 we have been assessing the nuclear safety and security aspects of two reactor designs. We are examining these particular designs as they have been identified by DECC, as those most likely to be built in the UK, and which could therefore present a potential hazard to the public.

We launched GDA in July 2007. GDA Step 1 was devoted to preparatory work and was completed in August 2007. GDA Step 2, the fundamental safety overview was completed in March 2008 and we published a series of reports summarising our work and concluding that we had found no safety shortfalls that would rule out eventual construction of these reactors on licensed sites in the UK.⁴

This report is on the subject of GDA Step 3 of our assessment of the Westinghouse AP1000 reactor, the overall design safety review, and it covers the period from June 2008 to the end of October 2009. The aim of GDA Step 3 was to provide an overall design safety and security review of each design submitted, and in this case the AP1000 reactor, and specifically to:

- improve our knowledge of the design;
- identify significant issues;
- identify whether any significant design or safety case changes may be needed;
- identify major issues that may affect design acceptance and attempt to resolve them; and
- achieve a significant reduction in regulatory uncertainty.

It was also intended that GDA Step 3 would allow HSE inspectors to further familiarise themselves with the design and safety case and provide a basis for planning subsequent assessment work.

To achieve these aims, HSE has undertaken an examination of the AP1000 reactor at the system level and analysed Westinghouse's supporting arguments. From a security perspective, the foundations for developing the conceptual security plan have been laid through dialogue with Westinghouse.

In this report we describe the work we have completed, the safety issues that have emerged, and we give a summary of our assessment findings. To help manage our work, we have split it into 15 technical topic areas and our progress in each of these is summarised below. There are some additional introductory sections to help put our work into context and there are some additional summary sections (that do not fit easily into the 15 technical topic areas) which describe other activities, such as our work with overseas regulators, and on public involvement.

¹ 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 including radioactive waste and spent fuel storage facilities.

This report is intended to inform the public of our work on GDA and we believe it provides a comprehensive overview of our assessment to date. Further details can be found in the detailed supporting technical reports which have also been published via our website at www.hse.gov.uk/newreactors.

HSE expectations for modern reactors

HSE will require any nuclear reactor that is built in the UK in the near future to 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 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 remain safe under all these scenarios. We expect to see a robust demonstration of three key features: the ability to shutdown the reactor and stop the nuclear chain reaction; the ability to cool the shutdown reactor; and 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 could threaten the reactor. This should show that the reactor design is sufficiently robust to tolerate 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*⁵ (SAP). To help ensure HSE applies good international practice in its assessment, the SAPs were revised and updated in 2006 and this included benchmarking against the International Atomic Energy Agency (IAEA) Safety Standards.

HSE expectations from the GDA process

Details of HSE's expectations for the GDA process as a whole, and specifically for GDA Step 3 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 for GDA Step 3, is summarised in Annex 1.

Details of the expectations of the Office for Civil Nuclear Security (OCNS), which is a part of HSE, for GDA Step 3, can be found in the OCNS guidance.² In summary, the expectation is 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 assessment of the information HSE has gathered from Westinghouse during GDA Step 3 to address the points listed in Annex 1.

The safety standards and criteria used

The main document used for the GDA Step 3 assessment was the 2006 edition of HSE's *Safety assessment principles for nuclear facilities*⁵ (SAP). For radiological protection we also considered the requirements of the *Ionising Radiations Regulations 1999* (IRR99) and the *Radiation (Emergency Preparedness and Public Information) Regulations 2001* (REPIR2001).

Assessment strategy

The aim of GDA Step 3 was to provide an overall design safety and security review of each design, and this report covers our assessment of the AP1000 reactor. We have focused on an examination of the AP1000 reactor at the system level and analysed Westinghouse's safety arguments. Our objective was to ensure that the arguments that supported the safety claims were complete and that they were reasonable in the light of our current understanding of reactor technology. Examination of the detailed evidence to support these arguments will come in our assessment during GDA Step 4.

As we apply a sampling approach to assessment, there were some technical topic areas which were not significantly covered by our GDA Step 2 assessment. Therefore for GDA Step 3 in these areas we focussed firstly on the claims and then considered the arguments supporting those claims.

In our GDA Step 3 assessment, we have made a judgement on the claims and arguments as presented in Westinghouse's *AP1000 Pre-Construction Safety Report* (PCSR)⁶ and the *AP1000 European Design Control Document* (DCD).⁷ We have compared these against the relevant parts of HSE's Nuclear SAPs.⁵ To help us in this task we developed a strategy to define both the technical areas to be sampled and those SAPs most relevant for GDA Step 3 of the GDA process, and we planned and conducted our assessment accordingly.

In doing this we took account of our expectations for modern reactors, as described above. So our sample included the defence-in-depth provided by the systems for shutting down and cooling the reactor, and for containment of radioactivity.

Technical Support Contractors

As part of our drive to increase the pace of GDA we have placed work packages with contractors to help us carry out our detailed technical assessment. We established a framework agreement, including 31 Technical Support Contractors, across a range of 15 technical areas using the Official Journal of the European Union (OJEU) process.

It is common practice for us to engage specialist contractors in this manner to give technical and scientific support and advice to our assessment process. The scale of GDA and the timescale we are operating to, means that we are undertaking significant amounts of assessment work and therefore need significant additional technical support. We have thus far placed over 40 separate contracts under this framework in support of GDA.

However, all regulatory decisions in the generic design assessment process will continue to be made by the Nuclear Regulators – not by contractors.

Main features of the design and safety systems

The AP1000, as proposed to us by Westinghouse, is described in the *AP1000 Pre-construction Safety Report*⁶ (PCSR) and the *AP1000 European Design Control Document*⁷ (DCD).

Westinghouse describes the AP1000 as a pressurised water reactor based closely on the AP600 design which, although it achieved US Nuclear Regulatory Commission (US NRC) design certification, was never constructed. AP1000 maintains the AP600 configuration and the US licensing basis by limiting the design changes. It has a claimed operational design life of 60 years 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 Westinghouse claims 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 has a design life of 60 years.

The reactor core is comprised of 157 fuel assemblies, 4.26 m long, each with a 17 x 17 matrix of fuel pins 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.

Westinghouse 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 Westinghouse are:

Reactor shutdown

- The **reactivity control system**, which Westinghouse claims provides the means to trip the reactor, maintain a safe shutdown condition, and control reactivity in the event of certain anticipated events. It comprises the protection and safety monitoring system, plant control system, the diverse actuation 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 Westinghouse 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, Westinghouse claims long-term containment recirculation can be provided by natural convection driven flow;
 - a **passive containment cooling system**, which provides the 'safety-related' ultimate heat sink for the plant. This is a gravity fed cooling water delivery system connected to the passive containment cooling water storage tank mounted on the reactor building roof that provides an even flow of water over the surface of the containment. Westinghouse 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; and
- the **main control room emergency habitability system**, which provides fresh air, cooling and pressurisation to the main control room to prevent it becoming contaminated in accident scenarios.

Westinghouse 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 expansion of compressed gas). They are activated by the operation of a few valves and Westinghouse claims they are designed to meet the single-failure criterion, and to support probabilistic risk analysis (PRA) safety goals.

Containment

- The reactor shield building is composed of a conventional reinforced concrete steel structure together with steel-concrete-steel (SCS) sandwich sections. Within the shield building is the steel containment vessel which provides a continuous, pressure retaining, envelope around the primary circuit heat transport systems. Westinghouse claims that a containment isolation system will ensure adequate isolation of the containment by ensuring relevant penetrations are closed.

Retention of molten core debris

- Westinghouse 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, provided either by 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 system design and security review which comprised Step 3 of the GDA process.

Internal hazards

Our safety assessment within this topic includes hazards such as fire, explosion, flood, dropped loads, pressure part failure, and steam release etc. within the reactor buildings. We have considered the adequacy of: the identification of hazards; prevention of hazards; and the protective barriers, segregation, separation, and active protection systems that are included within the design to provide mitigation in the unlikely event that such internal hazards should occur.

For GDA Step 3 our assessment sample covered internal hazards assessment of the claims and arguments contained within the PCSR[®] and other supporting documents. We also sought to confirm, or otherwise, that the observations made during GDA Step 2 had either been addressed or were in the process of being addressed during GDA Step 3.

From our assessment we have concluded that:

- the safety case provided by Westinghouse has significant shortfalls in comparison with our SAPs and our assessment has identified areas where

further work will be required before we can consider that the safety case is acceptable;

- the PCSR⁶ and supporting references to it have been presented in such a way as to make assessment of this topic area difficult, as it was not treated as a stand-alone subject and related claims and arguments are spread across different documents. This was identified to Westinghouse during GDA Step 3 and in response it committed to produce a new Topic Report whose scope is to present the safety case for internal hazards in a complete way with claims, arguments and evidence set-out in a structured manner;
- for our GDA Step 3 assessment, we have therefore only had the limited detailed information that is contained within the PCSR⁶ and supporting references. As a result, not all areas within this topic have, as yet, been assessed to the same extent and for some we have been unable to form a judgement about the adequacy of protection against internal hazards;
- in some of the areas that we have already assessed we found that there was a lack of detailed claims and arguments. We have asked Westinghouse to address these shortfalls by providing additional information and evidence; and
- as the Topic Report was only supplied to us close to the end of GDA Step 3, and in view of the other detailed information that Westinghouse needs to provide, we have not yet been able to form a judgement on the risk posed by internal hazards for the AP1000 reactor.

For GDA Step 4, we have identified areas where further work is required, or where additional information needs to be provided. These include the following items.

- The Internal Hazards Topic Report submitted by Westinghouse will be the subject of a detailed assessment within GDA Step 4.
- Westinghouse needs to provide additional information and evidence relating to claims and arguments for internal hazards and this will need to be provided by Westinghouse in sufficient time for it to be assessed by us during GDA Step 4.

In summary, there is additional work to be done by Westinghouse to satisfy our questions in the internal hazards area and to make and present an adequate safety case. However, we consider that this is achievable within the GDA Step 4 timeframe, and in sufficient time to allow us to carry out a meaningful GDA assessment. At this stage it is too early to say whether any of the additional work by Westinghouse or HSE will identify the need for design modifications (in the topic of internal hazards these could be, for example, additional fire barriers, or improved segregation of equipment).

Civil engineering

For GDA Step 3 our assessment has covered the claims and arguments contained within the PCSR⁶ and other supporting documents for the integrity of structural components such as steel-framed buildings and concrete structures.

From our assessment we have concluded the following.

- At this stage, Westinghouse has not presented an adequate safety case for the civil structures.
- Civil structures are normally built in accordance with approved design codes. These help the designer ensure, for example, that adequate safety margins are included, and their use therefore also gives regulators confidence in the safety of the structures. Our assessment found that there appears to be a lack of an appropriate design code for the novel steel-concrete-steel (SCS) sandwich modular construction proposed for the AP1000. Westinghouse states that the design is to an American code (ACI-349); however, this code is not applicable to this type of construction.

- Westinghouse did not supply a design methodology for the SCS modules when we first asked for this during GDA Step 3. We have recently received a report on this topic, but this was too late to consider as part of our GDA Step 3 assessment.
- Amongst our technical concerns are whether transverse shear, in-plane shear and thermal loads are acceptable in the SCS modules. In response to a request from us, we only received a report about the design of the Enhanced Shield Building (which in part is one of the SCS modular structures) towards the end of GDA Step 3, but this was too late to consider as part of our GDA Step 3 assessment.
- The plans in the PCSR⁶ are considered to be adequate at this stage in respect of civil engineering provision for decommissioning.

For GDA Step 4, we have identified areas where further work is required, or where additional information needs to be provided. These include the following items.

- Westinghouse should carry out a detailed review of the adequacy of the codes and standards used and to provide a justification of these early in GDA Step 4.
- Westinghouse should undertake an assessment of whether the combined effects of design code (or other design methodology) and the loads, analysis, modelling and construction verification will deliver the required reliabilities.
- Westinghouse should carry out an assessment of the building transitions (both in plan and in elevation) between conventional reinforced concrete and SCS sections of the Shield Wall and the similar Auxiliary Building transition.
- Westinghouse should address the topic of construction verification in its safety case.
- We will conduct a series of design audits and will use these to determine the compliance of the designs with the design methodology.

In summary, there is a significant amount of additional work to be done by Westinghouse to satisfy our questions in the civil engineering area and to make and present an adequate safety case. However, we consider that this is achievable within the GDA Step 4 timeframe, and in sufficient time to allow us to carry out a meaningful GDA assessment. It is possible that this additional work might identify the need for some modification to the design of civil structures.

External hazards

External hazards are those natural or man-made hazards that originate externally to both the site and the process and over which the operator has little control. External hazards include earthquake, aircraft impact, extreme weather, and flooding, and the effects of climate change. Terrorist or other malicious acts are also assessed as external hazards.

A complication for this assessment topic area is the site dependent nature of both the magnitude of the external hazards or the local conditions which may dictate design choices. As a consequence there are a large number of areas where definitive statements over the acceptability of the design cannot be confirmed until Phase 2 (site licensing).

For GDA Step 3, our assessment has covered the claims and arguments contained within the PCSR⁶ and other supporting documents.

From our assessment we have concluded the following.

- at this stage Westinghouse has not presented an adequate safety case for external hazards;
- Westinghouse has stated the generic design conditions that it has applied to the plant in the generic design. Site-specific aspects will require further

- consideration once a site or sites have been identified;
- the range of hazards considered is reasonable, except that there does not appear to be a consideration of lightning or malicious acts (other than malicious large commercial aircraft), or a specific recognition of climate change as a driver for a number of hazards; and
 - the approach Westinghouse has adopted appears to be to screen-out some external hazards and claim system availability rather than demonstrate how the functional performance of a safety component is to be delivered in response to that hazard. Our expectation is that external hazards that could affect the safety of the facility should be identified, treated as events that can give rise to possible initiating faults, and then there should be a demonstration that the component can perform its safety function.

For GDA Step 4, we have identified areas where further work is required, or where additional information needs to be provided. These include the following items.

- Westinghouse needs to provide justification that the range of hazards considered is comprehensive and that the treatment of these in the safety case is adequate, including those hazards that currently appear to be screened out, lightning and malicious acts (other than malicious large commercial aircraft).
- We will review Westinghouse's assessment of the impact of large aircraft.
- Westinghouse needs to provide justification that there are adequate defences in place to ensure that vulnerability to common cause failure is acceptably low.
- Westinghouse should consider whether adequate segregation is provided by the current arrangement where the battery rooms, the control room and the auxiliary control room are all located on the same side of the Auxiliary Building, close to the Main Steam Isolation Valves.

In summary, there is additional work to be done by Westinghouse to satisfy our questions in the external hazards area and to make and present an adequate safety case. However, we consider that this is achievable within the GDA Step 4 timeframe, and in sufficient time to allow us to carry out a meaningful GDA assessment. At this stage it is too early to say whether any of the additional work by Westinghouse or HSE will identify the need for design modifications (in the topic of external hazards these could be, for example, strengthening the civil structures, or improved segregation of equipment).

Probabilistic Safety Analysis

Probabilistic Safety Analysis (PSA) is an integrated, structured, logical safety analysis that combines engineering and operational features in a consistent overall framework. It is a quantitative analysis that provides measures of the overall risk to the public that might result from a range of faults (for example, failure of equipment to operate, human errors, or hazards such as fires). PSA enables complex interactions, for example between different systems across the reactor, to be identified and examined and it provides a logical basis for identifying any relative weak points in the proposed reactor system design.

For GDA Step 3, our assessment has examined the arguments presented by Westinghouse (ie the methods, techniques and scope of the PSA) that support its high level safety claims. We also carried out some in-depth spot checks of models and data to gather information on how the PSA methods and techniques have been applied by Westinghouse. In addition, we have reviewed in detail the part of the PSA that deals with the 'identification of internal initiating events during operation at power' to confirm whether the basis of the PSA is robust and to gain confidence on its completeness.

From our assessment we have concluded the following.

- The PSA provides some basis to help interpret the risk associated with the AP1000 reactor and to identify where the main design strengths and relative weaknesses may lie.
- The PSA has been presented in a modern framework consisting of a Level 1 (focusing on the potential for reactor core damage), Level 2 (considering magnitudes and frequencies of releases of radioactive material to the environment), and Level 3 PSA (addressing risks to the public from off-site releases). Our assessment so far has mainly focused on the Level 1 and Level 2 PSA. The Level 3 PSA has not been reviewed during GDA Step 3.
- In PSA, initiating events are those disturbances (for example the failure of a system to operate, or the start of a fire in an electrical system) that require mitigation to prevent radioactive releases. In this regard, the scope of the PSA includes consideration of initiating events originating from reactor system failures and from two internal hazards (internal fires and floods). The scope of the PSA covers full power, low power and shutdown operating states. We consider that this scope is reasonable in principle, except that it does not include external hazards (such as earthquakes) and the decision not to include other internal hazards has not been justified. In addition, we will require further justification that the range of initiating events included is comprehensive.
- The methods and data used in the PSA are well known, although not always up-to-date or aligned with the latest international good practices. For example we have raised questions regarding the completeness of the system models, the validity of the reliability data used, the method used for the detailed analysis of internal fires and the completeness of the analysis of internal flooding events.
- The results of the PSA presented by Westinghouse show that the risk to the public is low and they provide a degree of confidence that the relevant Numerical Targets of the SAPs⁵ will be met. Although we have identified shortcomings in the scope, methods and data used in the PSA, we do not have any reason, at the moment, to believe that this position will change dramatically once the PSA has been completed and updated. However, the completion and modernisation of the PSA is required so that it can provide a better input into the demonstration that the risk associated with the AP1000 is 'as low as reasonably practicable' (ALARP).

For GDA Step 4, we have identified areas where further work is required and where additional information needs to be provided. Westinghouse has committed to significant effort to update the PSA and bring it up to modern standards. We will discuss with Westinghouse in depth the (extensive) current, planned and expected developments of the PSA, including the methods, sources of data and programme. We will use the information compiled from, and outcome of, this dialogue to target our assessment in GDA Step 4.

In recent discussions we have reluctantly agreed with Westinghouse that it will not be reasonably practicable for it to complete all the activities required to update the PSA in sufficient time to enable us to carry out a full assessment during GDA Step 4. Therefore, we have identified aspects that we feel are necessary to be completed and assessed in GDA Step 4, and other aspects where we believe it is appropriate for them to be completed during Phase 2 (site-specific work). Those elements not available for assessment in GDA Step 4 may become 'Exclusions' to the 'Design Acceptance Confirmation', if one is issued, at the end of GDA.

Design basis analysis/fault studies

The design basis analysis and fault studies are the safety analyses of nuclear reactors on matters such as reactor core physics, thermal hydraulics, heat transfer and a wide range of other physical phenomena under steady state, transient and fault conditions.

Fault analysis involves a detailed study of the reactor system, its characteristics and mode of operation, with the aim of identifying possible faults that might occur and lead to a release of radioactive material. This is followed by a thorough examination of the conditions brought about by those faults. In particular, for those conditions which might affect the integrity of the nuclear fuel, the aim is to demonstrate the adequacy of the engineered protection systems in preventing the release of radioactive material.

This is a topic area where we did not have sufficient resource in place at the beginning of GDA Step 3 and this has limited the sampling that we have been able to undertake. We now have recruited additional staff to cover this topic area and intend to significantly accelerate our assessment during GDA Step 4. During GDA Step 3 our assessment has concentrated on reviewing the core design, design basis analysis and certain aspects of the severe accident analysis.

From our assessment we have concluded the following.

- Westinghouse has provided a safety analysis that is generally satisfactory but there are still some areas where further work and additional information is required. We see no fundamental reason to believe from the fault study perspective that a satisfactory safety case cannot be made for AP1000.
- In general, the range of faults considered within the DCD⁷ is less comprehensive than we require, and we are asking Westinghouse for additional work in this area. Nevertheless, there was adequate information to enable the characterisation of the fault conditions for the AP1000 to be made for the purposes of our assessment.
- Westinghouse will be required to provide more comprehensive information within the PCSR⁶, for us to assess during GDA Step 4. For example, judgements regarding the importance of the basic assumptions in fault analyses depend upon sensitivity studies in which input information is varied. While some information of this kind has been made available, more comprehensive sensitivity analyses will be necessary in GDA Step 4.
- The design basis analyses presented are only concerned with single events as initiators of a fault sequence. Attention needs to be paid to complex situations in which a combination of events may initiate a fault sequence.

For GDA Step 4, we have identified areas where further work is required, or where additional information needs to be provided by Westinghouse. These include the following items.

- Westinghouse needs to demonstrate that the list of design basis initiating events is complete, including faults at shutdown and for the spent fuel pool. The list of design basis initiating faults will need to be reconciled with those of the PSA. A design basis safety case is required for each fault.
- Westinghouse needs to review all design basis initiating events with a frequency of greater than 1×10^{-3} per year and demonstrate that a diverse safety system, qualified to an appropriate standard, is provided for each safety function. The single failure criterion also needs to be extended to include passive failures.
- A radiological consequence assessment needs to be performed for each design basis fault.
- The proposal to use the Westinghouse BEACON reactor physics code to demonstrate on-line compliance with the fuel safety technical specifications will need to show that an independent method exists for the operator to ensure compliance.
- Westinghouse needs to demonstrate that the fuel is protected from pellet-clad interaction (PCI) failure for frequent faults. The feasibility of connecting the in-core detectors to the reactor protection system needs to be considered.
- The group of faults that include the low probability of failure to trip the reactor by insertion of control rods (the so-called Anticipated Transient without Trip (ATWT)

faults) need to be included by Westinghouse within the design basis. Related to this, an ALARP justification for not installing an emergency boration system will also be required from Westinghouse.

- Westinghouse needs to provide further evidence to show that the engineered safety systems are not only capable of stabilising the plant immediately after a fault but are also capable of taking the plant to a 'safe shutdown' state that can be maintained in the long term.
- The assessment of large-break loss-of-coolant accidents compares the fuel cladding temperatures expected against safety limits. This analysis needs to include detailed consideration of the potential for fuel channel blockage caused by features of the transient such as plastic buckling of spacer grids.
- Westinghouse claims to have made a case for the retention of core material in the vessel should the core melt in a severe-accident. The modelling of melt progression is currently a complex area with significant uncertainty. We will further examine this research.

In addition to examining the outcome of the above, in GDA Step 4 we will:

- extend our assessment to examine the thermal hydraulic analysis performed in support of the PSA success criteria;
- review the internal and external hazards assessment safety cases from a fault study perspective; and
- review in detail the validation of the computer codes and carry out independent confirmatory analyses for selected cases.

The work to address some of our concerns may ultimately require changes to the plant design. In our judgement, these changes would largely be associated with changes to the reactor protection system or the qualification of systems to an appropriate standard.

Reactor protection and control

Control systems are typically those that are used to operate the plant under normal conditions and reactor protection systems are those safety systems that are used to maintain control of the plant if it goes outside normal conditions. The assessment in this topic area includes reviews of both hardware and software aspects. This topic is also commonly referred to as both Control and Instrumentation (C&I) and, confusingly, I&C, but we will refer to the former throughout this report.

For GDA Step 3 our assessment sample covered topics of particular relevance to C&I system-level design, including a review of C&I system architecture and diversity of systems implementing reactor protection functionality.

From our assessment we have concluded the following.

- Westinghouse's safety arguments for C&I set out in the PCSR⁶ include a claim of compliance to US C&I standards and guidance, and C&I provisions 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) and Diverse Actuation System (DAS));
 - plant control and monitoring systems (eg the Plant Control System that performs functions such as reactor power control); and
 - main control room with backup via the remote shutdown workstation, and communication systems for information transfer within and external to the plant.
- The PCSR⁶ and supporting documentation address the main C&I systems expected in a modern nuclear reactor but the safety case arguments need improving.

- The acceptability of the C&I architecture depends critically upon substantiation of the reliability values for the PMS, DAS and for the reliability values claimed for the combination of the two. Due to the importance of this aspect of the AP1000 safety justification, we will examine the C&I reliability claims in greater depth during GDA Step 4.
- The DAS design is incomplete and we have been unable to complete a meaningful assessment. If additional information is not available for assessment in GDA Step 4 this will become an 'Exclusion' to the 'Design Acceptance Confirmation', if one is issued, at the end of GDA.

For GDA Step 4, we have identified areas where further work is required, or where additional information needs to be provided. These include the following items.

- Improvement of Westinghouse's safety case arguments.
- Assessment by HSE of the sensitivity of the Plant Monitoring System (PMS) and Diverse Actuation System (DAS) reliability values claimed.
- Further substantiation is required from Westinghouse to support the categorisation of DAS functions, its equipment classification and its contribution to the safety groups that implement Category A (reactor protection) functionality
- Westinghouse needs to substantiate the adequacy of the diversity between the DAS and PMS.
- Westinghouse needs to provide further evidence for the adequacy of the process for development of the PMS application code (note that writing the actual application code for the UK implementation of the PMS has already been declared to be out-with the GDA scope by Westinghouse).

Some of our concerns may ultimately require changes to the design of the C&I.

Essential electrical power systems

Many of the important systems on a nuclear power station require electrical power for their operation (pumps, valves etc). The safety assessment in this topic area typically therefore covers the engineering of the essential electrical power supply systems, examines these under a wide range of transient and fault conditions and considers their likely reliability, and the performance of protection devices.

This is a topic area where we did not initially have sufficient resource and our assessment only commenced part way through GDA Step 3. This had the consequence of limiting the sampling that we have been able to do thus far but we intend to significantly accelerate our assessment during GDA Step 4.

During GDA Step 3, our assessment has concentrated on electrical systems reliability aspects, examining the scope and extent of arguments and considering whether the overall design is balanced in terms of the different contributors to the overall risk from the plant (ie considering what electrical plant failures could occur and where there is adequate protection to protect against or cope with such failures). We also considered the need for additional regulatory analysis and modelling of the electrical systems under normal and fault conditions.

From our assessment we have concluded the following.

- Westinghouse provided a safety analysis that was generally satisfactory for GDA Step 3, but there are areas where further work is required and additional information needs to be provided to enable a complete assessment of the scope and extent of the safety case. Examples include the need for more detail on the distribution network (including the DC system), the safe operating envelope and operating regime, the completeness of the design and justification of codes and standards used.

- At present there is insufficient detail in the Westinghouse submission to fully support our GDA Step 4 detailed review and to assess the validity of the arguments and evidence to support the safety claims made for the system.
- The topic of safety function categorisation and system safety classification, which is discussed elsewhere in this report, could be significant for the electrical system assessment. The safety categorisation and classification system used by Westinghouse is not in accordance with international good practice, and work needs to be done by Westinghouse to review this, and address the implications for electrical systems.

For GDA Step 4, we have identified areas where further work is required, or where additional information needs to be provided. These include the following items:

- The preparation and presentation of a complete set of claims, arguments and evidence to support the safety case.
- The topic of safety function categorisation and system safety classification could have a major impact on the design requirements for the AC electrical system. Westinghouse currently does not classify the AC system as a safety system but our preliminary view is that it should meet standards for safety systems. Further work is required in this area.
- Definition of applicable International Electrotechnical Commission (IEC) codes and standards and the justification of the design against these.
- Software and hardware verification for programmable devices and other embedded controls for systems that are significant for safety.
- Electrical system studies and load flows, electrical protection and relay discrimination and transient stability studies.
- Other detailed aspects covering maintenance philosophy, DC system design, operation and monitoring.

Westinghouse has committed to addressing these issues early in GDA Step 4.

Some of our concerns may ultimately require changes to the design of the essential electrical power systems, although it is currently too early to form a judgement on this.

Fuel design

Within this topic we typically look at the performance of the reactor fuel under a wide range of reactor and storage conditions.

This is a topic area where we did not have sufficient resource in place at the beginning of GDA Step 3 and this has limited the sampling that we have been able to do. We now have sufficient staff to cover this topic area and intend to significantly accelerate our assessment during GDA Step 4.

Our GDA Step 3 assessment has restricted itself to consideration of the fuel assembly and has to-date omitted detailed consideration of other fuel related components. We have concentrated on reviewing the design criteria against which the fuel integrity is assessed and areas for which existing pressurised water reactor operating experience has highlighted fuel performance shortfalls (eg the effects of fuel assembly irradiation growth, and the formation of crud and stress-corrosion cracking of the fuel cladding in power transients).

From our assessment we have concluded the following.

- Westinghouse has provided a wide-ranging safety analysis in the fuel design topic area and that the substantiation of claims and arguments is generally adequate for GDA Step 3, but with certain shortfalls. These will be assessed

further in GDA Step 4, focusing on fuel safety criteria such as Pellet Clad Interaction (PCI) and Critical Heat Flux (CHF).

For GDA Step 4, we have identified areas where further work is required, or where additional information needs to be provided by Westinghouse. These include the following items.

- Further work is required and additional information needs to be provided on fuel safety criteria including PCI, crud, CHF and high-temperature fuel deformation.
- The control of reactor coolant chemistry has a significant effect on fuel performance in normal operation; especially on the likely levels of crud deposited on the fuel. This aspect of the design has yet to be finalised.
- The safety criterion for the fuel is the peak fuel enthalpy in faults and the justification against this needs to be updated to reflect modern practice for fuel at moderate irradiation levels. The clad stress limit also needs to be reduced to better reflect the effect of rapid power changes on the likelihood of clad failure.
- The justification of safety by Westinghouse of the long-term storage of the fuel before final disposal, including focusing on the role of levels of burn up.
- A number of additional criteria that might be important for the fuel safety case are implied in the design substantiation and these will need to be included formally in the safety case. These include the peak fuel corrosion and the peak irradiation levels.

It is expected that the outstanding issues can be resolved by Westinghouse in sufficient time before the end of GDA Step 4 and in sufficient time to allow us to complete a meaningful GDA assessment.

Reactor chemistry

The safety assessment of the chemistry of new nuclear reactors includes the effects of coolant chemistry on pressure boundary integrity, fuel and core component integrity, fuel storage in cooling ponds, radioactive waste (accumulation, treatment and storage), and radiological doses to workers.

This is a topic area where we did not have sufficient resource in place at the beginning of GDA Step 3 and this has limited the sampling that we have been able to do. We now have sufficient staff to cover this topic area and intend to significantly accelerate our assessment during GDA Step 4.

Our GDA Step 3 assessment concentrated on reviewing the claims implied within the safety case as presented in the PCSR⁶ and the DCD.⁷ However, coupled with information gained from an on-going dialogue with Westinghouse, this was sufficient to allow us also to consider some of the arguments made by Westinghouse in support of these claims, mainly in relation to the main processes controlling primary circuit chemistry in normal operation.

From our assessment we have concluded the following.

- Westinghouse has put considerable effort into the chemistry of AP1000 but the principal aspects of the demonstration of safety need improvement.
- Severe accident chemistry has received significant attention, however some of the analyses appear to be dated and we will need to establish the relevance to the AP1000 during GDA Step 4.
- Not all areas have been assessed by us to the same extent due to the limited amount of detail in some of the analyses presented to date by Westinghouse.
- Westinghouse is not currently planning to undertake key analyses of secondary circuit safety and this is something we will be asking them to provide to us.

For GDA Step 4, we have identified areas where further work is required, or where additional information needs to be provided. These include the following items.

- Westinghouse should produce a comprehensive overview of reactor chemistry (including boron chemistry and faults).
- Westinghouse should provide further justification of the chemical behaviour of the chemistry control systems and other novel, simplified and passive systems.
- Westinghouse should provide further justification for Zinc dosing.
- Westinghouse should provide further justification of the relevance of severe accident chemistry analyses to the AP1000.
- We will assess the chemistry of fuel and accidents, in coordination with our assessment of fault studies.
- We will sample other chemistry aspects of severe accidents.

The possibility of changes to a part of the primary coolant circuit or its ancillaries arising from analyses and assessments during GDA Step 4 cannot be ruled out. Indeed, Westinghouse has itself recently identified design changes for specific chemistry aspects of the AP1000, in relation to control of gases in the primary circuit.

Radiological protection

This is a topic area where we did not have sufficient resource in place at the beginning of GDA Step 3 and this has limited the sampling that we have been able to do. We now have sufficient staff to cover this topic area and intend to significantly accelerate our assessment during GDA Step 4.

Our GDA Step 3 assessment strategy was to consider doses to workers during normal operation (including outages and maintenance work), doses to members of the public during normal operation due to direct radiation, and doses to workers and to members of the public during accident conditions. In particular we considered whether exposure to radiation was 'as low as reasonably practicable' (ALARP).

From our assessment we have concluded the following.

- Westinghouse has provided a reasonable safety analysis in the radiological protection topic area for the principal plant under normal operations.
- The substantiation of claims and arguments is adequate for GDA Step 3.

For GDA Step 4, we have identified areas where further work is required, or where additional information needs to be provided. These include following items.

- Westinghouse will need to provide the detailed evidence to demonstrate the robustness of the ALARP arguments.
- We will assess Westinghouse's arguments and evidence for occupational and public radiation exposure during accident conditions.
- We will assess the topic of radiation exposure associated with the fuel route.
- We will assess the Level 3 PSA (addressing risks to the public from off-site releases).

During our GDA Step 4 assessment of radiation protection there will be close liaison with other assessment areas, particularly human factors, probabilistic safety assessment, fault studies, mechanical engineering, reactor chemistry, radioactive waste management and decommissioning.

Mechanical engineering

This typically includes the safety assessment of essential mechanical items important to safety such as pumps, valves, lifting equipment including cranes, fuel

handling equipment, ventilation systems etc. It also includes the layout and routing of the mechanical equipment and systems to ensure appropriate maintenance regimes and protection from degradation.

For GDA Step 3 our assessment examined the claims and arguments and identified the evidence relating to mechanical engineering aspects. As mechanical engineering covers a broad range of equipment types, our assessment approach has been to review selected 'structures, systems and components' (SSC) in terms of their safety functions against our regulatory expectations. Our assessment focussed on the following.

- Assessing the scope and extent of claims and arguments presented.
- Reviewing the level of design completeness.
- Assessing relevant aspects of the safety case, specifically safety categorisation and classification, design and reliability claims and equipment qualification.
- Considering whether the mechanical design aspects are likely to meet their safety functions in normal and fault conditions.
- Considering the layout, access, ingress and egress provisions to facilitate operation, inspection, testing, maintenance and equipment replacement.

From our assessment we have concluded the following.

- Westinghouse has yet to present a fully satisfactory safety case for the mechanical aspects of the design.
- The topic of safety function categorisation and safety classification, which is discussed elsewhere in this report, is significant for the mechanical engineering assessment. The safety categorisation and classification system used by Westinghouse is not in accordance with international good practice, and work needs to be done by Westinghouse to review this, and address the implications for mechanical items.
- We have significant concerns regarding the Squib Valve concept, used as part of the Passive Core Cooling System, in respect of its present incomplete state of design and development. (Squib valves are a particular design of fast acting valve operated by propellant charges, whose application on AP1000 is novel).
- We have concerns regarding the adequacy of the High Efficiency Particulate Air (HEPA) filtration provided for Nuclear Ventilation systems. These filters play a fundamental part in protecting people, society and the environment from the hazards of radiation.
- We have gained a level of confidence in the design process applied by Westinghouse in certain areas. Sampled areas that provided this confidence included: the reactor cooling system pumps, where we reviewed Westinghouse's supply chain; control rod drive mechanisms, and the development tasks that are being undertaken; and in the selection process for valves.

For GDA Step 4, we have identified areas where further work is required, or where additional information needs to be provided. These include the following items.

- Westinghouse needs to prepare and present a more complete set of claims, arguments and evidence to support the safety case.
- A review by Westinghouse of the adequacy of the safety categorisation and classification of mechanical items. (Westinghouse has undertaken to carry out this detailed review of this aspect and to provide justification early in GDA Step 4).
- Westinghouse needs to provide adequate design qualification for the Squib Valve concept and design realisation.
- Westinghouse needs to address our concerns regarding the lack of adequate HEPA filtration in Nuclear Ventilation systems.
- Contrary to our requirement¹, the AP1000 design documents submitted to us are based on Imperial units. We have asked Westinghouse for a programme and an action plan for how they will convert the AP1000 to metric units. We

will expect this programme and plan to be comprehensive and compatible with timescales for potential construction in the UK.

Some of our concerns may ultimately require changes to the plant design. It is however too early to form a judgement on the need or extent of any design changes needed.

In addition, any design changes introduced by Westinghouse at this stage, such as the current proposals to make changes to the design (in relation to control of gases in the primary circuit) may well adversely affect our ability to carry out a meaningful GDA assessment by June 2011, in which case we would not accept them into the GDA assessment scope.

Structural integrity

This topic includes the safety assessment of nuclear safety related metal pressure vessels, piping, other components and their supports, including materials selection, design, fabrication, in-manufacture examination and testing, the analysis of structural integrity under normal load and faulted conditions (including fracture mechanics based analyses), and lifetime ageing of materials assessment (including neutron irradiation embrittlement).

For GDA Step 3, our assessment examined the arguments and identified the evidence relating primarily to the highest integrity structural integrity components such as the Reactor Pressure Vessel, Steam Generators and Pressuriser.

From our assessment we have concluded the following.

- For components where ‘the likelihood of gross failure is claimed to be so low it can be discounted’, a more comprehensive method of achieving and demonstrating integrity consistent with this level of safety claim needs to be implemented.
- Aspects of the chemical composition of the low alloy ferritic steels for the main vessels (Reactor Pressure Vessel, Steam Generators and Pressuriser) remain to be resolved. However, we anticipate that this can be done within GDA Step 4.
- For neutron irradiation embrittlement of regions of the Reactor Pressure Vessel, the design takes account of what is now known regarding chemical composition of the base materials and welds. However, the end-of-life maximum neutron dose to the forgings is quite high and requires further investigation.
- We have made useful progress in understanding the approach which Westinghouse has proposed for setting pressure-temperature limit curves for the Reactor Pressure Vessel. This is something we will look at further during GDA Step 4.
- The use of castings for the Reactor Coolant Pump Bowl construction has been justified. However, there are still aspects to resolve in how to deal with large repairs to the castings made by welding (this is a potential feature of the manufacturing process). The areas still open relate to how to obtain confidence that crack-like defects of a size of concern for integrity can be detected (defects might be introduced during the weld repair process).
- Westinghouse has proposed the use of Alloy 690 in the ‘Thermally Treated’ condition, and we consider this is a sound choice of material for Steam Generator Tubing.
- The design of the steel containment shell within the Shield Building complies with the relevant part of the American Society of Mechanical Engineers (ASME) code, but there are a number of matters to take forward for further assessment in GDA Step 4 (identified below).

For GDA Step 4, particular areas where programmes of work have been proposed, or where further work is required or additional information needs to be provided include the following.

- Westinghouse has proposed a programme to identify which components have the claim that the likelihood of gross failure is so low it can be discounted. Completion of the programme of work will extend well into GDA Step 4.
- Westinghouse has proposed a programme to implement an appropriate approach to achieving and demonstrating integrity for components where they claim 'the likelihood of gross failure is so low it can be discounted'. We expect to see significant progress on this during GDA Step 4.
- Aspects of the chemical composition of the low alloy ferritic steels for the main vessels (Reactor Pressure Vessel, Steam Generators and Pressuriser) remain to be resolved.
- Westinghouse should undertake an ALARP review of practical options for meaningful reduction of neutron dose to the Reactor Pressure Vessel. As a minimum this should consider the locations of peak neutron dose, which occur in the forging. There may be the potential to adopt a 'low leakage core' fuel management arrangement in service.
- Westinghouse needs to provide justification that the approach to be used for pressure-temperature limit curves for the Reactor Pressure Vessel is ALARP.
- For the Reactor Coolant Pump Casing construction, Westinghouse needs to provide justification that, for potential large weld repairs, crack-like defects of a size of concern for integrity can be detected.
- For the steel containment shell (enclosed by the Shield Building), Westinghouse needs to provide justification of the plate thickness available for corrosion allowance, the toughness properties of the plates and welds to meet the requirements for no post-weld heat treatment, and tolerance on plate thickness (which is relevant to both corrosion allowance and no post-weld heat treatment).
- We will undertake assessment of design specifications, analyses for loading conditions (mainly thermal-hydraulics analyses), design reports, and equipment specifications for a range of components.

A number of the areas identified for assessment in GDA Step 4 will require significant effort and programmes of work on the part of Westinghouse if a meaningful GDA is to be achieved by June 2011.

Human factors

The safety assessment of the human factors aspects of the new nuclear power stations is focused on ensuring that the human actions that are needed to contribute to safety are feasible.

This is a topic area where we did not initially have sufficient resource and our assessment only commenced part way through GDA Step 3. This had the consequence of limiting the sampling that we have been able to do thus far but we intend to significantly accelerate our assessment during GDA Step 4.

For GDA Step 3 our assessment concentrated on the following.

- Reviewing if the Westinghouse PCSR⁶ provides a clear justification for the role of human action on the nuclear power plant.
- Seeking to assure ourselves that Westinghouse understands and can justify the contribution of human actions to safety.
- Seeking assurance that Westinghouse has human factors analysis to support the human based safety claims and that the age of this supporting analysis is acceptable when compared to modern standards.
- Reviewing whether the standards Westinghouse has used are appropriate and that there has been an adequate integration of human factors into the overall design and into the PCSR⁶ and supporting documents.

From our assessment we have concluded the following.

- The PCSR⁶ and DCD⁷ do not present analysis and argument in a clear and acceptable structure (ie the claims, argument and evidence chain of reasoning) and they do not present an overview of the human based safety claims or clearly highlight what the human contribution to safety is for the AP1000.
- As part of our work on the PSA Human Reliability Analysis we have had some transparency on the human contribution to safety, however concerns on the scope and quality of the PSA have been raised in the GDA Step 3 PSA assessment (see the relevant section above).
- The human factors analysis and argument does not appear to be fully integrated with Westinghouse's PSA work.

Therefore, at this time we have limited confidence that the PSA includes a complete understanding of the human contribution to safety. This has presented us with difficulties in the area of human factors, considering that our assessment strategy for GDA Step 3 was focused on the safety claims. This will also limit us in our ability to progress our future assessment as the strategy for GDA Step 4 will be to target on a proportionate basis those areas where the human contribution to safety is greatest.

We have made several attempts to discuss with Westinghouse how to bridge what we consider to be a knowledge gap on its part in terms of our expectations for safety case presentation, but with limited success to date.

For GDA Step 4, we have identified a single overarching requirement for further work and that is for Westinghouse to prepare and present a complete set of claims, arguments and evidence to support the safety case.

In response Westinghouse has committed to developing a safety case in the area of human factors and has provided a programme of work for this which is fully resourced using suitably qualified and experienced personnel.

Westinghouse's detailed programme provides a commitment to deliver an adequate human factors safety case early in GDA Step 4, and successful delivery of this would allow us time to assess it before the end of GDA.

Quality management and safety case development arrangements

In GDA Step 3 we have continued our GDA Step 2 assessment to examine the quality assurance arrangements for delivery of an adequate safety case submission.

From our assessment we have concluded the following.

- The quality of the safety case relies heavily on the application of sound quality management principles. Westinghouse has a well established Quality Management System but we have yet to determine whether the full extent of this has been applied to the project for delivery of the UK AP1000 safety case.
- During the course of the project there have been a number of quality initiatives set up across Westinghouse, eg self-assessment. These initiatives support the concepts of a learning organisation and continuous improvement (including learning from experience) and as such we see these as positive.
- Through an Inspection early in GDA Step 3 we have confirmed that the configuration control/change management processes within Westinghouse are well established and that there is evidence that these documented arrangements are implemented. There is strong ownership of the processes which provides additional levels of assurance to the established independent review and the use of a properly constituted change committee.

- Westinghouse operates well established arrangements for the selection and surveillance of suppliers as part of its procurement activities. Particular attention is given to the controls applied through the procurement stages for safety related items and services.
- Westinghouse has experienced and knowledgeable staff and a commitment to retain adequate technical resources.
- Although a UK specific project quality plan and number of UK specific procedures have been produced, it is not apparent that these implement all aspects of the Westinghouse quality management system, and hence the full benefits of its quality arrangements have not been realised for Westinghouse's project to secure 'Design Acceptance Confirmation' for the AP1000 reactor design. This leads to doubt regarding the effective application of quality arrangements to the GDA project. This is currently being addressed by Westinghouse, eg a comprehensive internal audit specific to its project has been carried out and a number of areas for improvement have been identified.

For GDA Step 4, we have identified areas where further work is required, or where additional information needs to be provided. These include the following items.

- The application of the full breadth and depth of the Westinghouse quality management system to its UK AP1000 GDA Project.
- Demonstration of the adequacy of the Westinghouse quality arrangements being applied to its UK AP1000 GDA Project as part of the safety case development.
- Westinghouse needs to justify the approach, strategy and procedure that will be applied during any eventual construction and installation of AP1000 in the UK and show how this will result in a plant which meets the requirements of the safety case.
- Westinghouse needs to develop an outline commissioning and installation schedule which demonstrates that the as-built plant will meet the design intent.
- Westinghouse needs to demonstrate the adequacy of the arrangements for the future production of operational documentation, for establishing a 'Design Authority' (including knowledge transfer) and for the control of site-specific activities including design changes.

Our GDA Step 4 assessment will include assessment of the outcomes of the above, as well as carrying out one or more targeted inspections. We would seek to confirm the consistent and comprehensive application of adequate quality assurance arrangements.

During GDA Step 4 we will also focus on those aspects of GDA that are important to any prospective licensee that is developing its knowledgeable of the design and safety case, paying particular attention to the management of safety arrangements, design change and documentation configuration control. Particular emphasis will be placed on the interfaces with prospective licensees and their involvement in design and safety case development and control.

We have agreed a design reference point 'freeze' of 31 December 2009, although we have yet to agree the full details of how this will be implemented. We will progress this during GDA Step 4, paying particular attention to the documentation list that will be included in the design reference point, and to the change control process.

Radioactive waste and decommissioning

Under this topic, we typically examine the proposals for the safe minimisation, handling, storage and disposal of radioactive waste arising from all parts of the power station, and we review the proposals for decommissioning.

In undertaking our GDA Step 3 assessment, we have worked closely with the Environment Agency and Department for Transport (DfT) to ensure that

all significant waste arisings and discharge routes have been identified by Westinghouse and that those wastes can be effectively managed.

At the start of Step 2 of the GDA process the level of information on the management of radioactive waste was limited. Additional information has since been provided and we have been able to progress our assessment.

For GDA Step 3, our assessment looked at the safety case presented in the PCSR and supporting safety documentation and the claims, arguments and evidence provided. Our assessment sample included the type of waste produced and the long-term storage of wastes and spent nuclear fuel.

In view of the wide level of public interest in Radioactive Waste and Decommissioning, our GDA Step 3 assessment has also taken account of feedback from a wide range of stakeholders.

Westinghouse's case includes: details of the source and types of radioactive waste produced; the design and operation of the reactor spent fuel pond; details of the Waste Treatment Building (which will house the processing and packaging systems for operational wastes, other than spent fuel); proposals for an Intermediate Level Waste (ILW) storage facility that will provide retrieval, inspection and, if necessary, refurbishment of waste packages; and a number of options for the long-term storage of spent fuel.

Our assessment has not identified any significant issues, or significant design or safety case changes that could impact on radioactive waste arisings or have a significant negative environmental impact. Our assessment will continue in GDA Step 4.

We also considered whether an AP1000 can be safely decommissioned. We note that many of the features of AP1000 are designed to reduce complexity and reduce operator doses and these will provide a firm basis for facilitating decommissioning.

During GDA Step 3 Westinghouse provided oral assurance that the radioactive wastes and spent fuel produced by the AP1000 are likely to be suitable for disposal. The actual disposability assessment prepared by the Nuclear Decommissioning Authority is now complete, but has only recently been provided by Westinghouse. This will be examined as part of our GDA Step 4 assessment.

Security

Under this topic we consider whether the security protection provided on the nuclear power station is adequate to protect against the theft or sabotage of nuclear materials or associated facilities.

During GDA Step 3, The Office for Civil Nuclear Security (OCNS) has gained a good understanding of the security philosophy applied to the Westinghouse AP1000 design. No significant issues have been identified so far that would preclude this design from being adequately secured against malicious capabilities (as identified in the UK protectively marked Nuclear Industries Malicious Capabilities Planning Assumptions document).

Safeguards

Nuclear safeguards are measures to verify that States comply with their international obligations not to use nuclear materials (eg Plutonium and Uranium) for nuclear explosives purposes. Global recognition of the need for such verification is reflected in the requirements of an International Treaty on the Non-Proliferation

of Nuclear Weapons (NPT). The safeguard measures that currently apply in the UK include the provision of nuclear material accountancy information and independent inspections by the International Atomic Energy Agency (IAEA) and the European Commission to verify the facility design, the fuel inventory and associated records.

Any new nuclear reactors built in the UK will also be subject to safeguards obligations. HSE is encouraging early engagement with Westinghouse to ensure that the design of the AP1000 allows for the appropriate safeguards measures. During GDA Step 3 we have made initial contact with Westinghouse on this topic and we will continue further interaction during GDA Step 4.

Issues raised through the public involvement process

We recognise the importance of building public confidence in our ability to protect people and society from the hazards of new nuclear power stations, and that working in a way that is open and transparent is a good way of helping build that confidence.

The GDA process was designed to be open and transparent, and decisions were taken early on to encourage the Requesting Parties to publish their safety, security and environmental submissions and to invite comments from the public on those. Summaries of the comments received are published in reports on the 'public involvement process' at the end of each step of the GDA process.

During GDA Step 3 a total of 45 comments were received of which 26 were directed at the Requesting Parties and 19 at HSE. Of these, 32 related to the designs being assessed, three related to the GDA process more generally, and ten fell outside the scope of GDA.

Issues raised on the AP1000 included: the proposed turbine overspeed trip mechanism; protection against missile attack and aircraft impact in relation to the containment structure; and the need for the steam and power conversion system to be hydrostatically tested. Westinghouse has responded to all relevant comments and we took these into account, where appropriate, in our GDA Step 3 assessment.

In addition to this, we have revised the GDA website to make it easier to use. This currently receives around 5000 visitors per month. We use the website extensively to publish information on the GDA process. We also continue to publish joint 'new-build e-bulletins' with the Environment Agency to notify subscribers of any new developments.

As well as publishing general information, our GDA guidance and technical assessment reports, we have started publishing a range of other useful documents, including joint Quarterly Reports. These summarise where we are, highlight the key future challenges we face going forward and any Regulatory Issues we have raised against each of the designs we are assessing.

We also continue to speak at regional, national and international events, and proactively organise seminars for key stakeholders. During GDA Step 3, this included organising two events for non-governmental organisations and two for potential operators.

For more information on the public involvement process for GDA Step 3 see: *Update on the Public Involvement Process for GDA Step 3 of the Generic Design Assessment Process*.⁸

Working with overseas regulators

Our strategy for working with overseas regulators during GDA is given on our website.⁹ In accordance with this we have, throughout GDA, worked with overseas

regulators, particularly those in the USA, where the AP1000 is being assessed by US Nuclear Regulatory Commission. We have used these exchanges both to help our assessment (and theirs) during GDA Step 3 and to confirm that we are applying the best international standards.

This work has taken several forms in different topic areas.

- Taking information simply from overseas regulator websites.
- Sharing technical reports.
- Conducting joint inspections.
- Having bilateral or multilateral face-to-face meetings.

Of particular benefit have been the bilateral information exchange meetings with our overseas counterparts. Topics discussed have included control and instrumentation, probabilistic safety analysis, human factors, civil engineering, reactor fuel, fault analysis, reactor chemistry and oversight arrangements for long lead items.

In addition we have participated in working group meetings of the Multi-national Design Evaluation Programme (MDEP) (see www.nea.fr). The aim of MDEP is to promote international sharing of information between regulators on their new nuclear power station safety assessments and to promote consistent nuclear safety assessment standards among different countries. The participants are ten countries where new nuclear power station programmes are commencing: USA, Canada, China, France, Japan, the Russian Federation, UK, Republic of Korea, South Africa and Finland, plus the IAEA. HSE represents the UK and takes a full part in the information sharing activities. In specific meetings related to AP1000, discussion has included the following topics: civil engineering; control rod drive mechanisms; Squib Valves; and oversight of manufacturing; and fabrication of long lead items.

We have found these exchanges of information most valuable and we have taken account of them in the individual topic areas as appropriate.

Interactions with our overseas regulatory colleagues will continue throughout GDA Step 4.

Cross cutting issues

A number of issues were identified during the GDA Step 3 assessment which affected several technical areas. These are discussed below.

The demonstration of as low as reasonably practicable

Demonstration that risks from the AP1000 are ‘as low as reasonably practicable’ (ALARP) is not an individual topic area but is a topic that runs across all the areas and has been considered implicitly within each of our topic safety assessments.

In respect of ALARP for GDA Step 3, we required Westinghouse to provide an explanation of how the decisions regarding the achievement of safety functions ensure that the overall risk to workers and public is ALARP.

In looking to see if this was achieved, we expected a clear conclusion that there are no further reasonably practicable improvements that can be made to the plant and that the standards, codes etc used have been justified to the extent that we can deem them to be ‘relevant good practice’ when viewed against our Safety Assessment Principles (SAP)⁵ and Technical Assessment Guides (TAG).

Furthermore, we were looking to see that there is safety rationale for the design options chosen, and a demonstration that it is not reasonably practicable to do more to reduce the overall risk. We are also keen to see that risk assessment has been used in the design process to help identify potential improvements.

From our assessment we have concluded the following.

- Westinghouse draws a firm conclusion that it considers the design to have reduced risks ALARP but acknowledges that further considerations may be needed, particularly when the operational decisions and choices start to be made, post GDA.
- With respect to 'relevant good practice', Westinghouse has not provided an overall, explicit, justification of the codes and standards used, but it does state that such work is underway - in particular in the C&I area - and that reviews for other technical areas are likely and will be reported in future revisions of the PCSR.⁶
- Westinghouse notes that it has yet to translate its probabilistic risk analysis results to allow direct comparison with the numerical targets in the SAPs, although the values stated for core damage and large releases are encouragingly low.
- With respect to design options, the PCSR⁶ catalogues a series of design enhancements, discussing the advantages and disadvantages of them. In each case results are presented that show the cost of implementation is grossly disproportionate to the risk benefit. This appears to provide good support for Westinghouse's conclusions. However, the assumptions and methodology used will need to be assessed in more detail in GDA Step 4. Westinghouse acknowledges that it has yet to report on potential improvements for the Diverse Actuation System.

With respect to risk assessment, there has been extensive use of the PSA during the design phase and as part of the overall ALARP demonstration.

Our overall conclusion is that Westinghouse has made a reasonable effort in summarising the ALARP case, although there is more work to do.

For GDA Step 4, we have identified areas where further work is required, or where additional information needs to be provided by Westinghouse. These include the following items:

- Completion and presentation of a comprehensive ALARP justification.
- Justification of the acceptability of the methods and assumptions used to demonstrate the achievement of ALARP. This will be carried out, in the main, as part of our detailed assessments of each topic area.
- An explicit justification of the acceptability of all relevant codes and standards.
- Translation of the probabilistic risk analysis results to allow direct comparison with the numerical targets in the SAPs.⁵
- Analysis of potential improvements for the Diverse Actuation System.

In GDA Step 4 we intend to sample the evidence underpinning ALARP arguments reviewed in our GDA Step 3 assessments and to assure ourselves that the methods and assumptions used are reasonable. In general this will be done within each of our assessment topic areas but we will also examine the ALARP arguments made at an overall level.

Submission configuration control and design reference point

The safety submission freeze and the design reference point for GDA (sometimes referred to as the 'design freeze' for GDA) continues to be the subject of discussion with Westinghouse. This is important because we need to have an assurance that the designs and safety cases are sufficiently advanced and are not subject to significant change throughout the GDA process. An agreed design reference point is key to ensuring that there will be a sound basis against which

to issue a GDA 'Design Acceptance Confirmation' (HSE) or a 'Statement of Acceptability' (Environment Agency), should this be appropriate at the end of our assessments.

The fact that the design is currently not complete makes agreement on a frozen reference point more difficult. In some areas Westinghouse is offering to supplement UK specific information with detailed design information from current non-UK construction projects, even though the designs might not be identical to the GDA generic design.

We have agreed the principles underpinning the design reference point and Westinghouse has committed to setting this at 31 December 2009. The principles include proposals for how changes from the design reference point will be managed and controlled in a defined and auditable way.

This GDA design reference will then be used as the basis for any operator/site specific design and safety submissions that may be made during any future licensing and construction in the UK.

Categorisation of structures, systems and components

A nuclear power station is complex and contains many different structures and components. Some of these are more significant for safety than others, and it is important to understand which are the most significant as this can effect the requirements for reliability of the system, and the quality requirements for construction and maintenance etc. This is done through a process called categorisation and classification.

The safety categorisation and classification of 'structures, systems and components' (SSC) is therefore an important element of a safety case. It allows a graded approach to safety, based on importance, and allows us to focus our assessment on those functions which are the most important to safety. It also helps ensure that appropriate codes and standards are applied, according to the safety requirements for that system, structure or component.

Westinghouse has applied a simple safety categorisation system which assigns systems as 'safety-related' or 'non-safety'. This is not in-line with international good practice, which uses additional intermediate categories.

Westinghouse has committed to align its approach with international good practice in their GDA Step 4 version of the PCSR.⁶ The outcome of this could be particularly important for the design of civil structures, C&I, electrical and mechanical systems. If systems are of higher safety significance than currently assumed by Westinghouse, then the impact of this, and the possibility of the need for design changes, will be considered in the individual topic areas.

Metrication of the AP1000 design

The Guidance to Requesting Parties¹ requires that documents submitted for Generic Design Assessment (GDA) use SI units. However, recognising that the AP1000 was not designed in SI units, we have to date accepted documentation with non-SI units. The conversion of design and safety documentation to metric units is ongoing and we will require any AP1000 that is to be constructed in the UK to be fully metric.

This may require re-design of some components using the SI system, or it may mean just a translation of current US units into SI units. Changes to analyses will need to be done carefully, for example differential temperatures have to be converted in a different manner to absolute temperatures. In addition, all

documentation or other information in the possession of an eventual licensee operating a plant in the UK will need to be in SI units. This will include design documentation, drawings, specifications, operational procedures, maintenance instructions, technical specifications, supporting analyses etc.

We have asked Westinghouse to provide a programme for metrication of the AP1000 design and we will expect this to be comprehensive and compatible with timescales for potential construction in the UK. We will form a view on the adequacy of this as part of our GDA Step 4 assessment.

Summary of significant issues

There is significant additional work to be done by Westinghouse to satisfy our questions and to make and present an adequate safety case in the majority of the technical topic areas. Throughout this report we have highlighted areas where we believe there is additional work to be done by Westinghouse and additional assessment to be done by us.

Key to progress towards completing a meaningful GDA assessment will be the quality and timeliness of the additional information provided by Westinghouse.

If we feel that the additional information is delayed, or is insufficient to facilitate our GDA Step 4 assessment, then we will advise Westinghouse accordingly as we progress through GDA Step 4.

To help respond to these issues Westinghouse has recently reorganised its project management arrangements and committed to increase its presence in the UK. We believe these changes should help Westinghouse provide timely and quality information and thus help us to complete a meaningful GDA Step 4 assessment.

Areas where we currently feel that the issues we have raised are particularly significant include the following.

- **Civil Engineering:** Progress remains slow in providing adequate responses to our questions on design codes and standards. We have not seen evidence that the civil structure design conforms to the design standards we would expect to be applied to new nuclear construction. This is particularly true for the novel Steel-Concrete-Steel (SCS) sandwich modular construction proposed.
- **External Hazards:** The original submission on external hazards did not provide sufficient information. Westinghouse intends to fill the gap in its submission with a specific external hazards topic report. This has not yet been received and it is now delaying our assessment. In addition, because of security considerations, it has taken some time for us to provide the input data required for Westinghouse to analyse the resistance to aircraft impact. Westinghouse now has this and we will be looking to progress this important subject in GDA Step 4.
- **Mechanical Engineering:** The size and nature of the Squib Valves requires an extensive design and development programme, and we have asked Westinghouse questions about this. To date, Westinghouse has made minimal progress in addressing our concerns, and we consider that there is a significant risk that the depth of the issue and the resources and effort that are needed to address it have been underestimated.
- **Structural Integrity:** We have raised a number of issues with Westinghouse; in particular relating to components where it is claimed that the likelihood of gross failure is so low that it can be discounted. We have asked Westinghouse to clearly identify for which components they are making this claim and we have also asked for an appropriate approach to achievement and demonstration of integrity for these components.
- **Human Factors:** Discussions with, and documents from, Westinghouse have

failed to respond appropriately to our observations in this area. Westinghouse has not been able to frame the documentation and information it has into a safety context to facilitate our understanding of the relative risk contribution from human actions. There is a significant shortfall against our expectations for GDA in this topic area. However, Westinghouse has now provided a programme of work with the aim of producing the necessary safety case.

- The topic of safety function categorisation and safety system classification could be significant for a number of the technical topic areas such as electrical and mechanical systems and C&I. The safety categorisation and classification system used by Westinghouse is not in accordance with international good practice, and they need to review this and address the implications for the reactor design.

In resolving these issues it remains possible that design modifications may be proposed by Westinghouse.

Potential Exclusions

In conducting this GDA assessment, we have identified issues as early as possible in our assessment, and we will continue to do so. We discuss and progress these with Westinghouse, and attempt to resolve them. Those that we know of now are detailed in our supporting technical reports and are summarised in this report. If the responses to these are satisfactory, and we are content in all other respects that the reactor design meets HSE's Nuclear Safety Assessment Principles⁵ (SAP) and all the other relevant considerations which we have set out, then we would conclude GDA positively for AP1000.

However, previous HSE and international experience has shown that in projects such as GDA it is not unusual for industry to take significant time to completely resolve some of the technical issues raised by regulators, in view of the need for new analysis, tests or research etc to be carried out. Thus, in these instances, a 'satisfactory' response to a technical issue could be one where the issue is not fully closed-out in GDA, but there is a planned way forward that we judge is acceptable. It might then be appropriate for us to allow the project to proceed in a controlled manner to the site specific phase, and it is in these circumstances that we would identify the remaining issues as 'Exclusions'.

It is important to note that 'Exclusions' in the GDA context does not refer to things that are excluded from our assessment, but rather it refers to items where we have carried out assessment and where further work is required in future to respond to our issues that have arisen out of that assessment. The items would therefore be excluded from the scope of our GDA 'Design Acceptance Confirmation'.

So, if we have 'Exclusions', it will be because we are not yet fully satisfied on these issues, but we are content enough in the overall design to issue a 'Design Acceptance Confirmation'. Where we have 'Exclusions' we will make it clear what our expectations are in relation to their resolution.

Using 'Exclusions' in this way is not a new concept; it is an existing mechanism that is used in conjunction with hold points that are regulated under Conditions attached to a Nuclear Site Licence. Hold points are programme milestones that allow us to regulate progress through construction in a controlled manner, with technical issues being linked to appropriate stages in the programme. We ensure that construction cannot proceed beyond a hold point until related technical issues have been resolved to our satisfaction. If they are not resolved then further progress would not be permitted.

In this report we have identified the potential for 'Exclusions' in the areas of Probabilistic Safety Analysis and Control & Instrumentation.

Conclusions

This is an interim report on HSE's GDA work for the AP1000 reactor and it summarises our findings to date.

In undertaking this work we have:

- improved our knowledge of the design;
- identified significant issues;
- identified areas where significant design or safety case changes may be needed;
- identified major issues that may affect design acceptance and engaged with Westinghouse in attempting to progress them.

In doing the above and making our findings public we believe we have achieved a significant reduction in regulatory uncertainty.

Our work on GDA Step 3 has allowed allow HSE inspectors to further familiarise themselves with the design and safety case and has provided a basis for planning our GDA Step 4 assessment work.

We have undertaken an examination of the AP1000 reactor at the system level and analysed Westinghouse's supporting arguments. From a security perspective, the foundations for developing the conceptual security plan have been laid through dialogue with Westinghouse.

In undertaking our GDA Step 3 assessment, we have worked with the Environment Agency to ensure that all significant waste arisings and discharge routes have been identified by Westinghouse, and that those wastes can be effectively managed. We have not identified any significant issues, or significant design or safety case changes that could impact on radioactive waste arisings or have a significant negative environmental impact.

In arriving at our conclusions thus far we have taken into account comments raised via our public involvement process and information exchanges with overseas regulators.

We continue to believe that the AP1000 could be suitable for construction on licensed sites in the UK. However, we have identified a significant number of issues with the safety features of the design that would first have to be progressed. If these are not progressed satisfactorily then we would not issue a 'Design Acceptance Confirmation' at the end of GDA Step 4.

We will progress our assessment of these issues, in dialogue with Westinghouse during GDA Step 4 but at this stage it is too early to say whether they can be resolved solely with additional safety case changes or whether they may result in design modifications being necessary.

If during our GDA Step 4 detailed assessment we identify an issue that impacts on radioactive waste arisings or other environmental impact, we will notify the Environment Agency, which is, in any case, a partner with us in the GDA process. We will do this through our routine joint working arrangements on GDA, and where appropriate in response to the Environment Agency's consultation process.

We will summarise progress on our GDA Step 4 assessment, and on the issues we have raised, in our joint Quarterly Reports with the Environment Agency, which we will continue to place on our website, and in a final GDA report at the end of GDA Step 4, which is presently scheduled for June 2011.

Abbreviations

ALARP	As low as reasonably practicable
ASME	American Society of Mechanical Engineers
ATWT	Anticipated Transient Without Trip
C&I	Control and Instrumentation
CHF	Critical Heat Flux
DAS	Diverse Actuation System
DCD	Design Control Document
DECC	Department of Energy and Climate Change
DfT	Department for Transport
DTI	Department of Trade and Industry (now DECC)
EPRI	Electric Power Research Institute (United States of America)
GDA	Generic Design Assessment
HEPA	High Efficiency Particulate Air
HSE	Health and Safety Executive
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
ILW	Intermediate level waste
LLW	Low level waste
MDEP	Multi-national Design Evaluation Programme
ND	Nuclear Directorate
OCNS	Office for Civil Nuclear Security
OJEU	Official Journal of the European Union
PCI	Pellet Clad Interaction
PCSR	Pre-Construction Safety Report
PMS	Plant Monitoring System
PRA	Probabilistic Risk Analysis
PSA	Probabilistic Safety Analysis
PSR	Preliminary Safety Report
RPV	Reactor Pressure Vessel
SAP	Safety Assessment Principle
SCS	Steel-Concrete-Steel
SSC	Structure, System and Component
US NRC	Nuclear Regulatory Commission (United States of America)
Westinghouse	Westinghouse Electric Company LLC

Annex 1 Summary of HSE expectations for Step 3 of the GDA process

Details of HSE expectations for Step 3 of the GDA process can be found in the GDA guidance.¹ From that document, the key expectations of Requesting Parties for GDA Step 3 are:

Provide a detailed Pre-construction Safety Report that includes sufficient information for the GDA Step 3 Safety and Security Review, in particular:

1. Definition of the documentary scope and extent of the safety case.
2. Explanation of how the decisions regarding the achievement of safety functions ensure that the overall risk to workers and public will be ALARP.
3. Responses to any issues outstanding from GDA Step 2.
4. Sufficient information to substantiate the claims made in GDA Step 2 (in the Preliminary Safety Report).
5. Sufficient information to enable HSE Nuclear Directorate to assess the design against all relevant SAPs.
6. A demonstration that the detailed design proposal will meet the safety objectives before construction or installation commences, and that sufficient analysis and engineering substantiation has been performed to prove that the plant will be safe.
7. Detailed descriptions of system architectures, their safety functions and reliability and availability requirements.
8. Confirmation and justification of the design codes and standards that have been used and where they have been applied, non-compliances and their justification.
9. Fault analyses including Design Basis Analysis, Severe Accident Analysis and PSA.
10. Justification of the safety of the design throughout the plant's life cycle, from construction through operation to decommissioning, and including on-site spent fuel and radioactive waste management issues.
11. Identification of potentially significant safety issues raised during previous assessments of the design by overseas nuclear safety regulators, and explanations of how their resolution has been or is to be achieved.
12. Identification of the safe operating envelope and the operating regime that maintains the integrity of the envelope.
13. Confirmation of:
 - (a) which aspects of the design and its supporting documentation are complete and are to be covered by the Design Acceptance Confirmation;
 - (b) which aspects are still under development and identification of outstanding confirmatory work that will be addressed during GDA Step 4.

References

- 1 *Nuclear power station generic design assessment – guidance to Requesting Parties* (Version 3) HSE August 2008 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 www.hse.gov.uk/nuclear/notesforapplicants.pdf
- 4 *Public Report on the Generic Design Assessment of New Reactor Designs. Conclusions of the fundamental safety overview of the AP1000 Nuclear Reactor (Step 2 of the Generic Design Assessment process)* HSE GDA-004 March 2008 www.hse.gov.uk/newreactors
- 5 *Safety assessment principles for nuclear facilities* (2006 Edition Version 1) HSE December 2006 www.hse.gov.uk/nuclear/saps/saps2006.pdf
- 6 *AP1000 Pre-construction Safety Report* (Revision 1) Westinghouse Electric Company LLC UKP-GW-GL-732 10 March 2009 www.ukap1000application.com
- 7 *AP1000 European Design Control Document* (Revision 0) Westinghouse Electric Company LLC EPS-GW-GL-700 16 February 2009 www.ukap1000application.com
- 8 *Public Report on the Generic Design Assessment of New Nuclear Reactor Designs. Update on the Public Involvement Process for GDA Step 3 of the Generic Design Assessment Process* HSE GDA-007 November 2009 Available via HSE web-site: www.hse.gov.uk/newreactors
- 9 *New nuclear power stations generic design assessment - strategy for working with overseas regulators* HSE NGN04 March 2009 www.hse.gov.uk/newreactors/ngn04.pdf

HSE priced and free publications can be viewed online or ordered from www.hse.gov.uk or contact HSE Books, PO Box 1999, Sudbury, Suffolk CO10 2WA Tel: 01787 881165 Fax: 01787 313995. HSE priced publications are also available from bookshops.

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.G
Health and Safety Executive
Redgrave Court
Merton Road
Bootle
Merseyside
L20 7HS

www.hse.gov.uk

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

First published November 2009. Please acknowledge the source as HSE.