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

The Application of Risk Informed Design and Risk Informed Regulation to the External Hazards Design of Nuclear Facilities

Peter Ford[1]

[1] Director, Ford Nuclear Services Ltd, Broughton-in-Furness, UK (pford_fnsl@aol.com)

ABSTRACT

The traditional deterministic design of new nuclear power plants is increasingly augmented by probabilistic safety analysis (PSA) to optimise the design, making it a risk informed design process. The need for a risk balanced design is now recognised internationally.

This paper presents a risk model for application to natural external hazards, based on development work by others, particularly workers in the US nuclear industry e.g. NRC (2007), but is developed here with application to the UK nuclear regulatory regime in mind. Nuclear regulation in the UK is risk informed by legal statute and this requirement is promulgated at a principles level, ONR (2020), by the introduction of a number of numerical risk targets that collectively provide risk informed performance targets that a nuclear facility should meet. The principles in ONR (2020) are supplemented by a large number of Technical Assessment Guides (TAGs) and the one relevant to external hazards is TAG 13, ONR (2018).

TAG 13 categorises external hazards as *discrete* if they are defined in terms of one or more hazard severity/frequency data pairs, or *non-discrete* if they are defined in terms of a hazard curve[1]. The major natural hazards such as seismicity, extreme weather hazards and flooding hazards are all defined in terms of hazard curves, and this presents a problem to the application of traditional fault analysis because of the mathematical complexity of dealing with the continuous nature of non-discrete hazard definitions.

This work is developed with seismic hazard in mind. However, we take the view that, at a principles level, this technology is equally applicable to all non-discrete hazards. However, given this historical context, the presentation here is couched in terms that are seismic hazard related.

HAZARD, FRAGILITY, CONSEQUENCE (HFC) RISK MODEL

The basic risk model forming the backbone of the methodology described here is the hazard, fragility, consequence, or HFC model. These terms have been subject to various definitions over the years, but the definitions used here are as follows:

Hazard: External challenge to nuclear plant safety.

Fragility: Nuclear plant level response to the external challenge in respect of its ability to resist consequential effects arising to risk groups[2].

Consequences: The harm arising from plant failure to the external challenge, normally expressed as dose uptake to specific risk groups.

The HFC risk model for external hazards is derived from those models used to describe nuclear plant response to internal plant faults. For internal plant faults a random plant failure leads by itself or

[1] See ONR (2020) paras. 232 & 233 for definitions of discrete and non-discrete hazards.
[2] Risk groups are those human and/or environmental groups/actors for whom risk metrics have been defined.

via a series of subsequent failures (a fault sequence), to a possible release of nuclear material or radiation shine to the environment. This random failure is connected to a known single or small number of possible releases known as source terms, and it is these source terms that present the consequential effects to risk groups. The risk to each group must meet various regulatory risk targets; in the UK these are mostly cast in terms of annualised frequency/dose targets[3].

Since failure is postulated to be random, i.e. accidental, it is best described in probabilistic terms and therefore the implication is that the failure is considered to present a *risk* to the groups affected by the release. The most appropriate safety analysis is PSA. For use in external hazards PSA, the elements of the HFC risk model take the following or similar definitions, where a is an appropriate hazard severity metric (such as peak ground acceleration for seismic hazard):

Hazard: Annual exceedance probability of the external challenge, i.e. $H(A > a)$ in any one-year period of time.

Fragility: Plant failure probability given that the hazard $H(A > a)$ occurs. $F(a|H)$.

Consequence: Probability of fatality for dose, *D*, given that plant failure occurs as a result of the hazard. $C(D|H,F)$.

Note that to generate a risk event, the logical condition: $Risk = Hazard \cap Fragility \cap Consequence$ must occur. This relationship implies a functional risk model of the form:

$$R = H(A > a) * F(a|H) * C(D|H,F)$$

where $H(A > a)$ is the probability that the external hazard challenge *A* exceeds *a*, and where * indicates convolution if the parameters are probability distributions, or scalar multiplication otherwise.

A simple linear consequence model is assumed here of the form: $C(D) = \alpha D$, where α is a coefficient that converts radiation dose to probability of individual fatality. From SAPs para. A48 (ONR (2020)) we assume that doses D > 1Sv are fatal and from this a representative value[4] is inferred of α = 1/Sv. Therefore $C(D) = D$ for $0 \leq D \leq 1$.

For internal plant faults, the terms *H* and *F* are generally scalar values, so with the simple consequence model above, the risk is computed from:

$$R = H \cdot F \cdot D \tag{1}$$

For non-discrete external natural hazards (i.e. those defined by a hazard curve), where both hazard and fragility are described by probability distributions, we write:

$$R = [H(A > a) * F(a)] \cdot C(D) = \left(\int_0^\infty H(A > a) f(a) da \right) \cdot D \tag{2}$$

where $f(a)$ is the fragility density function: $f(a) = dF(a)/da$. The appendix summarises the hazard and fragility functions used in this paper. This convolution integral is an example of the conventional random failure model used in engineering reliability analysis applied here to the special case of an external hazard. To simplify matters, the integral term can be replaced by

$$P(\infty) = \int_0^\infty H(A > a) f(a) da \tag{3}$$

[3] A word of caution on use of the terms "frequency" and "probability". Traditionally in the UK nuclear industry the term "frequency" is used to describe both statistical analysis of data and the likelihood of plant failure and the future potential for consequential harm to risk groups. The latter two are cast as probabilistic terms here. This allows us to take advantage of various mathematical simplifications, in respect of surrogate risks and screening criteria. TAG 13 footnote 13 refers, ONR (2018).

[4] Dose consequence models are a complex topic that is beyond the scope of this paper. To apply the HFC model it is necessary to express *C*(*D*) in probabilistic terms as function of a single parameter, *D*, measured in Sv. This is the simplest model for this task.

where $P(\infty)$ is the scalar probability of failure due to the hazard challenge. The risk is now simply expressed as $R = P(\infty) \cdot D$. This is our HFC plant risk model for a single plant level fault sequence from a non-discrete external hazard. From now on we replace $H(A > a)$ by $H(a)$ for convenience. Finally, we note that eqn. (3) can be expressed in two forms[5]:

$$P(\infty) = \int_0^\infty H(a)f(a)da = \int_0^\infty h(a)F(a)da \tag{4}$$

Where hazard density function is $h(a) = -dH(a)/da$. Note that equality between these forms is only achieved when the upper limit of integration is taken to ∞.

Surrogate Risks Metrics

It is useful to examine possible simplifications to the HFC risk model. In this paper, such simplifications are termed surrogate risks and are considered legitimate if the surrogate is conservative to (i.e. overpredicts) the parent risk. This is most easily seen by examining the HFC risk model for internal plant faults, eqn. (1). Here we note that as long as the individual terms are described probabilistically so that they each can take a range of values between 0 and 1, then the following useful surrogates exist:

- $R^1 = H \cdot F$ (assumes $D = 1$), i.e. plant failure alone drives the risk, an unacceptable consequential dose *D* is guaranteed if failure occurs.
- $R^2 = H$ (assumes $F = D = 1$), i.e occurrence of the hazard alone drives the risk, failure and unacceptable consequential dose *D* always assumed to occur.
- $R^3 = D$ (assumes $H = F = 1$), i.e. plant failure is assumed to occur and the risk is driven by the consequential dose *D*.

Application of the surrogate risk concept to external hazards is more difficult because of the complex relationship between H and F. However, we can proceed by noting from eqn. (4) that $P(\infty)$ can be expressed as:

$$P(\infty) = \int_0^\infty h(a)F(a)da$$

A useful simplification is found by assuming that plant failure occurs at a defined hazard severity value, A_{FAIL} say. We refer to this as a deterministic fragility function:

$$F(a) \begin{matrix} = 0 & a < A_{FAIL} \\ = 1 & a \geq A_{FAIL} \end{matrix}$$

Therefore, we can write

$$P(\infty) = \int_0^{A_{FAIL}} h(a) \cdot 0 \cdot da + \int_{A_{FAIL}}^\infty h(a) \cdot 1 \cdot da = H(A_{FAIL})$$

If A_{FAIL} is set to zero, then $P(\infty) = H(0) = 1$.

The following surrogates to match the ones for discrete faults are thus defined:

- $R^1 = P(\infty)$, same as for discrete hazards.
- $R^2 = H(A_{FAIL})$, i.e. occurrence of the hazard alone drives the risk with failure assumed at a defined hazard level.
- $R^3 = D$, same as for discrete hazards.

Screening

Screening is routinely undertaken in PSA and allows complex problems to be simplified by concentrating the analysis only on those aspects that contribute significantly to risk. Screening is therefore a way of identifying those aspects that are insignificant in risk terms and removing these from the probabilistic analysis.

[5] This can easily be demonstrated by integration by parts, noting that $H(0) = 1$, $H(\infty) = 0$ and $F(0) = 0$, $F(\infty) = 1$.

Screening is typically employed if a fault sequence satisfies either low failure probability, or low dose potential even if failure occurs. For discrete hazards we can develop screening criteria from the surrogate risks above by defining a screening failure probability P_{SCRN}, and dose level D_{SCRN}, as follows:

- $R^1 = H \cdot F < P_{SCRN}$
- $R^2 = H < P_{SCRN}$
- $R^3 < D_{SCRN}$

For non-discrete hazards, we have:

- $R^1 = P(\infty) < P_{SCRN}$
- $R^2 = H(A_{FAIL}) < P_{SCRN}$
- $R^3 < D_{SCRN}$

In the UK, screening criteria for external hazards are developed from ONR SAP EHA.19, ONR (2020). For faults initiated by discrete hazards we can refer to ONR SAPs para. 235(a) & (b) and para. 631 and define plant failure screening criteria in terms of $P_{SCRN} = 10^{-7}/\text{yr}$.

However, ONR SAPs para. 649 advises that all fault sequences should be included that might reasonably influence the design and operation of the facility. It may therefore be reasonable to include external hazard-initiated faults below 10^{-7}/yr if risks from other faults are low by comparison, so that external hazard faults still make a significant contribution to overall facility risk[6].

The third surrogate can be invoked to enable screening on low consequences. The ONR SAPs do not specify a particular screening level in terms of dose. The use of such a criterion would need to be justified on a case-by-case basis by demonstrating that $R^3 = D_{SCRN}$ provided an insignificant risk by comparison to the risk from other hazards and fault initiators.

The criterion R^2 can be applied in a straightforward way to any discrete hazard acting as a fault initiating event. If R^2 does not apply, then R^1 can be used but reliance is then placed on the robustness of plant items. R^3 can be applied if the worst release dose to the risk group is insignificant by comparison to doses form other faults, either because of very low activity levels in the radioactive material itself, or because the stored inventory is so small or in such a form that dose uptake to risk groups is negligible.

For non-discrete faults, the equivalent screening criteria are: $P_{SCRN} = 10^{-7}/\text{yr}$ and D_{SCRN} defined as above.

The UK context generally presents risk metrics in terms of Basic Safety Limits (BSLs) and Basic Safety Objectives (BSOs). The rationale for this is as follows: nuclear plant can present a risk so long as it is assessed to be no greater than the BSL (except in exceptional cases) , in which case the plant is defined to be risk tolerable. However, the expectation is that the risk will be driven down using appropriate engineered and administrative control measures to a lower value. This lower value is the risk ALARP[7] point and varies from plant to plant depending on its context, such as age, nature of operations etc. However, a lower point is defined called the BSO, below which the regulator considers the plant is broadly acceptable. In practice, nuclear plant must at least meet the BSLs, except in exceptional circumstances, and should aim to get as close to or below the BSOs. It is the BSOs that can provide the screening criteria in the UK. However, the legal requirement in all cases is for plant operators to demonstrate that risks are ALARP and screening must not undermine this.

[6] Actually applying this principle to specific external hazards, especially non-discrete hazards, may present difficulties if defining them down to these very low probabilities of exceedance can only be achieved with large uncertainties.
[7] As Low As Reasonably Practicable

USING THE HFC MODEL TO GENERATE RISK INFORMED DESIGN BASIS EVENTS

Design basis events (DBEs) are required to develop plant designs and to assess their safety using the deterministic techniques of Design Basis Analysis (DBA). DBEs provide specific external hazard challenges (loads) to be used in the design process. In this section we explore how to take advantage of the HFC risk model to develop risk informed DBEs.

As noted above, we need to recognise both discrete and non-discrete hazards and treat them separately because of the added complexity of dealing with hazard curves associated with non-discrete hazards.

Design basis external hazards are defined in the UK based on the unmitigated consequential dose potential arising from the fault sequence for which the hazard provides an initiating event. The reason for this is that the plant is assessed initially on the basis that all safety features that can be challenged by the hazard are absent; the consequential dose released is called an unmitigated dose. The design safety features are then put in place and the plant re-assessed. If the design safety features are successful, they should reduce consequential dose releases down to very low levels, generally consistent with those from normal operations, or preferably zero. In deterministic DBA space a successful facility design subjected to DBE challenge will not have failed; in PSA space this is interpreted as a probability of failure that is very low.

ONR Numerical Target 4, ONR (2020), is the governing guidance and states that fault sequences are classed as DBA faults depending on a combination of initiating event frequency and unmitigated consequential dose. For large releases to individual members of the public > 100mSv, discrete hazards should have a design basis of 10^{-5}/yr assessed on a best estimate basis, whereas non-discrete hazards attract a design basis of 10^{-4}/yr defined on a conservative basis (refer to ONR SAPs EHA.4, FA.5 and para. 629).

Design Basis Events for Discrete Hazards

Applying the HFC model to a DBA fault sequence, we set D to the unmitigated dose D_U. The fault sequence is assumed to offer no protection, so set $F = 1$, i.e. failure state is guaranteed if the hazard event occurs. From ONR Target 4[8] we identify the BSL risk curve and from eqn. (1), we get:

$$R_{BSL} = H_{DBE} \cdot D_U \tag{5}$$

$$\therefore H_{DBE} = R_{BSL}/D_U$$

H_{DBE} is the hazard or initiating event frequency from Target 4, given the unmitigated dose D_U.[9]

For example, assuming D_U = 100mSv, from Target 4 $H_{DBE} = 10^{-5}$/yr. For the mitigated case, we can calculate the fault probability using Target 4 assuming the mitigated dose is the BSO values D_M = 0.01mSv = 10^{-5}Sv:

$$R_{BSO} = H_{DBE} \cdot D_M \tag{6}$$

The fault sequence (plant failure) probability, F, can be interpreted as $D_M/D_U = 10^{-5}/0.1 = 10^{-4}$, therefore $R_{BSO} = 10^{-5} \cdot 10^{-5} = 10^{-10}$/yr ~0. This is to be expected from a successful design against a DBE. Whether such plant designs can achieve this fully or only partially is assessed in the PSA.

Design Basis Events for Non-Discrete Hazards

Applying the HFC model to non-discrete DBA fault sequences is more complex because the hazard, H, and fragility, F, are continuous function of hazard severity.

[8] We consider only individual risk to the public in this paper, although the same approach could be applied to other risk groups.
[9] This linear relation does not recognise that Target 4 is expressed as a staircase rather than a continuous curve.

With discrete events, for the unmitigated case, we simply set $F = 1$, to provide a unique value for H from Target 4 (see TAG 13 fig. 3, ONR (2018)). But for the non-discrete case we cannot make this assumption, and a little thought will make clear why. Consider a typical non-discrete hazard event such as an earthquake or extreme wind. When hazard severity is very small ($a \to 0$) it is not credible that any failures occur, the fault sequence can be assumed not to occur. On the other hand, when the hazard is very large ($a \to \infty$) SSC failures on the fault sequence are highly likely if not certain to occur. Neither extreme is suitable as the basis for setting a DBE, but between these extremes is a point at which a DBE can be set that will satisfy the criteria for a Design Basis Event in the ONR SAPs.

We proceed as follows by making use of the deterministic fragility function defined above, in the following form:

$$F(a) \begin{matrix} = 0 & a < A_{DBE} \\ = 1 & a \geq A_{DBE} \end{matrix}$$

Making use of eqn. (2) and the second formulation in eqn. (4) gives

$$R_{BSL} = -\left(\int_{A_{DBE}}^{\infty} \frac{dH(a)}{da} \cdot da\right) \cdot D_U = H(A_{DBE}) \cdot D_U$$

which is now in the same form as the discrete case, eqn. (5).

With the unmitigated dose, D_U, specified, Target 4 immediately gives a value for $H(A_{DBE})$. Using this value, and the hazard curve, $H(a)$, it is easy to read off a value for A_{DBE}. A_{DBE} is now the DBE value for the non-discrete hazard.

The design can now proceed using RGP[10] deterministic standards with A_{DBE}. As for the discrete case, R_{BSO} can be computed from the mitigated dose, $D_M = 10^{-5}$Sv. The fault sequence failure probability can again be interpreted as the ratio $D_M/D_U = 10^{-4}$, and from eqn. (6), $R_{BSO} = 10^{-4} \cdot 10^{-5} = 10^{-9}/\text{yr} \sim 0$.

BEYOND DESIGN BASIS (BDB) EXTERNAL HAZARD CHALLENGE

Both the ONR SAPs and international guidance by IAEA (2016) and WENRA (2014) anticipate a need for a nuclear facility to remain demonstrably safe beyond the external hazard design basis challenge level. Traditionally this is considered in two ways: a margin analysis to demonstrate that the facility does not suffer a significant failure (cliff edge) just beyond the design basis level, and the potential for severe accidents from even larger (more remote) events. WENRA capture this in terms of DEC A and DEC B levels[11].

We can use the HFC risk model to investigate BDB cliff edge response in several ways (severe accidents are considered in the next section):

- In probability space we can investigate the BDB response at a lower hazard exceedance probability (higher severity) than the design basis, e.g. 10^{-5}/yr.
- In terms of hazard severity, we can examine the point at which a BDB cliff edge response could start. This can be examined in terms of a proportional increase in the DBE level, say 50%, 100%, i.e. $A_{BDB} = 1.5A_{DBE}$ or $A_{BDB} = 2A_{DBE}$, where A_{BDB} is the beyond design basis hazard challenge. This increase can be termed a margin. In this case the margins are 1.5 and 2 respectively.

The presumption is that at the Beyond Design Basis (BDB) event level, however it is defined, there is a high probability that significant failure will not have occurred, and the facility will remain

[10] Relevant Good Practice (RGP) is UK terminology for those codes and standards relevant to the design/assessment of nuclear plant and the type of faults to which it is subject.
[11] Design Exceedance Condition (DEC) A equates to the BDB cliff edge level and DEC B to a severe accident event.

substantially in its design basis condition. In deterministic DBA space the facility will not have failed; in PSA space this is interpreted as a probability of failure higher than the design basis but still low in absolute terms.

Using the HFC model we set (somewhat arbitrarily as an example) the following criteria for DB and BDB plant performance:

- Assume that at the DB event level, the plant fragility is $F(A_{DBE}) = 10^{-3}$, since if this was a discrete hazard, from eqn. (1) this would be the required probability of conditional failure required to just meet the Target 8 BSO risk of $R_{BSO} = 10^{-7}$/yr, with $H(A_{DBE}) = 10^{-4}$/yr.
- Assume that at the BDB event level, $A_{BDB} = a_m$ therefore $F(A_{BDB}) = F(a_m) = 0.5$.

We will contrast this with a more traditional approach that sets $F(A_{DBE}) = 10^{-2}$, in which case A_{DBE} is the HCLPF value (see appendix), and $A_{BDB} = a_m$ as before.

To examine the effect of setting these criteria in risk terms consider the following test cases and compute the resulting risks using the hazard and fragility functions summarised in App. 1.

- The BDB event level is set at a hazard exceedance probability of 10^{-5}/yr.
- The BDB event level is set at $A_{BDB} = 1.5A_{DBE}$.
- The BDB event level is set at $A_{BDB} = 2A_{DBE}$.

The following illustrative tests are defined. The results are collected in Tables 1and 2.

BDB event is set at $A_{BDB} = 1.5A_{DBE}$

Test 1: A_{DBE} = 0.25g, A_{BDB} = 0.375g, $F(A_{DBE}) = 10^{-2}, F(A_{BDB}) = 0.5, H(A_{DBE}) = 10^{-4}$/yr

This test has A_{DBE} set to the HCLPF value and $a_m = A_{BDB}$, $H(A_{BDB}) = 1.8 \cdot 10^{-5}$/yr.

The standard deviation can easily be calculated as $\beta = 0.174$.

Noting that the unmitigated dose $D_U = 1$, we can make use of the surrogate $R^1 = P(\infty)$ and therefore eqn. (4) to calculate the risk, which for this test is $P(\infty) = 2.4 \cdot 10^{-5}$/yr.

For high hazard plant such as the one assumed here, USNRC and USDOE standards anticipate a performance target of 10^{-5}/yr for facility failure, and this fragility definition approximately meets this target.

Test 2: A_{DBE} = 0.25g, A_{BDB} = 0.375g, $F(A_{DBE}) = 10^{-3}, F(A_{BDB}) = 10^{-2}, H(A_{DBE}) = 10^{-4}$/yr, $a_m = A_{BDB}$, $H(A_{BDB}) = 1.8 \cdot 10^{-5}$/yr.

The standard deviation is found to be $\beta = 0.131$. The risk now calculates as $P(\infty) = 2.2 \cdot 10^{-5}$/yr.

BDB event is set at $A_{BDB} = 2A_{DBE}$

Test 3: A_{DBE} = 0.25g, A_{BDB} = 0.5g, $F(A_{DBE}) = 10^{-2}, F(A_{BDB}) = 0.5, H(A_{DBE}) = 10^{-4}$/yr.

This is a variation on Test 1 with A_{DBE} set to the HCLPF value and $a_m = A_{BDB}$, but with an enhanced BDB margin. $H(A_{BDB}) = 4.7 \cdot 10^{-6}$/yr and $\beta = 0.297$.

In this case the risk is $P(\infty) = 1.1 \cdot 10^{-5}$/yr.

Test 4: A_{DBE} = 0.25g, A_{BDB} = 0.5g, $F(A_{DBE}) = 10^{-3}, F(A_{BDB}) = 10^{-2}, H(A_{DBE}) = 10^{-4}$/yr.

This is a variation of Test 2 for the enhanced BDB margin. $\beta = 0.224$ and the risk is $P(\infty) = 0.8 \cdot 10^{-5}$/yr.

BDB event is set at $H(A_{BDB}) = 10^{-5}$/yr

Test 5: A_{DBE} = 0.25, $F(A_{DBE}) = 10^{-2}, F(A_{BDB}) = 0.5, H(A_{DBE}) = 10^{-4}$/yr.

With $H(A_{BDB}) = 10^{-5}$/yr, from the hazard curve A_{BDB} = 0.426g.

Set the design basis as the HCLPF value, $F(A_{DBE}) = 10^{-2}$, keep the BDB level at the median acceleration and recalculate to find $\beta = 0.229$ and $P(\infty) = 1.7 \cdot 10^{-5}$/yr.

Test 6: A_{DBE} = 0.25, $F(A_{DBE}) = 10^{-3}, F(A_{BDB}) = 0.5, H(A_{DBE}) = 10^{-4}$/yr, $H(A_{BDB}) = 10^{-5}$/yr

In this case $\beta = 0.172$ and the risk is $P(\infty) = 1.4 \cdot 10^{-5}$/yr.

SEVERE NATURAL HAZARD EVENTS

The previous section covered BDB events that according to WENRA meet the requirements of DEC A. In this section we investigate use of the HFC risk model for DEC B events, or those that could constitute a severe accident. One way to do this would be to explicitly recognise the residual risk captured by the severe accident portion of the probability of plant failure risk curve. This can be calculated from eqn. (4) as:

$$P(\infty) = P(A_{BDB}) + P_{SA} = \int_0^{A_{BDB}} H(a)f(a)da + \int_{A_{BDB}}^{\infty} H(a)f(a)da \tag{7}$$

SA stands for "Severe Accident". $P(A_{BDB})$ is the risk accrued to the Beyond Design Basis event level. However, when we do this, the proportion of risk associated with severe accidents, P_{SA}, is relatively low. In other words, most of the plant failure risk is accrued up to the beyond design basis level, because the hazard exceedance probability values beyond this level become increasingly small.

This is a somewhat counter-intuitive result, since the expectation is that risk to the BDB level is low by design and increases significantly only for hazard levels beyond this. The reason for this that it is assumed that upon failure the entire unmitigated dose is released, even if failure occurs below the BDB event level. This is considered unrealistic, so here we assume that dose release up to the BDB level is relatively small and increases to unmitigated levels only in the severe accident region.

For consequential doses $D \neq D_U$

Noting that the risk scales linearly with dose in our simple consequence model, we can assume a lower release dose, say 1mSv, up to the BDB level, and D_U = 1Sv at the severe accident level. From eqn. (2) we can write immediately:

$$R_{BDB} = P(A_{BDB}) \cdot D = \left(\int_0^{A_{BDB}} H(a)f(a)da \right) \cdot 10^{-3}$$

$$R_{SA} = P_{SA} \cdot D_U = \left(\int_{A_{BDB}}^{\infty} H(a)f(a)da \right) \cdot 1$$

The results for R_{BDB} and R_{SA} for each of the seven tests in the last section are given in Table 3 and show that the contribution to risk up to the BDB event level is either low or trivial by comparison to the contribution above that level. This is intuitively correct.

Note that for $D = D_U = 1$, $R_\infty = P(\infty)$.

CONCLUDING COMMENTS

This paper introduces the HFC risk model. This is a model that has been used implicitly and reported extensively in the nuclear literature. The application here introduces the notions of surrogate risks and a function called in this paper a deterministic fragility function, i.e. one that postulates plant failure at a given hazard value. With these devices and with the aid of a very simple dose consequence model, an approach is described to develop risk informed Design Basis Events for external hazards, i.e. those defined by hazard curves (in the UK these are called non-discrete hazards).

The analysis is extended to Beyond Design Basis analysis and a simple application to severe accident analysis is also introduced. This theoretical analysis is illustrated by a small number of numerical tests using a simple analytical seismic hazard curve, a lognormal factor of safety fragility function and a simple dose consequence model.

REFERENCES

IAEA (2016), "Safety of Nuclear Power Plants: Design". *SSR-2/1 (Rev. 1)*.
NRC (2007), "Evaluation of the Seismic Design Criteria for Structures, Systems and Components in Nuclear Facilities". *NUREG/CR-6926*. US.
ONR (2020), "Safety Assessment Principles for Nuclear Facilities", *2014 Edition, Rev. 1*. UK.
ONR (2018), "External Hazards". *NS-TAST-GD-013 Revision 8*. UK.
WENRA (2014), "Safety Reference Levels for Existing Reactors". *Reactor Harmonisation Working Group*.

Table 1: Fragility parameters used or calculated for each test

Test	A_{DBE}	A_{BDB}	$A_{0.1\%}$	$A_{1\%}$	a_m	β
1	**0.25**	**0.375**	0.219	0.25	0.375	0.174
2	**0.25**	**0.375**	0.25	0.276	0.375	0.131
3	**0.25**	**0.5**	0.199	0.25	0.5	0.297
4	**0.25**	**0.5**	0.25	0.296	0.5	0.224
5	**0.25**	0.426	0.21	**0.25**	0.426	0.229
6	**0.25**	0.426	**0.25**	0.285	0.426	0.172

Table 2: Hazard, fragility and risk values used or calculated for each test

Test	$F(A_{DBE})$	$F(A_{BDB})$	$H(A_{DBE})$	$H(A_{BDB})$	$H(a_m)$	$P(\infty)$
1	$\mathbf{10^{-2}}$	**0.5**	$\mathbf{10^{-4}}$	$1.8\cdot10^{-5}$	$1.8\cdot10^{-5}$	$2.4\cdot10^{-5}$
2	$\mathbf{10^{-3}}$	$\mathbf{10^{-2}}$	$\mathbf{10^{-4}}$	$1.8\cdot10^{-5}$	$1.8\cdot10^{-5}$	$2.2\cdot10^{-5}$
3	$\mathbf{10^{-2}}$	**0.5**	$\mathbf{10^{-4}}$	$4.7\cdot10^{-6}$	$4.7\cdot10^{-6}$	$1.1\cdot10^{-5}$
4	$\mathbf{10^{-3}}$	**0.5**	$\mathbf{10^{-4}}$	$4.7\cdot10^{-6}$	$4.7\cdot10^{-6}$	$0.8\cdot10^{-5}$
5	$\mathbf{10^{-2}}$	**0.5**	$\mathbf{10^{-4}}$	$\mathbf{10^{-5}}$	$\mathbf{10^{-5}}$	$1.7\cdot10^{-5}$
6	$\mathbf{10^{-3}}$	**0.5**	$\mathbf{10^{-4}}$	$\mathbf{10^{-5}}$	$\mathbf{10^{-5}}$	$1.4\cdot10^{-5}$

Table 3: Tests re-run assuming 1mSv dose up to BDB level and 1Sv dose up to severe accident level

Test	$P(A_{BDB})$	$P(\infty)$	R_{BDB}	R_{SA}	R_∞
1	$1.9\cdot10^{-5}$	$2.4\cdot10^{-5}$	$1.9\cdot10^{-8}$	$5.3\cdot10^{-6}$	$2.4\cdot10^{-5}$
2	$1.5\cdot10^{-5}$	$2.2\cdot10^{-5}$	$1.5\cdot10^{-8}$	$5.9\cdot10^{-6}$	$2.1\cdot10^{-5}$
3	$1.0\cdot10^{-5}$	$1.1\cdot10^{-5}$	$1.0\cdot10^{-8}$	$9.6\cdot10^{-7}$	$1.1\cdot10^{-5}$
4	$0.7\cdot10^{-5}$	$0.8\cdot10^{-5}$	$6.8\cdot10^{-9}$	$1.1\cdot10^{-6}$	$8.0\cdot10^{-6}$
5	$1.4\cdot10^{-5}$	$1.7\cdot10^{-5}$	$1.4\cdot10^{-8}$	$2.5\cdot10^{-6}$	$1.7\cdot10^{-5}$
6	$1.1\cdot10^{-5}$	$1.4\cdot10^{-5}$	$1.1\cdot10^{-8}$	$2.9\cdot10^{-6}$	$1.4\cdot10^{-5}$

Notes for Tables
Values in bold are inputs to the calculations
Units: acceleration values in (g), probability values for *F* (/demand), for *H*, *P* and *R* (/yr)

APPENDIX

Seismic hazard curve: Seismic hazard is a complex phenomenon that is difficult to capture as a simple mathematical form suitable for use in the HFC risk model, however a typical representative mean seismic hazard curve for a notional "high seismicity" UK site has been used for the calculations in this paper and is shown in fig. 1. An algebraic form has been used to model this curve and calibrated to give $H(0.25) = 10^{-4}$/yr and $H(1.0) \sim 10^{-7}$/yr.

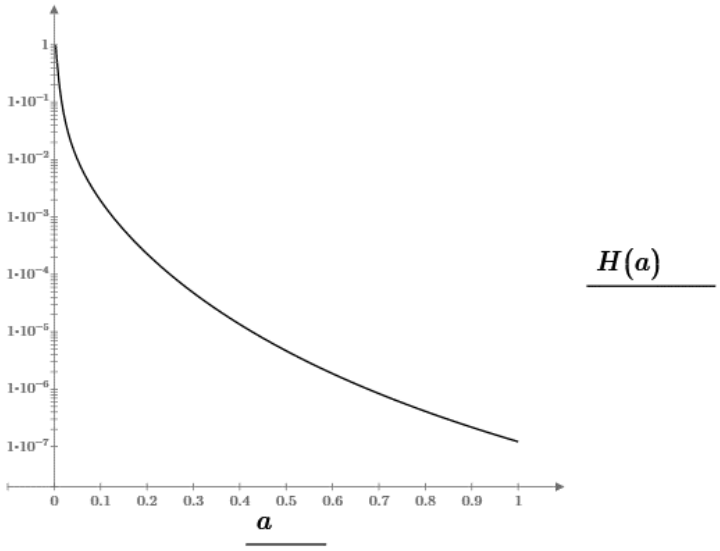

Figure 1: Seismic hazard curve used for calculation purposes. It is intended to represent a mean curve

Factor of Safety Fragility Function: The fragility function used here is the conventional factor of safety function developed by Kennedy and others, see NRC (2007). We use the from defined by just two parameters, median acceleration and logarithmic standard deviation. This later is a composite of the more complex form in which the fragility is expressed in terms of two standard deviation parameters. Whilst there is value in this more complex form, it is much more difficult to handle analytically, and its use would tend to obscure the inner working of the HFC risk model.

Given a median acceleration value a_m and a log. standard deviation value β, a fault sequence fragility curve can be computed from the following equation: $F(a) = \Phi[\ln(a/a_m)/\beta]$, where Φ is the standard normal probability distribution. This is the cumulative version of the lognormal probability distribution density function.

Although it is conventional to define the fragility function in terms of median acceleration, any other fixed point of the fragility curve can be used. We will have need of two special points defined as follows: The High Confidence of Low Probability of Failure (HCLPF) acceleration defined at the 1% failure point: $F(a_{1\%}) = 10^{-2}$, where $a_{1\%} = a_m \mathrm{e}^{-2.33\beta}$. And a lower acceleration defined at the 0.1% failure point: $F(a_{0.1\%}) = 10^{-3}$, $a_{0.1\%} = a_m \mathrm{e}^{-3.09\beta}$.