*Transactions*, SMiRT-23
Manchester, United Kingdom - August 10-14, 2015
Division VII, Paper ID 147

# LIMITATIONS AND UNCERTAINTIES IN THE ANALYSIS OF MAJOR EXTERNAL AND INTERNAL HAZARDS

**Tanya Macleod[1] and Simon Thompson[1]**

[1] Nuclear Safety Inspector, Office for Nuclear Regulation, UK

## ABSTRACT

The Office for Nuclear Regulation's (ONR's) Safety Assessment Principles (SAPs) require that duty holders identify and analyse internal and external hazards to ensure that risks from the hazards are kept as low as reasonably practicable (ALARP). However, limited operational experience with low frequency events and fault sequences and limited data availability mean that there is significant uncertainty involved in hazard analysis. This paper critically reviews the application of safety analysis to internal and external hazards with a particular emphasis on low probability but credible internal and external hazards.
The following topics are covered:

- A brief overview of Design Basis Accident Analysis (DBAA) and Probabilistic Safety Assessment (PSA)
- Sources of uncertainty when assessing the initiating frequency of internal and external hazards
- Special considerations for multi-facility sites
- The effects of uncertainty on the requirements for provision of adequate safety measures

The paper focuses on events for which frequency and severity are difficult to predict, but where adequately conservative estimates must be determined to provide initiating event input to fault analyses. Two examples are provided:

***Turbine Disintegration***

Examples of turbine disintegration have happened around the world and in recent years, in this paper, we will examine some of these. We will look at the deterministic and probabilistic arguments and how they can complement one another when applied correctly.

***Extreme Rainfall***

An analysis of two rainfall data sets provides an illustration of the uncertainty inherent in the estimation of extreme rainfall events.

The paper concludes that, given the uncertainty involved, emphasis should be placed on ensuring that robust safety measures include multiple barriers, defence in depth, and adequately conservative engineering substantiation analysis.

## INTRODUCTION

External hazards are defined by the ONR as hazards that originate outside the site boundary and are external to the process or primary circuit (ONR 2011). Internal hazards originate within the site boundary but are also external to the process or primary circuit (ONR 2013). The difference comes from whether the duty holder has any control over the hazard's initiating event. External hazards, over which the duty holder has little or no control, include earthquakes, flooding, and aircraft impact. Malicious acts such as terrorism are also considered external hazards. Internal hazards include internal flooding, fire, and other events over which the duty holder has some control over the initiating event. On multi-facility sites, an

internal hazard from one facility (such as a flood due to pipe breakage) could constitute an external hazard to another facility (e.g. external flooding) (ONR 2011). Regardless of whether a hazard is internal or external, the ONR SAPs require that the duty holder identify and analyse the hazard and ensure that risks from the hazard are kept ALARP. However, limited data availability means that there is significant uncertainty involved in hazard analysis, because many hazard events are of low return frequency

There are two types of uncertainty:

Aleatoric uncertainty (or stochastic or irreducible uncertainty) – the uncertainty due to random aspects within the physical processes being modelled. This is often modelled using methods such as Monte Carlo simulations.

Epistemic uncertainty – uncertainties due to limited data or modelling. This is often allowed for by deliberate conservatism in parameters or methods.

The purpose of this paper is to critically review the application of safety analysis to internal and external hazards with a particular emphasis on multi-facility sites. The inherent limitations and uncertainties involved in determining the likelihood and consequences of such events are discussed. Finally, the ways in which the requirements for safety measures can affect decision making are examined.

## SAFETY ANALYSIS – A BRIEF OVERVIEW

The principal criteria against which the plant or operation's safety must be judged are those presented in the ONR's Safety Assessment Principles. ONR SAP EHA.1 states that "external and internal hazards that could affect the safety of the facility should be identified and treated as events that can give rise to possible initiating faults,"(ONR 2014a). The SAPs then go on to provide advice on analysis and protection against faults, giving general information and information on specific faults.

Two complementary assessments to demonstrate that a plant is safe in assessment of both radiological and non-radiological hazards arising from normal operations and accident scenarios are (IAEA 2005):

- Design Basis Accident Analysis (DBAA) - a deterministic approach of demonstration that good engineering rules using concepts such as 'defence in depth' and other fundamental principles i.e. the safety hierarchy, with adequate safety margins taken into account.

- Probabilistic Safety Assessment (PSA) – an approach that demonstrates that the overall risk from the activity is tolerable and meets various criteria. PSA provides the calculated doses, frequencies, and risks to workers and the public on an individual hazard basis for both internal and external hazards.

Faults can be excluded from the design basis if they have an initiating frequency lower than about one in 10,000 years for natural external hazards (based on conservative assumptions) and 1 in 100,000 years for other hazards (based on best estimates) including man-made external hazards and faults in the facility (ONR 2011, 2014). These excluded faults, known as beyond design basis faults, are addressed by severe accident analysis if their consequences may result in high doses.

## EXTERNAL AND INTERNAL HAZARDS ANALYSIS – LIMITATIONS AND UNCERTAINTIES

Perhaps the greatest difficulty in safety analysis of internal and external hazards comes from the requirement to estimate initiating frequencies for events. Not only can the calculations involved be complex, but there are many sources of uncertainty when it comes to assessing the frequency of a hazard.

Internal hazards such as dropped loads may depend on operator behaviour which is difficult to predict accurately. They may also depend on the performance of components such as pipes and electrical components in the case of internal flooding or fires respectively whose reliability is not fully known and whose failures are difficult to predict. Many databases of reliability data have been produced, covering a wide range of electrical, electronic, mechanical and other types of component operated in a variety of environments. However, some of databases are more reliable than others. This is partly due to the treatment of uncertainty in relation to the data provided and partly due, in some cases, to doubts over the provenance of the data provided.

External hazard screening is also fraught with uncertainty, to an even greater extent than internal hazard screening. The amount of uncertainty present in estimates of frequency and consequences of rare events such as tsunamis and extreme winds is highly variable. This is because not enough data is available due to the rarity of the events themselves. Generally, in determining the frequency of an external hazard, a statistical technique such as the Gumbel, Frechet, or Weibull distribution is used. These techniques rely on extrapolating data from a limited number of years to predict return periods of 10,000 years or more. Making such long-term predictions based on limited data (if we are lucky we will have 100 years or so of historical data available for analysis) involves extending a best-fit line to the return period in question. Minute changes in the slope of the best-fit line can lead to large differences in predictions for the long time-scales required.

Both PSA and DBA are vulnerable to epistemic uncertainty in terms of overlooking a fault sequence. Robust fault identification measures that take a step-by-step, iterative approach and principles such as defence in depth can help combat this uncertainty (ONR2014a). Whilst faults may be screened out from detailed quantified risk assessment, the ALARP principle must still be applied.

Climate change is also a confounding factor in predicting the frequency of external events such as flooding, extreme wind, and extreme temperatures. Although there is a near-universal consensus among scientist that the climate is changing, there is a high level of uncertainty surrounding the changes that can be expected. This uncertainty is due to natural variability in the climate, incomplete understanding of climatic processes and the inability to model them perfectly, and uncertainty surrounding future emissions (DEFRA 2009).

DBA should be based on conservative estimates. In DBA, when developing a fault sequence, uncertainty regarding plant state is handled by assuming the worst case scenarios in terms of permitted operating states and configurations of equipment outages. Uncertainty surrounding the ability of components to withstand a design basis event should be taken into account – that is, if uncertainty is high then additional conservatism in plant withstand and/or lines of protection should exist to mitigate the potential for failure (ONR 2014). The single failure criterion must be taken into account, this states that it must not be possible for one single failure to prevent the operation of a safety function (SAP EDR.4)

Under extreme conditions likely to be encountered at beyond design basis levels, operator actions become even more uncertain as events progress, because human behaviour under stressful conditions is less predictable than under normal operating conditions. Again, uncertainty can be managed by building conservatisms into the analysis and/or by employing the hierarchy of safety where engineering features are preferred over operator actions.

In contrast to the conservatism built in to DBA, data used for PSA should be based on "best estimate" data. Calculations should be facility-specific if possible – otherwise generic data or professional judgment should be used. Modelling uncertainty should be minimised via validation and verification of the model. Quantitative methods should include a statistical analysis of both epistemic and aleatoric uncertainty using such methods as sensitivity studies (IAEA 2009).

## UNCERTAINTY IN FLOOD PROTECTION – AN ILLUSTRATION

The following diagram (figure 1) illustrates a calculation I performed using the Gumbel distribution to determine 24-hour rainfall return periods based on historical UK Met Office data for the north of Scotland and on data obtained from UKCP09 (DEFRA 2009) for the same area.

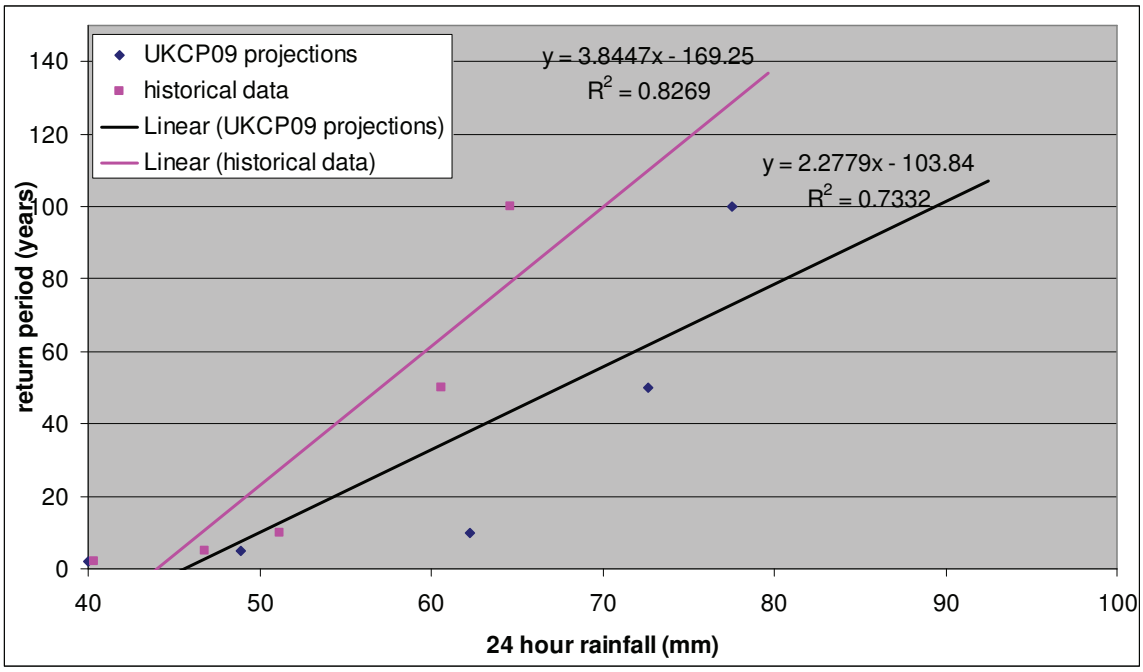


Figure 1 – Gumbel Distribution, 24 Hour Rainfall

Even when examining a relatively short return period of 100 years, it is clear there is a great deal of uncertainty present as illustrated by the discrepancy in predictions. Based on historical data from the Met Office, the 24-hour rainfall with a 100 year return period would be approximately 70mm. Based on UKCP09 data, the rainfall would be approximately 90mm. In addition, there is uncertainty surrounding the amount of rainfall that would be needed to cause a flood, as this depends on antecedent conditions (i.e. whether recent weather was wet or dry, the current soil moisture deficit, potential evapo-transpiration, etc.), the level of the water table, and the adequacy and state of the drainage systems. Compounding this uncertainty is the fact that a 100 year event (or indeed a 10,000 year event) could occur at any time.

When reporting the results of the rainfall study, it is important to be clear regarding the uncertainty that exists surrounding any predictions being made, and to quantify the levels of uncertainty. The resulting design basis flooding analysis for facilities should take a deterministic approach and conservatively assume that a flood will occur, providing defence in depth and adequate safety margins (IAEA 2005). The analysis should ensure that any resulting radiological hazards do not pose an unacceptable risk to workers, the public, or the environment.

For future research into the estimation of external event frequencies, consideration of modern statistical techniques such as Generalized Pareto Extremes over Threshold is recommended. This type of technique makes better use of limited data sets because it doesn't just take annual maxima into account but uses the entire dataset and selects extreme values over a certain threshold.

***Past Events***

***Le Blayais***

An example of a flood that occurred at a nuclear power plant was at Le Blayais in France which consists of 4 PWRs. This took place in December 1999 when a combination of high tide, storm surge, and wind driven waves lead to the sea walls being overwhelmed. Originally the designers had overlooked the combined effects of these hazards. Then in 1998 the annual review of safety had identified the need for sea walls to be raised. The work was planned for 2002.

The facilities flooded at a rate of around 30,000$m^3$ per hour – this amount of water could not be actively managed. The event lead to fundamental changes in the evaluation of flood risk at nuclear power plants in France including adding several additional factors to flood evaluation including wind-induced waves and rainfall of different intensities (IRSN, 2000).

***Fukushima***

On 11 March 2011, a magnitude 9 earthquake occurred followed by a tsunami that inundated the Fukushima Daichi site. The plant itself withstood the earthquake relatively well but the connection to the grid was lost. At that point, the back-up diesel generators started up as they were meant to, but these were located in the basements of the turbine buildings and all but one was lost due to flooding from the tsunami. Power was switched over to the batteries but these were only designed to last eight hours. Responders had difficulty getting additional back-up power supplies to site and connecting them up, and adequate cooling was lost (ONR, 2011).

For both of these events, flooding caused widespread damage – in summary, a common cause event knocked out or degraded a significant portion of the site's essential and emergency cooling services. The main difference between the two events was that at Le Blayais, unlike at Fukushima, the diesel generators operated correctly. Therefore, cooling was maintained and the safety of the plant was not impaired.

Both events have lead to fundamental changes in the evaluation of flood risk at nuclear power plants in Europe and worldwide.

## TURBINE DISINTEGRATION – AN ILLUSTRATION

A steam turbine is a device that extracts thermal energy from pressurised steam and uses it to do mechanical work on a rotating output shaft. Turbines exist on all nuclear generating facilities in order to convert heat from nuclear fission via steam to electricity. Numerous designs of nuclear power station exist

with differing steam turbine designs but in this paper we consider steam turbines in their generic form. When in operation, steam turbines turn at around 3000 rpm (UK/Europe) – 3600 rpm (USA) for full speed turbines and 1500 rpm for half speed turbines. Steam turbines usually consist of a high-pressure section, an intermediate-pressure section and a low-pressure section. Together, these three sections can weigh around 197 tons, of which the LP rotor accounts for around 85 tons (e.ON 2010) depending on the design

***Failure modes***

A turbine can fail via brittle fracture which would be expected to happen at normal overspeed, or ductile failure which would be expected following a runaway overspeed. In general for brittle failure:

- Low pressure (LP) rotors can be designed for the 120% speed condition.
- Historical probability of failure: $10^{-4}$ / year.

For ductile failure (runaway overspeed):

- In some cases, grid connection provides a braking force which makes runaway incredible.
- For the cases where the grid is not available:
    - Initiating fault frequency is dominated by loss of off-site power (frequencies of about $10^{-1}$/ year is typical but depends upon grid connections).
    - Failure probability of overspeed protection systems: [$10^{-5}$ - $10^{-6}$] / demand (on-load /Europe testing, redundant steam valves, redundant overspeed detection).
      This leads to an assumed value of $10^{-5}$ / year for disintegration at runaway overspeed.

***Past Events***

There have been a number of incidents around the world involving turbine disintegration and subsequent damage to plant. A selection of these incidents is discussed below.

Hinkley Point A – The turbine generator of the No.5 unit suffered a catastrophic failure on 19th September, 1969. The failure was caused by spontaneous brittle fracture of a shrunk-on low-pressure disc. The No.5 unit was disconnected from the grid for overspeed tests a few minutes before the accident. The failure occurred at the time when the rotation speed reached 3,200rpm. The rotor shaft fractured completely in five positions. Three discs of the low-pressure a rotor came free from the unit, and large fragments of them were found scattered in the machine hall. This was the first catastrophic failure of a turbine-generator caused by the brittle fracture of a rotating component in the United Kingdom. Fortunately, there were no casualties although seven operators were in the vicinity of the unit at that time (Kaldron 1972).

Vandellòs Unit 1 – was a gas-cooled natural uranium fuelled, graphite moderated reactor located 140 km South of Barcelona. On 19th October 1989, while the plant was operating at partial power (around 80%), the high pressure section of turbine number 2 ejected 36 blades. The blade ejection altered the balance of the turbine leading to high vibration and excessive friction around the turbine shaft. This friction caused the turbine to come to a halt within a few seconds. The vibration also caused the seals around the generator to fail allowing hydrogen gas to escape. It is believed that the hydrogen ignited on the hot surface of the shaft. The ejected blades also cut through turbine oil lubrication lines, the oil also igniting on the hot surfaces. The resulting fire led to major damage of the Turbine Hall. Vandellòs Unit 1 was closed down following this event and never returned to service (Nowlen et. al. 2001).

In the cases discussed above, turbine disintegration leads to local damage, fire and flooding which is a concern in itself. There is the potential that missiles generated as a result of the disintegration are propelled further than the turbine hall, therefore having the potential to threaten other facilities on the

nuclear licenced site. There is thus the potential that facilities impacted may be relied on to control and cool the reactor following say a loss of off-site power (LOOP). It is expected therefore that the licensee takes this into consideration when designing plant and finalising layout. It is also expected that a turbine disintegration event would be included in a fault schedule and that design basis accident analysis (DBAA) supported by a probabilistic safety assessment (PSA) would be carried out.

***What Would A Deterministic Presentation Of A Turbine Hazard Constitute?***

As discussed above and based on historical data, missiles from turbine disintegration should be accepted as a "credible fault", and appear in a fault schedule. The fault schedule should document what would be affected by the fault (e.g. the turbine failure would lead to loss of generation from the unit and in many cases a loss of offsite power due to electrical protection). It would also identify what would be expected to survive the fault (e.g. systems, structures and components (SSCs) protected by the aircraft protection shell).

The presentation of the DBAA would allow the licensee to therefore explicitly consider aspects of the safety case which may otherwise be opaque. When considering the example of diesel buildings housing emergency electrical generating capacity, it would allow decision makers within the licensee to decide whether they are content with the current design and layout or whether it may need enhancement. [Note: diesel buildings are used as an example – the issue is not confined to them.]

The deterministic presentation may lead to consideration of whether the diesel buildings themselves may need some substantiation against missiles, and to what extent. However, it will lead to the safety case being more complete and comprehensive which in turn makes it more obvious to decision makers where funds should be invested.

ONR's expectations for the purpose, scope, and content of safety cases are described in ONR's Technical Assessment Guide (TAG) NS-TAST-GD-051 (ONR 2013). This TAG was revised in 2013 and includes guidance informed by evidence presented at the Nimrod inquiry, and includes the need for safety cases to make risks visible to decision makers. Within the TAG, an appendix includes the following shortcoming which Haddon-Cave identified as common to safety cases in the report of the Nimrod review "*Self-fulfilling prophesies: Safety Cases argue that a platform is 'safe' rather than examining why hazards might render a platform unsafe, and tend to be no more than self-fulfilling prophesies*" (Haddon-Cave 2009).

***Determining Whether a Hazard is "Credible" / Should It Be within the Fault Schedule?***

When licensee's produce safety assessments, if effort is disproportionately placed on analysis rather than application of good engineering, there is the potential to under report the importance of that initiating event. Instead, the approach can lead to concentration on sequence outcomes (i.e. frequency of a missile strike onto particular buildings). This gives a false sense of comfort which may be ill-founded, since many judgements have gone into the derivation of the frequencies.

Turbine disintegration is a credible hazard at a power station. It isn't an "expected" occurrence, and modern designs are well protected against overspeed, but as detailed in this report there are examples, both in the UK and in other parts of the world, where turbine disruptive failures at nuclear power plants have occurred.

NRC RG 1.115 (NRC 2012) includes some description on the likely frequency for turbine overspeed. It concludes that "*the NRC considers the overall turbine failure rate of $1x10^{-4}$ per turbine year to still be valid*", but accepts that this data would be limited to turbines at nuclear power plant (and – not stated, but implied – in the USA). Elsewhere it suggests that a "*minimum reliability requirement for loading the turbine and bringing the system online*" should be reduced to "*< $1x10^{-5}$ for unfavourably oriented*

*turbines*". This would be done by enhanced quality assurance in design and fabrication, inspection and testing programs, and overspeed protection systems. It is worth bearing in mind that application of the US data would lead to higher frequencies for turbine major disruption than $10^{-4}$ per year.

At the frequencies suggested by NRC RG 1.115, the initiating event is one that should feature as a "design basis" accident and the guidance on deterministic safety cases – such as IAEA Specific Safety Guide No. SSG-2 (IAEA 2009) is appropriate.

The European Utilities Requirements for LWR Nuclear Power Plants (EUR 2012) includes a section on turbine missiles, which – as with the other guidance – recognises the need to site or protect *Safety Category I Structures and Equipment* such that they are not exposed to the risk of damage in the event of the turbine disintegration.

***Current UK Practice***

Current UK practice is mixed. There exist examples of turbine missile safety cases for reactors in the current UK fleet which are structured in a way compatible with the conclusions of this paper, and examples which do not align with the conclusions of this paper.

## MULTI-FACILITY SITES – SPECIAL CONSIDERATIONS FOR PREDICTIONS

One of the "lessons learned" from Fukushima is that common cause failure on multi-facility sites must not be ignored. The totality of risks from multi-facility sites must be considered in safety analyses. However, on most sites, individual safety cases are generally produced to cover individual facilities. Regardless of whether there is one or several operators for the facilities on a multi-facility site, risks must be combined in an overall site safety case so that interdependencies of facilities can be taken into account (ONR 2014). Clearly in the case of external hazards such as flooding and earthquake, all facilities on a site could be affected simultaneously (ONR 2011). An internal hazard in one plant could constitute an imposed hazard external to another plant. The fault sequence should therefore be traced to completion or there should be an interface with the second plant so that the effects on the second plant can be taken into account.

It is also important to note that multi-facility sites can have risks beyond simply adding together individual facility risks. Safety measures should not be dependent on assuming other plants are operating without fault, and sufficient back-up measures (such as pumps, etc.) should be available in case of common cause failures. Diversity and segregation should be used to reduce common cause failures.

## SAFETY MEASURES – THE EFFECT OF UNCERTAINTY

Uncertainty pervades all aspects of nuclear hazards safety case work. The presence of uncertainty in fault identification and analysis must not be used as an excuse to do nothing instead of taking preventative action. The precautionary principle means that it is necessary to err on the side of safety and to ensure that safety measures are adequate (HSE 2001).

The overall probability that an unacceptable consequence will occur, arising from an internal or external hazard, can be calculated using the following formula (HSE 2001) [1].

$$P = P1 \times P2 \times P3 \quad (1)$$

Where: P1 = the probability that the initiating event will occur
P2 = the probability that an initiating event will affect a structure, system or component (SSC)

[1] The formula is more complex for natural external hazards but the same principles apply

P3 = the probability of an unacceptable consequence to the SSC

Best practice requires placing the greatest emphasis on reducing P1, P2 and / or P3 depending on which of these can be most effectively controlled. When designing a new activity it is better to eliminate hazards rather than control them – in other words, reducing P1. Unfortunately, this is not always possible, particularly in the case of external hazards over which a site has no control. These external hazards should be taken into account during the siting phase of a project – for example, a nuclear installation should not be sited on a flood plain, near an active volcano, on a fault line or where any other external hazard is particularly likely to occur. However, it is impossible to prevent all external hazards and therefore a greater focus should be placed on mitigating their consequences. The same is true for internal hazards, although to a lesser extent. Although the facility does have control over the initiating event in the case of internal hazards, the uncertainties involved in estimating their frequencies are generally too great to be considered sufficiently reliable and justify screening out.

Because of the uncertainty inherent in estimating P1, P2 or P3, a worst case scenario should be determined via experiments and data analysis so that conservative approximations can be made (HSE 2001). Conservatisms can be used to handle uncertainties – however too much conservatism causes problems of its own. Sensitivity analysis and other specialised techniques can be used to estimate the amount of uncertainty present, but uncertainty itself cannot be wholly avoided. Therefore, due to the uncertainties involved in predicting internal and external hazards, the greatest emphasis should be placed on minimising their effects. This leads to a consideration of the requirements for safety measures.

In order of preference, safety measures should be:

1. Passive
2. Automatically initiated preventative engineered measures
3. Manually initiated preventative engineered measures
4. Administrative
5. Mitigating the effects of failure

The concepts of independence, redundancy, diversity and segregation are vital to ensure that safety measures are adequate. Independence means that each safety system must be fully independent from the initiating fault i.e. it must not be vulnerable to failure from the cause that produced the initiating fault. Also the safety systems must be demonstrably independent of one another i.e. not vulnerable to failures which may cause other safety systems to fail.

Redundancy is defined by the IAEA (IAEA 2000) as: "*Provision of alternative (identical or diverse) structures, systems or components, so that anyone can perform the required function regardless of the state of operation or failure of any other.*" The provision of redundancy can improve reliability and protect against single failures. However, common cause and common mode failures may still occur.

Diversity addresses common cause and common mode failures. Diversity is defined by the IAEA (IAEA 2000) as: "*The presence of two or more systems or components to perform an identified function, where the systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure."*

Segregation is defined in the ONR Safety Assessment Principles (ONR 2014) as: "*The physical separation of components and systems, by distance or by some form of barrier that reduces the likelihood of common cause failure."*

## CONCLUSION

This paper has critically reviewed the application of safety analysis to internal and external hazards with a particular emphasis on low probability but credible internal and external hazards. The paper concludes that in addition to the implementation of adequate safety measures, multiple barriers and defence in depth, and engineering substantiation, work should be done to ensure that uncertainty is reduced as much as possible. Estimates of the hazard severities for DBAA should be sufficiently conservative to account for the uncertainties inherent in the data and appropriate lessons should be learned from accidents that have occurred due to internal and external hazards.

Based on the uncertainties related to both internal and external hazards, safety assessment should be underpinned by a robust design basis assessment method which includes applying an appropriate combination of engineering, deterministic and probabilistic methods. The design basis event should be derived conservatively to take account of data and model uncertainties.

It is important to remember, when carrying out safety assessments not to rely on "the numbers", low estimates of sequence frequency or simple estimates of hazards consequence especially when these numbers are poorly substantiated based on the data sets used. It is always important to carry out an assessment based upon looking at unmitigated hazards, taking no account of the safety measures available and looking at options to see what can reasonably be done to improve safety This is implied by the requirement to drive risks to the ALARP level, a legal requirement. The safety case should be clear with plant essential for bringing the reactor under control and carrying out essential cooling clearly identified.

A probabilistic assessment is useful at providing information regarding information regarding vulnerabilities amongst other things and should be provided as part of a PSA (probabilistic safety assessment). When changes are required as part of design evolution, incidents or breakdowns, individuals responsible for spending and budgets must be able to make informed decisions as to where the money should be spent. This can only be done with clear concise safety cases utilising both deterministic and probabilistic safety assessments where applicable.

## REFERENCES

Defra (2009). UK Climate Projections.
Available at: http://ukclimateprojections.defra.gov.uk/

EDF, "*Assessment of turbine missile impact frequencies on Hinkley Point C building structures*", HPC-NNBOSL-U0-ALL-RET-000002, 16281-709-HPC-RPT-0001, Revision F, November 2011, TRIM 2013/26779.

eON "*The Steam Turbine*" https://www.eon.se/upload/eon-se-2-0/dokument/broschyrarkiv/in-english/%C3%96resundsverket%20%20factsheet%20for%20the%20steam%20turbine.pdf 2010

Engineering Tips.com http://www.eng-tips.com/viewthread.cfm?qid=360571, 17 March 2014

Haddon-Cave, Charles "*The Nimrod Report*" October 2009

Health and Safety Executive (2001). "*Reducing Risks, Protecting People*."
Available at: http://www.hse.gov.uk/risk/theory/r2p2.pdf

IAEA (2000). Safety of Nuclear Power Plants – Design.
Available at: http://www-pub.iaea.org/MTCD/publications/PDF/Pub1099_scr.pdf

IAEA (2005). "*Risk informed regulation of nuclear facilities: Overview of the current status*".
Available at: http://www-pub.iaea.org/MTCD/publications/PDF/TE_1436_web.pdf

IAEA (2009a), "*Deterministic Safety Analysis for Nuclear Power Plants*".
Available at: http://www-pub.iaea.org/MTCD/publications/PDF/Pub1428_web.pdf

IAEA (2009b) " *SSG-2 Deterministic Safety Analysis for Nuclear Power Plants*" 2009

EUR, "European Utilities Requirements for LWR Nuclear Power Plants: Safety Requirements (Part 1)", Chapter 2.1 revision D October 2012

IRSN (2001). "*Rapport sur l'Inondation du site du Blayais Survenue le 27 Decembre 1999*".

Kalderon D, "*Steam Turbine Failure at Hinkley Point 'A'*," Proc. Instn. Mech. Engrs., Vol.186, pp.341-377(1972).

Nowlen, N. P, Dr. Kazarlans M, Wyant F, "*Risk Methods Insight Gained from Fire Incidents*", 2001

NRC 2012. U.S. Nuclear Regulatory Commission. Regulatory Guide RG 1.115, "Protection against Turbine Missiles" January 2012, Revision 2

ONR 2011. Office for Nuclear Regulation (2011). "*Japanese earthquake and tsunami: Implications for the UK nuclear industry,*"
Available at: http://www.onr.org.uk/fukushima/final-report.pdf

ONR 2013a. Office for Nuclear Regulation (2013),"*The Purpose, Scope and Content of Safety Case Nuclear Safety Technical Assessment Guid*e", NS-TAST-GD-051 Revision 3 Review date July 2016
Available at: http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf

ONR 2013b. Office for Nuclear Regulation (2013). "*Internal Hazards - Nuclear Safety Technical Assessment Guide*", NS-TAST-GD-014 Revision 3, review date April 2016.
Available at: http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-014.pdf

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

ONR 2014b. Office for Nuclear Regulation (2014). "*External hazards - Nuclear Safety Technical Assessment Guide*", NS-TAST-GD-013 Revision 5, Review date September 2017.
Available at: http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-013.pdf