LESSONS LEARNT FROM THE UK GENERIC DESIGN ASSESSMENT PROCESS

Dr J R Jones*, Dr R Moscrop†, Prof A Tehrani†, R Exley†

Office for Nuclear Regulation

**St James House, Cheltenham, GL50 3PR*

†*Redgrave Court, Bootle, Merseyside, L20 7HS*

ABSTRACT

UK government policy recognises that the construction of new nuclear power plants in the UK will play a vitally important role in providing reliable electricity supplies and a secure and diverse energy mix as the UK makes the transition to a low carbon economy. As an enabler to this construction programme, it is necessary to ensure that adequate levels of safety are guaranteed by design. The Office for Nuclear Regulation (ONR), the UK national body responsible for the regulation of nuclear safety and security, together with the Environment Agency (EA), the national body responsible for the relevant regulation in England and Wales, have developed a design acceptance process for the preliminary assessment of new reactor designs called the Generic Design Assessment (GDA). The process allows ONR and EA to interact with reactor designers at an early stage to maximise their influence. It also allows designers to understand and address regulatory concerns while the design is still on paper, which reduces the financial and regulatory risks for power station developers. The process has been in place since 2007 and is now well established and mature with one reactor design (AREVA/EDF UKEPR™) already having received a design acceptance certificate and two further designs (Westinghouse AP1000® and GE Hitachi ABWR) well into the later stages of the process.

The lessons learnt to date from application of the GDA process are presented in terms of the common regulatory issues that have been identified with international designs and the changes needed in order to meet UK safety expectations.

ONR expects a safety case which demonstrates defence in depth in the design process as well as in the operation of the plant. Requirements include:

- The need for comprehensive fault and hazard identification;
- A graded approach to safety analysis, including consideration of design basis analysis and beyond design basis analysis (design extension conditions) integrated with probabilistic safety analysis to reduce assessed risk as far as reasonably practical;
- Deterministic analysis of the design of safety systems, incorporation of adequate redundancy and diversity;
- The use of equipment designed and manufactured in accordance with a systematic safety categorisation based on the class of safety function supported.

Treatment of essential support systems within the design basis is considered, with attention given to the essential electrical systems, the supporting cooling chain and ultimate heat sink, and heating, ventilation and cooling systems (HVAC). ONR's expectations also include addressing the Vienna declaration for new designs and responding to the lessons learnt from Fukushima and the use of software to support control-room operations.

Guidance is provided on the UK requirements for the production of a safety case in order to justify and substantiate the adequacy of a design and the UK legal requirement to demonstrate that a design has reduced risks to "As Low As Reasonably Practicable – ALARP".

1. Introduction

UK government policy [1] recognises that the construction of new nuclear power plants in the UK will play a vitally important role in providing reliable electricity supplies and a secure and diverse energy mix as the UK makes the transition to a low carbon economy. As an enabler to this construction programme, the Office for Nuclear Regulation (ONR), the UK national body responsible for the regulation of nuclear safety and security, together with the Environment Agency (EA), the national body responsible for the relevant regulation in England and Wales, have developed a design acceptance process for the preliminary assessment of new reactor designs called the Generic Design Assessment (GDA) [2].

The process allows ONR and EA to interact with reactor designers at an early stage to maximise their influence. It also allows designers to understand and address regulatory concerns while the design is still on paper, which reduces the financial and regulatory risks for power station developers. In this context, ONR and EA are not exercising their regulatory powers, but rather providing technical advice to the vendors on the licensing of the designs. The process has been in place since 2007 and is now well established and mature with one reactor design (AREVA/EDF UKEPR™) already having received a design acceptance certificate [3-8] and two further designs (Westinghouse AP1000® [9] and GE Hitachi ABWR) well into the later stages of the process.

The purpose of this paper is to use these previous GDA assessments as a way of illustrating UK regulatory requirements. The lessons learnt to date from application of the GDA process are presented in terms of the common regulatory issues that have been identified with international designs and the changes needed in order to meet UK safety expectations.

The licensing arrangements in the United Kingdom were introduced in the late 1950s in response to an accident at a military facility in west Cumbria [10]. Legislation was introduced which required plant operators who handle nuclear material to apply for a site licence. The government established a Nuclear Installations Inspectorate (the predecessor organisation to ONR) to enforce compliance with the licence conditions and the ONR remains responsible for enforcement of the legislation to date.

The licence conditions relevant to the design of new reactor require an *adequate safety case* justifying operations and *operating rules* defining the boundary of safe operation [11]. These requirements were originally addressed by performing *Deterministic* safety analysis to demonstrate safety margins between operation and plant damage. This includes transient analysis of Design-Basis faults against Fuel Design Criteria.

In subsequent years, a number of incidents outside the nuclear industry caused the UK government to revise health and safety legislation generally. The associated legislation extended the duties of licensees; requiring them to consider whether additional measures to mitigate the risk inherent in their operations were reasonably practicable [12]. This requirement has been reinforced by recent events such as TMI, Chernobyl and Fukushima.

The principles behind this approach are not unique to the UK and their impact on the design and licensing of new reactor designs is to some extent universal. This paper considers first the issue of Reasonably Practicable safety enhancements and then discusses the application of Deterministic Analysis.

In making the decision on whether to sample a particular topic in detail and potentially to intervene, the regulator is required to follow the ONR enforcement principles [13].

These require:

- Regulatory action be proportion to the risk;
- Consistency with other regulatory decisions;
- Targeted, Transparent and Accountable.

These principles are designed to ensure that assessment resources are appropriately targeted and that licensees can have predictable interaction with the regulator.

In order to comply with these requirements, the inspectorate has issued guidance to its staff in the form of safety assessment principles [14] and technical assessment guides (for example [15]). The following discussion is based on this guidance.

2. The Test of As Low As Reasonably Practicable

The UK law requires that the licensee consider measures that can be taken to eliminate or protect against a risk and to apply the test of whether the cost and trouble incurred is grossly disproportional to the incremental reduction in risk. Explanation of the thinking behind this approach is found in [16].

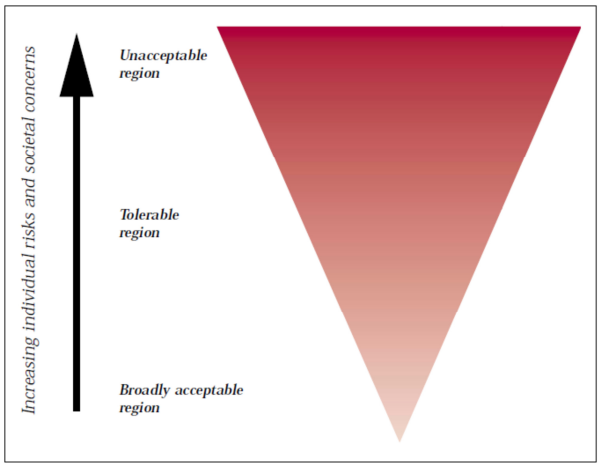

Fig 1. The Tolerability of Risk framework [16]

The framework is illustrated in Figure 1. The triangle represents increasing level of 'risk' for a particular hazardous activity (measured by the individual risk and societal concerns it engenders). As we move from the bottom of the triangle towards the top the need for mitigation is increased.

The dark zone at the top represents an unacceptable region. For practical purposes, a particular risk falling into that region is regarded as unacceptable whatever the level of benefits associated with the activity. Any activity or practice giving rise to risks falling in that region would, as a matter of principle, be ruled out unless the activity or practice can be modified to reduce the degree of risk so that it falls in one of the regions below, or there are exceptional reasons for the activity or practice to be retained.

The lighter region represents an area where the risk could be accepted but mitigation measures should be taken unless analysis of the balance between benefit and risk shows that it is not reasonably practicable.

In developing a safety case, it is tempting to assign a value to the tolerable risk associated with a radiation dose; based on the risk of widely accepted in similar activities. However, ONR is likely to take a wider view. Risk can include consideration of the consequences of damage to trade and reputation. In a number of cases this has been the dominant risk [15]. The Three-mile Island Accident is one illustration: The individual risk to members of the public was low, but the impact on the development of nuclear power within the USA was severe.

The assessment of what is reasonably practical therefore becomes a qualitative rather than a quantitative process and the law regards relevant good practice as an illustration of an accepted balance.

3. Scope of Deterministic Design Basis Analysis

In the UK, identification of *reasonably foreseeable* Design Basis faults is the responsibility of the licence holder. However, ONR does provide guidance to help limit the scope of the task [14]: The licensee is required to consider the likelihood of the fault and the magnitude of the hazard.

Faults with a return frequency of less than once in 100,000 years, and faults where the unmitigated dose would be insignificant, can be excluded. Quantitative guidance is provided [14] and this is illustrated for off-site dose in Figure 2.

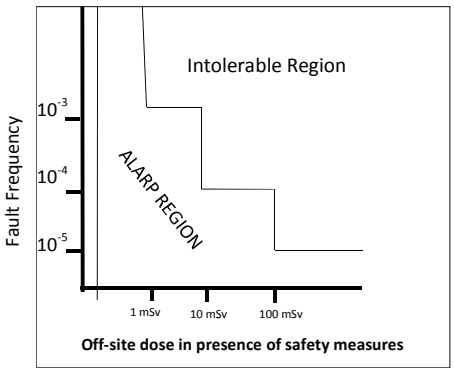

Fig 2. ONR Target Levels of Off-site Exposure from Postulated Accidents

The criterion for tolerability varies with the frequency of the fault; increasing as the fault frequency is reduced.

Measures taken to reduce the likelihood of a fault so that it falls outside the return-frequency targets, permit the analyst to relax the conservative assumptions used in analysis of a fault, but this does not necessarily justify neglecting the fault entirely. ONR would still require consideration of whether the risk from the fault was reduced to levels as low as reasonably practicable and in some cases, this has required substantial amounts of work. While we favour fault prevention over protection, experience shows that high-integrity arguments for individual manufactured components need to be treated with caution and are accepted only where alternatives are not practical.

From application of the GDA process to the assessment of international designs [3, 9] it is clear that a first lesson to be learnt from GDA is that the derivation of the list of design basis faults (generally called the Fault Schedule in the UK) based on the most extreme failure of each plant system, tends not to be sufficiently comprehensive to meet UK requirements. Faults often omitted from the design basis analysis of safety analysis report [3, 4, 6, 8, 9] include:

- Faults initiated by common mode failure of essential support systems;
- Faults during shutdown and part-power operations;
- Faults involving the spent fuel pool and fuel handling;
- Faults involving heterogeneous boron dilution (on PWRs);
- Faults involving spurious computer software failure on C&I platforms including the primary protection system and where the fault is assumed to affect multiple redundant trains, and;
- Internal and external hazards.

The faults initiated by common mode failure of essential support system should include consideration of the essential electrical system, HVAC system or the cooling chain including loss of ultimate heat sink as well as long term loss of off-site power since it is difficult to conclude that the common mode failure rate for any of these faults is less than 10^{-5} per year target given in Fig 2. While it is recognised that design provision for internal and external hazards are often considered within the safety analysis report there is often a lack of rigour in how the adequacy of the provision is substantiated sufficient to meet the requirements expected for a UK safety case.
In summary, the UK expectation [14] is that the process for fault identification should be systematic, auditable and comprehensive covering:

- significant inventories of radioactive material;
- planned operating modes and configurations including shutdown states and decommissioning operations and any other activities that could present a radiological risk, and;
- chemical and other internal hazards, man-made and natural external hazards, internal faults from plant failures and human error, and faults resulting from interactions with other activities on the site.

4. Defence in Depth and Design Extension Conditions

International guidance [17-19] has recently been revised and developed to take account the lessons learnt from Fukushima. These new requirements include the need to enhance the defence in depth concept covering Design Extension Conditions (DEC), consideration of practical elimination, avoidance of cliff edges just beyond the design basis for external hazards and combinations of credible initiating events including internal and external hazards. The aim of these objectives is to avoid large early releases or releases that can result in the long-term contamination of land. There are two categories of DEC:

- DEC-A sequences for which prevention of severe fuel damage in the core or in the spent fuel storage can be achieved;
- DEC-B sequences associated with postulated severe fuel damage.

The selection process for DEC-A sequences starts with the consideration of those events and combinations of events which cannot be considered with a high degree of confidence to be extremely unlikely to occur and which may lead to severe fuel damage in the core or in the spent fuel storage and covers:

- Events occurring during the defined operational states of the plant;
- Events resulting from internal or external hazards;
- Common cause failures.

The set of category DEC-B events are postulated and justified to cover situations, where the capability of the plant to prevent severe fuel damage is exceeded or where measures provided are assumed not to function as intended, leading to severe fuel damage.
Many of these developments were already established as relevant good practice [14] in the UK although ONR guidance undergoes regular review to maintain compliance with relevant international practice. In particular, it has been a long standing practice in the UK to consider fault sequences with frequencies greater than 10^{-7} per year to be within the design basis. In practice this drives for the inclusion of functional diversity within a design for each major

safety function consistent with DEC-A approach, although in the UK there is the additional expectation that the safety classification for such equipment will be designed to meet nuclear design codes and standards (associated with a system safety classification of at least Class 2 as discussed in Section 6 below) rather than industrial codes and standards.
From application of the GDA process to the assessment of international designs [3, 9] a second lesson to be learnt from GDA is that generally the new designs have through the use of level 1 and 2 Probabilistic Safety Analysis (PSA) included design provisions to meet the DEC-A and DEC-B requirements. However, the UK requirement to systematically demonstrate functional diversity for each safety function has often identified the need for significant additional transient analysis studies covering sequences such as anticipated transients without scram (ATWS) events and this analysis has sometimes identified the need for additional design modifications. Specifically, these design changes have included:

- Upgrading of the diverse safety systems [3, 5, 8, 9] to meet Class 2 design requirements;
- Provision of a hard-wired diverse protection system [5] to provide functional diversity for failures in the computer based primary protection system;
- Provision of additional actuation signals on the diverse protection systems [3, 5, 8, 9].

Other lessons to be learnt [3, 9] from GDA are that in developing design basis fault sequences explicit accident analysis and ALARP justification is needed to justify:

- Passive single failures including accumulator non-return (check) valves;
- Interface loss of coolant accidents (LOCA) with the potential for containment by-pass;
- Consequential steam generator tube rupture (SGTR) failures following steamline faults;
- Consequential LOCA faults following Safety Relief Valve (SRV) lift, and:
- The transition from the controlled state to the safe shutdown state.

In summary, the UK expectation [14] is that correct performance of safety-related and non-safety equipment should not be assumed where this would alleviate the consequences. Where failures or unintended operation of equipment not qualified for specific accident conditions could exacerbate the consequences, or otherwise make the fault more severe, this should be assumed within the DBA.
Each design basis fault sequence should include as appropriate:

- Failures consequential upon the initiating fault, and failures expected to occur in combination with that initiating fault arising from a common cause;
- Single failures in the safety measures in accordance with the single failure criterion;
- The worst normally permitted configuration of equipment outages for maintenance, test or repair, and;
- The most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.

Sequences with very low expected frequencies need not be included in the DBA. Judgement should be exercised in this regard, but for high hazard facilities, a fault sequence frequency of 10^{-7} per year would be a typical cut-off when applying design basis techniques.

The analysis should establish that adverse conditions that may arise as a consequence of the fault sequence will not jeopardise the claimed performance of the safety measures.
Operator actions can be claimed as part of safety measures only if sufficient time is available, adequate information for fault diagnosis is presented and, for existing facilities, appropriate written procedures exist and compliance with them is assured.

5. Acceptance Criteria for Design Basis Safety Analysis

From application of the GDA process to the assessment of international designs [3, 9] a third lesson to be learnt from GDA is that in the UK it is considered good practice where possible (i.e. subject to reasonable practicability) to prevent the fuel from entering Departure from Nucleate Boiling (DNB) for all design basis faults. Adjusting reactor trip set points, limits and conditions of safe operation, fuel cycle design or the control system parameters are all seen as reasonable practicable measures to implement this objective.
For this reason, the UK expectation [14] is that analysis for each fault sequence should demonstrate, so far as is reasonably practicable, that the correct performance of the claimed passive and active safety systems ensures that:

- None of the physical barriers to prevent the escape or relocation[1] of a significant quantity of radioactive material is breached or, if any are, then at least one barrier remains intact and without a threat to its integrity;
- There is no release of radioactivity; and
- No person receives a significant dose of radiation.

Where these criteria cannot be fully met within the design, the expectation is that the consequences will be minimised subject to ALARP. This is reflected in numerical dose target illustrated in Fig. 2 above which defines the Basic Safety Objectives for the mitigated consequences of design basis fault sequences; these Basic Objectives reflect the view that it is not generally appropriate to design a protection system so that, in an anticipated fault for which the protection is intended, releases to the environment are expected to breach normal discharge limits.
Further more detailed guidance on this specific point can be found in reference [20]. It should also be noted that appropriate radiological assessments need to be performed when comparing against the relevant UK numerical dose targets [3, 9, 14].

6. Categorisation and Classification of Structures, Systems and Components

From application of the GDA process to the assessment of international designs [3, 9, 21] a fourth lesson to be learnt from GDA is that a graded approach needs to be adopted to the categorisation of safety functions and classification (of structures, systems and components) that takes account of their safety significance as determined by the fault analysis of the facility. The UK expectation [14] is that all important structures, systems and components are designed, manufactured, installed and then subsequently commissioned, operated and maintained to a level of quality commensurate with their classification.
The identification of safety functions and their associated categorisation should follow a systematic approach linked to the fault analysis for the facility and addressing the three fundamental safety functions of a nuclear reactor. The following safety function

[1] Relocation means the material is no longer in its designated place of residence or confinement

categorisation scheme and its associated classification scheme are regarded as good practice in the UK [14]:

- Category A – any function that plays a principal role in ensuring nuclear safety.
- Category B – any function that makes a significant contribution to nuclear safety.
- Category C – any other safety function contributing to nuclear safety.

The method for categorising safety functions should take into account:

- The consequence of failing to deliver the safety function;
- The likelihood that the function will be called upon, and;
- The extent to which the function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults.

The categorisation of safety functions should take no account of any redundancy, diversity or independence within the design – these aspects relate to the structures, systems and components that deliver the safety functions. The categorisation assigned to each safety function should then be used as input into classification the structures, systems and components that deliver the function as follows.

- Class 1 – any structure, system or component that forms a principal means of fulfilling a Category A safety function.
- Class 2 – any structure, system or component that makes a significant contribution to fulfilling a Category A safety function, or forms a principal means of ensuring a Category B safety function.
- Class 3 – any other structure, system or component contributing to a categorised safety function.

Methods for classifying the safety significance of structures, systems or components should be based primarily on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgement, with account taken of factors such as:

- The category of safety function(s) to be performed by the item;
- The probability that the item will be called upon to perform a safety function;
- The potential for a failure to initiate a fault or exacerbate the consequences of an existing fault, including situations where the failure affects the performance of another system, structure or component, and;
- The time following any initiating fault at which, or the period throughout which, it will be called upon to operate in order to bring the facility to a stable, safe state.

Appropriately designed interfaces should be provided between (or within) structures, systems and components of different classes to ensure that any failure in a lower class item will not propagate to an item of a higher class. Equipment providing the function to prevent the propagation of failures should be assigned to the higher class.
Auxiliary services that support components of a system important to safety should be considered part of that system and should be classified accordingly unless failure does not prejudice successful delivery of its safety functions.

Appropriate nuclear industry-specific, national or international codes and standards should be adopted for Class 1 and 2 structures, systems or components. For Class 3, if there is no appropriate nuclear industry-specific code or standard, an appropriate non-nuclear-specific code or standard should be applied instead.

7. Conclusions

The intention of the system of regulation set out above is not to provide a prescriptive set of steps by which utilities can meet regulatory requirements, but a set of flexible guidelines which allow utilities to design, construct, commission and operate safely and to engage constructively with the regulatory body.

The aim is to provide a robust demonstration that the plant can meet the challenges presented by anticipated faults and that all reasonably practical measures have been taken to reduce the risk to a broadly acceptable level.

8. References

1. National Policy Statement for Nuclear Power Generation (EN-6), Vol I of II, Department of Energy and Climate Change, July 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/47859/2009-nps-for-nuclear-volume.pdf
2. New Nuclear Reactors: Generic Design Assessment Guidance to Requesting Parties, ONR guidance ONR-GDA-GD-001, Revision 3, http://www.onr.org.uk/new-reactors/ngn03.pdf
3. Generic Design Assessment – Step 4 Fault Studies – Design Basis Fault Assessment of the EDF and AREVA UK EPR™ Reactor, ONR-GDA-AR-11-020a, November 2011
4. GDA Close-out for the EDF and AREVA UK EPR™ Reactor – GDA Issue GI-UKEPR-FS-01 Revision 0 – Heterogeneous Boron Dilution Safety Case, ONR-GDA-AR-12-010, March 2013
5. GDA Close-out for the EDF and AREVA UK EPR™ Reactor – GDA Issue GI-UKEPR-FS-02 Revision 0 – Diversity for Frequent Faults, ONR-GDA-AR-12-011, March 2013
6. GDA Close-out for the EDF and AREVA UK EPR™ Reactor – GDA Issue GI-UKEPR-FS-03 Revision 0 – Spent Fuel Pool Safety Case, ONR-GDA-AR-12-012, March 2013
7. GDA Close-out for the EDF and AREVA UK EPR™ Reactor – GDA Issue GI-UKEPR-FS-04 Revision 0 – Steam Generator Tube Rupture Safety Case, ONR-GDA-AR-12-008, March 2013
8. GDA Close-out for the EDF and AREVA UK EPR™ Reactor – GDA Issue GI-UKEPR-FS-05 Revision 0 – Design Basis Analysis of Essential Support Systems, ONR-GDA-AR-12-013, March 2013
9. Generic Design Assessment – Step 4 Fault Studies – Design Basis Fault Assessment of the Westinghouse AP1000® Reactor, ONR-GDA-AR-11-004a, November 2011
10. Proceedings of the Board of Enquiry into the Fire at Windscale Pile No 1, UKAEA, 1957. http://www.discovery.nationalarchives.gov.uk/details/r/C11295198
11. Office for Nuclear Regulation Licence condition handbook, October 2011. http://www.onr.org.uk/documents/licence-condition-handbook.pdf
12. Health and Safety at Work Act 1974. http://www.legislation.gov.uk/ukpga/1974/37/contents
13. ONR Enforcement Policy Statement, 2014. http://www.onr.org.uk/documents/2014/enforcement-policy-statement.pdf
14. ONR Safety Assessment Principles for Nuclear Facilities, 2014. http://www.onr.org.uk/saps/index.htm
15. ONR Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), T/AST/005 - Revision 7, December 2015. http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-005.pdf

16. Reducing Risks, Protecting People, HSE's decision-making process, ISBN 0 7176 2151 0, 2001, http://www.hse.gov.uk/risk/theory/r2p2.pdf
17. Safety of Nuclear Power Plants: Design, Specific Safety Requirement, No. SSR-1/2 (Rev. 1), IAEA, March 2016
18. On principles for the implementation of the objective of the Convention on Nuclear Safety to prevent accidents and mitigate radiological consequences, Vienna Declaration on Nuclear Safety, Convention on Nuclear Safety, CNS/DC/2015/2 Rev 1, February 2015, https://www.iaea.org/sites/default/files/cns_viennadeclaration090215.pdf
19. WENRA Safety Reference Levels for Existing Reactors, September 2014 http://www.wenra.org/media/filer_public/2016/07/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf
20. Assessment of Fuel Designs for New Commercial Nuclear Power Reactors within the United Kingdom, TOPFUEL 2012, September 2012
21. GDA Close-out for the EDF and AREVA UK EPR™ Reactor – GDA Issue GI-UKEPR-CC-01 Revision 0 – Categorisation and Classification of Systems, Structures and Components, ONR-GDA-AR-12-023, March 2013