Transactions, SMiRT-23
Manchester, United Kingdom - August 10-14, 2015
Division VII, Paper ID 431

RECENT CHANGES TO ONR'S SAFETY ASSESSMENT PRINCIPLES RELEVANT TO CONSIDERATION OF ACCIDENTAL INTERNAL & EXTERNAL HAZARDS

S Thompson[1], T Allmark[2], L Ash[1], C Belsham[1], P Ford[3], R Fowler[1]
M Lloyd-Davies[1], T MacLeod[1], G Williams[3]

[1]Inspector, Office for Nuclear Regulation, UK
[2]Superintending Inspector, Office for Nuclear Regulation, UK
[3]Principal Inspector, Office for Nuclear Regulation, UK

ABSTRACT

In 2011 ONR published its initial response to the events at Fukushima, ONR (2011a). One of the recommendations, Interim Recommendation 5 (IR5), recommended that once the lessons from this event were understood, ONR should seek to update its Safety Assessment Principles (SAPs), ONR (2006) accordingly; ONR SAPs have now been updated, ONR (2014a). This paper considers the implications for internal and external hazards, especially fire, internal flood, and the natural hazards: extreme weather, flooding and earthquake that formed a major part of the post Fukushima learning.

ONR's internal and external hazards teams have taken the opportunity to significantly enhance the SAPs and make more explicit what constitutes an adequate safety justification for nuclear plant where such hazards are relevant. This paper only covers hazards arising from accidents; it does not cover hazards arising from malicious threats. The topics covered are:

- The importance of and relationship between Design Basis Analysis (DBA), Beyond Design Basis Analysis (BDBA), Probabilistic Safety Analysis (PSA) and Severe Accident Analysis (SAA), where these are relevant to hazards.
- The implications of considering external hazards described by *hazard curves* that are defined at a range of exceedance frequencies[1]. This applies to most natural hazards and has implications for nuclear site risk that ONR has not seen fully explored in licensee safety cases:
  - The effect of selecting design basis external hazard levels at the 10^{-4}/yr point on the hazard curve and the importance to be attached to BDBA, especially in terms of the risk arising from the hazard.
  - The importance of BDBA and associated cliff edge analysis, given that the site risk from natural hazards especially, will likely be dominated by the plant failures beyond the design basis hazard level.
- The contribution of the various analysis types to providing a safety case demonstration that plant risks in respect of hazards are As Low As Reasonably Practicable (ALARP) and risk targets can be met.

FUKUSHIMA AND LESSONS LEARNED RELEVANT TO EXTERNAL HAZARDS AND NUCLEAR SAFETY IN THE UK

A number of major documents have been produced by ONR in response to the Fukushima event in Japan, the most significant of which are ONR (2011a), ONR (2011b) & ONR (2014b). ONR's "Fukushima Final Report", ONR (2011a), contains the following recommendation:

> **Recommendation IR-5**: Once further detailed information is available and studies are completed, ONR should undertake a formal review of the Safety Assessment Principles to determine whether any additional guidance is necessary in the light of the Fukushima accident, particularly for "cliff-edge" effects.

[1] Strictly these are exceedance probabilities, but hazard curves are normally expressed in frequency format. At the low frequencies being considered here, the differences are not significant.

Looking broadly across the learning experience from the Fukushima Dai-ichi event, a number of significant learning opportunities were identified for Nuclear Licensees on severe accident management, including resilience enhancements to plant, and external hazards because of the nature of the event. Those relevant to external hazards include:

- The importance of characterising external hazards properly so that adequate design bases can be defined.
- The importance of identifying cliff edge effects and the need to demonstrate a margin to failure beyond the design basis.
- The importance of employing probabilistic analysis to reinforce the deterministic design basis analysis and provide a robust demonstration that the risk arising from design and beyond design basis faults are ALARP.
- The need to re-enforce emergency arrangements to account for external hazards events leading to widespread common cause failure across both the site and surrounding infrastructure.

A number of ONR Recommendations, ONR (2011a), and Findings in response to the Stress Tests defined by ENSREG[2], ONR (2011b), were also made and reflect the learning points noted above; for details refer to these reports. The UK Licensees have made substantial progress at this time to respond to these Recommendations and Findings; details can be found in the latest ONR Progress Report, ONR (2014b).

In terms of the UK's nuclear regulatory process and in particular the licencing process ONR applies to nuclear sites, the Final Report concluded as follows:

> **Conclusion IR-4**: To date, the consideration of the known circumstances of the Fukushima accident has not revealed any gaps in scope or depth of the Safety Assessment Principles for nuclear facilities in the UK.
>
> **Conclusion IR-5**: Our considerations of the events in Japan, and the possible lessons for the UK, has not revealed any significant weaknesses in the UK nuclear licensing regime.

The 2006 edition of the SAPs, ONR (2006), was current at this time. While this version was supported as acceptable and already covered the issues raised by the Fukushima event, it was considered appropriate to review them with the advantage of five years' experience with their use. In the hazards area, the opportunity was taken to strengthen the existing SAPs and add additional explanatory text in the following areas:

- The notion of discrete and non-discrete hazards has been introduced, to distinguish between those hazards that can be characterised at a specific frequency of occurrence and those, such as natural hazards, that must be specified over a range of frequencies, typically by means of a hazard curve.
- Substantial new explanatory text has been added to support the safety assessment principle on external flooding, including the definition of design basis flood, the importance of allowing for ground conditions and topography, layout, design and consideration of the protection requirements. There is also some discussion on arrangements to forewarn the licensee of flooding event, and of the need to consider off-site effects.
- A new principle has been added specifically on hazard screening. This issue was previously covered implicitly by the text supporting hazard identification and characterisation.
- A new principle and supporting text has been added on BDBA. This augments the previous version that only included a principle on "cliff edge" effects.
- Several generally applicable principles on calculational methods and data validity and assurance are now explicitly referenced by the hazards section of the SAPs.

CONSTRUCTION OF THE SAFETY ASSESSMENT PRINCIPLES

[2] ENSREG – European Nuclear Safety Regulator. ENSREG is part of the European Commission and wrote the set of Stress Tests to be addressed by nuclear states in the European Union, following the Fukushima event. These tests were formulated to enhance defence-in-depth protection against fault progression.

The SAPs document is ONR's primary reference for inspectors assessing Licensee safety cases and explains how such cases should demonstrate that plant operations meet the legal test of adequacy, as required under Licence Condition 23 (LC23) attached to each Nuclear Site Licence (NSL) in the UK. The Licensee's themselves will normally have their own nuclear safety principles and may write safety cases in ways that best suit their needs. However, ONR inspectors will still assess them against the SAPs.

The SAPs are statements of principle, not mandatory requirements that plant operations must meet. They are however intended to convey to the industry what ONR considers to be a high level statement of relevant good practise (RGP) and they have been written specifically to be consistent with IAEA safety guides and WENRA[3] guidance.

The SAPs themselves are organised into twelve broad categories covering all aspects of nuclear safety. Internal and external hazard issues interact with all of these categories to some degree, but this paper will concentrate on those aspects relevant to safety cases for high hazard nuclear plant such as nuclear reactors. On this basis, the most important categories and associated principles are:

FUNDAMENTAL PRINCIPLES
- FP – Fundamental principles

THE REGULATORY ASSESSMENT OF SAFETY CASES
- SC – Safety cases

SITING ASPECTS (from para. 127 on)
- ST – Siting

ENGINEERING PRINCIPLES
- EKP – Key principles
- EHA – External and internal hazards
- ECE – Civil engineering
- EHF – Human factors

FAULT ANALYSIS
- FA – Fault analysis
- AV – Assurance of validity of data and models

NUMERICAL TARGETS
- NT – Numerical targets and legal limits

ACCIDENT MANAGEMENT AND EMERGENCY PREPAREDNESS
- AM – Accident management and emergency preparedness.

The sub-headings refer to particular categories of principles and each principle within a category carries a two or three letter identifier, as indicated here. Internal and external hazards principles, of which there are now 19, are all designated EHA.

Traditionally, nuclear safety of plant and operations is underpinned by a number of different but complementary analyses. These analyses together enable the licensee to demonstrate, through a safety case, that operation of plant is such that risk is *As Low As Reasonably Practicable* (ALARP) (Principle FA.1)[4]. The ALARP principle is a cornerstone of UK nuclear safety regulation (Para. 9 et seq.). The ALARP principle may be expressed in numerical terms – as specific targets within the SAPs, but ONR recognises that meeting relevant good practice (RGP) in engineering, operation and safety management in many cases leads to risks that are reduced to levels that are compatible with these targets.

Safety cases must consider both operational conditions and fault conditions. Internal and external hazards are considered as potential initiators of fault conditions and so this paper concentrates only on those SAPs relevant to fault analysis.

[3] IAEA – International Atomic Energy Agency. WENRA – Western European Nuclear Regulators Association.
[4] The SAPs, ONR (2014a), will be referred to frequently in this paper. Individual safety assessment principles will be referred to explicitly by their letter designator and number, and supporting text will be referred to by paragraph number.

Conservative design[5], good operational practice, and adequate maintenance and testing should minimise the likelihood of faults. Nevertheless, faults may still occur and so a facility must be capable of tolerating them (Principle FA.4). Nuclear facilities are therefore designed to cope with, or are shown to withstand, a wide range of faults without unacceptable consequences by virtue of the facility's inherent characteristics or safety measures. This is known as the design basis. Design basis analysis (DBA) is a robust demonstration of the fault tolerance of the facility, and of the effectiveness of its safety measures. Its principal aims are to guide the engineering requirements of the design and to determine limits and conditions to safe operation (LC23(1) Operating Rules), so that safety functions can be delivered reliably during all modes of operation and under reasonably foreseeable faults. In DBA, any uncertainties in the fault progression and consequence analyses are addressed by the use of appropriate conservatism. In this approach, risk is not quantified, but the adequacy of the design and the suitability and sufficiency of the safety measures are assessed against deterministic rules (e.g. design codes). These rules are derived from RGP, including the SAPs.

DBA as applied to internal and external hazards involves defining a design basis for each credible hazard (Principle FA.5, Para. 628), analysing the facility to determine how the plant might fail under the design basis and developing protection and mitigation features to its design and operation, so that these faults conditions cannot develop into a release of radioactivity to workers or the public. An important feature of hazards DBA is that there may well be parts of the facility that are allowed to fail, but no such failures will lead to a consequential radiological release. Hazards DBA makes use of the fundamental engineering principles (EKP) and specific hazards principles (EHA), to ensure that required safety functions can be delivered if a hazards design basis is inflicted on the facility.

However, DBA alone is unlikely to be sufficient to demonstrate adequate safety of the facility for faults initiated by internal and external hazards.

- Firstly, a feature of hazards induced faults is that the loss of safety function may be subject to so called "cliff edge" effects, where small changes in the hazard severity, facility response, or design basis analysis could lead to a disproportionate increase in radiological consequence. This can be due to uncertainties in the hazard definition for the design basis event, uncertainties in how the plant is modelled, or uncertainties in how the plant response to this design basis is computed. Whatever the reason, there is the potential for the DBA to miss-represent the loss of safety function for a hazards induced fault sequence. For this reason, the notion of Beyond Design Basis Analysis (BDBA) for hazards faults is used in the SAPs; such analyses should:
  - Confirm the absence of 'cliff edge' effects just beyond the design basis (Principle EHA.7);
  - Identify the hazard level at which safety functions could be lost (i.e. determine the beyond design basis margin) (non-discrete hazards only);
  - Provide an input to PSA to establish whether risk targets are met (see Para. 713 ff.);
  - Ensure that safety is balanced so that no single type of hazard makes a disproportionate contribution to overall risk (see Para. 749); and
  - Provide an input to severe accident analysis (non-discrete hazards only) (see Para. 663 ff.).
- Secondly, additional analysis may be needed to understand the overall risk presented by the facility and to allow comparisons to be made against the SAPs Numerical Targets (Principle NT.1, Para. 695 ff.). It may also be essential for understanding the strengths and weaknesses of a design with complex systems and interdependencies; as part of evaluating modifications to plant; or changes in operating conditions; and for many other applications to safety decision making. These matters are normally addressed in the nuclear industry through PSA.
- Thirdly, it will not always be reasonably practicable to incorporate the robust, conservatively designed preventative and protective safety measures expected for design basis faults when the initiating event is highly unlikely or difficult to predict. However, planning for how events with more severe consequences than allowed for in the design basis would be managed, and providing the plant,

[5] The rest of this section is adapted from ONR (2014a) paras. 605-613.

equipment and procedures that would be needed to control or mitigate their consequences is often reasonable. Plant states which could merit such planning include those arising following:

- high consequence events of very low frequency for which the design safety measures may be ineffective; and
- design basis events where, conservatively, the safety provisions are assumed to fail.

The principle of defence in depth (EKP.3) means that these types of 'beyond design basis' plant states where the potential consequences are severe should be considered in the safety case. Severe accident analysis (SAA) is therefore used to complement engineering judgement, DBA (and BDBA for external hazards) and PSA to help understand such accidents and determine safety measures to mitigate their consequences and/or protect against further escalation (Principle FA.5). SAA differs from the DBA in that it is usually (though not exclusively) performed on a best-estimate basis and its starting point is the degraded plant state following an event, rather than the event itself. Its main aims are to help plan for potential severe accidents and to assist with identifying what further plant, equipment and human actions are required beyond what has been identified through DBA and PSA are reasonably practicable.

In line with wider international guidance, the SAA should form part of a demonstration that potential severe accident states have been 'practically eliminated'. To demonstrate practical elimination, the safety case should show either that it is physically impossible for the accident state to occur (can be difficult) or that design provisions mean that the state can be considered to be extremely unlikely with a high degree of confidence. Each instance where practical elimination is claimed should be assessed separately, taking into account relevant uncertainties, particularly those due to limited knowledge of extreme physical phenomena.

Fault analysis of nuclear facilities often involves consideration of fault sequences and accident conditions for which there is limited or no experience. This may result in significant uncertainties and gaps in the physical and statistical data that are needed for the analysis. Handling quantifiable uncertainties, stemming from imprecision in knowledge and data, should be regarded as an intrinsic part of the risk assessment under ONR's precautionary approach to decision making (Para. 30). These uncertainties may be handled by introducing conservatisms, sensitivity analysis, or by a variety of explicit uncertainty analysis techniques. In every case, professional judgement on whether the assumptions or estimates are supported by appropriate evidence will be a key element of the assessment.

SPECIAL FEATURES OF INTERNAL AND EXTERNAL HAZARDS THAT NEED TO BE CONSIDERED

Hazard initiated faults are often similar to internal plant faults, following the same sequence of component failures and yielding similar consequential effects if such failures result in a radiological release. However, there are a number of important and significant differences that are captured as specific principles in the EHA category, and we cover these in this section of the paper.

Hazards

Para. 228 defines external hazards as those natural or man-made hazards to a site and facilities that originate externally to both the site and its processes, i.e. the dutyholder may have very little or no control over the initiating event. External hazards include earthquake, aircraft impact, extreme weather, electromagnetic interference (off-site cause) and flooding as a result of extreme weather/climate change (this list is not exhaustive). Terrorist or other malicious acts are assessed as external hazards under duties deriving from security legislation (see Para. 39).

Para. 229 defines internal hazards as those hazards to the facility or its structures, systems and components that originate within the site boundary and over which the dutyholder has control in some form. The term is usually limited to apply to hazards external to the process, in the case of nuclear

chemical plant, or external to the primary circuit in the case of power reactors[6]. Internal hazards include internal flooding, fire, toxic gas release, dropped loads or impact and explosion/missiles. Again, this list is not exhaustive.

Each of the EHA Principles is discussed below.

Hazard Identification and Characterisation

Principle EHA.1 and Para. 234 make clear that reasonably foreseeable hazards and their combinations (e.g. tidal surge and astronomical tide), causally-related hazards (e.g. extreme wind and high waves) and consequential events resulting from a common initiating event (e.g. internal flood following earthquake, or smoke damage following fire) should be identified. An important qualification is that only those hazards that can affect safety need to be identified and characterised. In the UK, the direct effects of volcanic eruption are not considered credible, but the indirect effects from volcanic ash may be credible.

Discrete and Non-discrete hazards - Paras. 232 and 233 cover a new feature of the SAPs, specifically an explicit recognition of the differences between those hazards characterised at a single frequency (or small number of frequencies) and those that can only properly be characterised over a continuous range of frequencies. The latter category is meant to capture natural hazards such as extreme wind, flooding and earthquake, which are best described in terms of a hazard curve.

Hazard Analysis – SAP EHA.1 expects that hazards that have been identified as credible are analysed to establish their frequency of occurrence and severity. The nature of such analyses will vary substantially depending on the type of hazard and its perceived significance to nuclear safety at the site. Some hazards, such as fire and steam release, and natural external hazards relating to extreme weather and earthquake phenomena, will normally attract detailed analyses from multi-disciplinary teams of specialists. Other hazards, in particular man-made external hazards such as those due to off-site transport, or explosion from an off-site hazardous facility, may be characterised more conveniently on the basis of an estimate of their maximum credible effect, rather than in frequency/severity terms (Para. 242).

There are a number of generic features of hazard analyses that are worthy of note:

- *Outputs from hazard analyses* – Hazards should be characterised in sufficient detail to facilitate the screening process, enable adequate design bases to be defined for the DBA, and provide sufficient information to enable appropriate Beyond Design Basis, Probabilistic Safety and Severe Accident Analyses to be undertaken (Principles FA.1, FA.5, Para. 628).
- *Data* – The data used to support hazard analyses often contain significant uncertainty. Natural hazards especially can be difficult to analyse for this reason and care must be taken to obtain good quality data representative of the site and to take advantage of any relevant good practise that applies (Principles EHA.2 & AV.3). Where available data is inadequate or absent, then good engineering and scientific judgment by qualified individuals should be sought (Para. 237). For earthquake hazard there is well developed relevant good practise on the use of expert judgment, see e.g. US Nuclear Regulatory Commission (USNRC (2002)).
- *Data collection and site monitoring of hazards parameters* – Data on hazards parameters that can reasonably be monitored and measured in and around the site vicinity should be collected through the life of the site, (Para.238 & Principle AV.7). This is especially relevant to natural hazards, where parameters, such as windspeed, wind direction, rainfall, air and sea temperatures, seismicity and sea level, collected through the life of the site, can be used to calibrate and augment data used in earlier hazard analyses. Clearly, site based data collection takes time to become useful to hazard analyses, but can provide valuable additional data for the periodic reviews of safety required under LC15.
- *Calculational methods and models* – Hazard analyses should include a model of the site, its surroundings and relevant on-site (internal hazards) and off-site (external hazards) infrastructure, so

[6] Initiating events that are internal to the process and primary circuit are known as internal plant faults.

that the required outputs can be computed with sufficient confidence to enable adequate deterministic and probabilistic safety analyses to be undertaken (Principles AV.1 & AV.2).

Calculation methods should enable design bases to be computed as best-estimates, except for natural hazards, which should be computed conservatively (Principle EHA.4, Paras. 239 & 629). This is because the initiating event frequencies applied to hazards generally is set at 10^{-5}/yr, but for natural hazards where data collection and analysis methods may exhibit high levels of uncertainty at these low frequency levels, a conservative estimate at 10^{-4}/yr is considered reasonable.

Probabilistic analyses should be conducted on the basis of best estimate hazards input (Para. 655). For hazards characterised by the use of complex analyses, relevant good practise would normally expect a quantitative analysis of uncertainty to develop percentile confidence levels and other probabilistic measures of hazard definition. As a final sanity check on the validity of a hazard analysis, sensitivity studies should be considered, SAP AV.9

Hazards Screening

Principle EHA.19 is a new principle that was captured rather informally as Para. 212 in the 2006 version. This principle is now recognised as an important feature of any hazard analysis. The supporting text anticipates that discrete hazards can be screened on either low frequency and/or low consequence grounds. Low frequency is considered to be $<10^{-7}$/yr and reflects the advice in Para. 749 under Target 8 dose/frequency requirements related to accidental radiological release to the public.

Para. 236 makes a number of important points related to the nature of external hazards in particular, namely that these hazards do not respect the artificial man-made boundaries of licensed nuclear sites, and most natural hazards are likely to affect adjacent sites as well. The emergency arrangements covering these sites should make allowances for this common cause effect, see Para. 139 after Principle ST.6, and Principle AM.1 & Para. 773.

Defining Effective Hazards Design Bases

As noted above, DBA makes use of deterministic methods to analyse design basis fault conditions. Once a hazard has been identified as credible and screened into the DBA process, hazard analysis is used to determine an appropriate design basis (Principle EHA.2). For internal fire hazard this could be the amount of fire inventory in a compartment or the energy content and power delivered by a conflagration. An important feature of DBA is that it should assume the facility's most adverse permitted operating state, Principle EHA.5. This implies that plant should be presumed to be operating at the most adverse pressure, temperature and loading conditions; it also implies more esoteric assumptions, such as the most adverse astronomical tide conditions under which plant for which this is relevant (sea water intake and discharge systems for example) would be allowed to operate.

Discrete hazards – For internal hazards and man-made external hazards the design basis is defined in one of two ways:

- Probabilistically, as a best estimate (mathematically this is a mean estimate) value of hazard severity at a frequency of 10^{-5}/yr (Principle EHA.4), or
- Deterministically, as a maximum credible event (Para. 242).

Non-discrete hazards – For natural external hazards defined by hazard curves, the design basis is defined:

- Probabilistically, as a conservative estimate (mathematically this is often interpreted as the 85% confidence level) of hazard severity at the 10^{-4}/yr point on the hazard curve (Principle EHA.4).

The 10^{-4}/yr value has stood the test of time as a suitable single point description of the hazard upon which to develop and analyse plant design. On the one hand the hazard severity at this frequency provides a robust challenge to plant safety so that most of the hazard initiated faults likely to militate

against the plant being risk ALARP will be analysed and protected against; on the other, the challenge is not so severe that designers will be driven to mitigating very extreme faults through the DBA process, leading to excessive hazard protection measures and unbalancing the overall plant design with respect to other fault conditions. The DBA process, using a conservative design basis at the 10^{-4}/yr level, should lead to a plant design that is risk ALARP and balanced. However, the DBA process cannot by itself guarantee this and for non-discrete hazards especially, beyond design basis analysis and hazards PSA are important to demonstrating that the ALARP principle has been met.

Principle EHA.4 expects the 10^{-4}/yr value to be used for DBA, but the Licensee is at liberty to select another point on the hazard curve if this can be justified, as might be the case for facilities containing low levels of radioactive inventory or otherwise unable to deliver large consequential doses to workers and the public, refer to Paras 726 et seq and Target 4. Where consequences are low, normal industrial standards may be acceptable (Para. 241).

Hazards Beyond Design Basis Analysis – An Important Additional Analysis Step

Principle EHA.18 is a new principle that explicitly embodies beyond design basis ideas; Para. 246 makes clear the relationship between BDBA and PSA and the demonstration of a balanced plant design where "no single hazard makes a disproportionate contribution to overall risk" (Para. 246(d)). Paras. 246(e) and 248 explain the relationship between BDBA and SAA, and exemplify one of the major elements of the ENSREG Stress Tests, namely the need to identify the margin between the design basis hazard level and the level where claimed safety functions can no longer be achieved. This has also now been reflected in the civil engineering section, especially Para. 334, supporting Principle ECE.1 on safety functions of structures.

Para. 246(a) refers to cliff-edge effects and to Principle EHA.7 and existed in the previous revision of the SAPs, ONR (2006). Para. 247 defines a cliff edge as "where a small change in analysis assumptions … is predicted to lead to a disproportionate increase in radiological consequence". The concept of cliff edges is useful for highlighting those sorts of failures that can lead suddenly to an escalation of adverse plant response to the hazard, making it difficult for operators to intervene using normal procedural or emergency arrangements.

Non-discrete hazards – As noted above, BDBA is an important additional step to DBA for non-discrete hazards. It assists in demonstrating that the facility is very robust to hazard challenges at the design basis level and contributes to demonstrating that facility risk is ALARP. It also demonstrates the absence of additional significant faults initiated just beyond the design basis hazard level.

The importance of analysing severe accidents beyond the design basis was first recognised as a significant safety concern after the Three Mile Island Unit-2 accident in the US in 1979. Following that event, the USNRC instigated a number of work programmes that had the effect of investigating plant response to challenges beyond the design basis, USNRC (1988) & USNRC (1991). For external hazards USNRC (1991) recommends two approaches: one involves examining the conservative assumptions employed in the DBA to establish a margin to failure beyond the design basis, known as *margins analysis*. The other is to employ the PSA method (Probabilistic Risk Analysis in the US) to examine the plant response to beyond design basis events. The intent of both is to provide assurance that the plant has capability beyond the design basis, so that the design basis value, which is a man-made criterion to assist plant designers, rather than a parameter with intrinsic safety value in itself, does not artificially drive the safety of the plant or lack thereof.

Subsequently, following the Fukushima event, there has been renewed interest world-wide in BDBA. In Europe the concept has been expressed in terms of Design Extension Conditions and WENRA has been developing guidance on this, WENRA (2015a, 2015b), but in the UK regulatory context, the concept is best expressed as Beyond Design Basis Analysis.

Two of the authors have submitted another paper to SMiRT23, Ford et al (2015), specifically investigating the role of BDBA applied to seismic hazard using simplified risk techniques. Although these results are indicative and do not apply to any specific facility, they indicate that for a seismic design basis set to 10^{-4}/yr, the majority of seismic risk is accumulated in the region of the hazard curve from 10^{-4}/yr to 10^{-5}/yr. This is just the region in which BDBA should be most powerful, and the faults involved are those that would be classed as *Design Extension Conditions Type A* (DEC A) by WENRA (2015a). They also indicate that beyond this point, it is likely that the seismic risk will have saturated or peaked, and investigating the effects of earthquakes at exceedance frequencies below 10^{-5}/yr, is likely to be a SAA consideration, or *Design Extension Conditions Type B* by WENRA (2015a).

Hazards PSA and Understanding the Balance of Facility Risk

The effect of hazards on facility risk has traditionally been poorly analysed in the UK nuclear industry, with only primitive representations of the hazards and plant response. Yet there is good world-wide experience to indicate that hazards, especially, fire, earthquake and external flood, can make a significant contribution to overall plant risk. The SAPs, as noted extensively above, now make much more explicit the expectations of ONR in this regard through Principle EHA.18 and Para. 608, and through stronger linking between the hazards principles and the fault analysis principles generally.

The requirement for an adequate safety case to cover the operations at nuclear facilities on UK nuclear sites is covered by LC23, and is met principally by demonstrating that the nuclear risk to workers and public from the facility is ALARP. For major nuclear hazards plant, the expectation is that a Level 2 PSA will be undertaken and this is reflected in the UK's response to the Fukushima event as FR 4, ONR (2011a).

The SAPs and Individual Hazards

The SAPs contain specific principles for the following hazards:

Aircraft impact
Earthquakes
Electromagnetic interference
Extreme weather
Flooding (external)
Use, storage and generation of hazardous materials
Internal fire and explosion
Internal flooding

Both the principles and supporting text remain mostly unchanged in the new revision of the SAPs, except as below:

Aircraft impact (Principle EHA.8) – The previous revision of the SAPs covered only the statistical evaluation of crash frequency. This has now been extended to provide more clarity on the sorts of issues that Licensees should consider in mitigating the consequences from accidental aircraft impact.

External flooding (Principle EHA.12) – The intent of the principle remains the same but has been re-worded to include explicit reference to severe accidents, in deference to the Fukushima event. The supporting text (Paras. 260 et seq) has been extended substantially to add a number of features not previously part of the SAPs:

- The expectation that nuclear plant will meet the dry site concept is made explicit. This concept has been made part of recent IAEA guidance, IAEA (2011), and involves safety related plant and equipment being placed above the design basis flood level, so that the possibility of flooding, at least from a design basis event, becomes extremely remote.

- A further expectation is that Licensees will take flood warning advice from external agencies, to enable preparatory actions to be implemented.
- Para. 262 refers to civil engineering Principle ECE.23 regarding the importance of inspecting flood defences, including any required defences off the licensed site. This latter is an important aspect because flood protection at the site may depend on defences owned and operated by third parties. Licensees are expected to have arrangements with third parties upon whose defences they depend, sufficient to provide confidence that any claims made on these defences can be delivered.

Use, storage and generation of hazardous materials (Principle EHA.13) –The supporting text (Paras. 268 et seq.) has been re-written to clarify the guidance in the areas of: elimination and or substitution for less hazardous substances; and combined or consequential hazards in which hazardous material may be released.

Internal fire and explosion (Principles EHA.14. EHA 16, EHA.17) – The supporting text (Paras. 271 et seq.) is amended to be consistent with terminology elsewhere in the SAPs and in particular to be consistent with the changes described earlier relating to Principles EHA.2, EHA.4 and EHA.18.

Internal flooding (Principle EHA.15) - There is now a clear cross-reference between Principle EHA.15 and EHA.12, showing the relationship between protection against external and internal flooding.

CONCLUSIONS

This paper has reviewed the important changes relevant to internal and external hazards that have recently been made to ONR's SAPs in light of the learning from the Fukushima event in Japan in 2011. ONR's post Fukushima work examined the process used in the UK for regulating nuclear licensed sites and concluded that it remained fit-for-purpose, however the opportunity to enhance the SAPs (ONR's primary guidance on what constitutes an adequate safety case) was taken. Significant additions have been made to the hazards section of the SAPs, especially with regard to external hazards, to enhance the principles that already existed, and these are discussed in detail in this paper. The most significant enhancements are:

- Additional explanation of relationship between Design Basis Analysis (DBA), Beyond Design Basis Analysis (BDBA), Probabilistic Safety Analysis (PSA) and Severe Accident Analysis (SAA), where these are relevant to hazards.
- The implications of considering external hazards described by *hazard curves* that are defined at a range of exceedance frequencies, noting this applies to most natural external hazards.
- The effect of selecting design basis external hazard levels at the 10^{-4}/yr point on the hazard curve and the importance to be attached to Beyond Design Basis Analysis, especially in terms of the risk arising from the hazard.
- The importance of Beyond Design Basis Analysis and associated cliff edge analysis, given that the site risk from natural hazards especially, will likely be dominated by the plant failures beyond the design basis hazard level.
- Various amendments to the SAPs covering internal hazards to improve clarity and better link in to other Principles.

REFERENCES

Ford, P., Brighton, P. W. M., Fowler, R. (2015), "The Influence of Design Basis and Beyond Design Basis Seismic Analysis on Risk Using a Simplified Seismic Risk Approach", SMiRT 23, Manchester, UK, August 10-14, 2015.

IAEA (2011), IAEA International Fact Finding Expert Mission of the Fukushima Dai-ichi NPP Accident Following the Great East Japan Earthquake and Tsunami, Report to the IAEA Member States,

http://www-pub.iaea.org/MTCD/meetings/PDFplus/2011/cn200/documentation/cn200_Final-Fukushima-Mission_Report.pdf

ONR (2006), "Safety Assessment Principles for Nuclear Facilities", 2006 Edition, Revision 1, http://www.onr.org.uk/saps/saps2006.pdf

ONR (2011a), "Japanese earthquake and tsunami: Implications for the UK nuclear industry", Final Report, September 2011, http://www.onr.org.uk/fukushima/final-report.pdf

ONR (2011b), "European Council "Stress Tests" for UK nuclear power plants, National Final Report", Rpt. ONR-ECST-REP-11-002 Revision 0, http://www.onr.org.uk/fukushima/stress-tests-301211.pdf

ONR (2014a), "Safety Assessment Principles for Nuclear Facilities", 2014 Edition, Revision 0, http://www.onr.org.uk/saps/saps2014.pdf

ONR (2014b), "UK ONR ENSREG Related 'National Action Plan', Updated Progress Report Chief Inspector of Nuclear Installations", 31 December 2014, http://www.onr.org.uk/fukushima/ensreg-report-2014.pdf

USNRC (1988), "Generic Letter 88-20, Individual Plant Examinations for Severe Accident Vulnerabilities", 10CFR50.54(f).

USNRC (1991), "Generic Letter 88-20 Supplement No. 4, Individual Plant Examinations for External Events (IPEEE) for Severe Accident Vulnerabilities", 10CFR50.54(f) final.

USNRC (2002), "Guidance for Performing Probabilistic Seismic Hazard Analysis for a Nuclear Plant Site: Example Application to the South-Eastern United States", NUREG/CR-6607. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6607/

WENRA (2015a), "Guidance Document Issue F: Design Extension of Existing Reactors", Reactor Harmonisation Working Group, 29 September 2014. http://www.wenra.org/media/filer_public/2014/10/28/wenra-rhwg_guidance_on_issue_f.pdf

WENRA (2015b), "Guidance Document Issue T: Natural Hazards Head Document", Reactor Harmonisation Working Group, 22 April 2015. http://www.wenra.org/media/filer_public/2015/04/23/wenra-rhwg_t1_guidance_on_issue_t_head_document_2015-04-21.pdf