Transactions, SMiRT-26
Berlin/Potsdam, Germany, July 10-15, 2022
Division VII

STATE-OF-ART REVIEW OF BEYOND DESIGN BASIS EVALUATION APPROACH OF A GENERIC NUCLEAR POWER PLANT IN THE UK

Dr. Ming Tan[1], Dr Svetlin Filipov[2], Peter Ford[3], Xunjia Zhuo[4]

[1] Technical Principal, Mott MacDonald Ltd, United Kingdom (*ming.tan@mottmac.com*)
[2] Principal Safety Engineer, Mott MacDonald Ltd, Bulgaria (*svetlin.filipov@mottmac.com*)
[3] Director, Ford Nuclear Services Ltd, United Kingdom (pford_fnsl@aol.com)
[4] Senior Engineer, State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Corporation, China (zhuoxunjia@cgnpc.com.cn)

ABSTRACT

The Fukushima accident prompted rapid development in the appreciation and codification of BDB methodology into regulatory guidance and this is still continuing, especially at IAEA, which has recently and is due to publish several new standards documents directly relevant to BDB analysis. The objective of this paper is to provide a state-of-art review on how BDB evaluations are undertaken in the UK nuclear industry. Then, using the work undertaken for the Generic Design Assessment (GDA) in the UK for UK HPR1000, this paper proposed a more systematic approach for “cliff-edge” evaluation based on a generic nuclear power plant design currently being developed in the UK.

INTRODUCTION

The licensing process of a nuclear installation requires consideration of the beyond design basis (BDB) events to ensure that the plant response to External Hazards (EHs) beyond design basis is robust. In the United Kingdom (UK), the Regulator highlighted this requirement in their Safety Assessment Principles for Nuclear Facilities (SAP) [ONR, 2020], in particular EHA 18 and EHA7, and Technical Assessment Guide 13 (TAG13) [ONR, 2018] is often being used by the nuclear industry as a guide.

As noted in TAG13, there are generally two levels of BDB events for external hazards, of which their purposes are to:

- demonstrate that the plant design is robust to uncertainties in the definitions of external hazard design bases and plant design that flows from them. This is also commonly known as “cliff-edge” evaluation.
- demonstrate for external events significantly beyond the design basis, what failure modes can occur and how are plant safety functions challenged.

To achieve the above purposes, the UK (and international) nuclear licensees and Requesting Parties (RP) adopted varying approaches and there is not usually a set rule how this is being tackled. The objective of this paper is to provide a state-of-art review on how BDB evaluations are undertaken in the UK nuclear industry. Then, using the work undertaken for the Generic Design Assessment (GDA) in the UK for UK HPR1000 [GNSL, 2020], this paper will focus on proposing a more systematic approach for “cliff-edge” evaluation based on a generic nuclear power plant design currently being developed in the UK.

UK HPR1000

The UK HPR1000 is a Pressurised Water Reactor using the Chinese Hualong technology with electric output of approximately 1180MW. The UK HPR1000 has evolved from a sequence of reactors that have been constructed and operated in China since the late 80s, including the M310 design used at Daya Bay and Ling'ao (Units 1 and 2), the CPR1000, the CPR1000+ and the more recent ACPR1000. The first two units of CGN's HPR1000, Fangchenggang NPP Units 3 and 4, are under construction in China. Fangchenggang NPP Unit 3 is the reference plant for the UK HPR1000.

With the intention to be deployed to the Bradwell 'B' site in the UK, the UK HPR1000 was put forward for GDA in January 2017, to be assessed jointly by the regulators - Office for Nuclear Regulation (ONR) and the Environment Agency. The regulators provided independent scrutiny to ensure that the reactor design is applicable to UK regulatory standards of safety, security and environmental protection. The GDA for the UK HPR1000 was successfully completed in February 2022, with the issuing of a Design Acceptance Confirmation (DAC) from the ONR and a Statement of Design Acceptability (SoDA) from the Environment Agency [ONR, 2022].

REGULATORY APPROACH AND RELEVANT GOOD PRACTICE

In the UK, the safety of a nuclear plant subject to external hazards is typically analysed by three complementary approaches. Although the extent to which each is pursued in any particular case depends on the hazard, the plant complexity, the potential consequences of failure, and its history:

- Design Basis Analysis (DBA),
- Beyond Design Basis Analysis (BDBA),
- and Probabilistic Safety Analysis (PSA).

Conventional fault analysis, from the initiating event through fault sequence to potential consequences, is captured by DBA and PSA. These two parallel analysis streams are complementary but philosophically quite different. DBA is deterministic and makes use of good engineering principles applied to design protection and mitigation to DB faults. PSA uses probabilistic methods to analyse all significant faults. The net aspiration of using both methods is to demonstrate:

- That the risk of nuclear consequences from plant failure is As Low As Reasonably Practicable (ALARP).
- That the risk is balanced such that no single class of fault initiating event (or hazard) dominates.
- That the design meets various risk targets.

Both DBA and PSA analyse a plant's design. The design process itself is a heavily codified engineering process; it is deterministic and uncertainty analysis is incorporated methodologically, through conservative assumptions applied to loads and material parameters. The level of conservatism is usually based on engineering judgment derived from experience and statistical analysis of how structures and materials actually perform. In a well-founded design, the risk from DB faults should be close to zero. For natural external hazards we expect that the majority of risk is accumulated from events beyond the design basis.

For fault initiating events caused by natural external hazards, the SAPs recognise that such hazards cannot be uniquely defined in terms of hazard severity, but instead are manifested probabilistically according to a hazard curve. A DBA and the design process itself cannot handle this type of probabilistic input directly; instead, the hazard curve must first be mapped onto a representative deterministic parameter called a design basis event (DBE). The rationale behind design basis event definitions is based on the notion that a plant design developed using DBE inputs to mitigate DB faults is likely to be risk ALARP. As noted above, for major nuclear power plants it is the job of the PSA to provide quantitative support to the demonstration that the design does indeed meet the risk ALARP objective.

The ONR SAPs call for natural external hazard Design Bases to be defined as the hazard severity, defined conservatively by the 10^{-4}/yr point on the hazard curve. As a starting point, this can be taken to be the 84th percentile confidence limit of the epistemic uncertainty distribution at the 10^{-4}/yr point. The choice of confidence level to define the design basis event should form part of the overall justification that the event is appropriate and fit-for-purpose. Discrete hazards and other plant fault initiators assume a hazard frequency of 10^{-5}/yr generally to mean estimate (or not explicitly conservative).

Beyond Design Basis Analysis is often a natural extension of DBA, where obvious conservatisms are removed from the design basis plant response model to give an indication of the plant's "best estimate" response to the design basis hazard. BDBA therefore predicts that the plant response will be stronger and more resistant to hazard induced design loads compared to the DBA and implies that it will fail at higher hazard levels, but with less confidence that the required safety functions will be delivered at these levels.
In terms of plant response, the accident at Fukushima in 2011 has generally been interpreted as a BDB event and is a perfect example to highlight the importance of BDB. It raised serious concerns over the operator's knowledge of how the plant would respond to such an event and highlighted the lack of adequate protection in place to mitigate the deleterious effects of consequential plant failures.

The revised SAPs provide greater detail on what the regulator expects such an analysis to deliver, which in summary are:

a) Confirm the absence of "cliff-edge" effects just beyond the design basis.
b) Identify the hazard level at which safety functions could be lost (i.e. determine the beyond design basis margin).
c) Provide an input to probabilistic safety analysis to demonstrate that risk targets are met.
d) Ensure that safety is balanced so that no single type of hazard makes a disproportionate contribution to overall risk.
e) Provide an input to severe accident analysis.

TAG13 also provides guidance that the RP (or the Nuclear Licensees) should consider two levels of BDB events for external hazards, one of which is primarily concerned with the potential for cliff-edge plant failures, for events marginally above the design basis. The second concerns more severe extreme events that could severely challenge plant safety functions across the site. The purposes are to demonstrate that:

- the plant design is robust to uncertainties in the definitions of external hazard design bases and plant design that flows from them ("cliff-edge" evaluation), and
- external events significantly beyond the design basis, what failure modes can occur and how the plant safety functions are challenged ("more severe BDB event").

The role of BDB analysis has also attracted significant interest worldwide, including recently published standards by WENRA and IAEA. The following provides a summary of the work currently being undertaken by WENRA and IAEA with regards to BDB.

WENRA has recently published a comprehensive set of Reference Levels (RLs) for natural hazards, both for existing plant as Issue T [WENRA, 2016], and new plant. WENRA does not use the term BDB event, preferring instead the term Design Extension Condition (DEC), a term that applies primarily to existing plant.

WENRA defines two levels of Design Extension Conditions (DEC) that can be broadly mapped to the levels defined by ONR TAG13:

- DEC “A” - for which prevention of severe fuel damage in the core or in the spent fuel storage can be achieved. This is broadly equivalent to the cliff-edge effects.
- DEC “B” with postulated severe fuel damage. This is broadly equivalent to the expectations regarding to the more severe BDB and Severe Accident Analysis (SAA) expressed in ONR TAG13.

IAEA is currently developing an approach to natural hazards safety analysis applied to nuclear plants that includes the concept of “design robustness”. It recognises that historically there has been much heated debate on the definition of BDB hazard events, and how to meet them. Professional opinion diverges in discussions on how best to do this: whether to lock additional conservatism into the design analysis, or whether to invoke a completely new BDB analysis, or even a PSA. The selection of a BDB event is generally seen world-wide as a good idea, but the method of selection is problematic. Existing IAEA guidance adopts the view that the design of plant should be conservative and contain “*adequate margin*”.

The main external hazards design guides for new NPPs are SSG-68 [IAEA, 2021a] and SSG-67 [IAEA, 2021b]. SSG-67, although aimed specifically at seismic hazard, contains the most developed IAEA views to date on how to specify DBE’s and the role of BDBA. The advice here is completely consistent with this.

Cliff-edge Analysis

As noted earlier, the cliff-edge analysis is broadly consistent with DEC “A” as defined by WENRA. A cliff-edge is where a small change in analysis assumptions, such as those relating to design basis hazard severity, facility response, or design basis analyses, is predicted to lead to a disproportionate increase in radiological consequence.

The main objective is to “*demonstrate that the design remains fit-for-purpose despite these uncertainties and there is a high degree of confidence that it will be able to deliver design basis safety functions as intended*” [TAG13 para. 115] It is expected that there is a demonstrable margin between the design basis and the loss of the design basis safety function that reflects the known uncertainties in both hazard analysis and plant response analysis.

This is typically achieved by undertaking a form of stress test study to show that uncertainty in the design (and construction) process is captured by the use of conservative margins, such that the ability of the plant to withstand DB faults at the DBE input level is demonstrably very robust, with no significant potential for cliff-edges or additional faults occurring at this hazard level. This can be achieved by one or a combination of:

- Increasing the design basis input level and re-calculating the DB analysis to show that plant failure still does not occur, either to DB faults or other faults that might be initiated just beyond the design basis.
- Identifying obvious conservatisms in the DB analysis plant and DB input models to show that there is an inherent net margin of safety in the design.
- By re-calculating the DB analysis at elevated DB input values to show at which hazard level plant failure from DB faults occurs.

The increase of the design basis input level for the “stress test” can be subjective. Fortunately, the ONR has provided some guidance for non-discrete hazards (hazards that can be characterised by hazard curves), such that “*if a single BDB event is selected for the BDB Analysis, a reasonable starting position is to consider the* 10^{-5}*/yr event*” [TAG13 para. 124].

For discrete hazards, it may be appropriate to postulate an event of increased severity such that the design basis can be tested in light of the uncertainties involved in both the design basis definition and the associated plant design process, to ensure that safety functions can still be reliably delivered.

“More Severe” Beyond Design Basis Events

With regards to “more severe” BDB events, this is broadly equivalent to DEC “B” from the WENRA definition, and is related to postulated or unforeseen severe plant faults or fuel damage, where significant nuclear safety functions have been severely challenged. This is closely linked with Severe Accident Analysis (SAA).
For external hazards, this could be applicable for non-discrete EHs having an estimated occurrence frequency below the design basis criterion, but which cannot be screened out, and are therefore considered to be “high consequence event of low frequency beyond the design basis”. Unlike cliff-edge analysis, the “more severe” BDB event is expected to have different acceptance criteria, as it is not expected that the usual design basis safety function can be achieved. The acceptance criteria are likely to focus on the integrity and continuous cooling of the reactor core and the spent fuel pool if such an event occurs.

It is anticipated that the analysis of nuclear safety to EH events in this region will be captured by an EH PSA. A further consideration is the need to identify plant and SSC damage states arising from very severe EH events for input to the SAA if these differ from those identified for other reasons.

It is also noted that such events may have the potential for widespread common cause effects and the likely islanding of the site from off-site services and supplies. Implementation of emergency preparedness arrangements would generally be considered if such an event were to occur.

OVERALL APPROACH FOR BDB EXTERNAL HAZARDS EVALUATION

This section provides a high-level analysis and evaluation approach for “cliff-edge” evaluation of external hazards for the UK HPR1000. To evaluate the BDB event, it is important to first understand how the DBE is defined for the generic UK HPR1000 design.

As part of the GDA, the Requesting Party may specify generic site characteristics, which should, as far as possible, envelop or bound the characteristics of known potential sites in Great Britain. In doing so, the intent is to demonstrate to the regulators that the chosen reactor design can be sited at a variety of suitable locations across the UK.

The UK HPR1000 Generic Site Report adopted the methodology of obtaining external hazard parameters, including identification, screening and design basis value derivation. The external hazards values are derived and selected for the generic site based on a systematic methodology to ensure the values are appropriate and bounding. These have been derived from published standards, experience of previous GDA projects, appropriate databases or relevant studies undertaken by other UK nuclear operators. These external hazards values constitute the Design Basis for the UK HPR1000 generic design.

The UK HPR1000 is based on the reference plant FCG3 that has its own sets of design basis external hazard values. CGN has decided that the UK HPR1000 generic design will be based on bounding the Generic Site Envelope (GSE) and FCG3 design values. This bounding process will lead to a more conservative design but will minimise changes between the FCG3 and UK HPR1000 designs. The relationship of GSE and final UK HPR1000 design values are shown in the below figure.

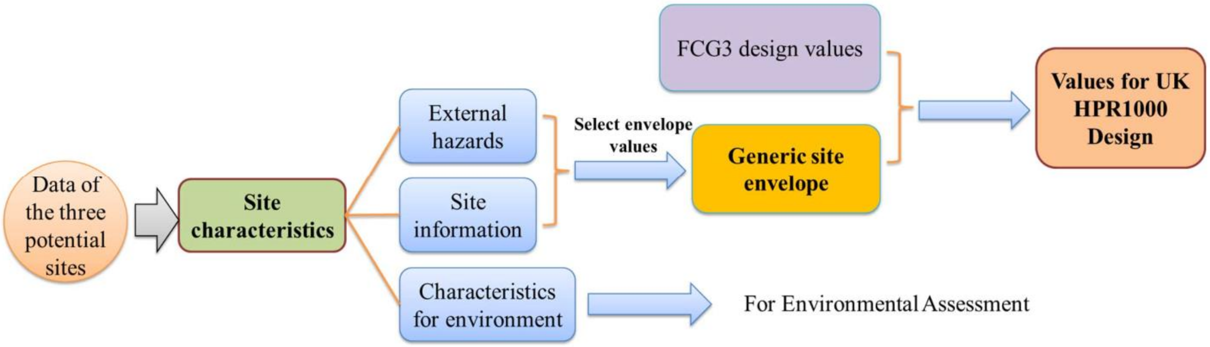
Data of the three potential sites
Site characteristics
External hazards
Site information
Characteristics for environment
Select envelope values
FCG3 design values
Generic site envelope
Values for UK HPR1000 Design
For Environmental Assessment

Figure 1. Inputs Considered for UK HPR1000 Design Values.

General approach for Cliff-edge Evaluation

The objective of the cliff-edge evaluation is to demonstrate the absence of cliff-edges just beyond the design basis, associated with both the external hazard severity and plant response. This will be achieved by a demonstrable margin between the design basis, defined in the GSE, and the loss of the design basis safety function that reflects the known uncertainties in both the hazard analysis and the plant response analysis.

From the hazard analysis perspective, as detailed in the above section, the GDA design of the UK HPR1000 has been performed using the bounding hazard definition values from FCG3 and the GSE and that the design basis is the GSE. Where the FCG3 values are bounding, the design will already have inherent margins. However, since the approach to FCG3 design treats non-discrete hazards as a set of discrete hazard severity values, rather than deriving them from a hazard curve, it can sometimes be unhelpful to interpret these values in terms of a UK generic hazard curve. This is because they correspond to very low frequency events on such hazard curves, somewhat lower (i.e. more severe) than those normally associated with BDBA. This implies that some (what would have been) "non-discrete" hazards, as one would expect, would be considered as "discrete" hazards.

Hence, to allow for efficient and systematic analysis of cliff-edge evaluations for the UK HPR1000, the external hazards are to be divided into the following categories:

- Category 1 - The first category contains the hazards of which the Design Values are significantly higher than the GSE values. This means that the design will be more robust than the one following the Generic Site data values. It is anticipated that no further assessment is required other than demonstrating that the margin is significant.
- Category 2 - The second category are hazards which are quantifiable by hazard curves during the GDA process. This means that the hazard parameter is explored in the frequency of occurrence of 10^{-5}/yr and below (case specific). The identified relevant Structures, Systems and Components (SSCs) are to be assessed against this value to demonstrate that a disturbance in the Design Basis input parameter/parameters will not bring the plant into an uncontrollable state, exceed safety limits, or cause non-fulfilment of a critical safety function. In some cases, BDB manifestations of a Hazard may be assessed as being bounded by another Hazard (based on the Hazard and expected impact). The 10^{-5}/yr is selected based on recommendations from TAG13 which it states "ONR considers that if a single BDB event is selected for the BDBA, a reasonable starting position is to consider the 10^{-5}/yr event". It is noted this this is considered as "a starting point" and can be reduced or increased if considered necessary to establish an adequate level of margin.

- Category 3 - The third category contains hazards which cannot be quantified by hazard curves (during the GDA process or otherwise). The acceptable way of reflecting such phenomena during the GDA is to consider the impact of the hazard and the consequences rather than estimating the hazard parameter value. Examples for such hazards are Seismic and External Flooding (for example, external flooding has several contributors; rain, tide, waves, etc. which are highly site-specific). A pre-assigned numerical hazard value will be set for cliff-edge analysis. The evaluations will focus more on the impact of the hazard and the consequences. The pre-assigned values are selected based on Relevant Good Practice (RGP). During the GDA, for hazards that can be defined by hazard curves during site specific stage, a commitment is made by the RP that such hazards will be revisited during the site-specific stage and cliff-edges will be evaluated based on the approach of Category 2 instead.

In addition to the categorisation above, some of the design basis hazards are being used in the design are already considered to be Maximum Credible Events (MCE) of which no cliff-edge evaluations are necessary.

The following flow chart shows the process and decision tree for how external hazards are categorised:

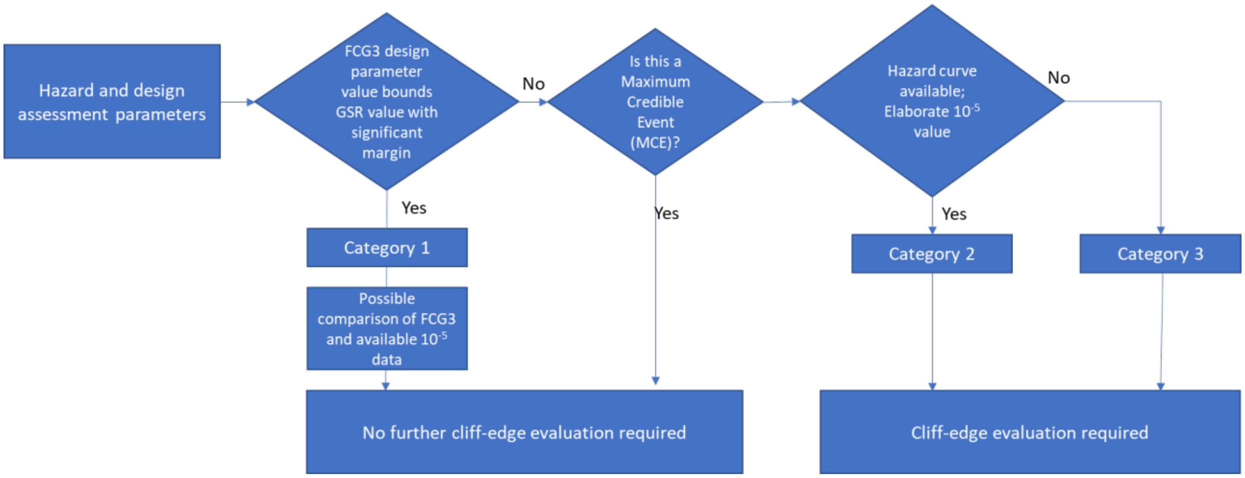
Hazard and design assessment parameters
FCG3 design parameter value bounds GSR value with significant margin
No
Yes
Category 1
Possible comparison of FCG3 and available 10^{-5} data
Is this a Maximum Credible Event (MCE)?
Yes
Hazard curve available; Elaborate 10^{-5} value
No
Yes
Category 2
Category 3
No further cliff-edge evaluation required
Cliff-edge evaluation required

Figure 2. Decision tree and external hazards categorisation process.

Based on the process defined above, the following table shows the categorisation of all external hazards within the GDA.

Table 1: Categorisation of external hazards within the GDA.

Hazard			Category Classification
Natural Hazards	Earthquake		Category 3
	External Flooding		Category 3
	Wind	Extreme Wind	Category 1
		Extreme Wind Generated Missiles	Category 1
	Torna do	Tornado	Category 1
		Tornado Generated Missiles	Category 1

	Extreme Temperatures	Air	Low	Category 2
			High	Category 2
		Water	Low	MCE
			High	Category 1
	Extreme Hail, Sleet, Snow and Icing			Category 2
	Lightning			MCE
	EMI and Space Weather			Category 2
	Heat Sink Specific Hazards			Category 3
Man-Made Hazards	External Explosions			Category 3
	Aircraft Crash			Not applicable

For the external hazards classified as Categories 2 and 3, care is required such that a BDB event is not defined to be so much larger than that of the DBE itself that it causes the plant design to be driven by BDBE rather than the DBE. What is needed is a way to demonstrate that the basic assumption stated above is confidently met.

The BDB event should be set such that the delta between the BDB event and the DBE exceeds, in a qualitative sense, the reduction/removal of uncertainties in the design process. If the design can be shown to work at this higher level then, in an engineering sense, there is confidence that it will deliver its expected design functions when launched into the real world where it is potentially subjected to a real 10^{-4}/yr event. To ensure efficiency in the evaluation of cliff-edge, the following high-level evaluation steps will be undertaken for the GDA design of the UK HPR1000 for the external hazards within categories 2 and 3, with incrementally increase in effort:

i. Evaluate if the current design can satisfy the higher BDB values using the same conservatisms inherent in the design process.
ii. If step 1 is not satisfied, remove various known conservative assumptions involved in the design process with the “best estimate” design loaded with the BDBE and re-analyse.
iii. If this is still not satisfied, increase hazard incrementally from DBE very slightly and reanalyse with the “best-estimate” design until a cliff-edge is reached to determine the margin at which this is achieved. Then, refer back to the hazard analysis to determine the frequency at which the cliff edge is reached and consider the adequacy of the margin in light of this, in the same way as for a Category 2 hazard.

Together with above, for those that required the third step, the design is also to be interrogated qualitatively for possible faults/failures that might occur suddenly as hazard load increases. Typically, these are classed as brittle structural failures, failures arising from interaction effects, or the onset of sudden SSC functional failures. This can be achieved with good design practice. For example, the civil structures are designed to be linear elastic, but in principle non-linearity is allowable if it occurs slowly and predictably, so that loss of safety function (containment, support etc.) can be maintained to an event significantly higher than DBE.

SUMMARY

The Fukushima accident prompted rapid development in the appreciation and codification of BDB methodology into regulatory guidance and this is still continuing, especially at IAEA, which has recently published several new standards documents directly relevant to BDB analysis. This paper provided a state-of-art review on how BDB evaluations are undertaken in the UK nuclear industry. Then, using the work undertaken for the Generic Design Assessment (GDA) in the UK for UK HPR1000, this paper proposed a more systematic approach for “cliff-edge” evaluation based on a generic nuclear power plant design currently being developed in the UK.

REFERENCES

GNSL (2020), *Pre-Construction Safety Report, HPR/GDA/PCSR/0016, Rev 001*.
IAEA (2021a), *Design of Nuclear Installations Against External Events Excluding Earthquake, SSG-68*
IAEA (2021b), *Seismic Design for Nuclear installations, SSG-67*
ONR (2018), *NS-TAST-GD-013 Revision 7 - Nuclear Safety Technical Assessment Guide*
ONR (2020), *Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Revision 1 (January 2020)*
ONR (2022), https://www.onr.org.uk/new-reactors/uk-hpr1000/dac-soda.htm
WENRA (2016), *Issue T: Natural Hazards Guidance on External Flooding, WENRA, October 2016.*