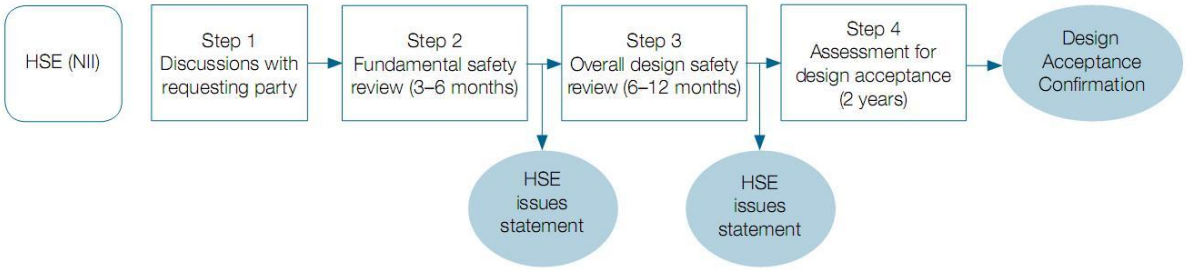
White Paper

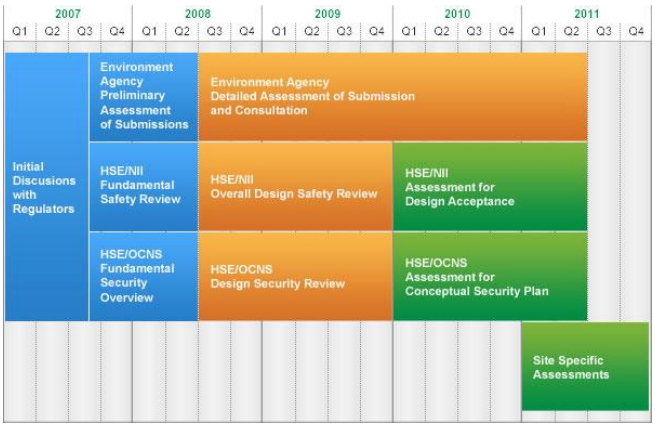
Case Study– Generic Design Assessment Westinghouse AP1000 PSA

Jacobsen Analytics was selected by the UK Office for Nuclear Regulation (ONR) to perform the Generic Design Assessment (GDA) of the probabilistic safety assessment (PSA) for the UK submission of the Westinghouse AP1000 reactor design. The final report of the assessment of the AP1000 PSA [1] by the HSE based on Jacobsen's supporting analysis has been released to the public and can be found on the HSE website. The Generic Design Assessment (GDA) was a process of four steps whereby the Requesting Parties (RP) submitted their designs for regulatory approval for potential new-build in the UK.



The PSA review covered all the technical areas of the Level 1 and Level 2 PSA including shutdown modes, internal fire and internal flooding, and external hazards, although some of these elements were limited in scope. The evidence supporting the PSA claims and arguments (assessed during GDA Steps 3 and 4) on how the PSA Safety Assessment Principles (SAP) are met, have been assessed on a sampling basis. The sampling has been done in a focused, targeted and structured manner with a view to revealing any specific or generic weaknesses in the PSA.

The GDA assessment has been conducted following the guidance and structure of the Nuclear Directorate's PSA technical assessment guide [2]. The Assessment Expectation Tables within the TAG were followed and the level of detail in the analysis implicit in each of the above areas has been assessed. It was decided that the justification provided or adequacy of the documentation would be judged as (A) Adequate, (P) Partial, (N) None or Not met, (N/A) Not Applicable or Not Assessed. Where appropriate, Jacobsen has recommended or suggested issues to be further considered by the HSE. For most items rated as (P) or (N) Proposed Technical Queries (PTQs) were suggested by Jacobsen.



The assessment of the PSA by Jacobsen of the AP1000 PSA was performed in two stages:

i) ***Step 3 GDA***, which focussed on methods applied to the various aspects of the PSA and identification of additional documentation required to support a detailed review, and

ii) ***Step 4 GDA***, which performed the detailed review.

Jacobsen Analytics Ltd., 6 Whiteside, Off Station Road, Holmes Chapel, Cheshire CW4 8AA
Office: +44 1477 537 745 www.jacobsen-analytics.com
Registered Office: 1 Statham Close, Lymm, Cheshire WA13 9NN Company Registered in England Number: 02279951

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

During the GDA review of the PSA the following specific topics below have been subject to detailed review and to help to reach a conclusion of whether an AP1000 meets the basic safety objective and can be constructed and operated safely in the UK, and to evaluate the importance of the findings in the various PSA technical areas, a Risk Gap Analysis (RGA) was conducted.

Level 1 PSA:

- Initiating Events– Completeness of selected IEs and grouping of Initiating events.
- L1 PSA Accident Sequence modelling. (SLOCA, LMFW, SGTR, ATWS, MLOCA, SLB-IC).
- L1 Success Criteria (applied to Event Trees).
- Systems analysis (4 Systems - Non-safety AC Emergency Electrical Systems, Component Cooling System, Passive Injection Systems, and Start-up FW system).
- Data Analysis, CCF and HRA.

Level 2 PSA:

- Level 2 specific systems - Containment isolation, Hydrogen igniters.
- Plant Damage State (PDS) grouping structure and assignment of Level 1 sequences to groups.
- Identification of potential impact of alternative allocation of sequences to groups.
- For each PDS identified by the RP the following will be produced:
  - [1] Identification of potential subgroups to provide better discrimination of PDS
  - [2] Identification of apparently misallocated sequences
- Assessment of Source Term Grouping Structure (This task will comment on the adequacy of the RPs grouping structure and identify potential alternative representative sequences.
- Assessment of Containment Event Tree (CET) structure, identification of top events and treatment of dependencies within the CET.
- Review of supporting MAAP analysis, structural analysis and branch probability evaluations, phenomenological probabilities, structural capability, source term analysis.
- Review of CET / PDS quantification and impact of dependency modelling.
- Model sensitivity:
  - [1] Confirmation / review / opinion on scope of licensee sensitivity studies
  - [2] Identification of model sensitivities not identified by the RP.

Artist's impression of an AP1000 nuclear plant

Hazards PSA:

- External Hazards Screening Analysis
- Seismic Analysis
- Internal Fire Analysis and Other Hazards
- Internal Flooding Analysis

Risk Gap Analysis (RGA):

- The RGA took into account responses from WEC to the TQs in all areas of the Level and Level 2 PSA. This required evaluation of the TQs and additional requests for information where necessary.
- Screening (qualitative and /or quantitative) of findings from TQs.
- Evaluation of specific concerns in the Base case.
- Sensitivity analysis where potential for significant uncertainty had been identified.

- Identified Qualitative gaps and Errors in the PSA:
  - Perceived risk gaps that depend on operation, final detailed design, site specific characteristics, specific analysis and modelling.

- Missing Initiating Events:
  - IRWST draining
  - Loss of support systems
  - SLOCA through PRHR

- Systems Analysis:
  - Missing CCFs
  - Missing Type A HFEs
  - IRWST tank failure
  - Consequential LOOP (sensitivity)

- Success Criteria and Accident Sequence:
  - Failure to open PZR SVs on demand
  - Long term containment failure sequences
  - Reactor trip FT missing mechanical failure
  - Spurious PMS actuations
  - Spurious PLS actuations
  - Induced SGTR after SLB

- Human Reliability Analysis:
  - Identified type C HEPs with cognitive elements /screened by importance measures / increased HEPs by 2E-3 (based on THERP non-response curves at 30 min).
  - 4 most important HEPs adjusted / increased based on HCR method using WEC time windows and stated "actual" (median) time (gives values in range 0.03 to 0.2).

- Data Analysis:
  - Revised Interfacing Systems LOCA frequency.
  - Updated failure rates/probabilities with NUREG/CR-6928 generic data.
  - Revised DG mission time, and compressor T&M unavailability.

- External Hazards:
  - External flooding, Extreme temperatures, External fire.
  - Seismic (a simplified and bounding seismic risk evaluation on important structures with fragility data).

- Low Power and Shutdown PSA:
  - IE frequencies and Frequency of over-draining event.
  - Maintenance unavailabilities.
  - HRA dependencies.

- Level 2 PSA:
  - Revised In Vessel Retention (IVR) failure probability.
  - Revised operator actions for Spurious ADS operation and LLOCA.
  - Explicit modelling of systems for IVR.
  - Included dependency for L2 operator action with L1 HEPs.
  - Corrected allocation of ATWS sequences to PDS.
  - Linked missing PDS with LOOP.

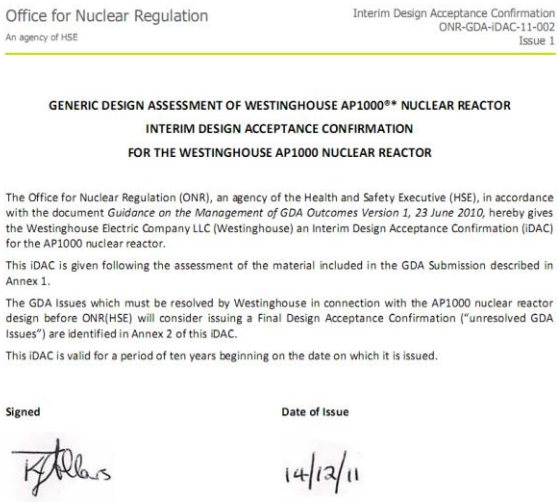
Additional Reviews requested by HSE:

- ***Detailed Review of C&I System:***
  A more detailed review assessed the application of the PSA methods and techniques of the three parts of the I&C Systems Analysis, PMS, DAS and PLS was performed the system fault tree modelling was compared with the design and operation of the PMS and the interface between instruments used in the PMS and the control system, and sensitivity analyses were performed to determine the sensitivity of core damage frequency to the I&C.

- ***Review of Spurious C&I Faults:***
  This analysis identified potential events, and potential failure modes / mechanisms, due to spurious C&I faults, identified what other component/systems have been impacted simultaneously by the spurious fault, the development and quantification of failure models for the potential critical failure modes.

- ***Review of the new In Vessel Retention (IVR) Analysis:***
  This analysis reviewed the adequacy of cavity flooding to promote natural circulation flow through the reactor cavity, and verified the claim that there is significant margin to vessel failure for the AP1000. Jacobsen Engineering developed a tool to evaluate and assess the validity of this claim and a probabilistic model of IVR heat transfer was used to evaluate the probability of vessel failure with successful IVR. A Crystal Ball model was constructed to allow for the performance of sensitivity analyses and a review of long term pressurisation of the containment was performed.

The estimated risk gap addressing the review findings, which could be evaluated quantitatively in GDA, concluded that the CDF and LERF for the AP1000 are likely to be higher than the current figures estimated by Westinghouse, but are still lower than those figures of merit for currently operating PWRs. Also, it is acknowledged that there are conservatisms in some aspects of the AP1000 PSA model and data. All this suggests that the risk associated with the AP1000 design could be low enough to meet the Basic Safety Objectives (BSO) for Targets 7 and 9 from NT.1 of the Health and Safety Executive's Safety Assessment Principles.



Office for Nuclear Regulation
An agency of HSE

Interim Design Acceptance Confirmation
ONR-GDA-iDAC-11-002
Issue 1

GENERIC DESIGN ASSESSMENT OF WESTINGHOUSE AP1000® NUCLEAR REACTOR
INTERIM DESIGN ACCEPTANCE CONFIRMATION
FOR THE WESTINGHOUSE AP1000 NUCLEAR REACTOR

The Office for Nuclear Regulation (ONR), an agency of the Health and Safety Executive (HSE), in accordance with the document *Guidance on the Management of GDA Outcomes Version 1, 23 June 2010*, hereby gives the Westinghouse Electric Company LLC (Westinghouse) an Interim Design Acceptance Confirmation (iDAC) for the AP1000 nuclear reactor.

This iDAC is given following the assessment of the material included in the GDA Submission described in Annex 1.

The GDA Issues which must be resolved by Westinghouse in connection with the AP1000 nuclear reactor design before ONR(HSE) will consider issuing a Final Design Acceptance Confirmation ("unresolved GDA Issues") are identified in Annex 2 of this iDAC.

This iDAC is valid for a period of ten years beginning on the date on which it is issued.

Signed **Date of Issue**

14/12/11

References:

[1] HSE AP1000 PSA GDA Assessment Report Reference Report ONR-GDA-AR-11-003, Revision 0

[2] Health and safety Executive, Nuclear Directorate – Business Management System Probabilistic Safety Assessment Technical assessment Guide, T/AST/030 Issue 3

[3] Nuclear power plants – Instrumentation and control important to safety – Use of probabilistic safety assessment for the classification of functions. PD IEC/TR 61838:2009, British Standards Institute

[4] Interim Design Acceptance Confirmation (ONR-GDA-iDAC-11-002 Issue 1)