SECED 2023 Conference
Earthquake Engineering & Dynamics for a Sustainable Future
14-15 September 2023, Cambridge, UK

THE DEVELOPMENT OF EXTERNAL HAZARDS IN THE UK NUCLEAR INDUSTRY AND WHAT THE FUTURE MIGHT HOLD- A PERSONAL VIEW

Peter FORD[1]

Abstract: *The development of external hazards in the UK nuclear industry, as in the rest of the world, has not been linear and straightforward. In the 1950s and '60s, the term "external hazards" had not been coined and the approach of those pioneering nuclear engineers was similar to how they would treat any other major construction project. Some, now very familiar hazards, such as aircraft crash and seismic strong ground motion, were not considered at all. This paper will briefly chart that history, then propose a possible future direction in terms of adopting the quantitative performance goal approach to risk informed design. It will show how the UK's risk-informed, nonprescriptive regulatory framework is well suited to a risk-informed design approach.*

External hazards

The most important feature that distinguishes external hazards from all other types of fault initiator is captured by the hierarchy of safety principle, namely that the site operator has very little if any control over the timing, frequency, and severity of external hazard events that may affect its site. The hierarchy of safety has been expressed in many ways, but (at least in the UK) expects that site/plant operators control the risk first and foremost by limiting the hazard at source. This is the most important element of the hierarchy, and the one to which plant operators should attend before any mitigation or protection measures are introduced. Yet, for external hazards, protection and mitigation, either engineered or administrative, are the only measures the plant operator can employ to limit risks to SSCs and personnel on an existing site[2].

We can characterise the essential features of external hazards in a useful way, where we categorise natural hazards and human-induced hazards separately:

Natural hazards

- Stochastic uncertainty: Modelling such uncertainty can dominate the development of design parameters.
- Physical complexity: All natural hazards reflect a complex underlying process for which the hazard in question is just one representation of a larger physical system.
- Energy release: Massively energetic regionally. Distance from source provides only limited protection.
- Geometric spreading of event effects: Energy transfer is generally diffuse and nondirectional, significant attenuation with distance from source occurs, but events can be sufficiently energetic to affect large geographical regions.
- Combinations: For some hazards (e.g., weather related ones) significant opportunity for combinations occur.

Human induced hazards

- Stochastic uncertainty: Most parameters knowable in principle (man-made) or can be bounded relatively easily.

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

[2] This feature applies to existing sites, but not necessarily to all external hazards for new sites, since judicious site selection can mitigate the effects of or even the possible occurrence of some external hazards. The classic example is that coastal flooding is not possible at sites removed from coastal influence. Seismic hazard however always applies; no part of the UK is immune from this hazard.

- Physical complexity: Mostly relatively simple underlying processes, or ones that can be modelled relatively easily.
- Energy release: Relatively low levels of energy release on a regional scale, can be highly energetic locally. Main protection is distance.
- Geometric spread of event effects: Energy release can be non-directional (offsite explosion) and focussed (aircraft & vehicle crash).
- Combinations: Unlikely to combine with other human-induced hazards except by random chance.

The most researched and developed external hazard is that of seismic strong ground motion and its effects on SSCs. This development has progressed to the point where the expectation from the regulator is for a very significant analysis of both the hazard itself and its effect on SSCs. And yet the UK resides in a tectonic region of low seismicity. This juxtaposition of low hazard and significant design/analysis costs is a conundrum that the industry has tried with mixed success to grapple with.

In the author's opinion, this conundrum derives from a number of historical threads that together create an environment that has tended to increase the analysis burden, rather than reduce it. The traditional engineering design process is heavily deterministic, and code based. This assumes that the loads to be designed against are amenable to rational deterministic analysis. In the case of seismic hazard, this is not true, and to a lesser extent the same applies to other natural hazards. Seismic hazard and the way the earthquake process works is well understood in a qualitative sense, but in a tectonic region like the UK, where there is as yet no known association between a recorded event and a causative fault, a deterministic analysis of the local geology to yield representative seismically induced loads is simply not possible. Instead, the hazard must be characterised probabilistically based mostly on historical events known only from social historical accounts. The degree of uncertainty is large, and the natural impulse of engineers is to introduce conservatism in both the assumed design loads, and through the analyses that predict the SSC response. The net effect is an analysis that is very conservative, costly, and almost certainly unrepresentative of actual SSC response in a real design basis event. But on the plus side, the SSC is very unlikely to fail!

One development that has not been pursued with much vigour in the UK is the notion of quantitative performance goal analysis as support to a risk-informed design process. Whilst (as will be shown in this paper) the UK regulatory context is ideally suited to such an approach, its development has been muted by reliance on the traditional deterministic design process. The author's opinion is that while this persists, the conundrum of low seismicity and significant design costs will remain, with licensee and regulator endlessly arguing over the analysis methodology or design code application. Such arguments miss the point. Without addressing the underlying philosophical problem of highly uncertain hazard loads, being used as input to a largely traditional deterministic SSC analysis, the conundrum of costly designs is unlikely to be resolved.

This paper presents an approach to quantitative performance goal analysis as a support to riskinformed design and concludes that this type of analysis provides a possible way forward for the future development of assessing external hazards analysis in the UK nuclear industry.

Historical development of external hazards as a discipline

The development of external hazards as a discipline has been very heavily influenced by world events such as major floods, earthquakes, terrorist attacks and nuclear accidents. These events have shaped this development, both its direction and urgency. A selection of these events is presented below with a brief summary of their significance in safety terms:

Three Mile Island (1979): This accident needs no introduction to a nuclear audience. It was not caused by an external hazard, but the implication and learning from the event provided a watershed in nuclear safety analysis and led to a significant R&D programme into external hazards in the US through the USNRC IPEEE program, USNRC (1991).The origins of much of the seismic hazard approach (SSHAC), the SSC analysis using experience data and seismic margins analysis can be traced back to the IPEEE program.

Pan AM Flight 103 (1988): A terrorist bomb exploded causing the plane to crash near Lockerbie, Scotland. This promoted consideration of aircraft crash risk onto nuclear sites. Research into accidental aircraft crash has been undertaken in several countries and in the UK had been

ongoing for some time before this event, mostly by the UKAEA, see Byrne (1997), but there is no doubt that this event galvanised interest in this hazard.

La Blaiyais NPP site (1999): Flooding occurred at this French river estuary site through a combination of high tide, wind driven waves and storm surge. This led to floodwater spreading onto the nuclear island and damage to SSCs at low level. The flood height was above the design basis flood level and overtopped the flood defence. Although some SSCs were lost, alternative systems brought the affected reactors to safe shutdown.

Kashiwazaki-Kariwa NPP site (2007): This is one of the largest multi reactor sites in the world. It was hit by a shallow 6.6 moment magnitude earthquake. Motions at the site were recorded as significantly above design basis levels. Nevertheless, all reactors were shut down safely and on inspection it was found that there were no significant failures of safety related SSCs, IAEA, (2008).

Fukushima Daiichi NPP site (2011): The site was subjected to a very large moment magnitude 9.0 Tohoku earthquake event. Seismic motions on site exceeded the design basis and caused a Loss Of Offsite Power (LOOP) fault, but back-up electrical supplies started as expected and there was no damage to nuclear safety SSCs from the earthquake itself. Shortly after the earthquake a large tsunami affected the site, breaching flood protection and swamping three of the four reactors on site, for further details see IAEA (2014) and ONR (2011). Unfortunately, the back-up electrical equipment was mostly located in basement areas and failed when it became flooded. It was this that led to the loss of ability to cool the reactors and subsequently to the release of radioactive material, The flood event exceeded the design basis, and there was too little margin beyond the design basis to protect against this event.

Fort Calhoun NPP site (2011): This NPP site is situated on the Missouri river which suffered an extraordinary rise in water level during a prolonged extreme weather event. River levels exceeded the design basis and the site had to be protected by temporary barriers. The reactor was shut down for re-fuelling at the time and there was no damage to safety related equipment. Information taken from Wikipedia, (2023),

Two things are notable from a review of these events:

- An appropriately defined design basis is critically important to ensure safety. In all the flooding examples just noted, the initial design basis contained insufficient margin to account for the uncertainty in the hazard. This shows the importance of using rigorous and robust external hazards analysis to underpin design bases and recognising the importance of beyond design basis and cliff edge capability.
- Implementing a conservative design process is an excellent way to ensure safety. In the seismic related examples, it is clear that the safety systems performed well and exceeded their stated design withstand capability by a substantial margin.

The development of external hazards analysis in the UK nuclear industry rested very much on the developments worldwide that were gradually absorbed into IAEA and WENRA guidance.

The only significant departure from worldwide practise that the author is aware of, in addition to the aircraft crash example already cited, was the early development of a bespoke probabilistic seismic hazard analysis methodology by a group of subject matter experts collectively known as the Seismic Hazard Working Party (SHWP). This was done for the CEGB to service a significant PWR new build programme and started in the late 1970s. Unfortunately, the SHWP's (in many ways) ground-breaking R&D work was curtailed in the early 1990s, once the Sizewell B reactor had been designed and no more PWR's were planned. Moreover, the work was never properly published so has remained unavailable to a wider non-UK audience and unable to influence e.g., IAEA guidance[3]. Today, the SHWP methods have been eclipsed by more recent PHSA work in the US, reported most recently in USNRC (2021). In the author's opinion, the SHWP work represented best practise at the time and was arguably ahead of equivalent work in the US. Disbanding the SHWP and failing to fully publish its work has left the international community impoverished, most notably in the way social historical records are used in the UK to augment sparse instrumental seismic data. In this the UK, through the approach pioneered by the SHWP, was and almost certainly remains, the best in the world.

[3] The most comprehensive account of SHWP work is in TAG 13, Annex 1, App. A, ONR, (2018) & Mallard, (2003).

The UK nuclear regulatory approach

As noted elsewhere, there is interest in moving the analysis of external hazards towards a more risk informed basis. The regulatory approach in the UK is uniquely positioned to take advantage of this development because it is inherently risk informed by legal statute, and the non-prescriptive nature of the regulatory process applied to safety analyses provides nuclear licensees or operators in the UK with the flexibility to explore both the opportunities and constraints presented by such developments.

A summary of the ONR's risk informed regulatory process as it applies to external hazards has been presented in a recent paper by Ford (2022a). A number of aspects are worth highlighting here for the purposes of this paper:

- The risk informed process is captured quantitatively by a set of ONR Numerical Targets, ONR (2020a), that nuclear plant on licensed nuclear sites should meet.
- Numerical Targets capture the range of acceptable (or tolerable) dose/frequency values, with the added requirement that the actual risk for any plant should be driven down by means of engineered and administrative controls to the point where the risk is *As Low As Reasonably Practicable* (ALARP). This is the risk ALARP point and varies from plant to plant given factors such as age, lifecycle stage, radioactive inventory and the nature of the operations taking place. The risk ALARP point is defined as the point where the effort required to implement further risk reduction through additional measures is grossly disproportionate to the risk averted.
- Safety analyses typically fall into three categories ○ *Deterministic safety analysis or design basis analysis*: A rigorous analysis of the faults against which the plant is designed. The intent is to show that the plant design adheres to appropriate codes and standards collectively termed Relevant Good Practice (RGP).
  ○ *Probabilistic safety analysis*: An analysis of the entire spectrum of faults to which the plant might be subject, extending beyond just design basis faults. The PSA should demonstrate that the Numerical Targets are met and that risks are ALARP. ○ *Severe accident analysis*: A scenario-based analysis intended to show how plant failures leading to significant release of radioactivity can be mitigated. The IAEA has recently introduced a concept to be observed by new designs of the Practical Elimination of severe accident consequences, IAEA (2016). This idea is now promulgated in ONR guidance, ONR (2020a) paras. 611 & 666.

It is a basic assumption in the UK that if the Licensee has properly selected and adhered to RGP during the design process and implemented good design principles, including the IAEA's defencein-depth principle, IAEA (1996), then it is likely that the plant and its operations will be risk ALARP, see ONR (2020a) para. 11.

One of the most important aspects of good practice is the selection of a design basis to characterise each external hazard for the purposes of providing hazard load input to the design process and deterministic safety analysis. For natural hazards RGP anticipates design bases at or conservative to the 10^{-4}/yr point on the mean hazard curve; for human-induced external hazards a best estimate 10^{-5}/yr value is considered more appropriate – see ONR (2020a) SAPs EHA.4 & FA.5. ONR has recently published research on the rationale for using a conservative 10^{4}/yr hazard level as the design basis, see ONR (2020b). This research concludes that while there is no well-defined rationale for this criterion, it is consistent with international practice.

Development of a risk informed approach

An argument is made in this paper that the traditional deterministic design process applied to external hazards has led to the use of excessive conservatism in order to demonstrate that designs that are adequately safe. There has been growing recognition both by industry and regulators that the traditional deterministic design basis approach, which is heavily code based and prescriptive, should move to a more performance-based approach, in which the objective of any safety analysis is to demonstrate that the nuclear plant (almost always an NPP) meets certain performance goals; see USNRC (2007a), USNRC (2007b) and IAEA (2021). These performance goals can be expressed either in plant performance terms, e.g., ability to maintain a safety

[4] The IAEA is currently engaged in a project to develop the idea of "design robustness" and is expected to link this to the related concepts of risk informed design, performance goals and the adequacy of beyond design basis margins.

function, such as containment, or in risk terms, e.g., the ability to limit the consequences of failure to certain numerical target values of dose/frequency to specified human risk groups[4].

The only published risk-informed approach for nuclear design this author is aware of is in the US and forms a connected set of R&D into the (primarily) seismic design of nuclear facilities. The intent is to provide a graded approach to design factors of safety depending on the site hazard and the unmitigated dose potential of the facility. This work was developed in the 1980s and early 1990s as a joint USDOE/USNRC project, see Ford (2022a), and has spawned a number of important documents that describe the approach for both USDOE facilities and US reactor plant, USDOE (2016), USDOE (2017), ASCE 43-05, USNRC (2007a), USNRC (2007b).

ASCE 43-05 is applicable to seismic hazard only, however the USDOE standard, USDOE (2016), has been adapted from ASCE 43-05 and extends it to other natural external hazards[5] including flooding, extreme wind and precipitation. The method starts by assigning each safety System, Structure and Component (SSC) to a target performance goal known as a NPH Design Category (NDC) based primarily on the unmitigated dose arising from failure.

In this paper we adapt the basic philosophy expressed in these documents but pursue a different implementation that takes advantage of the way UK regulatory guidance is constructed.

We start with an expression for the probability of plant failure $P(\infty)$, eqn. (7) from the appendix. To solve this equation, we take advantage of an analytical solution put forward originally by Kennedy and used in USNRC (2007b). It works with the first formulation of eqn. (7) by assuming a power law approximation for the hazard curve *H*(*a*):

$$H(a) = h_0 \cdot a^{-n} \tag{1}$$

Where h_0 and n are constants matched to the local site seismicity[6]. Substituting into eqn. (7) along with the standard composite uncertainty lognormal fragility function yields the following solution:

$$P(\infty) = H(a_m) \cdot \exp(n^2\beta^2/2) \tag{2}$$

Where a_m = median fragility function hazard severity

β = fragility function log standard deviation.

This analytical formulation is used to derive, under various assumptions including use of the HCLPF fragility assumption[6], a set of design factors for use with relevant US codes, such that plant and equipment designed to these factors will offer the same probability of failure under seismic loading.

We investigate a different approach here by noting that eqn. (2) can be used to derive the fragility parameters for a plant level design basis fault sequence as follows. Eqn. (8) from the appendix makes use of ONR's Target 4 to compute the BSL risk based on unmitigated dose release as:

$$R_{BSL} = H(A_{DBE}) \cdot D_U$$

Assuming that (in probability space) the BSO risk level is achieved by the design, then using the solution (2) and substituting into eqn. (5) gives

$$R_{BSO} = P(\infty) \cdot D_U = H(a_m) \cdot \exp(n^2\beta^2/2) \cdot D_U$$

We can now estimate the fault sequence fragility parameters by forming the ratio R_{BSL}/R_{BSO} and solving for the fragility median acceleration, a_m. Since A_{DBE} is pre-defined and β is typically based on plant specific features alone (usually a value in the range 0.3-0.6), a unique value for a_m can be computed:

$$R_{BSL} \qquad n2\beta2 \quad \frac{1}{n}$$

[5] The US nuclear industry refers to natural external hazards as natural phenomena hazards (NPH). [6] This is a simplification of the actual hazard curve and is intended to operate with reasonable accuracy over a range of +/- a factor of 10 in frequency terms around the design basis hazard level. Its use here exceeds this constraint and is presented as an illustration of what can be achieved in principle, rather than a fully developed methodology.

[6] High Confidence Low Probability of Failure (HCLPF) is the 1% failure point on the standard composite lognormal fragility function described by parameters a_m and β.

$$a_m = A_{DBE}\left[\left(\frac{}{R_{BSO}}\right)\exp\left(\frac{}{2}\right)\right] \quad (3)$$

a_m and β fully define the lognormal fragility function needed to show that the plant designed to A_{DBE} will meet the target risk value, R_{BSO}.

Conclusions – a possible future

The understanding and analysis of external hazards should be considered mature but still developing. It is mature because, for the most important hazards, there is now extensive knowledge and experience with designing nuclear plant against them. But developing because natural hazards especially are subject to significant uncertainty that militates against precise calculation and confident prediction. This is why moving to a more risk-informed design process, where those uncertainties can be more readily modelled probabilistically, should provide an avenue to reduce conservatism and cost.

Seismic hazard has clearly been subject to the most extensive R&D in the nuclear industry worldwide, and the high quality of existing designs is evidenced by the robust performance of NPPs during earthquakes. However, the evidence for other natural hazards has not been so complementary, with clear failure to recognise the severity of extreme flood hazard events in particular.

In the authors view, an ideal future would see the analysis of all natural hazards placed on a similar footing commensurate with their likely risk contribution prior to protection measures being put in place. This does not mean the amount of analysis has to be the same, but the aim should be that the quality of the analysis is similar. Seismic hazard will probably always attract a disproportionate amount of analysis because its effects get to all SSCs, whereas weather and flood hazards, at least in principle, can be prevented from gaining entry to the facility in the first place.

This paper has presented an outline approach to risk informed external hazards design that takes advantage of the UK's risk-informed, goal oriented, non-prescriptive regulatory framework.

References

ASCE Standard 43-05 (2005), Seismic Design Criteria for Structures, Systems, and Components in Nuclear Facilities.

Byrne J.P. (1997), The Calculation of Aircraft Crash Risk in the UK, Health and Safety Executive, Research Rpt. 150/1997.

Ford (2022a), External Hazards Design Bases and Safety Analysis in the UK Risk Informed Regulatory Context, 4th Int. Conf. on Nuclear Power Plants: Structures, Risk, Control & Decommissioning (NUPP 2022), 19-20 September 2022

Ford (2022b), The Application of Risk Informed Design and Risk Informed Regulation to the External Hazards Design of Nuclear Facilities, Conf. Structural Mechanics in Reactor Technology-26 (SMiRT-26), Berlin/Potsdam, Germany, July 10-15, 2022.

IAEA (1996), Defence in Depth in Nuclear Safety', INSAG-10.

IAEA (2008), Follow-up IAEA Mission in Relation to the Findings and Lessons Learned from the 16 July 2007 Earthquake at Kashiwazaki-Kariwa NPP, Mission Rpt,, 28 Jan.-1 Feb. 2008.

IAEA (2014), The Fukushima Daiichi Accident, Rpt. by the Director General, GC(59)/14.

IAEA (2016), Safety of Nuclear Power Plants: Design, SSR2/1 (Rev. 1).

IAEA (2021), Seismic Design for Nuclear Installations, SSG-67.

Kennedy et at (1989), Kennedy, R., et al., Design and Evaluation Guidelines for Department of Energy Facilities Subjected to Natural Phenomena Hazards, UCRL015910.

ONR (2011), Japanese Earthquake and Tsunami: Implications for the UK Nuclear Industry. Final Rpt. HM Chief Inspector of Nuclear Installations.

ONR (2018), External Hazards, NS-TAST-GD-013 Revision 8.

ONR (2020a), Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Rev. 1.

ONR (2020b), Underpinning the UK Nuclear Design Basis Criterion for Naturally Occurring External Hazards - Final Report, prep. Fraser Nash for ONR, FNC 62366-49823R Iss. 1.

USDOE (2016), Natural Phenomena Hazards Analysis and Design Criteria for DOE Facilities, DOE-STD-1020-2016.

USDOE (2017), Natural Phenomena Hazards Analysis and Design Handbook for DOE Facilities, DOE-HDBK-1220-2017.

USNRC (1991), Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities (NUREG-1407), NUREG1407.

USNRC (2007a), A Performance-Based Approach to Define the Site-Specific Earthquake Ground Motion', Reg. Guide 1.208.

USNRC (2007b), Evaluation of the Seismic Design Criteria in ASCE/SEI Standard 43-05 for Application to Nuclear Power Plants. NUREG/CR-6926.

USNRC (2018), Updated Implementation Guidelines for SSHAC Hazard Studies, NUREG-2213.

WENRA (2013), Safety of New NPP Designs, Reactor Harmonization Working Group.

Wikipedia (2023), Fort Calhoun Nuclear Generating Station, Fort Calhoun Nuclear Generating Station - Wikipedia.

Appendix: Application of the HFC risk model in the UK – risk informed design

Although the design process is an inherently deterministic activity it is possible to make it risk informed if a suitable risk model is available. A simple (single fault sequence) risk model for a facility is proposed here and adapted for the purposes of DBA – the HFC model. We concentrate in this paper of natural hazards and seismic hazard in particular, since this is likely to be the most risk significant.

The risk model can provide the hazard challenge for each DBA fault from ONR Numerical Target 4 (Target 4), ONR (2020a), and an estimate of the fault occurrence probability or fragility needed to ensure a risk ALARP design from Targets 7 & 8. The fragility of the facility is the inverse of its reliability, and it is this reliability that becomes a design constraint on the SSCs collectively that form the fault sequence.

The HFC Model

The basic methodology described here is the hazard, fragility, consequence, or HFC model. 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 oneyear 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* ∩ *Fragility* ∩ *Consequence* must occur. This relationship implies a functional risk model of the form:

$R = [H(A > a) * F(a)|H] \cdot C(D)|H, F$ (4) where $H(A > a)$ is the probability that the external hazard challenge *A* exceeds ***a***, and where * indicates convolution because *H* and *F* are probability distributions. For comparison purposes, the equivalent formulation for a discrete event like a human-induce external hazard or a plant process fault would be: $R = H \cdot F|H \cdot C(D)|H, F$.

A simple linear consequence model is assumed here of the form: $C(D) = D$; see Ford (2022b) for justification of this.

For non-discrete external natural hazards (i.e. those defined by a hazard curve), where both hazard and fragility are described by probability distributions, from (4) we can write:

$$R = [H(A > a) * F(a)] \cdot C(D) = \left(\int_0^\infty H(A > a) f(a) da\right) \cdot D \quad (5)$$

where $f(a)$ is the fragility density function: $f(a) = dF(a)/da$. The familiar cumulative lognormal fragility function with a single composite standard deviation parameter is assumed here, see Ford

(2022b) for more details. 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

$$P(\infty) = \int_0^\infty H(A > a) f(a)_{da} \qquad (6)$$

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. (6) can be expressed in two forms[7]:

$$P(\infty) = \int_0^\infty H(a) f(a) da = \int_0^\infty h(a) F(a) da \qquad (7)$$

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

Surrogate Risks Metrics

Possible simplifications to the HFC risk model exist, in this paper termed surrogate risks, and are considered legitimate if the surrogate is conservative to (i.e., overpredicts) the parent risk. As long as the individual terms are described probabilistically so that they each take values in the range 0 and 1, then a surrogate exists whenever one or more parameters in the model are set to unity.

Application of the surrogate risk concept to external hazards is made difficult because of the complex relationship between H and F. However, we can proceed by noting from eqn. (7) 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:

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

Therefore, we can write

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

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

The following surrogates are then defined:

- $R^1 = P(\infty)$, assumes *D* = 1. Plant failure alone drives the risk, an unacceptable consequential dose is guaranteed if failure occurs.
- $R^2 = H(A_{FAIL})$, assumes *F* = *D* = 1. Occurrence of the hazard alone drives the risk with failure at the defined hazard level, A_{FAIL}, and unacceptable consequential dose always assumed to occur.
- $R^3 = D$, assumes H = F = 1. Plant failure is assumed to occur, and the risk is driven by the consequential dose.

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.

[7] 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. 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:

- $R^1 = P(\infty) < P_{SCRN}$.
- $R_2 = H(A_{FAIL}) < P_{SCRN}$.
- $R_3 < D_{SCRN}$.

Defining risk informed Design Basis Events

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. In deterministic DBA space a successful facility design subjected to DBE challenge will not have failed[9]; in PSA space this is interpreted as a probability of failure that is very low.

Target 4, ONR (2020a), 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, nondiscrete hazards attract a design basis of 10^{-4}/yr defined on a conservative basis (refer to ONR (2020a) EHA.4, FA.5 and para. 629).

As noted above, applying the HFC model to non-discrete DBA fault sequences is made complex because the hazard, *H,* and fragility, *F*, are both continuous function of hazard severity. With discrete events such as internal plant faults or human induced external hazards, 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, ONR (2020a).

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

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

Making use of eqn. (5) and the second formulation in eqn. (7) gives

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

(8) which is now in a form where Target 4 can be applied.

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[10].

Beyond Design Basis (BDB) External Hazard Challenge

The ONR SAPs and international guidance by IAEA (e.g., IAEA, (2016) & IAEA, (2021)) and WENRA (WENRA, (2013) 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[8].

[8] Design Exceedance Condition (DEC) A equates to the BDB cliff edge level and DEC B to a severe accident event.

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

[9] Failure here is defined as failure to perform one or more safety functions. There may well be extensive damage across the site, but there should be no, or very limited release of nuclear material.

[10] This linear relation between risk and dose does not recognise that Target 4 is defined as a staircase, rather than a continuous curve.

- 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 substantially in its design basis condition. In deterministic DBA space the facility, or at least the significant safety functions, 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.

A recent paper by the author, Ford (2022b) has analysed a number of simple BDB examples to illustrate the effect of these different assumptions in risk terms.

Severe natural hazard events

In this section we investigate use of the HFC risk model applied to severe accidents, or DEC B events in WENRA terminology, WENRA, (2013); these are events that can credibly lead to plant failure and consequential release.

It is almost certainly unrealistic to assume the same level of dose release for plant failure up to the Beyond Design Basis event level as for a severe accident. For the purposes of illustration therefore, we assume a lower release dose, say D_M = 1mSv, up to the BDB level, and D_U = 1Sv at the severe accident level. From eqn. (5) we can write immediately:

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

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

A number of simple test cases were developed by the author and reported in Ford (2022b) to illustrate the risk contribution of severe accidents to seismic risk. Interested readers are referred to Ford (2022b).