Challenges in Risk Informed Decision Making – Some Insights from the Nuclear Industry in Sweden

Erik Sparre[a] and Stefan Authén[b]
[a] Risk Pilot AB, Malmo, Sweden[*]
[b] Risk Pilot AB, Stockholm, Sweden

Abstract
This paper discusses uncertainties in applications and the challenges that arise when risk informed decisions are addressed. The expanded use of PSA in the integrated risk informed decision-making process requires that the PSA possesses certain features to ensure its technical consistency and quality. The paper gives examples of a number of challenges that can occur, for example how to handle conservatisms, simplifications, review and quality control, result interpretation and communication. The use of guidelines is discussed and the challenge of how to incorporate the recommendations from the large number of available guidelines is addressed. Further the paper addresses the challenge of documenting and controlling the different types of uncertainties that affect the outcome. In order to visualize the effects of uncertainties, three examples inspired from real events are presented.

Keywords: Decision making, Uncertainty, Applications, PRA

1. INTRODUCTION

Worldwide, PSA has recently been more broadly applied to support numerous applications and risk informed decisions on various design related, operational and regulatory issues. The expanded use of PSA in the integrated risk informed decision-making process requires that the PSA possesses certain features to ensure its technical consistency and quality, hence there are a number of challenges that need to be addressed. The ASME/ANS RA-Sa-2009 Standard, [2], sets forth the requirements for PSA used to support risk-informed decisions and prescribes a method for applying these requirements for specific applications. There are a number of challenges, which in general are covered by the ASME-standard, but nevertheless aren't always easy to address, such as:

- Conservatisms that may skew the results must be addressed. It is not always obvious how conservatisms should be handled. Increasing realism may for instance increase conservatisms. This may for example be the case when modelling spurious operations in fire PSA. As the capability category (using ASME) increases, the depth of the analysis also increases and when additional spurious operations are identified the calculated risk increases. This risk increase is subject to large uncertainties.
- Sometimes there is a need (or wish) to evaluate a design change, although the system in focus may be modelled in a simplified way. How should this be handled? Is there an acceptable way of using results from a simplified model or should the model in these cases always be expanded?
- How do we assure that the model used in a particular application is properly reviewed and understood? The application PSA-model is based on a reviewed and approved baseline PSA, where numerous man-hours have been used for quality assurance. The application PSA must be equally well reviewed in this aspect. A related problem is that the baseline PSA may have been developed by a different team that not necessarily still works with the particular PSA-model. Although the PSA documentation usually is extensive, there may be assumptions that

[*] erik.sparre@riskpilot.se

aren’t explicitly described, thereby increasing the risk of making model changes that may cause unwanted effects.

- How do we interpret the results, and can we trust the results to be accurate enough to be used? The results, cutsets, must be carefully reviewed so that the effect of the e.g. plant modification is understood. This may lead to an iterative process where further model changes are being made after interpretation of results. This also raises the question of how to use risk monitors. A risk monitor that continuously monitors risk – how can it be assured that certain risk level changes are relevant and not merely the effect of a conservatism (or non-conservatism) coming into play when the configuration is changed?
- How are results communicated in an efficient way?
- There are many standards and guidelines available on the subject; from IAEA, ASME, EPRI, NUREG etcetera. These sources provide many useful insights and recommendations; how do we assure that we use this information in our applications?

In this paper the above-mentioned challenges will be discussed, using insights from real examples.

2. STANDARDS AND GUIDELINES

There are several relevant frameworks and guidelines intended to support the work. Some examples are given below:

EPRI

- 1013491, Guideline for the Treatment of Uncertainty in Risk-Informed Applications: Applications Guide, 2006

- 1016737, Treatment of Parameter and Model Uncertainty for Probabilistic Risk Assessments, 2008

- 1026511, Practical Guidance on the Use of PRA in Risk-Informed Submittals with a Focus on the Treatment of Uncertainties, 2012

- 3002003116, An Approach to Risk Aggregation for Risk-Informed Decision-Making, 2015

IAEA

- INSAG 25, A Framework for an Integrated Risk Informed Decision Making Process, 2011

NRC

- NUREG 1855, Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making, 2009

NPSAG

- 51-001:01, Uncertainties in PSA Results, 2018

The guidelines present valuable insights and recommendations, but since the task of producing risk informed applications, considering uncertainties in a structured way, is very complex there is unfortunately not an easy way of handling uncertainties by using checklists etcetera. The number of guidelines is on one hand positive since there is a lot of available information. On the other hand, it may be difficult to select which guideline (or guidelines) to use.

3. ABOUT UNCERTAINTIES

Uncertainty are divided into aleatory uncertainty and epistemic uncertainty, where aleatory uncertainties are a stochastic uncertainty, which is the randomness, i.e. the basis of events and phenomena occurring (or not occurring). Aleatory uncertainty cannot be reduced by increased knowledge of the function being analyzed and is hence not further addressed in this paper. Epistemic uncertainty on the other hand describes uncertainty related to a lack of knowledge, information or methods, also known as "State-of-knowledge uncertainty".

When speaking of uncertainties, one generally means *epistemic* uncertainties and *parametric* uncertainties in particular. Parametric uncertainties relate to the analyst's confidence in the parameter values and are represented by uncertainty distributions. Most modern PSAs have distributions defined for the major part of the parameters used for calculating failure data, and the impact of parametric uncertainty on the analysis result, e.g. CDF, can be calculated by the PSA software. Hence, parametric uncertainty can be taken into consideration when using PSA for the cause of risk-informed decision making, e.g. suitable percentile of the CDF distribution can be used in order to demonstrate achievement of a certain risk criteria, or the CDF distribution can be transferred to another software for further analysis, e.g. to a simulation tool. Even though it may be challenging in some situations, there are to this day no real obstacles when considering parametric uncertainties in PSA applications, and it should be considered mandatory in any decision-making process.

The real challenge lies in taking the other two main areas of epistemic uncertainty into consideration in risk informed decision making; model and completeness uncertainties. Model uncertainty is introduced when several alternative approaches exist without anyone being considered superior. Sources to this uncertainty are the assumptions and simplifications made within the different PSA activities.
Completeness uncertainty concerns known and unknown conditions which will affect the result of the analysis but are not addressed. Hence, the sources to completeness uncertainty are found within limitations of the analysis' scope.

It may be somewhat of a sweeping statement, but historically these types of uncertainties have many times been ignored in PSA applications, and in any case, they have not been sufficiently addressed. Some part of this is due to limitations in methods, tools and technology, i.e. there are no obvious and/or reliable ways to evaluate the specific uncertainty. One example for instance is how to evaluate the uncertainty introduced by using static methods to describe dynamic sequences of events. To a large part however, the reasons for excluding the consideration of most, if not all, sources of model and completeness uncertainties from a PSA application are simply lack of time, budget and/or routines.

State-of-practice today is to log sources of uncertainties throughout the different parts of the plant PSA documentation without classification and ranking, and to select sensitivity cases to run based on engineering judgment (at best). With this approach it is impossible for anyone, with certainty at least, to identify the sources of uncertainty with the largest impact on the quantitative and qualitative results of the PSA. Of course, the robustness of conclusions concerning whether safety goals are met, the plants safety margins and possible plant improvements, will be questionable. When it comes to using the plant PSA for applications it is difficult to verify whether a PSA is suitable for a specific application or not, and the process of identifying the sources of uncertainty that needs to be addressed can be resource demanding.

The effort does not however need to be overwhelmingly large; the key lies in having routines in place for mapping, classification, ranking and documentation of all sources of model and completeness uncertainties when developing and updating the plant PSA. When this is the case, the choice of which sensitivity analyses to run in the plant PSA, and the identification of uncertainties that may affect the results of an application of the plant PSA, will be traceable and well substantiated, and in the latter case also performed within a manageable budget.

There are, as mentioned above, guidelines available which describes methods to achieve this, e.g. NUREG 1855 and EPRI 1026511. These guidelines can be perceived as somewhat extensive and difficult to penetrate, though when broken down into separate activities it comes clear that the methods are rather simple and straight-forward and not especially resource demanding once the routines are in place.

The work is further facilitated if/when all sources of uncertainty and their classifications are collected in a separate document of the plant PSA, or, even better, in a database. When a PSA application is performed, a copy of the uncertainty database (UDB) can be used for the necessary review of the classification of sources of uncertainties with respect to impact on the application case model, as well as specific case model(s). The UDB supplemented with actions performed to address significant sources of uncertainty, can then serve as part of the PSA application documentation.

At Forsmark NPP, Sweden, a process for treatment of uncertainties, both in plant PSA and in applications, has been developed based on the NUREG 1855 guideline. The process has successfully been implemented in an evaluation of allowed outage times in the Technical Specifications by use of PSA.

The Forsmark plant PSAs contains an UDB where all sources of uncertainties have been classified with regard to properties such as PSA activity, keywords, type of uncertainty, initial treatment (ignored, simplified modelling etcetera), estimated impact on the PSA (conservative/optimistic and degree of impact) and whether a consensus approach has been applied. Based on this information, a qualitative screening of uncertainties is performed, and unscreened uncertainties are ranked with respect to the impact on the PSA results. The highest ranked uncertainties are selected for sensitivity analysis, where further screening is performed in the case when low impact is shown.

When transferred to an application, the UDB is reviewed with regard to possible new uncertainties due to specific properties of the application. Classification and screening are performed for all new uncertainties, but also for all relevant old uncertainties since properties of the application may affect the impact of an uncertainty. The review needs to be performed for both application base models and specific application analysis case models.

Decisions on model updates necessary for achieving realistic results of the application, and/or need for sensitivity analyses, is based on an acceptance criteria for change in importance measures compared to the plant PSA, for all events with a significant risk contribution. The update of the application model(s) is performed with the goal to eliminate or significantly reduce the uncertainty. This is primarily performed with the use of simplified modelling, but in cases where this leads to unacceptable conservatism in the results, detailed modelling is applied. The process is iterative in several dimensions until specified criteria on realism is met and/or significant uncertainties have been reduced as far as possible/reasonable.

Sensitivity Analysis cases are defined for the application models if the uncertainty has not been addressed (modeled or screened) and may have a significant impact, or if the uncertainty has been addressed by simplified modelling.

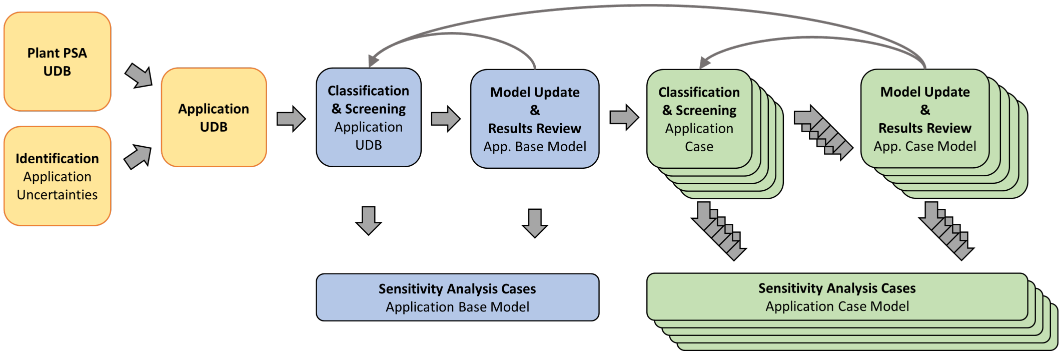

Plant PSA UDB
Identification Application Uncertainties
Application UDB
Classification & Screening Application UDB
Model Update & Results Review App. Base Model
Classification & Screening Application Case
Model Update & Results Review App. Case Model
Sensitivity Analysis Cases Application Base Model
Sensitivity Analysis Cases Application Case Model

Figure 1: Process at Forsmark NPP for treatment of uncertainties in applications.

4. EXAMPLES OF UNCERTAINTIES

As shown in the chapter above uncertainties can be classified based on their properties. Some uncertainties are easier to handle, such as parametric uncertainties, but often it is not obvious how an uncertainty should be handled, and the analyst is left to his/hers own judgement. In the following subchapters some examples are given in order to illustrate the complexity of the work.

4.1. Example No. 1

The first example is taken from an update of an analysis of external events where one of the analyzed events is *extreme snow*. The relatively new regulations from the authorities in Sweden [1], require that equipment should be verified to withstand loads from external events with a return period of 100 000 years, using state-of-the-art deterministic structural mechanic methods.

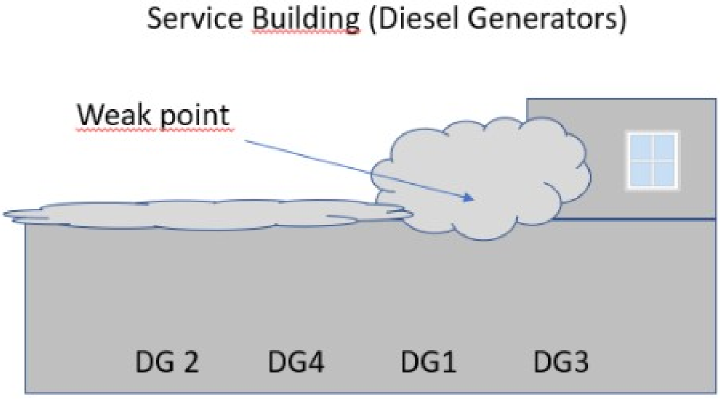
No details about these calculations will be given here, but in short, the evaluations are made by calculating the *utilization factor* (UF) for each affected structure. The UF is expressed as the ratio between the load and the resistance of the structure. Hence, in a deterministic analysis a UF >1 means that the structure cannot withstand the load, and UF ≤ 1 means that the structure can withstand the load. In order to quantify the results from the deterministic evaluation into the PRA-study, all conservatisms need to be considered and the value of the UF needs to be carefully considered. PRA-experts in co-operation with structural mechanical experts have been trying to quantify the results. As an example, it is more likely that a roof with a UF of 20 will collapse than a roof with a UF of 1.01. In conclusion, the results from these assessments have been transferred into failure probabilities for different scenarios involving the buildings.

The figure below shows a sketch of the service building housing the diesel generators. The calculations have given that the roof may collapse if a “snow pocket” forms, as in this case either one or two diesel generators may be damaged[†]. Probabilities for each scenario have been assigned, but obviously, even though the results are based on state-of-the-art calculations, the results contain large uncertainties.

It is of course undesirable to have large uncertainties regarding important initiating events, heavy snowfall is generally of interest in Swedish PSA, but what is worse in this case is that the uncertainty causes an “unbalance” in the overall uncertainty picture of the plant.

Figure 2: Snow Formation on Service Building

[†] The roof of the service building will shortly be considerably reinforced.



From the figure it is obvious that not all diesels are affected by the snowfall, the diesel 2 and 4 are judged to be placed in such a way that they are safe. The diesel 1 and 3, on the other hand, may be damaged in the case of a collapsing roof which means that 1) the failure data for these diesels are significantly larger and 2) that the uncertainty distribution for the total failure probability is considerably wider (larger error factor in the case of a lognormal distribution). In the studied case, the NPP is a three-loop Westinghouse PWR and this plant has a mix of two, three and four train safety and support systems. Without going into details about the structure of the PSA-model, the results depend on the chosen configuration (which trains that are in operation), which in turn means that the uncertainty of the result is dependent on the configuration.

This is bad news for two reasons. Firstly, since the uncertainty is dependent on the configuration, the analyst needs to be very careful when analyzing the results. The use of online risk monitoring becomes complex when changes in plant configuration may cause changes in the instantaneous core damage frequency which are not necessarily relevant. Secondly, the uncertainty is very hard to remove. The whole practice of transferring results from structural mechanic calculations into failure probabilities is a time consuming and difficult activity.

When performing applications, the uncertainty may be assessed by evaluating several different configurations of running trains and elaborating with the probabilities of failing building structures. The analyst may also consider excluding the analysis of the external events, depending on the situation.

4.2. Example No. 2

The second example concerns the modelling of electrical dependencies. In modern PSAs, all dependencies needed for activation and power supply are modelled in detail, meaning that the fault tree pages for e.g. electrical pumps include transfers to underlying busbars of different voltage levels. Power to the electrical motors belonging to safety systems are usually provided via diesel-backed busbars, typically between 500 V and 6 kV. Control voltages needed for the actuating of components are often supplied from battery-backed busbars of lower voltages. These busbars are in turn provided from the diesel-backed busbars.

In addition, the model may credit that there is a large chance that the offsite power can return in case of an initial loss of offsite power. The modelling of the electrical system is therefore complex, and in order to correctly capture how power is provided during a disturbance or accident sequence, there is a need to divide the power supply in different “time windows”, where different sources of electrical power are present at different points in time. This fact might be realized creating a set of fault trees for every individual busbar, for instance:

- Fault tree representing power supply the first 4[‡] hours where return of offsite power isn't credited.
- Fault tree representing power supply during the period 5-24 hours where return of offsite power is credited.
- Fault tree representing a battery backed busbar where the batteries are credited, e.g. the first 4 hours and hence connected to the corresponding diesel backed busbar.
- Fault tree representing a battery backed busbar where the batteries are not credited, e.g. the period 5-24 hours.
- Fault tree representing a battery backed busbar where only batteries are credited used for the initial diesel activation after a grid failure.
- Other special cases.

When modelling the power supply to motors and control circuits for a particular motor (belonging to a valve, pump, compressor, fan, etcetera) the analyst needs to consider when the component is needed. Some safety functions are obviously needed immediately, such as reactor trip breakers or opening of relief valves, but other functions or components are needed later in the sequence, such as activation of the residual heat removal system. In these cases, it is straightforward to assign the correct fault tree representing power supply.

In other cases, the same component may be needed, for different reasons, during the sequence. Regarding certain PWRs such a component is the charging pump that is used for a number of functions, such as RCP[§] seal water injection, charging and high pressure safety injection. Therefore, in order to capture the electrical dependencies correctly, there is a need to create different fault tree pages for the same pump depending on which safety function the pump is part of. In the studied PSA-model this hasn't been done, instead the same fault tree is used for several safety functions and in order to be conservative batteries are never relied upon for starting the standby pumps (since the batteries may be depleted if the actuation is needed late in a sequence).

Usually this conservative assumption has a minor effect on the overall calculation of the core damage frequency. When investigating the importance of different power sources, this simplification is however yielding unrealistic results which needs to be addressed. The good news is that it is relatively straightforward (albeit maybe time consuming) to remove and also easy to find when studying the cutset list.

Some might say that this example isn't an example of modelling uncertainty, but instead that the model is "wrong". However, since the task of performing a PSA of a nuclear power plant is a very complex and time-consuming task, it is necessary to make simplifications throughout the work. Otherwise the scope would be unacceptably large. The common strategy is thus to make certain wise simplifications when needed, noting them in a list/database of modelling assumptions to be addressed whenever possible. The assumptions and simplifications therefore lead to an overall *uncertainty* that needs to be considered.

4.3. Example No. 3

Some disturbances are such that the available time before an undesired consequence occurs is long. Such an event can for instance be loss of cooling of a spent fuel pool where the operators have several hours before boiling occurs and even days before fuel uncovery. Historically these events have not been analyzed with the same effort as events related to core uncovery during power operation or low power modes. The Fukushima accident nevertheless confirmed the importance of examining all possible strategies to ensure cooling of the spent fuel pool and several research programs are therefore ongoing to learn more about these kinds of accidents from many perspectives. From a PSA point-of-view, the most important challenges are related to the possibility of crediting recoveries and repairs

[‡] 4 hours are chosen arbitrarily in this case

[§] Reactor Coolant Pump, RCP, used for circulating the primary coolant in a PWR.

and also the use of HRA-methods suitable for handling long grace times. For example, the Nordic PSA Group (NPSAG) has initiated the "PROSAFE"-project where these issues will be investigated.

There is thus reason to believe that the PSA-models regarding spent fuel pools will be improved, but still the uncertainties will continue to grow large when calculating frequencies for undesired events. Due to the long grace time, and that different strategies exist in order to cope with a cooling failure, the calculated frequencies will be very low and therefore the need for further refining the analysis may be limited if a conservative approach can verify that safety goals are met. This means that the model of the spent fuel pool can be of limited use in applications. If, for example, the importance of power supply (1 or 2 connections to the offsite grid) is of interest, the result is "fuzzy" with regard to fuel damage. If probabilistic methods at all should be used, the analyst may therefore need to consider different measures, such as the reliability of the power supply to the cooling pumps.

The uncertainty is thereby handled by moving the focus to a consequence where the uncertainties are significantly lower. In order to make a complete assessment regarding reactor safety, such a reliability analysis must be complemented with deterministic considerations on how the overall risk picture is affected with regard to the principles of maintaining consistency with the defense-in-depth philosophy, safety margins etcetera (as pointed out in e.g.[3]).

4. DISCUSSION AND CONCLUSIONS

Six examples of challenges were presented in chapter 1 and these will be discussed below.

1. Conservatisms. The conservatisms that are important to a specific application must firstly be identified. This step is facilitated by having a proper uncertainty database where all assumptions etc. are noted. In some cases, conservatisms may be possible to remove by refining particular parts of the model. In other cases, it may be harder to actually remove the conservatisms and a set of properly defined sensitivity cases need to be defined.
2. Evaluation of design changes where the system in focus are modelled in a simplified or conservative way. It is obviously desirable to always use a realistic and fully developed model, but in some cases it is difficult to improve the model well enough. One of the presented examples in this paper addressed an evaluation of a spent fuel pool, where a realistic core damage frequency is hard to calculate, mainly due to that the loss of cooling results in a slow scenario giving the staff plenty of options to handle the situation. One approach is therefore to analyze "loss of power" instead of core damage if the proposed design change involves changes in the configuration of power supply.
3. Review of an application model. One important challenge is that the base model often has been developed continuously over many years by different teams. Although each PSA is thoroughly documented there may still be important assumptions and limitations that are not obvious to the team developing or reviewing the application model. One important measure to handle this is to use an *Uncertainty Database*, i.e. a database including all relevant assumptions and limitations. The importance of having the (known) uncertainties gathered into a database cannot be stressed enough. The PSA-documentation contains a large number of reports such as data, sequence and system analyses. Within the reports, assumptions, limitations and uncertainties are noted when relevant, and most vital information is probably captured. The problem is however that the information is spread out through many reports, and also that not necessarily all uncertainties are clearly documented. In the worst case, some information exists purely inside the head of key staff. If a utility wants to use the model for applications, one early step must be to gain control of the modelling uncertainties.
4. Interpretation of results. Evaluation of results (cut sets) are stressed in all guidelines concerning PSA in general. This is very important when it comes to applications, since it must be verified that the observed changes are "real" and not the effect of a conservatism coming into play. The work is in nature iterative and a number of changes are often needed, introduced step-by-step as the analyst review the results. It is worth mentioning that this is of particular interest when using risk monitors. One basic idea of risk monitoring is to quickly be

able to observe changes in risk profile if the system configuration is changed. Before launching a risk monitor it must therefore be verified that the model doesn't include conservatisms that are dependent on e.g. which trains that are in operation.

5. Result communication. Substantial effort must be made in explaining the results in detail so that the effect of the e.g. design change is highlighted. It is also important to include a discussion on how the change affect the plant with regard to the principles of maintaining consistency with the defense-in-depth philosophy, safety margins etcetera.
6. Guidelines. Based on experiences from working with numerous applications of various kinds, it is the author's opinion that it is very difficult to create a complete manual on how to assess uncertainties in PSA-applications since every situation is unique, and for each application the analyst needs to have a thorough understanding of how the model works and what the limitations are. This is the situation even if the uncertainties are documented in a structured way. Nevertheless, it is important to capture all the insights that are given in the guidance documents and it is hence recommended that each organization makes an effort in reading available guidelines, and from this makes a choice of either using one (1) as a basis or extracts all relevant recommendations, and use this as input to produce a guidance document valid within the organization, and that is consistent with National standards and regulations.

Acknowledgements

The authors would like to thank Ringhals and Forsmark NPP for providing relevant material and technical input.

References

1. SSMFS 2008:17, "The Swedish Radiation Safety Authority's Regulations concerning the Design and Construction of Nuclear Power Reactors", Stockholm, 2008
2. ASME/ANS RA-Sa-2009, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," Addendum A to RA-S-2008, ASME, New York, NY, American Nuclear Society, La Grange Park, Illinois, February 2009
3. NRC, RG 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis", Washington DC, 2018
4. NRC, NUREG-1855, "Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making", Washington DC, 2017