Propagating Uncertainty in Phenomenological Analysis into Probabilistic Safety Analysis

A. El-Shanawany[a,b*]
[a] Imperial College London, London, United Kingdom
[b] Corporate Risk Associates, London, United Kingdom

Abstract: The operation of nuclear power plants is supported by numerous analyses, both computational and experimental. Probabilistic risk analysis models attempt to quantify the risk of power plants, and implicitly use the supporting analyses during this process. The way in which these analyses are used in risk models is usually conservative, but could instead be represented as an uncertainty distribution. The conservatisms are often hidden, but affect every aspect of risk models; for example in the definition of success criteria. This paper uses operator reliability as an example to quantitatively demonstrate how conservative interpretations of supporting analyses can affect risk model predictions.

The influence of human factors is recognised to be crucially important to risk models for nuclear power plants. Human error probability quantification is a key aspect in determining the relative risk importance of human actions in the context of a holistic probabilistic safety analysis model. However, there are large degrees of uncertainty in numerous aspects of human factors analysis and in the resulting quantification, many of which can be traced back to supporting transient analyses, such as thermal hydraulic and neutronic analyses. Risk models have historically used conservative judgements resulting from these analyses as an input into human reliability assessment. This paper presents a method for incorporating uncertainty distributions arising from phenomenological analyses into human reliability quantification. The method is illustrated using uncertainty in the timescale available to the operator for performing specified actions. This paper shows how to include uncertainty distributions over the time available to the operator and provides updated quantitative analysis. An illustrative example of operator initiated long term hold down of reactivity is presented.

Keywords: PRA, Uncertainty, Success Criteria, Risk, Human Reliability.

1. INTRODUCTION

Previous studies have considered the effect of success criteria uncertainties (using auxiliary feedwater pumps as an example) on the risk model results [1, 2]. In summary, it was found that model uncertainty, for these case studies, was order of magnitudes larger than parameter (statistical) uncertainty. This type of result suggests there is an unmet need to properly characterise the model uncertainty in the results of risk models. This paper seeks to contribute to the issue of model uncertainty by considering the plant based source of uncertainty. Nuclear power plants (NPP) have numerous supporting nuclear analysis codes; the nuclear analysis codes cover a wide spectrum of knowledge domains. Assessing uncertainty is a key part of the scientific method, and computational advances have allowed quantitative uncertainty estimates to be routinely calculated in a number of contexts. However, frequently these estimates are only used within a small knowledge domain and the uncertainty information is often passed on to other experts in a summarised form, for example as a conservative estimate. This type of information reduction certainly features in the construction of Probabilistic Risk Analysis (PRA) models, which uses conservative success criteria estimates. In this paper, the effect of uncertainty arising from phenomenological analyses on human reliability estimates is considered.

* Author email: ashanawany@c-risk-a.co.uk

In this paper the interaction of success criteria with operator actions is considered. Operator actions are typically assessed to be significant contributors to the overall estimated risk of operating nuclear power stations. The effect of operator actions on the predicted plant risk is typically a significant fraction of the total risk, although the precise figure is highly dependent on the specifics of the plant design and operation. The task of estimating human reliability, hence, has a very significant bearing on the results and insights of probabilistic risk models, and is a valuable example to use.

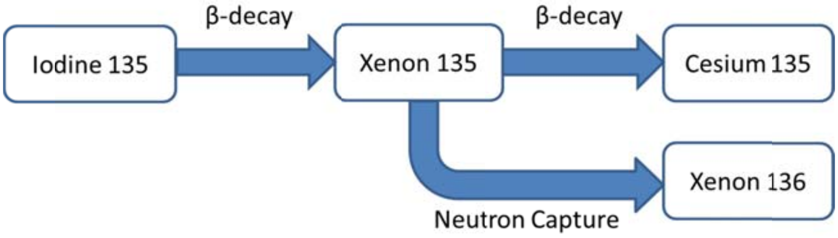
Quantitative human reliability assessment has numerous open questions associated with it and is an active area of research. Many methods have been developed over a number of years to quantitatively estimate human reliability. For example, some early methods include Technique for Human Error Rate Prediction (THERP), Accident Sequence Evaluation Programme (ASEP), and Human Error Assessment and Reduction Technique (HEART) [3, 4, 5]. A 2009 review [6] by the UK Health and Safety Executive (HSE), identified 72 potential methods. Some of these methods are public domain, while others are proprietary methods. This paper is written without reference to any specific method, but it does draw upon ideas that have been developed by the human reliability quantification methods. In particular the concept of factors which modify human reliability is considered in this paper.

It is widely accepted that there are numerous variables that can affect the performance of operators. These factors can be coarsely split into internal station factors and external station factors. The internal station factors include issues such as familiarity with a task, the time available to complete a task, and clarity of feedback. External factors include all those aspects of life which will impinge on an operator’s state of mind, for example their personal life outside of work. Generally human reliability quantification methods consider only the internal to station factors. A description of the factors which can affect human reliability is provided in Reference 7. Quantitative techniques have been developed to estimate the impact of these factors on human reliability. However, uncertainty arising from these factors has not previously been considered quantitatively. Instead the implicit ethos adopted by human error quantification techniques has been the same as the ethos traditionally used throughout probabilistic safety analysis; that is to make conservative judgements whenever a judgement needs to be made. However, the tools used to estimate the impact of a given factor can usually be extended to incorporate the effect of uncertainty. For example the effect of available time on operator reliability has been characterised by several methods, and can be extended to consider uncertainty over the time available. This paper demonstrates how uncertainty over the time available for an operator to perform an action can be incorporated into risk models, and links the uncertainty in the time available to the underlying plant physics.

2. NITROGEN EXAMPLE

The large range of factors which affect human performance can each have several different sources of uncertainty. In this paper the problem is restricted to the time available to the operator to perform a specified task, and the uncertainty in the time available which is attributable to the underlying phenomenological modelling. For example, following a trip at a gas cooled reactor, the primary shutdown mechanism is to fully insert the control rods, thereby making the reactor subcritical and terminating the fission reaction. However, if some control rods fail to insert then nitrogen gas can be used to provide an additional safety margin for shutdown and to ensure the long term hold down of reactor reactivity [8]. The key parameter determining the timescale available for nitrogen shutdown, assuming a fixed number of rods fail to insert, is the Xenon-135 transient. Xenon-135 is a strong neutron absorber (~2.6E+06 barns) and reaches a steady state in an at power reactor [9]. Xenon-135 formation and decay is primarily dictated by the processes shown in Figure 1 below.

Figure 1: The major Xenon formation and decay processes



During at power operation Xe-135 is continually "burnt off" due to the high neutron flux. However, once the fission process is terminated the neutron flux falls to a low value, and the neutron capture method of decay shown in Figure 1 ceases to be a significant decay mechanism of Xe-135. This causes the Xe-135 levels to rise initially as I-135 is converted into Xe-135 faster than Xe-135 decays into Ce-135. However, I-135 is primarily produced from at power decay processes, and once the reactor is shutdown, the production of I-135 falls to a low value. Following shutdown the decay rate of I-135 is greater than the production rate, causing a steady decline in the level of I-135. As the level of I-135 falls, the production rate of Xe-135 falls. Eventually the production rate of Xe-135 falls below that of the decay rate, and the level of Xe-135 falls asymptotically to zero. Once the Xe-135 level begins to fall this effectively represents a reactivity insertion into the reactor. This phenomenon is well understood and described in many texts, for example Reference 9.

The rationale behind nitrogen injection is to insert extra negative reactivity before the Xe-135 transient causes an insertion of positive reactivity, thus maintaining the shutdown margin. However, the precise form of the Xe-135 transient depends heavily on the operating history of the reactor, although it will follow the general form described above. For any given reactor state, the Xe-135 transient can be accurately predicted and can be used to infer the time available to start nitrogen injection in order to maintain the safety margin in the event that primary shutdown is not fully achieved. The possible scenarios can be bounded by a "worst case" scenario which is used to define the minimum time that could elapse before positive reactivity insertion due to Xe-135 decay could occur. This minimum time is then, conservatively, used to define the time available to the operators to commence nitrogen injection. This conservatism is largely hidden from view during a typical procedure for quantitative human reliability estimation. The framework for considering time pressure as a factor in the estimation of human reliability has existed since the first generation HRA methods [6]. The existence of such methods facilitates including uncertainty over the time available for an action into the estimate of human reliability. The method used to incorporate time pressure can be complex, depending on the overall human reliability method used, but this will be substantially simplified for the purposes of this paper. The next section gives an outline of a simple theoretical way of incorporating time factors into HRA.

3. TIME FACTORS

There are numerous ways in which time could be incorporated into HRA estimates, and different human reliability quantification methods take different approaches. Most modern methods acknowledge that time pressure has a quantitative impact on human reliability, and to a varying extent provide a mechanism for quantitatively estimating this effect. However, as noted above, these methods can be involved. The aim here is to demonstrate an overall method for incorporating important thermodynamic uncertainties into HRA estimates, rather than the HRA methods themselves. To that end a grossly simplified method of incorporating time factors will be used by using a multiplicative factor applied to the human reliability estimate. The multiplicative factor is a negative exponential decay model of the effect of additional available time over some baseline time for performing a task, as shown in the equation below:

$$TF = \exp(-(t_a - t_b)/s) \tag{1}$$

Where t_a and t_b are the time available and a "baseline time" respectively. The baseline time is a nominal "normal" amount of time which should be available in order for the operator to perform the action successfully. 's' is a scaling factor that can be used to adjust for the effect of the selection of the units. Deviations from the baseline time are weighted using a negative exponential factor. In this paper the baseline time will be taken as being the conservative time limit that would be used in existing risk modelling processes. Hence in this paper t_a is always greater than or equal to t_b.

It is emphasised that the model described above does not have a basis in quantitative human reliability research, and is chosen primarily for simplicity. The curve does also satisfy the intuitive properties that increases in the available time increase reliability while increases in reliability decline as more time is made available, so that in a finite time it is not possible to achieve an arbitrarily low reliability using this model. Any alternative method for assessing the impact of time on human reliability could be substituted for this model without changing the overall method described, and without altering the overall message of the paper.

4 INCORPORATING UNCERTAINTY

Section 3 has provided a simplified method for incorporating time factors into quantitative human reliability assessment. Hence to create an uncertainty distribution ***based on the effect of time uncertainty only***, we can assess the reliability at all of the possible time points. In general this is a continuous distribution, but practically we will restrict it to a discrete distribution over possible time states. This is demonstrated below in the context of the nitrogen injection example.

To incorporate uncertainty in the time factor of nitrogen injection we need to estimate the probability distribution over the time to injection. This is a difficult task. Fortunately, known phenomena and transients that can occur at nuclear power stations invariably have already been subjected to rigorous analysis. From a risk analysis perspective we can simplify the task to collating existing analyses which provide estimates on uncertainty. In this example the information needs to be discretised into "reasonable" time chunks permit analysis. Each time period is assigned a probability mass, which in this case is nominal, but in practice can be based on existing analyses. This is illustrated with a hypothetical operator action which is assigned a nominal human error probability of 1.00E-03. This defines the human error probability in the baseline time, which is set to be 3 hours in this example. Table 1 below gives a breakdown of time periods and probability masses, together with the multiplicative factor calculated using our simple model, and the revised human error probability estimate for that time period.

Table 1: Discrete Probability Distribution Over the Human Error Probability Estimate

ID	Time Available	Probability	Multiplicative Factor	Human Error Probability Estimate
1	3-6 hours	0.1	0.94	9.39E-04
2	6-12 hours	0.2	0.78	7.79E-04
3	12-18 hours	0.5	0.61	6.07E-04
4	18-24 hours	0.2	0.47	4.72E-04

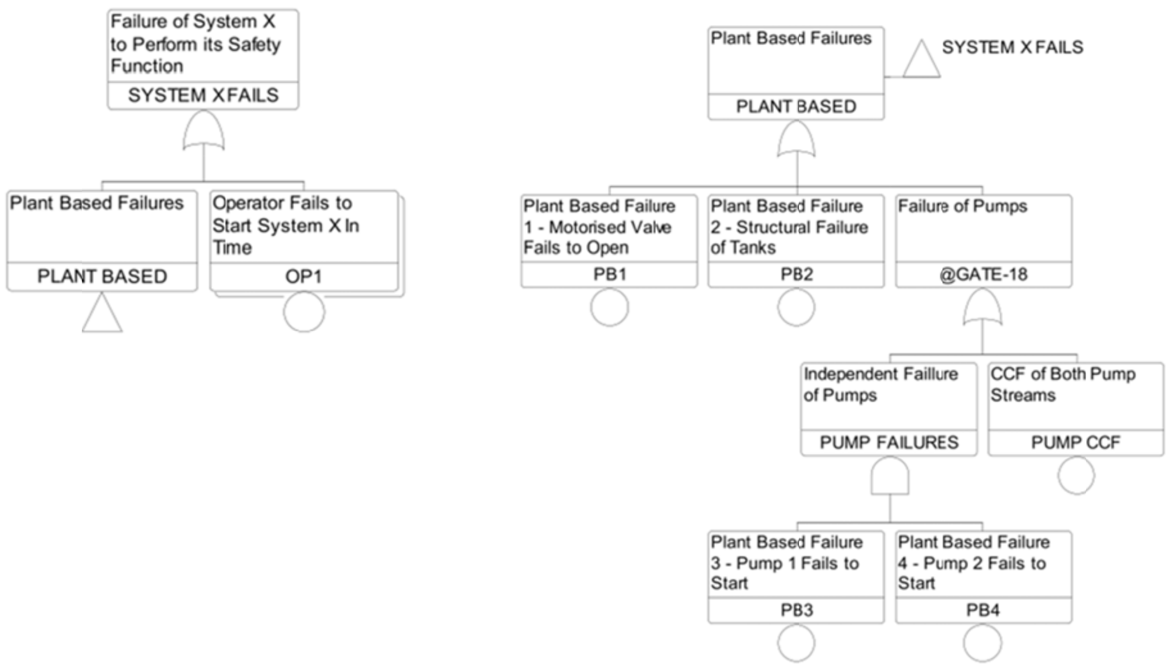
In each case the midpoint of the range has been used in estimating our multiplicative factor. The greater the number of intervals used the more detailed the resulting uncertainty distribution will be. The method is just as well demonstrated using a small number of intervals as using many intervals, since it still provides the shift from a conservative assessment to a best estimate plus uncertainty case. It is in making this shift that the greatest difference is observed, rather than by increasing the number of intervals further. Beyond a 24 hour time horizon there is likely to be significant offsite support available and the problem fundamentally changes character from predicting the reliability of a single team or single operator. For this reason the simple model presented above is considered wholly inapplicable for times beyond 24 hours and times on longer scales are not considered in this paper.

Table 1 shows that the best estimate of the time available to complete the action is in the 12-18 hour bracket, rather than the conservative estimate of 3 hours. A probability distribution is formed by the intervals defined in Table 1 above, and this is assumed to be available as the result of phenomenological modelling. As noted previously, this information is already available in many instances. The next section considers the impact of incorporating the information presented in Table 1 into a simple model. Using the values from Table 1 the mean estimate of the human error probability is calculated to be 6.48E-04 rather than the conservative estimate of 1.00E-03.

5 RESULTS USING A SIMPLE MODEL

A simple example fault tree is shown below, and will be used to demonstrate the concept of including time uncertainty for human error probability.

Figure 2: Simple Fault Tree Example



A table of basic events used in the model is provided in Table 2 below:

Table 2: Summary of Basic Events

ID	Description	Mean
OP1	Operator Fails to Start System X In Time	6.48E-04
PB1	Plant Based Failure 1 - Motorised Valve Fails to Open	2.00E-04
PB2	Plant Based Failure 2 - Structural Failure of Tanks	1.00E-05
PB3	Plant Based Failure 3 - Pump 1 Fails to Start	1.00E-03
PB4	Plant Based Failure 4 - Pump 2 Fails to Start	1.00E-03
PUMP CCF	CCF of Both Pump Streams	1.00E-04

In the base case the conservative assumption is that 3 hours are available to perform the operator action. This conservative assumption is the one which would be made in any standard probabilistic risk model, and represents the current practice in incorporating human error probabilities into risk models. The parameters used for this model are shown in Table 3 below.

Table 3: Model Failure Parameters Table

Parameter Name	Description	Mean	Uncertainty Distribution	Error Factor	Median	5th Percentile	95th Percentile
Base Case HEP	Base Case Conservative Value for Human Error Probability	1.00E-03	None	N/A	1.00E-03	1.00E-03	1.00E-03
Uncertainty HEP	Human Error Probability Inc Time Uncertainty	6.48E-04	Discrete	See Table 1	6.07E-04	9.39E-04	4.72E-04
Pump CCF	Pump CCF	1.00E-04	Lognormal	5.00	6.20E-05	1.24E-05	3.10E-04
PumpFS	Pump Fails to Start	1.00E-03	Lognormal	2.00	9.15E-04	4.58E-04	1.83E-03
Tankfail	Structural Failure of Storage Tanks	1.00E-05	Lognormal	5.00	6.20E-06	1.24E-06	3.10E-05
ValveFC	Valve Fails Closed	9.00E-04	Lognormal	2.00	8.23E-04	4.12E-04	1.65E-03

The model has been analysed using RiskSpectrum PSA v1.1.4.3, using standard analysis settings, to provide an estimate of the probability of failure on demand of the top gate shown in Figure 2. The software has been used to find the minimal cutsets of the fault tree, calculate importance metrics and estimate the uncertainty distribution of the top gate. The minimum cutsets for the base case are shown in Table 4 below:

Table 4: Minimum Cutsets for the Base Case

ID	Sequence Probability	Percentage Contribution	Event 1	Event 2
1	1.00E-03	49.8	OP2	
2	9.00E-04	44.8	PB1	
3	1.00E-04	4.98	PUMP CCF	
4	1.00E-05	0.5	PB2	
5	1.00E-06	0.05	PB3	PB4

The percentage contribution is a standard importance measure used to evaluate cutset results. Note that the percentage contribution has the property that the sum of all cutset percentage contributions is not (usually) 100. The formula used for calculating fractional contributions is copied below for reference.

$$FC_i = 1 - \frac{Q_{TOP}}{Q_{TOP}(Q_i = 0)} \tag{2}$$

Where FC_i is the fractional contribution of the i^{th} component, Q_{TOP} is the probability of failure on demand of the top event (or unavailability in some problem setups), and $Q_{TOP}(Q_i=0)$ is the probability of failure on demand of the top event with the probability of failure of the ith component set to zero.

Table 5 below shows summary results for the basic events in the base case:

Table 5: Basic Events Importance and Sensitivity for the Base Case

ID	Basic Event	Mean	Fractional Contribution	Risk Decrease Factor	Risk Increase Factor	Sensitivity (RIF/RDF)
1	OP2	1.00E-03	4.97E-01	1.99	4.98E+02	9.90
2	PB1	9.00E-04	4.47E-01	1.81	4.98E+02	8.41
3	PUMP CCF	1.00E-04	4.97E-02	1.05	4.98E+02	1.51
4	PB2	1.00E-05	4.97E-03	1.00	4.98E+02	1.05
5	PB3	1.00E-03	4.97E-04	1.00	1.50E+00	1.00
6	PB4	1.00E-03	4.97E-04	1.00	1.50E+00	1.00

The risk decrease factor is the ratio of the top event failure probability with the defined model parameters to the top event failure probability if that specific basic event has a zero failure probability. In simple examples, such as this one, this is easily relatable to the fractional contribution: for example OP2 contributes ~1/2 of the probability of top event failure, and the risk decrease factor is hence 2. The risk increase factor is the same ratio but with the specific basic event failure probability set to one. Sensitivity is the ratio of the risk decrease and risk increase factors.

The analysis has then been repeated but replacing the point estimate of 1.00E-03 with the discrete distribution given in Table 1 above. The minimum cutsets in this case are shown in Table 6 below:

Table 6: Minimum Cutsets for the Uncertainty Case

ID	Sequence Probability	Percentage Contribution	Event 1	Event 2
1	9.00E-04	62.1	PB1	
2	4.38E-04	30.2	OP1	
3	1.00E-04	6.9	PUMP CCF	
4	1.00E-05	0.69	PB2	
5	1.00E-06	0.07	PB3	PB4

Table 7 below shows the fractional contributions of basic events in the uncertainty case:

Table 7: Fractional Contributions of Basic Events for the Uncertainty Case

ID	Basic Event	Mean	Fractional Contribution	Risk Decrease Factor	Risk Increase Factor	Sensitivity (RIF/RDF)
1	PB1	9.00E-04	6.21E-01	2.64	6.90E+02	14.9
2	OP1	4.38E-04	3.02E-01	1.43	6.90E+02	5.11
3	PUMP CCF	1.00E-04	6.89E-02	1.07	6.90E+02	1.73
4	PB2	1.00E-05	6.89E-03	1.01	6.90E+02	1.07
5	PB4	1.00E-03	6.89E-04	1.00	1.69E+00	1.01
6	PB3	1.00E-03	6.89E-04	1.00	1.69E+00	1.01

Comparing Table 4 and Table 6 it can be seen that the importance ranking of the operator action is altered when uncertainty is included in the estimate. This type of permutation in the importance of cutsets is very significant since the analysis of cutsets is a primary method for understanding the plant risk, and providing input into risk informed decision making. In the list of fractional contributions of basic events (Table 5 and Table 7), there is a corresponding permutation in the ordering of basic event importance in the uncertainty case compared to the conservative case.

6. DISCUSSION

PSA models are filled with hidden examples of uncertainties that arise from uncertainties in the underlying analyses of physical processes that have been performed. The incorporation of uncertainties is not always as straight forward as in this case. For example some uncertainties could only be incorporated through changes to the structure of the model. For example if using a fault tree paradigm, then some uncertainties could only be incorporated by structural changes to the number of inputs to gates.

The observation arising from Section 5 is essentially a very simple one; that is that using a best estimate plus uncertainty to represent a failure parameter value can have significant effects on the risk profile of a model, and of the risk importance of cutsets. This is an obvious statement, but the insight and contribution of the paper really comes from the source of the re-assessment of the value of the failure parameter. The source is one that falls between domains of knowledge; the Relap analyst typically knows little about human factors analysis, and the human factors analyst rarely considers the details and implications of Relap analysis. The uncertainty that would be considered by quantitative human reliability methods is that associated with statistical uncertainty in the data used; and that uncertainty is only considered in the latest methods. This clearly misses the uncertainty considered in this paper, and as a result provides a misleading representation of having assessed the uncertainty; as noted by Zio and Aven [10], recourse to a quantitative evaluation method without detailed understanding of the underlying factors can easily lead to a misrepresentation of the risk results, and may place an unwarranted level of certainty about the results of the analysis

Hence the significant uncertainty considered included here would normally fall between the gaps of knowledge domains. The need for multi-disciplinary teams in general is, of course, well established, but appeals for multi-disciplinary collaboration are often vaguely justified or even presented as an end in itself, rather than serving a specific useful purpose. The type of observation made in this paper is one specific justification for increased interaction between diverse domain experts to allow high level understanding of how domains of knowledge interact. This gestalt understanding is important to nuclear safety.

7. CONCLUSION

There are many hidden conservatisms within the model structure of probabilistic risk models. The source of these conservatisms can often be traced back to a conservative interpretation of a supporting physical analysis. Often the conservative interpretation is a simplification of the actual analysis available and uncertainty is routinely calculated in many domains. This paper provides a joined up use of uncertainty for the purposes of risk assessment. This paper has presented a method to quantitatively incorporate uncertainty in human reliability due to underlying uncertainties in physical analyses. This type of uncertainty has not been quantitatively assessed before, but probabilistic models have instead relied on conservative judgements. Indeed this uncertainty remains largely hidden from view in probabilistic models, unless a joined up view of the analysis processes involved, including an understanding of the basic physical processes and how uncertainties in one sphere of knowledge can propagate through to other analyses in the course of risk analysis.

The uncertainty analysed here is also an example of how quantitative human reliability analysis can unwittingly hide uncertainties. This is true of all existing methods, even those which purport to estimate the uncertainty of operator reliability. The methods surveyed which do provide an estimate of uncertainty provide only an estimate of statistical variation between responses to controlled conditions. This is a useful factor to try to estimate but it is a misleading to portray this as a full characterisation of the uncertainty associated with the problem. Aleatory uncertainty is only the tip of the iceberg in terms of the uncertainties that contribute to human reliability. There is a significant body of work to be performed in identifying and, where possible, quantifying, latent uncertainties in human reliability assessment that have, to date, been masked by conservative judgements.

More generally the method presented here can be extended to conservatisms latent throughout probabilistic risk models. A model with numerous hidden conservatisms limits itself to make statements of the form “the risk is at least better than X”. Iteratively re-assessing conservatisms is a vital part of transforming risk analysis of hazardous plants and the type of statement that risk models can be used to make. This work is likely to modify our understanding of the overall risk profile of nuclear power plants, and as shown in this paper it can significantly affect our understanding of the risk importance of operator actions.

The contribution made here is one part of assessing model uncertainty. The assessment of model uncertainty in this sense could be expanded to all parts of PRA models using existing uncertainty estimates. This is similar in spirit to the uncertainty analysed in the case study of success criteria uncertainty for auxiliary feedwater pumps in Reference 2.

In addition to the uncertainty induced by time uncertainty, there is also uncertainty in the “effects model” used to represent the effect of time. That is, the correct form of equation 1 is unknown. This is another area for further work.

ACKNOWLEDGEMENTS

The author is very grateful to the EPSRC for funding and to Corporate Risk Associates for additional funding and technical support. Thanks to Rebecca Brewer for reviewing the paper and providing useful feedback. Thanks to Lavinia Raganelli for helpful discussions and feedback. The author would like to thank Dr Simon Walker, Dr Charles Shepherd and Jasbir Sidhu for their continuing support.

REFERENCES

[1] J. M. Reinert and G. E. Apostolakis, *"Including model uncertainty in risk-informed decision making"*, Annals of nuclear energy 33.4, pp354-369, (2006).

[2] J. K. Knudsen and S. L. Curtis, *"Estimation of system failure probability uncertainty including model success criteria"*, Proceedings of the 6th International Conference on Probabilistic Safety Assessment and Management (PSAM 6), Vol. 1, (2002).

[3] A. D. Swain and H. E. Guttmann, *“Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications”*, Final Report, NUREG/CR- 1278 SAND80-0200 RX, (1983).

[4] A. D. Swain, *“Accident Sequence Evaluation Program Human Reliability Analysis Procedure”*, NUREG/CR-4772, (1987).

[5] J.C. Williams, *“A Data Based Method for Assessing and Reducing Human Error to Improve Operational Performance”*, IEEE Fourth Conference on Human Factors and Power Plants, pp 436 – 450, (1998).

[6] Health and Safety Laboratory, *“Review of human reliability assessment methods”*, Health And Safety Executive, (2009).

[7] J.C. Higgins, J.M. O'Hara, P.M. Lewis, J.J. Persensky, J.P. Bongarra, S.E. Cooper, and G.W. Parry, *“Guidance for the Review of Changes to Human Actions”*, NUREG-1764, U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research, (2007).

[8] E. NonbØl, *“Description of the Advanced Gas Cooled Type of Reactor (AGR)”*, NKS/RAK2(96)TR-C2, RisØ National Laboratory Roskilde, Denmark, (1996).

[9] J.R. Lamarsh, A.J. Baratta, *“Introduction to Nuclear Reactor Theory”*, 3rd edition, Prentice Hall, (2001).

[10] E. Zio and T Aven, *“Industrial disasters: Extreme events, extremely rare. Some reflections on the treatment of uncertainties in the assessment of the associated risks”*, Process Safety and Environmental Protection 91, pp 31–45, (2013).