Unclassified **NEA/SEN/SIN/SMAP(2006)3**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development **30-Aug-2006**

English - Or. English

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/SEN/SIN/SMAP(2006)3
Unclassified

Task Group on the CSNI Safety Margins Action Plan (SMAP)

SMAP TECHNICAL NOTE

Task 3: Safety Margin Evaluation Methods

JT03212857

English - Or. English

FOREWORD

Recent NPPs operating experience shows that in some cases operational and design modifications may lead the plant far away from the original design. Power uprates, life extension or increased fuel burnup as well as cumulative effects of simultaneous or subsequent design changes in a plant, which can be larger than the accumulation of the individual effects of each change, can challenge original safety margins while fulfilling all the regulatory requirements. It has been recognised that currently used methods for safety analysis may not be sufficient to guarantee that enough safety margin exists.

To address this problem the CSNI approved in December 2003 an Action Plan on Safety Margins (SMAP) and established an international Working Group aimed at developing a framework for integrated assessments of the changes to the overall safety of the plant as a result of simultaneous changes in plant operation/conditions. The SMAP plan consists of five tasks:

Task 1 : Definition of Safety Margins and Related Concepts
Task 2 : Assessment Process for Safety Margins
Task 3 : Safety Margin Evaluation Methods
Task 4 : Quantification of Safety Margins
Task 5 : Preparation of a CSNI Guidance Document.
This Technical Note, which represents a SMAP working document, is the result of the SMAP Task 3 - Safety Margin Evaluation Methods consisting of

Sub-Task 3A: Methods used to estimate the dynamic behaviour of the plant under accident conditions
Sub-Task 3B: Guidance on Application of Computational Analysis to Define Safety Limits, including Uncertainties and Non-Linear Effects
Sub-Task 3C: Methods for frequency quantification, including uncertainties, of sequences and damage states
Sub-Task 3D: Examples of methods applied

Although this paper is an outcome of extensive discussions of the whole SMAP Group, the special appreciation belongs to A. Prošek (Institut "Jožef Stefan", Ljubljana, Slovenia) who provided the first outline of this document and J. Hortal (CSN, Spain) and M. Gavrilas (US NRC), who provided contributions to document and valuable written comments.

TABLE OF CONTENTS

1. INTRODUCTION

Recognizing that computational methods and tools are necessary elements for any approach to safety margin assessment or evaluation, SMAP Task 3 has been devoted to identify, summarize and provide general guidance on suitable tools currently used or potentially applicable to safety margin problems. The scope of these computational tools includes plant simulations, determination of safety acceptance criteria and frequency evaluations, corresponding to Sub-tasks 3A, 3B and 3C, respectively. Examples of methods applied are also given corresponding to Sub-task 3D. A very important concern in the use of any of these tools is a proper consideration of the uncertainties involved in the calculation process. Inadequate treatment of uncertainties may lead to poorly supported or even wrong conclusions whose final consequence is a loss of adequate level of safety.

2. CLASSIFICATION AND SEPARATION OF UNCERTAINTIES

2.1 Classification of uncertainties

It is the state of the art in many applications of safety analysis to discriminate between two fundamental types of uncertainty: the **aleatory** and the **epistemic** uncertainty.

Aleatory uncertainty results from the effect of "inherent randomness" or "unpredictable variability". It is element of the modeled phenomenon and is therefore also called *inherent, natural, ontological, irreducible, stochastic etc.* uncertainty. It represents the indeterministic and unpredictable random performance of the system and its components and can, roughly speaking, be associated with the question "*what can happen?*".
Aleatory uncertainty is quantified by probability. Probability of an event is considered as a quantitative measure of the "chance-of-occurrence" of that event. The "frequentistic" concept of probability interpretation is therefore appropriate: probability ≈ "relative frequency in a large number of independent random trials". Variables subject to aleatory uncertainty are random in nature. They have intrinsic probability distributions which represent "random laws" and which can be derived from statistical observations.
Aleatory uncertainty is directly addressed in Probabilistic Safety Analysis (PSA) to quantify the "chance of occurrence" of a system failure, i.e. to express probabilistically how safe the system is.
Principal sources of aleatory uncertainty in nuclear safety analyses are:

- Occurrence of accidents
- Initial conditions (state) of the plant at the beginning of an accident
- Performance of system components and humans during an accident.

Epistemic uncertainty results from the "imperfect knowledge" or "incomplete information" regarding values of parameters of the underlying model. It is also called *state-of-knowledge, subjective, reducible etc.* uncertainty. The uncertain parameters as such are deterministic in nature, i.e. they have an invariable, fixed, appropriate, right, true value, which is not precisely known. Epistemic uncertainty can, roughly speaking, be associated with the question "*which value is the right one?"*. It can be reduced, at least in principle, or even eliminated by improving the state of knowledge, e.g. by more investigations, experiments, research.
Epistemic uncertainty can also be quantified by probability. Probability distributions associated with uncertain parameters represent the "state of knowledge" about the "right" values of the parameters and are therefore very often derived from expert judgment. The "subjectivistic**"** concept of probability interpretation is appropriate: probability ≈ "degree of belief or confidence that a statement is true".

Epistemic uncertainty is directly addressed in Uncertainty and Sensitivity Analyses of results from deterministic as well as probabilistic computational models. Such analyses quantitatively express how imprecise the result of the computation is and which are the principal sources of this imprecision.

In nuclear safety analyses epistemic uncertainty is principally due to approximation, simplification, incompleteness, lack of information, etc. E.g.:
Approximations made in developing the governing conservation equations, including averaging over (often fairly large) volumes (uncertainty due to approximation).
Codes do not have models for various physical phenomena, such as local mixing and thermal stratification, viscous shear effects, turbulence effects on flow patterns, diffusion, vorticity, etc. (uncertainty due to incompleteness and/or simplification)
Model uncertainty represented by parameters (uncertainty due to simplification)
Geometry, material properties (uncertainty due to lack of information, simplification)
Additional specific epistemic uncertainties appear in probabilistic calculations: Uncertainties in distributional parameters of aleatory variables, e.g. component failure rates/probabilities accounted for in traditional PSA (uncertainty due to lack of information).

2.2 Separation of uncertainties in probabilistic safety analyses

In many safety relevant applications of computational models both types of uncertainty are present. The underlying computational model must therefore be complemented by a probabilistic model for the aleatory and epistemic uncertainties comprising the probability distributions for both types of variables and the complete structure of dependences between them.

It is now increasingly recognized and accepted that in such cases the two types of uncertainty must be distinguished very carefully and treated separately. The separation must be maintained throughout the analysis and appropriately displayed in the final results.

This may be seen from the following consideration:

It may intuitively be argued that the safety of a system as such, i.e. its reliability performance represented by a probabilistic quantity like failure probability or expected core damage frequency in a PSA, must be independent of anybody's state of knowledge or information. It is therefore due solely to the aleatory uncertainty, i.e. to the random performance of the aleatory variables involved in the computational/probabilistic model of the system. Hence, solely the aleatory variables with their probability distributions may directly be involved in the probabilistic quantification of the system safety via quantities like failure probability or core damage frequency. However, due to the effect of epistemic uncertainties, such probabilistic quantities cannot be determined precisely. Their right values remain unknown to the extent to which the right values of the epistemic variables are unknown. Thus, the epistemic uncertainties can solely contribute to the precision with which probabilistic quantities like failure probability or core damage frequency can be determined, i.e. to the state of knowledge about the probabilistically expressed system safety but not to the system safety as such.

In other words: the analysis of aleatory uncertainty can tell us how safe is the system as such, whereas the analysis of epistemic uncertainty can tell us how well do we know that.

Thus, since the two uncertainty types contribute to different kinds of statements, it is clear that they must also be treated separately in different ways. A recognized and consistent approach of uncertainty separation is the so-called "two-dimensional nested" probabilistic analysis:

- the epistemic uncertainties are treated directly in the "outer" probabilistic analysis "loop" (usually with Monte-Carlo simulation methods),
- the aleatory uncertainties are treated in the nested "inner" probabilistic analysis "loop" by the underlying computational/probabilistic model (usually with (a) pure Monte-Carlo simulation methods or (b) analytical-approximate methods like Fault- and Event-Tree or FORM/SORM or (c) combined methods like Monte Carlo Dynamic Event Tree (MCDET) in dynamic PSA).

Specifically, in most applications the "two-dimensional nested" probabilistic analysis may be performed in the following way:

1) Generate values of the epistemic uncertain parameters randomly from the respective distributions. Insert these parameter values into the underlying computational/probabilistic model. Thus the resulting restricted model will contain only aleatory uncertainties.
2) Perform the corresponding conditional (aleatory) probabilistic analysis with the restricted model. This can be accomplished in various ways depending on the type of problem and the computational/probabilistic model at hand. The most appropriate methods are e.g.
   - pure Monte-Carlo simulation methods (for computationally "cheap" models),
   - analytical/approximate methods like Fault- and Event-Tree analysis in traditional PSA or FORM/SORM methods in structural safety,
   - mixed methods, like MCDET which combines Monte-Carlo sampling with Event-Tree analysis ("dynamic" PSA).

   In each case the analysis will provide the corresponding conditional aleatory probabilistic results of interest given the parameter values from step 1, e.g. results in form of :

   - the conditional expected core damage frequencies determined analytically by Fault- and Event-Tree analysis in traditional PSA, or
   - the conditional failure probability determined analytically e.g. by FORM/SORM methods in structural safety, or
   - the (approximate) entire conditional aleatory probability distribution function of a safety relevant quantity of interest like peak clad temperature (PCT), determined e.g. by pure Monte-Carlo simulation methods or by mixtures of simulation and analytical methods e.g. in "dynamic" PSA with MCDET.

3) Repeat all previous steps independently N times.

A direct result of such two-dimensional epistemic/aleatory probabilistic analysis will be a sample of (aleatory) probabilistic results from the inner analysis loop, e.g. a sample of expected core damage frequencies, or of failure probabilities, or of entire aleatory (approximate) probability distribution functions for the safety relevant quantity of interest.

This sample represents the epistemic probability distribution for the specific (aleatory) probabilistic result from the inner loop analysis. It quantifies the state-of-knowledge uncertainty about the probabilistically expressed system safety and can be statistically analyzed in various ways.

E.g. for a safety-oriented probabilistic analysis usually the 95%-quantile of this (epistemic) distribution will be of interest. It can be interpreted as the value, which covers 95% of the epistemic uncertainty in the probabilistic quantification of the system safety. An upper bound for this quantile can be determined even from small samples by the well-known tolerance limit approach if the underlying model is expensive to run. The entire two-dimensional epistemic/aleatory probabilistic analysis will thus be condensed in a single number: an upper bound covering e.g. at least 95% of the epistemic uncertainty in

the probabilistic quantification of the system safety with a statistical confidence of at least 95% due to the limited sample size. It is well known that for such statements a sample of size of at least 59 is necessary, i.e. 59 independent repetitions of the probabilistic analysis in the nested "inner" probabilistic analysis "loop".

The "two-dimensional nested" probabilistic analysis approach is for a long time a common practice in traditional "Probabilistic Safety/Risk Assessment" (PSA/PRA) for nuclear power plants. The actual objective of a PSA/PRA as such is to quantify aleatory uncertainties, i.e. to express the system safety probabilistically e.g. in terms of expected core damage frequencies determined by Fault- and Event-Tree Analyses. The computational model underlying a traditional PSA consists essentially of binary functions in binary variables (Boolean expressions) representing the performance of the entire system as a function of the performance of its components. The quantification of the corresponding epistemic uncertainties ("outer loop") is conducted routinely by Monte-Carlo simulation of the Fault- and Event-Trees taking into account only the epistemic uncertainties in the probabilistic reliability parameters of the system components, i.e. uncertainties in failure rates and in failure probabilities per demand.

A "two-dimensional" probabilistic analysis is also increasingly performed in safety analyses of nuclear waste disposals.

However, it is immediately clear that the computational effort for a full "two-dimensional nested" probabilistic analysis may not always be feasible, particularly when the underlying models are computationally expensive as is often the case in nuclear safety analyses.

But it is also clear that it would not be appropriate to ignore the necessity of uncertainty separation and to perform a single, "cheap", "one-dimensional" probabilistic analysis with both uncertainty types treated in the same manner. The results of such analysis can be difficult to interpret, misleading or even completely wrong.

A full "two-dimensional nested" probabilistic analysis may sometimes be circumvented by the so-called "conservative" treatment of either aleatory or epistemic uncertainties. In such cases either all aleatory or all epistemic variables are replaced by the corresponding appropriate "conservative" values such that only a single "one-dimensional" (either aleatory or epistemic) probabilistic analysis has to be performed. It is clear that the results of such analysis have a rather restricted bounding character.

A conservative treatment of both types of uncertainty, i.e. when both aleatory and epistemic variables are replaced by the corresponding conservative values, requires only a single deterministic calculation. However, it is clear that such calculation may provide extremely conservative results.

3. GENERIC APPROACHES IN THE NUCLEAR INDUSTRY

To make an adequate determination of safety margin in either design basis or risk space requires that both the code predictions and the acceptance criteria be determined with sufficient accuracy and that the uncertainty in each is quantified in a usable format. Here, the set of design basis accidents (DBA) is named design basis space. Design basis accident is in IAEA Safety Report Series No. 23 [1] defined as accident conditions against which an NPP is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits. On the other hand, the set of all possible scenarios having non-negligible frequencies of occurrence is named the risk space. Whether the analysis is performed for design basis or risk space applications, deterministic code predictions must be made. The number of cases and the amount of detail will vary, but nevertheless, system codes will be used to simulate plant response to various simulated events in either case. A number

of system codes are available for deterministic analyses including CATHARE, RELAP5, ATHLET, TRAC, CATHENA and TRACE.

In addition, more specialized codes such as fuel behavior codes or containment codes are also needed to evaluate to evaluate safety margins in relation to several fuel-related limits as well as to containment limits. A number of codes are publicly available, e.g. FRAPTRAN, FALCON, TRANSURANUS for fuel behavior analysis, GOTHIC, CONTAIN, MAAP, MELCOR for containment analysis. The following considerations can be easily applied to these categories of codes.

The first step is to assure that the code is applicable for the analysis to be performed. That is, it includes the physical models needed to represent the phenomena that have been identified as highly ranked. If multi-dimensional effects are important, the code should include these in an acceptable manner. One criterion to apply is to determine whether the code has been used in the past for similar applications and whether it has been qualified against relevant experimental data.

User guidelines are available for each code that provide examples of how to develop a plant model. While these guidelines are a necessary tool, they are not sufficient to allow an inexperienced code user to complete a plant model. Training and participation in collegial meetings to share experiences with other users is essential for the code practitioner. There is a significant code user effect, i.e. variation in code results for the same simulation that remains even among very experienced users.

Other essential elements of the model development process include an understanding of the code limitations and the need to perform nodalization and numerics (i.e. time step size, convergence criteria, solution method) sensitivity studies. These studies improve the quality of the results by demonstrating a converged solution and by providing information on the uncertainty that results from the choice of nodalization and solution technique.

In order to identify and reduce the effects of inadequate nodalization schemes, use of physical models outside their applicability range, inconsistent options in different physical models and other sources of avoidable errors in code calculations it is essential to verify that the code results are compatible with the physical models, i.e., with the set of equations supposedly solved by the code. Post-processing techniques have been developed to check this consistency, allowing to distinguish between uncertainty in the calculation and modelling errors often included under the concept of "user effects". Reference 2 provides guidance on the application of these post-processing techniques.

Applicability of the code for the intended application is established by adequate assessment against experimental data. The CSNI has published extensive separate effects [3, 4] and integral effects [5] test matrices that provide information on existing experimental data.[1] The test matrices include a set of information sheets that briefly describe the capabilities of each test facility and the range of its test programme. The matrices collect together in a systematic way the best sets of test data for code validation, assessment and improvement. While these data have been used to assess and improve the system codes listed above, the user should not rely solely on the work in this area performed by others. As a minimum, the user should set up a model or models for an integral facility/ test cases that are similar to the application at hand to assure that the modeling techniques used for the plant model will adequately predict the test data. Additional assessment against separate effects tests that exhibit the phenomena identified as being important for the application is also prudent. The guidelines above are applicable to any of the current deterministic methods.

[1] Similar information is also available for fuel behavior, e.g. NSC's International Fuel Performance Experiments (IFPE) Database.

The deterministic methods used to estimate the dynamic behavior of the plant under accident conditions can be summarized as follows:

- very conservative (Appendix K approach for LOCA),
- best estimate bounding,
- realistic conservative,
- best estimate plus uncertainties (BEPU).

Similar classification was done in the IAEA document [6] where the transient analyses for licensing purposes were identified as shown in Table 1. The very conservative method agrees well with IAEA no. 1 safety analysis approach, realistic conservative with IAEA no. 2 and BEPU with IAEA no. 3. The IAEA no. 4 safety analysis approach has not yet been used. It is connected with risk-informed regulation.

The "best estimate bounding" approach is very similar to realistic conservative, except that in the latter besides conservative initial and boundary conditions with respect to licensing parameters some other conservatism is added by penalizing code models (for example the Deterministic Realistic Model), using plant operating parameters at their bounding limits for full power operation, or taking values of code parameters to penalize the results.

Table 1: Safety analysis approaches for licensing purposes [6]

ID	Applied Codes	Input & BIC (Boundary and Initial Conditions)	Assumptions on systems availability	Approach
1	Conservative codes	Conservative input	Conservative assumptions	Deterministic
2	Best estimate (realistic) codes	Conservative input	Conservative assumptions	Deterministic
3	Best estimate codes + Uncertainty	Realistic input + Uncertainty	Conservative assumptions	Deterministic
4	Best estimate codes + Uncertainty	Realistic input + Uncertainty	PSA-based assumptions	Deterministic + probabilistic

Important information on uncertainty analysis methods was given at the special OECD/NEA workshop, London 1-4 March 1994 [7], where eight new methods were presented: CSAU, UMAE method (Uncertainty Methodology based on Accuracy Extrapolation, Italy), AEA method (Atomic Energy Authority, UK), NE Method (Nuclear Energy, UK), GRS method (Gesellschaft für Anlagen- und Reaktorsicherheit, Germany), IPSN method (Institut de Protection et de Sureté Nucleairé, France), Tractebel method (Tractebel, Belgium) and Limit value approach (ABB, USA). For the details the reader can refer to the reports [7, 8]. In the following each of the safety analysis approaches will be briefly described.

3.1 Very conservative approach (Appendix K)

Historically the initial licensing procedures that governed analysis were established in 1974 when the USNRC published rules for loss-of-coolant accident (LOCA) analysis in 10CFR 50.46 and Appendix K [9]. Analysis following these rules is known as the (very) conservative approach. It is the first one used in safety analysis. The basic reason for developing the conservative method has been the need to make

allowance for the lack of knowledge of physical phenomena. It is an approach based on the notions of consequences (maximisation) and criteria (restrictive).

10CFR 50.46 established the primary safety criteria for peak cladding temperature (PCT), maximum cladding oxidation, maximum hydrogen generation, coolable geometry, and long-term cooling (these remain unchanged today in the US). Emergency core cooling systems (ECCS) cooling performance is evaluated using a computer code model. Appendix K to Part 50 establishes required and acceptable features of the evaluation model. Discussion of the relative importance of the various features of Appendix K is of course not found in Appendix K nor in the documentation of that time. Since then, several studies have been carried out to provide some information in this regard [10]. For LBLOCA the most important features appeared to be use of high peaking factors, lockout of return to nucleate boiling, steam-only cooling during reflood and bounding decay heat. For small-break (SB) LOCA these were the single failure criterion and bounding decay heat.

Problems raised by the conservative approach are: a) there is no way to prove that the conservatisms that are verified on scaled down experiments are also valid at full scale reactor size; b) due to nonlinearity, the additivity of several conservative measures cannot be verified and c) the method is inappropriate for emergency operating procedures (EOP) studies (especially obvious after TMI2 accident). All these limitations have been the motivation for developing best estimate codes.

3.2 Best estimate bounding

In the best estimate bounding approach, the best estimate computer code is used while the uncertain input parameter values are selected conservatively to bound the parameter of interest.

This approach represents the uncertainties by taking upper bounds for the ranges of uncertain parameter values. The approach has many similarities with best estimate plus uncertainties. However, the major difference is that instead of quantifying the impact of input uncertainties the result is expected to be bounded.

One of the major limitations of such methods is that they may involve unquantifiable over conservatism due to the linear combination or bounding of all conservative assumptions. Sometimes, the final licensing results are comparable with or even more conservative than the Appendix K type approach.

The bounding best estimate approach using SECY-83-472, as licensed by Westinghouse and General Electric, is no longer allowed in USA.

3.3 Realistic conservative

Current licensing practice in many countries consists of using conservative boundary and initial conditions and assumptions as input for a best estimate or realistic code. It is believed that in this way all other uncertainties are adequately covered.

3.4 Best estimate plus uncertainties (BEPU)

Original criteria for LOCA were formulated at a time when limitations in knowledge made conservative approaches necessary. Research conducted during 1974-1988 provided a foundation sufficient for the use of realistic and physically based analysis methods [11]. A large number of experimental programs was completed internationally. Several advanced best estimate computer codes were developed in parallel with experiments for replacing conservative evaluation models: RELAP, TRAC, COBRA-TRAC, RETRAN, CATHARE, ATHLET etc. Based on these research results the United States Nuclear Regulatory Commission (USNRC) initiated an effort to develop and demonstrate a best estimate (BE) method acceptable for licensing which could bring benefit to nuclear plant operators (less conservative, consideration of uncertainties, economic gains). In September 1988, the NRC approved a revised rule for the acceptance of emergency core cooling systems (ECCS) [12]. The revised rule for ECCS evaluation contains three key features: the original acceptance criteria were retained; evaluation model methods based on Appendix K may continue to be used as an alternative to best estimate methodology; and an alternate ECCS performance, based on BE methods, may be used to provide more realistic estimates of plant safety margins, provided the licensee quantifies the uncertainty of the estimates and includes the uncertainty when comparing the calculated results with prescribed acceptance limits. It is required with a high level of probability that the criteria would not be exceeded while it is not prescribed how to account for uncertainties. The Code Scaling, Applicability, and Uncertainty (CSAU) method was developed [13] and demonstrated for LBLOCA in a pressurized water reactor (PWR) [14]. After the pioneering CSAU, several new methods were developed which were presented together at a special OECD/NEA/CSNI (Organisation for Economic Cooperation and Development/Nuclear Energy Agency/Committee on Safety of Nuclear Installations) workshop on uncertainty analysis methods in 1994 [7]. One of the objectives of the workshop was also the preparation of the uncertainty methodology study (UMS). In the UMS study (1995-97) five uncertainty methods were compared [15]. The OECD/CSNI workshops in Annapolis-1996 [16], Ankara-1998 [17] and Barcelona-2000 [18] also dealt with uncertainty evaluation methods. More recently, the BEMUSE task group (in the framework of CSNI/GAMA) undertook during the first 3 phases a quantitative comparison of different uncertainty evaluation methodologies, based on the LOFT L-2-5 experiment. The reports documenting this effort are to appear shortly. The international conferences Best Estimate 2000 and 2004 were also held.

The developed methods significantly differ in the way that uncertainties were quantified. Different techniques for the uncertainty propagation in best estimate thermalhydraulic code calculations were identified, including Monte Carlo analysis, Response Surface (RS) methods and statistical tolerance limits [19]. In the following each of the techniques will be briefly described.

3.4.1 Monte Carlo analysis

In Monte Carlo analysis, a probabilistically based sampling is used to develop a mapping from analysis inputs to analysis results. This mapping then provides a basis for both the evaluation of the probability (i.e. uncertainty analysis) and the evaluation of the effects of individual input parameters on output parameters (sensitivity analysis). A number of possible sampling procedures exists, including random sampling, stratified sampling, and Latin Hypercube sampling.

Due to time-consuming calculations with complex thermal-hydraulic codes the Monte Carlo analysis has not yet been applied for sensitivity and uncertainty analysis using complex codes. However, parts of it are today the basis of most statistical techniques.

3.4.2 Response surface methods

Response surface methods (RS) are similar to Monte Carlo analysis except that instead of a thermalhydraulic computer code a response surface is used. However, for response surface generation code calculations are needed. The number of uncertain input parameters is limited because of the required number of code calculations. The response surface can be defined as a collection of techniques used in the empirical study of relationships between one or more responses, or product characteristics, and a group of input variables. Regression is the relationship between the mean value of a random variable and the corresponding values of one or more independent variables.

Once the response surface (regression model) is built, uncertain input parameters are randomly chosen. When the underlying probability distribution function is uniform a random generator number is used to generate a number between 0, 1 (or –1, 1 or a, b) where a and b are the minimum and maximum of the uniform range. The location of the number on the allowed range defines the value of the parameter being chosen. If more than one uncertain parameter is used at a time (as in a multinomial) then independent random numbers are chosen for each parameter, which by the definition of regression must be independent. The values of parameters chosen are then inserted into the regression multinomial and the value of the safety parameter is found. This process is repeated many times (50,000 for example). The output values may be accumulated in preselected bins and normalized by the total number of trials. The result is a frequency histogram that is interpreted as a probability distribution function. From the histogram we may determine the standard statistics desired (mean, 95 percentile, etc.). The standard statistics desired may be obtained also directly from the sample values without binning. When response surface methods are used the number of code calculations increases exponentially by the number of uncertain parameters. In the case of discrete parameters (e.g. alternative submodels) the response surface methods may be poor, too.

Usually parametric and nonparametric regression analysis is used. In parametric regression of the form $y = f(x) + e$, where f is some known, smooth function, and e is error, the modeler must determine the appropriate form of f. The regression coefficients are calculated from known output variable calculated by the computer code for a combination of input variables (uncertain parameters). In nonparametric regression, f is some unknown, smooth function and is unspecified by the modeler. A data-driven technique determines the shape of the curve. As in parametric regression, a weighted sum of the output observations is used to obtain the fitted values. An example of nonparametric regression analysis is optimal statistical estimator [20]. The derived estimator is expressed as a linear combination of prototype sample vector (code calculated values of output uncertain parameter) multiplied by the coefficients (weights), which are highly non-linear functions of the input parameters. It was applied for response surface generation of LB and SB LOCA calculations [21, 22].

3.4.3 Tolerance limit methods

In the case of relatively many input uncertainty parameters the uncertainty could be determined from the distribution of key code output uncertain parameter. Statistical upper and lower bound of the distribution are then determined as the tolerance limits with a specified probability. There are two ways to calculate the tolerance limit: parametric and nonparametric statistics. Parametric statistics are based on parameters that describe the population from which the sample is taken. In the parametric approach the tolerance limit is calculated from the distribution. Nevertheless, parametric tolerance limits can be determined in very few special cases: normal, exponential distribution type.

Nonparametric statistics are not based on a specific distribution. They are often referred to as "distribution free". When the distribution hypothesis is rejected by goodness-of-fit test (it is unknown) it is possible to determine tolerance limits by randomly sampling the character in question. The consideration of nonparametric tolerance limits was originally presented by Wilks. Wilks' study showed that for continuous populations, the distribution of P, the proportion of the population between two order statistics from a random sample, is independent of the distribution where the sample comes from.

In this case the tolerance limit is determined from order statistics (highest, second highest etc.). When the tolerance limit is given by the maximum order statistics, the required minimum number of calculations given by Wilks' formula for 95% confidence is 93 for a two-sided tolerance limit and 59 for one-sided tolerance limit.

The confidence level is specified because the probability content is not analytically determined. Namely, the quantile as such (not the associated probability content) cannot be determined analytically nor estimated with high accuracy from large samples. It accounts for the possible influence of the sampling error due to the fact that the statements are obtained from a random sample of limited size. Thus, the number N of calculation runs depends only on the desired probability content and confidence level of the statistical tolerance limits. All of the uncertainty parameters are sampled simultaneously N times.

The advantage of nonparametric statistics is that the number of input uncertain parameters is limited only by ability of the user to define and implement uncertainties and that all uncertainties are propagated together. Other important advantages of distribution-free tolerance limits are: a) sample size is small and independent of input and output parameters, b) applicable to any computational model without restrictions, without adjustments c) permits sensitivity analysis without additional runs, d) appropriate for computationally expensive codes etc. However, there are other weaknesses, e.g. conservativity.

Recently, new studies were performed for derivation of the precise number of code calculations, N, needed for a given tolerance level even for several statistically dependent uncertain output parameters. Again, methods from order statistics were used. In paper [23] the formulae developed provide a basis for calculating multiple tolerance limits for a variety of problems, in particular, for computer codes that calculate several parameters on which individual acceptance criteria are imposed. The proposed direct extensions of the tolerance limit concept to several output variables are not satisfactory in nuclear safety applications. A modified concept seems more useful: the lower confidence limit for the probability of "complying with the safety limits for several outputs".

3.4.4 Internal Assessment of Uncertainty

An important technique for determining uncertainty bounds is the Code with capability of Internal Assessment of Uncertainty (CIAU) [24]. Namely, all of the uncertainty methodologies used in UMS suffered from two main limitations on resources needed for uncertainty methodology development and dependence of results on methodology/user. CIAU has been developed having in mind the objective of removing these limitations. The idea of the CIAU is the identification and the characterization of standard plant statuses and the association of uncertainty with each status. One hypercube and one time interval identify the plant status. The RELAP5/MOD3.2 and UMAE uncertainty methodology have been coupled to constitute the CIAU. However, any of the available system codes or the uncertainty methodologies can be combined to constitute CIAU.

3.4.5 Approaches in other areas or disciplines

A methodology for determining the probability distribution of a model prediction arising from uncertainty in input values is described by McKay [25]. Model inputs that are the dominant causes of uncertainty in the predicted results are identified through comparison of calculated prediction distributions with conditional prediction probability distributions. Replicated Latin hypercube sampling and variance ratios are used in estimation of the distributions and in the construction of importance indicators. The replicated LHS method is not appropriate for computationally expensive codes. One of two examples is an application of the MELCOR code to a severe accident scenario. Focus was on three outputs and 36 inputs that were identified as the dominant contributors to prediction uncertainty. However, it should be mentioned that in the severe accident area the uncertainty evaluation is still in the beginning phase. Also there are larger uncertainties and the number of uncertain parameters is larger than in the safety analysis of design basis scenarios.

Work on incorporating uncertainty estimation into computer code evaluations is ongoing in other disciplines where complex modeling is essential to nuclear regulation. Reference 26 provides a picture of how issues related to modeling uncertainty are being addressed in the area of environmental modeling. The focus is on new approaches for parameter estimation, as well as sensitivity and uncertainty analyses, including various approaches and applications of these strategies and tools, and specific lessons learned and research needs. One of the interesting aspects discussed is development of a common software application programming interface (API) for methods and tools used in parameter estimation, sensitivity analysis, and uncertainty analysis in the area of complex environmental system modeling. Development of similar standard interfaces in the nuclear system code area could promote the adoption of uncertainty analysis techniques, particularly those based on internal assessment of code uncertainty. In particular, with an agreed upon API, uncertainty methods would be more easily adapted to the existing system codes.

In the area of safety analyses some tools for sensitivity and uncertainty have already been developed, examples are the French SUNSET (Statistical UNcertainty and Sensitivity Evaluation Tool) and the German SUSA (Software system for Uncertainty and Sensitivity Analysis). The SUSA methodology was adapted both to ATHLET and RELAP5/MOD3.3. These two tools could be a good basis for a common API.

4. EXAMPLES OF GENERIC APPROACHES

The examples of application of safety analysis approaches for licensing are mostly limited to quantification of safety margins using system thermalhydraulic codes.

4.2 Application of very conservative approach

The Appendix K approach uses prescribed conservative initial and boundary conditions, conservative assumptions (e.g. single failure criterion) and conservative evaluation model with prescribed correlations and models. It is still in use, mostly for LB LOCA margins calculations. An example are analyses performed for the Krško Nuclear Power Plant (NPP) modernization project in 2000 with a replacement of both steam generators and an up-rating of its thermal power from 1882 MW to 2000 MW [27]. The Krško NPP is a Westinghouse 2-loop PWR. In the safety analyses the Westinghouse LOCA methodology approved in 1987 was used, with the evaluation model based on Appendix K requirements. The following major assumptions, required by Appendix K were used:

- initial power at 102% of licensed (core) power,
- maximum peaking factor allowed by the technical specifications,
- decay heat based on 120% of fission product decay rate specified by the ANS Standard for infinite operating time,
- the Baker-Just equation shall be used to calculate the metal-water reaction rate,
- the Moody model with at least three discharge coefficients shall be used for two-phase break flow,
- the most damaging single failure of ECCS equipment shall be considered.

The results for the worst case break showed that licensing margin for PCT was smaller then before power uprate (only a few 10 K of margin after power uprate). Also, to achieve this margin the maximum assembly average power was limited to a lower value as was planned before power uprate.

4.2 Application of best estimate bounding approach

In the best estimate bounding approach the uncertainties are not statistically combined but selected in such a way to bound the uncertainties. First example is application of Sizewell B large LOCA uncertainty methodology [28]. As a result of public inquiry concerns were raised with regard to the use of the evaluation methodology for LOCA analysis (Appendix K approach). The concerns were related to the difficulties of quantifying the margins, and hence in demonstrating that the Appendix K approach resulted in a conservative assessment of PCT. The licensing framework in the UK, unlike the USA, was not prescriptive, therefore best estimate bounding approach was developed. The method has many similarities with CSAU; the major difference is that an engineering judgement is used to ensure that final PCT has an associated high level of confidence. This is achieved by using bounding plant operating parameters (e.g. core power 102%) and selecting conservative accident boundary conditions (decay heat from ANS 79 standard plus uncertainties, control rods fail to insert on reactor trip etc.) including break location. Sensitivity analyses were performed to determine effect of parameter uncertainties on the PCT. For the uncertainties, which have the largest effect on the PCT, a number of combined uncertainties calculations were performed. A final combined uncertainties calculation was then performed, with uncertainties selected using a judgmental process based on the results of the previous single and combined parameter analyses. The biases for three uncertain parameters were then added to the final calculation of PCT. In addition calculation was performed using more realistic plant operating and boundary conditions, giving a reduction of 330 K on the PCT.

Another example is the best estimate bounding approach approved in Belgium [29, 30]. In this approach, a frozen version of the best estimate code is chosen, which has to be demonstrated adequate for simulating all relevant key physical phenomena. An exhaustive list of the deficiencies of the code can be set up together with possible remedies to overcome them. The uncertainty of the code can be either bounded by changing the input parameters (the deterministic bounding approach [30]), or included by adding the uncertainties quantified through comparing with relevant experimental data (i.e., the super-bounded approach [29]). The conservatism of the analysis is further ensured through an enveloping choice of the conservative assumptions on the initial and boundary conditions. This approach has been applied for both LOCA and non-LOCA accidents. In particular, it has been applied to steam line break accident analysis using the coupled RELAP5/PANTHER/COBRA code package [31].

4.3 Application of realistic conservative approach

The realistic conservative approach is similar to the very conservative approach except for the fact that best estimate computer code is used in lieu of conservative code. However, it must be noted that in certain countries realistic conservative approach is referred to as conservative analysis. First example is German licensing practice where a best estimate code is used with conservative assumptions on availability of plant systems and conservative initial and boundary conditions [32]. Uncertainty quantification is not required. Since some of the initial and boundary conditions are more conservative compared with those internationally used (e.g. 106% reactor power instead 102%, a single failure plus a non-availability due to preventive maintenance is assumed, etc.) it is claimed that the uncertainties of code models are covered. Two different categories of conservative input data are distinguished. The first one considers data related to assumptions on availability of plant systems (normal operation systems, control systems, safety systems). Typical examples of conservative assumptions on availability of NPP systems are non-operability of normal operation systems and control systems in accident situations, adoption of the worst single failure criterion for safety systems, and combination of an initiating event with loss of power supply in some cases. The second kind of conservative assumption is applied to cover insufficient knowledge with respect to all other NPP initial and boundary conditions.

Second example is deterministic realistic method (DRM) [33] evaluation model that consists of using a penalized best estimate code (penalized CATHARE GB) with penalized initial and boundary conditions.

Second example is application of the Deterministic Realistic Methodology (DRM) to the French Bugey 2, a three-loop PWR [33]. The DRM evaluation model introduces a penalization mode covering uncertainties of the calculation. It consists in using a penalized code (penalized CATHARE GB) with penalized initial and boundary conditions. The validation of the penalized code on relevant LB LOCA experiments demonstrates the conservatism of the predictions. The comparisons of calculations performed by the penalized code with calculations performed with the best estimate models demonstrate that the penalization mode does not distort the physics. This confirms the adequacy of the penalization mode of the DRM evaluation model. From a licensing point of view, the DRM evaluation model has been approved by French and by Belgian Safety Authorities, for each according to their specific requirements.

4.4 Application of BEPU

There are several applications of BEPU methods. In the following only a few examples are given. The pioneering work was done with CSAU application to LBLOCA in 1989. In the study the RS approach was used for the uncertainty evaluation of the peak cladding temperature (PCT) [13]. The input uncertain parameters were varied based on engineering judgment. In total seven parameters were varied and 8 TRAC code runs yielded 184 clad temperature traces. For the response surface generation the regression analysis

(4th order polynomial fit) was used. The 95/95 (95% probability and 95% confidence level) PCTs were calculated for blowdown, first and second reflood PCT.

The application of CSAU to SBLOCA was done in 1992 [34]. Because no core heatup occurred in the selected PWR Babcock & Wilcox Company the liquid inventory in the reactor vessel was also selected as safety parameter. The eight input parameters were varied as single, double or triple variations (minimal and maximal values of parameter). In total 34 calculations by RELAP5/MOD3 were performed. For regression analysis 3rd order polynomials were used. The results indicate a probability of $4.5 \cdot 10^{-4}$ that the primary safety criterion is less than 85% of the nominal value.

First real demonstration (with core heatup) of BEPU to 6% cold leg SBLOCA was done with the application of Uncertainty Method based on Accuracy Extrapolation (UMAE) to Krško NPP [35]. The RELAP5/MOD2 computer code was used for analytical simulation model of Krško NPP. The upper and lower continuous uncertainty bounds were derived from accuracy achieved for four similar SBLOCA tests.

In 1996, the USNRC approved a Best Estimate Loss of Coolant Accident (BELOCA) methodology, based on CSAU, developed by Westinghouse (recently referred as Westinghouse 1996 BELOCA Methodology) [36]. It is the first approved application of CSAU. The methodology takes advantage of both response surface methods and Monte Carlo analysis to predict the probability distribution of the hot rod behavior as a result of variations in "local" variables. The BELOCA methodology was applied to more than 20 nuclear power plants (3- and 4-loops W PWRs), as well as to the AP600 plant [37].

Also, other methods like Generic Statistical Uncertainty Analysis Methodology (GSUAM), DRM, Ontario Power Generation (OPG) initially used response surface technique for uncertainty evaluation. In the case of DRM the RS approach was not accepted.

The GRS method plays one of the most important roles for uncertainty and sensitivity evaluation besides the CSAU. It was developed rather early and its first application was to experimental facilities. It is the method, which first uses nonparametric approach according to Wilks and for this reason they avoid LHS. All uncertain input parameters were simultaneously varied. Special attention was paid also to sensitivity analysis. Different steps of uncertainty analysis are supported by the software system SUSA (Software system for Uncertainty and Sensitivity Analyses). In 1997 GRS method was applied to SBLOCA in German PWR 1300 MWe [38]. For 5% cold leg SBLOCA the ATHLET computer code was used for 77 calculations (two sided tolerance limit, a=0.95, b=0.90) and 45 input uncertain parameters were simultaneously varied. It should also be noted that the calculated uncertainty ranges of clad temperatures are continuous time-dependent valued.

The LBLOCA uncertainty evaluation using GRS method was recently compared to conservative calculation [39] for the German PWR 1300 MWe. A total number of 100 calculations were performed using the ATHLET Mod 1.2 code. The conservative maximum clad temperature does not bound the 95/95 one-sided limits of the uncertainty analysis over the whole transient. Namely, in Germany the use of best estimate computer codes is already practice for "conservative" calculations.

As already mentioned the tolerance statistical tolerance limits (intervals) approach for statistical combining uncertainties was first proposed by GRS [38]. Nevertheless it is not yet approved for licensing in Germany. On the other hand, the methods based on nonparametric statistical tolerance limits were already approved in other countries. Examples are the KREM method [40] developed in Korea and approved in 2002, the Framatome ANP method (now AREVA) called RLBLOCA [41] approved in 2003 and the Westinghouse Automated Statistical Treatment of Uncertainty Method (ASTRUM) recently approved [42].

The KEPRI Realistic Evaluation Methodology (KREM) for LBLOCA was demonstrated for Kori 3/4 which are 3-loop W PWR located in Korea. The method uses a combined code of CONTEMPT4/MOD5 and RELAP5/MOD3.1. The method was developed strictly following the philosophy of CSAU with few improvements and differences. KREM adopts nonparametric statistical tolerance limits to quantify the overall uncertainty of a LBLOCA at 95% probability and 95% confidence level from 59 plant calculations according to Wilks formula. The maximum cladding temperature was 1212 K. This value was also confirmed when 640 calculations are performed, whose 95 percentile PCT is 1206 K. The 640 PCT data were shown to have normal distribution with the mean of 1145 K and the standard deviation of 58.2 K. Its one-sided PCT is found to be 1210.2 K, which is again much comparable with 1212 K. When biases were added, resultant PCT was 1319 K.

AREVA method follows CSAU with relying on nonparametric statistical tolerance limits instead of response surface and the RODEX3A fuel rod code and S-RELAP5 frozen system code were used. In the application a set of 59 calculations were performed random sampling a few ten of input uncertain parameters to obtain tolerance limits for PCT, maximum nodal and core oxidation for three- and four-loop Westinghouse plants. The 95/95 PCTs for three- and four-loop plants were 919 K and 1012 K, respectively.

ASTRUM also follows CSAU evaluation methodology framework. The ASTRUM method uses same code and same uncertainty distributions as BELOCA methodology and a revised method for combining the uncertainties. The nonparametric order statistics is used while response surfaces and superposition correction uncertainty is eliminated. To establish 95^{th} percentile PCT at 95% confidence level the highest PCT for 59 case run matrix or alternatively, second highest for 93 case run matrix is used. When three output parameters are treated 124 runs are used for 95/95 statement. The comparison between W 1996 BELOCA and ASTRUM was done for 3-loop W plant [42]. For 3-loop plants the calculated 95^{th} percentile PCT with the W 1996 BELOCA is 1444 K as opposed to 1318 K using the ASTRUM. In the case of W 1996 BELOCA, several uncertainty contributors were bounded while the explicit treatment of more uncertainty parameters in ASTRUM provides some additional margin.

The alternative to these methods is CIAU [43]. An example of CIAU application is LBLOCA in Kozloduy unit 3 (VVER-440/230) [6]. In the application to LBLOCA the interesting finding was that the CATHARE prediction is bounded by the uncertainty limits derived for RELAP5/MOD3.2 prediction. The calculated 95/95 PCT was 1335 K. The performed sensitivity analysis also showed that parameters that are influential in LBLOCA analysis of Western PWR do not affect the Kozloduy unit 3 scenario prediction. The independent qualification of CIAU tool showed that the tool is suitable for use although an enlargement of the current uncertainty database is necessary. At the end of 2004, 29 qualified tests were included in the database. The CIAU requires about 100 tests to be acquired to make statistical evaluation reliable. Therefore, the process to include new qualified tests is the main priority of the CIAU methodology.

5. GUIDELINES FOR UNCERTAINTY TREATMENT IN DETERMINISTIC CALCULATIONS

A number of techniques have been developed and are being used to estimate the uncertainty in deterministic predictions of nuclear plant response to transient and accident scenarios. Virtually all of the methods have focused on design basis space applications. That is, the intended application is to one or at best a few events. A number of the existing techniques were summarized in the preceding section. Strengths and weaknesses of each of the described approaches were mentioned. Depending upon the application, one technique may be preferable to another, but at the present time the tolerance limits approach is most appealing. Some further considerations regarding uncertainty methods in design space are

provided in this section, but the emphasis is shifted to include applications to deterministic calculations in risk space.

Design basis space applications permit considerable effort to be expended on the target scenario, but even when concentrating on one event, computationally intensive methods such as Monte Carlo are still impractical. Methods that rely on statistical tolerance limits, e.g. the GRS method, require 59 calculations to obtain a one sided limit at the 95% confidence level. While this is a very practical procedure for a limited number of design basis events, it has limitations for risk space applications. Similar statements apply to the other approaches that are suitable for design basis space.

In risk space, like in the design basis space, a large number of event scenarios are "binned" and a representative case that may envelope the majority of scenarios in the bin is subject to deterministic simulation. The response for the chosen case is considered to be representative of all events in the bin. One difference between the analysis in the design basis space and the risk space is that, in the former, the number of bins is much lower and the size of the bins is larger. As a consequence, some of the binned events in a particular group may be very different from the dynamic scenario used as the bin representative.

While the uncertainty issue is also important in the risk space analysis, the higher number of bins results in less demanding enveloping requirements for the representative scenarios. An important consequence is that more realistic scenarios are allowed as representatives in the risk space. This fact, along with the important increase in the number of analyzed cases, makes unpractical to spend significant resources to obtain results for the representative cases at the 95% confidence level. While establishing an uncertainty band on the deterministic responses is necessary, it is clear that the technique used should be tailored to the context in which the results will be used. A justifiable band on the key responses that are compared to acceptance criteria and failure limits appears to be the desirable level of rigor for this application. Before discussing plant response simulations the acceptance criteria in light of safety margins will first be discussed.

5.1 Acceptance Criteria

Acceptance criteria play a pivotal role in discussions of safety margins (see SMAP TN, 2005a). This is primarily because acceptance limits are set with due consideration of epistemic uncertainty. The value of acceptance limits is set such that if operating conditions remain below the predetermined value, the probability of loss of function is negligible.

Acceptance criteria in the design basis space are developed to ensure the integrity of barriers to the release of radioactive materials. They are set as safety limits such that meeting the criteria assures that the subject barrier is very likely to remain functional. As discussed in Section 4 of SMAP TN (2005b), the barrier failure probability is given by the convolution of the load and resistance probability distributions, assuming they are known. However, when developing a statistical measure for the failure distribution is not possible or practical, lower limits for the failure loading, i.e. resistance, are established as safety limits, which is equivalent to replace the whole failure distribution by a Dirac's Delta located at the point of the safety limit. In this case, the failure probability is given by the point at which the safety limit cuts the load distribution. Finally, a normalized safety index makes it possible to include damage mechanisms that are known to occur as a probability distribution function, e.g., failure of the containment due to internal pressure buildup. In that case, the peak pressure prediction from the deterministic analysis is used to read the cumulative probability of failure for the distribution, which becomes the safety index in the analysis.

An example of safety index that measures the ascent of a peak cladding temperature as the safety variable into the non-negligible damage probability range was given in Section 4 of SMAP TN [44]. Other safety indices based on barrier damage mechanisms could also be defined, for example, based on the

amount of clad oxidation, either local or core wide, or on time at temperature. The indices might also be event specific with the index selected based on the type of challenge to the cladding.

Other safety indices for containment and pressure boundary integrity also need to be based on the type of challenge to the barrier. Pressure boundary integrity can be challenged by overpressurization, in which case the acceptance criterion is maximum system pressure. This could apply to either the pressure boundary or the containment structure. The failure limit will generally be significantly above the design pressure, probably by at least a factor of two. For the containment boundary, acceptance criteria for severe accidents should consider the failure mode, i.e. catastrophic failure versus an increased leak rate.

Thermal loadings can also challenge pressure vessel integrity, as is the case for pressurized thermal shock. In this case an acceptance criterion based on minimum temperature relative to a reference temperature [45], e.g., reference temperature of nil-ductility transition (RTNDT), is feasible. Another is the initiation of crack propagation.

5.2 Plant Response Simulations

The bounding approach to safety analysis has been successfully used since the inception of the nuclear industry. Provided that sufficient conservatism is maintained, this approach has proven to be acceptable. There are, however, a number of disincentives deriving from use of the bounding approach. It is a qualitative approach with the uncertainty essentially being unquantified, but judged to be sufficient based on the available knowledge base. It can focus safety considerations on only a few events and leaves other possibly risk significant events without sufficient consideration. Guidelines that exist, e.g. 10-CFR-50.46 and Appendix K, tend to be prescriptive. Bounding methods are fairly well developed and guidelines for their use are readily available. While the bounding approach has been used for many years, economic and technical pressures have driven the development of more realistic methods for dealing with uncertainty.

Optimising the output of nuclear power plants makes very often the plants more reactive to accident initiators. As a consequence, in several cases, it was impossible to fulfill the criteria with the traditional conservative methods used in the past to design nuclear plants. Those traditional conservative methods were generally the same or of the same type than the ones on which safety margins evaluation were asked in the seventies. To reach the compliance with the criteria, new methods have to be used. This necessarily leads one toward realistic or best estimate calculations with quantification of the uncertainty in the calculated results.

There are a number of general considerations that apply to the quantification of uncertainties and to the determination of the approach that is best suited to the application. Figure 3 is a schematic that attempts to summarize the process of determining uncertainties. Some sources of uncertainty in deterministic analysis results are very difficult to quantify, in particular user effects and intrinsic computer code numerical effects. Therefore, the first manner of dealing with uncertainties is to take appropriate measures to minimize some of them like user effects and intrinsic computer code numerical effects. Use of a well-designed code that is applicable to the analysis at hand by experienced code practitioners is essential to achieving this goal. If there are choices in models, modeling options and correlations, these should be consistent with the assessments and code qualification usage. Convergence of both the nodalization and time step/numerics should be assured by sufficient sensitivity studies. The level of uncertainty can also be reduced by adherence to good user practices, as described in Reference 46. Examples of user and related effects are discussed in some detail in Reference 47. The primary examples for identifying user effects include ACHILLES Reflooding Test and LOBI Natural Circulation test. Summary discussions are also included for tests in the SPES, ROSA-IV and BETHSY facilities. Recommendations for reducing the user effect given in Reference 47 include improving user training, user guidelines, user discipline, quality

assurance and the choice of computer codes. Computer and compiler effects are discussed by Trambauer in Reference 48.

In this effort of minimizing avoidable sources of error, both code adequacy and quality of the plant model are equally important. However, while the same code is often used by a significant number of users, allowing to exchange experiences to a large extent, plant models are much more specific and, therefore, more difficult to qualify. Some of the above mentioned sources of uncertainty are actually errors or inconsistencies in the plant model developed. Specific guidance on how to develop and qualify plant models for simulation codes can be found in Reference 49.

Once the uncertainties like user effects and intrinsic computer code numerical effects are minimized, the manner of addressing the effects of uncertainty on code results depends on the nature of the uncertainty and on the intended uses of the code results. There will generally be more sources of uncertainty than can be realistically included in an analysis, so it is important to identify which sources of uncertainties are the most significant and must be included. The intended uses of the results will assist in determining the required level of accuracy. For example, is a probability distribution/density function needed, or are statistical parameters sufficient to obtain confidence intervals required, or will a bounding approach suffice.

If a Phenomena Identification and Ranking Table (PIRT) has been developed for the event of interest, it should provide information on which phenomena/models are most important (highly ranked). It is apparent that the PIRT should focus on the same safety variable/acceptance criteria as the current analysis. If a change of the parameter within its range of uncertainty has an insignificant affect on results, further consideration is not warranted. Code assessments are also generally a good resource for identifying the significant contributors to uncertainty in code results. However, when the number of uncertain parameters is not limited like by tolerance limits method and most of uncertainties are treated, sensitivity analysis can be derived directly from the uncertainty analysis (no need to reduce the number of uncertain parameters).

Once the significant sources of uncertainty have been identified, the approach to be used to quantify the uncertainty will depend on the desired accuracy requirements. For design basis analysis where confidence levels are required, use of a method that determines how uncertainty in input parameters is propagated to the output is indicated. On the other hand, if the expected margin is large, or the application is in risk space where the higher number of analyzed cases provides a better support to the conclusions of the analysis, making them less dependent on a high confidence level on the accuracy of the results, a conservative bounding approach can be used.

Where a statistical approach is necessary, the choice will depend on availability of the required software, accuracy requirements, and the amount of resources (human and computer hardware). There may be a bias in the results, and if so this needs to be determined regardless of the method applied. Namely, the frozen code version can still consistently overpredict or underpredict certain parameters and the resulting inaccuracy is termed code bias. The CSAU application to large break LOCA [14] is an example of an application that includes a determination of bias. In this application the biases were not treated statistically but separately, and finally added to the mean and 95% PCT. The CSAU application to SBLOCA [34] is an example where biases were treated statistically. In most cases it will not be possible to obtain the probability distribution for input parameters; however statistical measures such as the mean value and standard deviation may be available from reference sources. For example, correlations used in the codes may include statistical information.

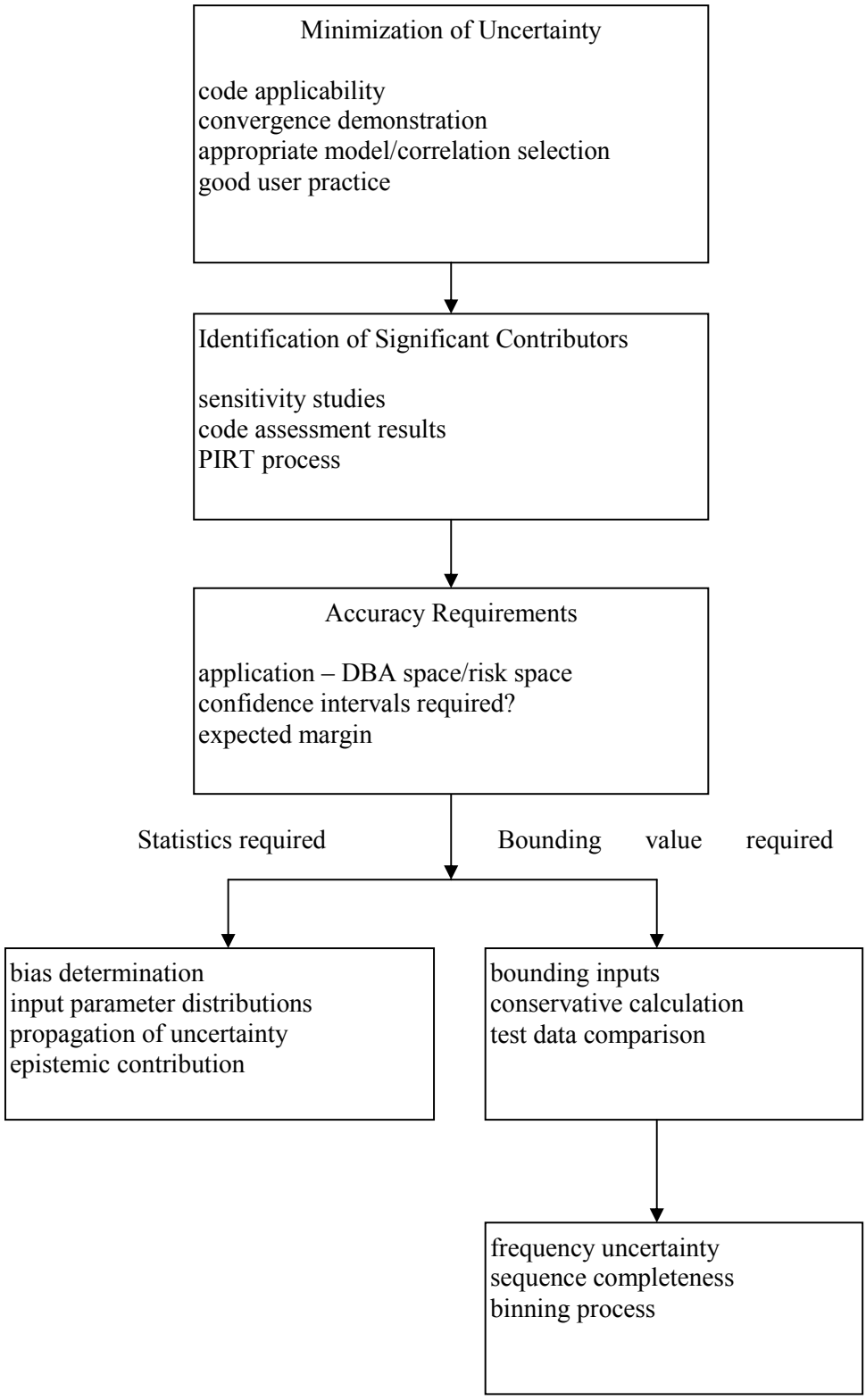

Figure 3. Schematic of Uncertainty Quantification Process

One of the criticisms of the existing statistical uncertainty methods is that they require intensive computer resources and there is considerable variability in the results (not in the GRS method where the variability of the results is quantified and controlled), depending on both the practitioner and the method. They were developed and have been applied for single events to determine the uncertainty in (generally) a single output variable, e.g. peak clad temperature. For applications to safety margins in risk space, uncertainty will need to be determined over a large number of events of different types. It is clear that:

1. Addressing uncertainties must be an integral part of determining safety margins
2. Methods used must be applicable to a wide range of events
3. Required resources for existing methods may require approximations (for example, to reduce the effort, an uncertainty can be established for a particular safety variable for a particular type of transient and then used in all the transients that fit into that category)

The general approach to accounting for uncertainty in PRA results (CDF and LERF) is discussed in Section 2.2.5 of Regulatory Guide 1.174. In that discussion, uncertainties are categorized as parameter, model, and completeness uncertainties. It should be noted that uncertainties in the choice of an appropriate thermalhydraulic model are typically addressed by making assumptions and adopting specific model. The reader should distinguish between uncertainties in PRA results and in deterministic code predictions. When determination of a two-sigma limit on the output over a range of event types may be possible based on running a series of conservative calculations and/or comparisons to appropriate integral test data, conservative bounding approaches are appropriate for applications to safety margins in risk space without the need to quantify uncertainties of best estimate code.

For a PRA application, there will be considerable uncertainty (in estimating the probability the event sequence will occur) introduced by use of estimated frequency of event initiators, safety system failure rates, operator action assumptions, the binning process, completeness of scenarios, etc. In this case, the uncertainties introduced by these factors will easily justify the use of bounding values for uncertainties in the supporting deterministic analyses. Treatment of uncertainties in PRA applications is further discussed in Section 4.0

6. METHODS FOR FREQUENCY QUANTIFICATION

The figure of merit in probabilistic analyses is the exceedance frequency of the safety objective, also known as the frequency of the damage state of interest. This is so in traditional level 1 PSA where the safety objective is to avoid core damage and the figure of merit is the Core Damage Frequency (CDF), i.e., the exceedance frequency of the sequence success criteria. For level 2, the safety objective is to avoid large early releases and the corresponding figure of merit is the Large Early Release Frequency (LERF). The same is true for analyses in the risk space where the same type of figures of merit (possibly including other safety objectives) are being proposed in the framework of the safety margin assessment. Some frequency quantification methods are reviewed in this chapter.

The frequency of a damage state is an aggregate of the frequencies of transient paths[2] where the corresponding safety objective is exceeded. Each sequence in an event tree, described by a particular combination of header states, is the set of all the possible transient paths with that combination of header states. Among these paths, some will result in exceedance of the safety objective (they will be called *damage* paths with respect to that objective) while others will end in a safe state without exceeding the safety objective at any time (*success* paths with respect to the analyzed safety objective). Event tree headers describe the status of essential safety features like availability of safety functions in terms of

[2] In this context, a transient path can be interpreted as a deterministic transient that can be calculated with the TH codes of previous sections.

safeguard systems configurations, assuming they are demanded during the transients. Damage paths are dependent not only on the state of the set of headers but also on the times in-between events requiring safety functions header activation, once given initial conditions. The set of header states then conditions the damage frequency, but does not entirely determine it.

It is not practical to classify each individual path as damage or success. Neither it is practical to evaluate frequencies of individual paths as contributors to the damage frequency. Instead, classical PSA classifies a sequence as *success* or *damage* according to the expected end state of the majority of the paths grouped under that sequence, which is decided as a function of the sequence header states. The contribution of damage sequences to the exceedance frequency of the safety objective is given by the total sequence frequency, which is computed from the expected frequency of the initiator and the probabilities of the header states.

In section .0 a summary of the classical PSA event tree/fault tree techniques is given. Section 0 is a review of quantification methods that can be used in classical PSA and 0 briefly addresses the uncertainty problem.

An implicit assumption in classical PSA is that all the safety functions represented by the headers composing a sequence are actually demanded in any transient path included in the sequence. This is reflected in the fact that header probabilities are labeled in "per-demand" terms. This raises the question of the probability of the demand, which is discussed in section 0 along with other issues regarding the accident-timing problem or the estimation of the fraction of the sequence frequency that actually contributes to the damage state frequency.

6.1 A brief review of event tree / fault tree concepts

The standard procedure to quantify the CDF (in the general case, the exceedance frequency of any safety objective) consists of modelling the logical (boolean) state of each header in each event tree sequence, then obtaining the plant logical state for each sequence by intersecting the boolean models of the intervening headers and finally obtaining the boolean union of the sequences leading to core damage. The resulting boolean function, called the core damage equation, logically combines the initiating events of the event trees and the basic events composing the header boolean functions and identifies which combinations of these events result in severe core damage. This structure function is then used to calculate the core damage frequency from frequency data for the initiating events and from probabilities of the basic events.

The usual tools for the boolean function build-up are the fault trees and the event trees. The reader can further refer to References 50, 51, 52 and 53 for fault trees and References 54 and 55 for event trees.

6.1.1 Fault trees

As is widely known, fault trees (FTs) are deductive, graphical tools to represent an undesired event (the *top event*) by means of logical gates. Starting from the consequence one wants to study, its possible causes are studied and further decomposed recursively until no more decomposition is possible, either because elementary causes have been found or because it is impractical to look for them. The decomposition uses the logical gates AND and OR. The NOT gate, allowed in theory, is seldom used in the nuclear industry. The structure thus obtained is a graphical representation of a certain boolean function whose onset (the set where the function evaluates to true) is the set of combinations of failures that lead to the consequence. The boolean function is obtained by simply putting together all the information collected. How this is turned to a useful expression is explained below.

As can be easily imagined, the depth of the FT analysis is —more or less— decided by the analyst. In any case, it clings strongly to the quality and quantity of data available for the components of the plant. In general, FT analyses stop at the component level since data are usually available for the failure rates and probabilities of failure under demand of valves, pumps and such —components.

The bottom-line elements of the PSA, called *Basic Events* (BE), then represent the causes by which the systems of the plant may fail to perform their intended safety function. In general, they are unavailability of the equipment due to failures, maintenance or test, probability of human errors that may impair system performance and other data needed to model the sequences. Repair of the components is not assumed to occur during the accident, unless enough time is granted to perform the *recovery actions* (verified with thermalhydraulic calculations). Failure data (failure-on-demand probabilities, failure rates in operation and in stand-by) thus represent the reliability of the components. However, repair is assumed to occur if a component is found failed during test and maintenance activities. Unavailability caused by these activities, both planned (due to the maintenance schedule and surveillance tests required by Technical Specifications) and unplanned (due to repairs) are addressed as separate basic events. Note that the time of the repair (the moment at which the repair is performed) is not considered. Only a probability that the component is down due to these activities is computed as the relative downtime of the component. Markov models that more accurately follow the time evolution of the availability function (see section 6.2.3 below) are seldom or not at all used.

The resulting structure can be reduced by means of the boolean algebra rules to obtain a canonical form of the boolean function that represents the system failure. This canonical form is usually the Disjunctive Normal Form (DNF), also called Minimal Cut Set (MCS) representation of the boolean function, given by a non-reducible set of terms linked by union operators, each term (called a MCS) consisting of the intersection of several BEs and representing a sufficient combination of basic events which results in the loss of the safety function represented by the top event. There are other canonical representations of the boolean functions, Decision Diagrams being the most useful (see 6.2.2 below).

Little effort again is needed to understand that several FTs may share BEs, since this only means that the corresponding systems share the corresponding components. A clear example of this is supporting AC power that is used by several systems. Those shared basic events introduce dependencies among the FTs that make their processing difficult.

In the reliability modelling of certain components, it is not possible to assume that the failures are solely due to ‘independent’ causes. It is customarily assumed that some of the possible failures come from sources that can affect also other components. Such failures are termed ‘common cause failures’ and arise due to a variety of reasons such as manufacturing, design, human actions, and so on. The modelling of common cause failures is assumed specifically for redundant components, components manufactured by the same supplier, calibrated or maintained by the same crew or in the same shift, placed together (to account for environmentally-induced failures), etc. Components that can be affected by a common cause failure are associated in what is called a common cause group and receive a unified treatment.

6.1.2 Event Trees

In terms of systems failures, an Event Tree can be viewed as a set of sequences of events, starting at the initiator and ending in some (previously defined) damage state[3].

[3] In the general case, damage states are defined by the safety objectives being exceeded along the sequence, including a no-damage state for the case of no exceeded objective. In the case of classical PSA there are only two end states, namely, *success* (no damage) and *core damage*.

The correct way of reading an event tree is starting from the initiating event and traversing it left to right counting a failed (successful) mitigating action - represented by an event tree header - whenever the line goes downwards (upwards), so that each sequence is a set of failures and successes yielding either success (no damage) or one of several categories of damage. The final state of each sequence is thus indicated to the right of the graphic.

The boolean function of each sequence is obtained by considering that the several header failures occur concurrently (disregarding the time evolution of the probability, as the time scale during the accident is much faster than that of the probability evolution of most BEs). For this reason, PSA event trees are also referred to as 'static event trees'.

The sequence boolean function then amounts to doing the boolean product of the initiating event and the failed headers fault trees (*i.e.* of their boolean functions), and performing the boolean reduction over the result to obtain its canonical form (usually MCS). The headers in a working (i.e., non failed) state are usually considered in the following way. Any cut-set from these that is included in a cut-set of the boolean product of the failed headers provokes the latter to be deleted (this is the so-called *delete term* operation). The reason for this apparently artificial operation (instead of the more natural of making the product with the reverse of the boolean function of the fault tree) is that, when represented in DNF, the inversion of a boolean formula is a very costly process. The *delete term* operation removes 'impossible' combinations that would arise if the same component lies in different headers, some entering the sequence in a failed state, some in a working state.

Once the boolean functions of all the sequences of all the event trees are obtained, the final equation of each damage state is obtained by the logical union of all the sequences ending in that damage state. Note that the union of sequences from the same event tree may give rise to additional boolean reductions because of absorptions in the boolean operations, something cannot happen when performing the union of sequences from different event trees, since they involve different initiating events which make these sequences (and their respective MCSs) disjoint.

6.2 Frequency evaluation methods applicable to classical PSA

6.2.1 Quantification of Minimal Cut Sets

The process by which the MCS equation of a damage state is obtained and then used to calculate the damage state frequency is called the quantification of the event/fault tree. The MCS equation is obtained by the repeated application of the boolean absorption and idempotency rules until no further reduction is possible. The difficulty in finding the *exact* MCS equation of an arbitrary boolean function is that the number of MCS representing the function may be very large.

The reduction of a boolean formula to a MCS representation is not exclusive to reliability. It is used in testing the correctness of the design of electronic circuits. Several techniques have been devised to perform this reduction (like Karnaugh maps or the Quine-McCluskey procedure), to be found in any reference in computer aided design of integrated circuits. For reliability uses, though, other algorithms that restrict the search for MCSs in terms of probability are preferred.

A number of algorithms are available for finding the truncated list of MCSs, similar to the exact ones but discarding along the way those cut-sets (or groups thereof) whose probability is less than a given cutoff value. A widely used procedure is the one conveyed by the RiskSpectrum tool. RiskSpectrum is an integrated graphical tool for the development and quantification of PSAs, running under Microsoft systems (Windows95, Windows NT, and such). Other tools in the same line are **Kirap** (from KAERI, Korea), **Cafta Risk and Reliability Workstation** (from SAIC, USA) and IRRAS (developed under the auspices of

the US NRC). The algorithms used by these tools are not known because of proprietary restrictions. One of the most powerful tools in them is finding *modules*. These are boolean functions that can be treated as a unity in the fault tree, that is, functions that have a void intersection with the rest of the fault tree.

Once the MCS representation of the damage state has been obtained, its frequency can be calculated in terms of the frequency of the individual MCSs. Each MCS is composed by the boolean product of an initiating event and several independent basic events. An exact approach for frequency or probability calculation runs as follows[4]. The basic assumption is that the basic events are pairwise independent, as well as any BE with respect to the initiating event, so that the probability of the event 'both x_1 and x_2 occurring' is $P(x_1 \cdot x_2) = P(x_1) \cdot P(x_2)$, translating the boolean product to a probability product. Unfortunately, this is not as straightforward for the OR operation. The probability of the event '(at least one of) x_1 or x_2' is given by, $P(x_1 + x_2) = P(x_1) + P(x_2) - P(x_1)P(x_2)$, mirroring the known rule for the probability of the union of two sets. The iterative use of this formula for the boolean sum (set union) of basic events yields,

$$P\left(\sum_i^m x_i\right) = \sum_i^m P(x_i) - \sum_j^m \prod_{i<j} P(x_i)P(x_j) + \ldots + (-1)^{m+1} \prod_i^m P(x_i). \tag{4}$$

When the above formula is applied to the damage state equation, the number of terms grows exponentially with the number of MCSs (it is $2^m - 1$), rendering it inapplicable for practical usage. Thus, the probability of the boolean formula has to be approximated in some way. The first approach is to keep only the first term of Equation (4), which is called the rare event approximation. It gives good results when the probability of each term is small ($<<10^{-1}$). Keeping successive terms of this equation yields a sequence of results that alternatively bounds above and below the true value. These approximations can be made only if the boolean function has been reduced to an MCS representation.

A different approach is obtained through using the De Morgan's laws. For a boolean sum in terms of BEs x_1 and x_2, one has

$$x_1 + x_2 = \overline{\overline{x_1 + x_2}} = \overline{\overline{x_1} \cdot \overline{x_2}} \tag{5}$$

so that, bearing in mind that $P(\bar{x}) = 1 - P(x)$, the following formula holds

$$P(x_1 + x_2) = P(\overline{\overline{x_1 + x_2}}) = 1 - (1 - P(x_1)) \cdot (1 - P(x_2)). \tag{6}$$

It so happens that this approximation gives a much closer value than the rare event approximation, and has similar computational effort. The generalisation of this formula expressed in terms of the MCSs yields

$$\begin{aligned} P\left(\sum_i MCS_i\right) &= 1 - \prod_i (1 - p(MCS_i)) \\ P(MCS_i) &= \prod_j (MCS_i^j) \end{aligned} \tag{7}$$

Note that none of these approximations is good if the equation contains a BE that appears both in the negated as well as in the non-negated form.

[4] In the following description *x* may represent either an initiating event or a basic event. In the former case *P(x)* has the meaning and units of frequency while, in the latter, *P(x)* is the probability of the basic event.

In section 6.1.2, the procedure for computing the boolean formula of a sequence was outlined. In particular, it was said that the *delete term* would be applied to take into account the systems that were not in a failed state. To fully take into account those, the one's complement of the probability of the header failure can be multiplied to the probability of the sequence, which is usually done if the corresponding failure probability is high.

6.2.2 Binary Decision Diagrams

The Binary Decision Diagrams BDDs [56, 57] are a particular way of representing boolean functions that has as the main advantages:

1. It is canonical: two functions having the same BDD representation are the same
2. It is compact, in the sense that the memory requirements are low as compared with other representations
3. The boolean operations have a simple expression and can be achieved with reduced computational effort
4. The probability calculations can be done without approximations.

It does also have drawbacks. The main one is related with point 3 above. The optimal representation is not easily found, and the size of a BDD depends strongly upon the ordering of the variables involved.

The construction of the BDD representing a boolean formula is as follows. We first define the Shannon expansion of a boolean formula.

Let $f(x_1, x_2, ..., x_n)$ be a boolean function. The Shannon expansion of f with respect to x_1 is $x_1 \cdot f(1, x_2, ..., x_n) + \overline{x_1} \cdot f(0, x_2, \mathrm{L}\ , x_n)$

The complete expansion of the formula is obtained by repeatedly expanding it with respect to variables $x_1, x_2, ..., x_n$.

Then, a BDD is a compact representation of the Shannon expansion in which

1. useless expansions have been deleted,
2. identical formulae are referenced only once.

A useless expansion occurs if the formula being expanded does not depend on the variable of the expansion. For instance, if

$$f(x_1, x_2, x_3) = x_1 x_2 + x_3 \tag{8}$$

The expansion of f with respect to x_1 yields

$$f(x_1, x_2, x_3) = x_1(x_2 + x_3) + \overline{x_1} x_3 \tag{9}$$

expansion with respect to x_2 now gives

$$f(x_1, x_2, x_3) = x_1(x_2 + \overline{x_2} x_3) + \overline{x_1}(x_2 x_3 + \overline{x_2} x_3) \tag{10}$$

the last expansion is useless, since

$$x_2 x_3 + \overline{x_2} x_3 = x_3$$

The second item occurs because it may happen that identical functions occur in different expansions. Let

$$f(x_1, x_2, x_3, x_4) = x_1 x_3 x_4 + x_2 x_3 x_4 \tag{11}$$

The Shannon expansion with respect to x_1 and then x_2 yields,

$$f(x_1, x_2, x_3, x_4) = x_1(x_3 x_4) + \overline{x_1} x_2 (x_3 x_4) \tag{12}$$

where the term $x_3 x_4$ can be referenced only once.

The effect of the ordering of the variables in the size of the BDD can be appalling, changing linear to exponential in the number of nodes in terms of the basic variables.

Since the Shannon expansion is frequently used, there is a standard notation for it, namely

$$F =< x_F, T_F, E_F >= x_F \cdot T_F + \overline{x} \cdot E_F \tag{13}$$

where T_F (E_F) is referred to as the Then (Else) part of the Shannon expansion, and x_F is the *root* or the *radix* of the expansion. If $F, G, \text{and } H$ are BDD,

$$< F, G, H >= F \cdot G + \overline{F} \cdot H. \tag{14}$$

This formula is implemented by Shannon expansion as:

$$< F, G, H >=< x, < T_F, T_G, T_H >, < E_F, E_G, E_H >> \tag{15}$$

where x is the lowest of the three radices x_F, x_G and x_H.

The boolean operations are easily expressed in this notation since the usual connectives AND, OR, NOT, etc. are orthogonal with respect to the <> operation, i.e., $Op(f^1, ..., f^n) =< x, Op(f_T^1, ..., f_T^n), Op(f_E^1, ..., f_e^n) >$, where the *Then* and *Else* parts are taken with respect to x.

Besides, these usual connectives can be expressed in terms of the <> operation as

- AND: $F \cdot G =< F, G, 0 >$
- OR: $F + G =< F, 1, G >$
- NOT: $\overline{F} =< F, 0, 1 >$.

It is not the purpose of these notes to give a full description of BDDs. The interested reader is referred to [58], or [59]. Recently also comparison was done between MCS and BDD in assessing event trees [54].

Consider now a boolean function expressed by a BDD, say $f =< x_0, f_{x_0=1}, f_{x_0=0} >$. If probabilities are assigned to the variables appearing in the BDD, the probability of the function is readily obtained since $p(f) = p(x_0) p(f_{x_0=1}) + (1 - p(x_0)) p(f_{x_0=0})$, and the probability of the then and else parts are obtained in the same fashion. Moreover, this calculation contains no approximation whatsoever, so that the outcome is

the exact probability of the boolean function, with a computational effort considerably less than in the MCS representation case.

Nonetheless, the MCS representation of the function, full of qualitative information, is not lost by using BDDs. Several effective algorithms exist to obtain the MCS list to any degree of truncation.

6.2.3. Markov models

In section 6.1.1, the probability of a top event is calculated in terms of the probability of occurrence of the individual cut sets that constitute its elementary causes, as per equations (4) or (7) above. Similar relations hold for other reliability figures of merit.

Given a reliability function in the MCS form, there are different approaches for quantification. As mentioned in section 6.2.1, the most commonly used is based on assuming the basic events to be independent on each other. This is the classical quantification approach that has proved very useful, particularly for very large systems with many basic events.

However, BE independence cannot always be demonstrated. For instance, for basic events representing component failures, independence implies the failure rate of a component to be independent on the state of the other components. This assumption does not often hold, and Markov models are mainly used to account for it. Additionally, the explicit time dependence of the reliability and unavailability functions are only easy to handle with the above techniques if no repair of components is assumed (both functions, reliability and unavailability, then become the same). Using Markov models, they come out naturally and do not pose additional complexities.

Markov models are state based models where the system state is described in terms of a collection of the state of single elements. Transitions among states are due to a sequence of single element failures/repairs. There is a known transition rate among states, which is found from the addition of individual single element failure/repair rates, each one now dependent on the state of the other elements. Thus, the order in which the single events take place does matter. In a Markov stochastic process, the probability for the system to stay in a given state during a given sojourn time is independent on the time at which the state is entered, so state probabilities are independent on the past history (memory-less stochastic systems). When transition rates only depend on the individual elements that change with the transition and are independent on the rest of the elements, Markov models should provide the same result as the classical approach.

The equations to be solved may be described in its differential form by

$$\begin{aligned} &\frac{d}{dt}\pi_{\vec{j}}(t) = -\lambda_{\vec{j}}\pi_{\vec{j}}(t) + \varphi_{\vec{j}}(t) \\ &\lambda_{\vec{j}} \equiv \sum_{\vec{k}\neq\vec{j}} p_{\vec{j}\to\vec{k}} \\ &\varphi_{\vec{j}}(t) \equiv \sum_{\vec{k}\neq\vec{j}} p_{\vec{k}\to\vec{j}}\pi_{\vec{k}}(t) \end{aligned} \quad . \qquad (16)$$

where $\vec{j}$ is the system state vector, composed by the set of component states, $\pi_{\vec{j}}(t)$ is the probability of being in state $\vec{j}$ at time *t* and $p_{\vec{j}\to\vec{k}}$ is the transition rate from state $\vec{j}$ to state $\vec{k}$. The term $\varphi_{\vec{j}}(t)$, as

defined in Equation (16), is called the *ingoing density*, i.e., the instantaneous frequency at which state $\vec{j}$ is entered from any other state at time *t*.

As in 6.2.1, states involved in the top events of interest should be first identified, using the MCS techniques, then expanded to account for the component dependencies, so as to determine Markov states. It amounts to a great number of potential state probabilities to evaluate, this being the most important limitation of using Markov techniques for large sets of plant components. Grouping of states becomes necessary and some general grouping techniques have been devised.

Additional extensions of the Markov theory are possible in cases where the probability to stay in a given state during a sojourn time also depends on the time at which the state was entered (semi-Markov systems). Some additional details about them are given in section 6.4.

In a typical plant, there are a lot of components and component configurations, and component failure rates are often independent on the configuration, but not at times. The possibility exists to provide a modelling scheme that combines the virtues of both classical and Markov approaches. Markov modelling then handles the configuration dependent portion that becomes of reasonable size.

6.3. Uncertainties in frequency evaluation

In section 2 above it was discussed how the PSA techniques are by their very nature a way to analyze aleatory uncertainties associated to the behavior of a plant, especially under accident conditions. The outcome of this analysis is the expected likelihood (i.e., expected frequency) of the damage states of interest. However, it was also noted that the parameters involved in the frequency quantification model are also subject to uncertainty (usually modeled as epistemic), leading to a double loop solution scheme. This scheme is usually applied in classical PSA where the input parameter uncertainty is propagated throughout the model in order to characterize the uncertainty of the PSA outputs.

For analyses in the risk space, where the frequency calculation is expected to be more closely coupled to dynamic calculations, the external uncertainty loop, should also include the propagation of the parametric uncertainties of the plant simulation models. The discussion on the uncertainties in plant simulations included in previous sections is not, therefore, decoupled from the uncertainty in frequency evaluation. However, we are focusing in this section in those aspects of uncertainty wich are more frequency-specific and are currently addressed in classical PSA methods.

The way reliability data are collected makes the failure parameters amenable to statistical treatment. Large industry databases are maintained with failure data (probability of failure on demand, rate of failure to run, etc.) that are collected from a large sample of equipment serviced at different plants around the world. The values provided by these databases are the mean value for the parameter and a statistical distribution of possible values reflecting those observed. These distributions represent industry averages and are often corrected with plant-specific data by means of Bayesian analyses to take into account the actual operating experience of the plant. The Bayesian analysis then provides plant-specific distributions without discarding the generic information.

The PSA basic events are thus represented by a distribution whose mean value is taken as point estimate for the initial quantification. Once the MCS list is obtained with the point values (mean values of the parameters), the parameter distributions are propagated to provide a distribution of the outcome.

PSA computer programs offer different techniques to compute the uncertainty distribution of the core damage frequency. In general, they are based on Monte Carlo (MC) simulation, taking samples from

the joint distributions of the parameters and running simulations, i.e. computing the CD frequency using the values sampled. To achieve a given degree of accuracy by pure MC runs, the number of simulations needed may be too large to be of practical use. Because of this, modified MC methods are used, in which the samples are intelligently taken to achieve high accuracy with a minimum of runs.

The most extended method is *Latin Hypercube* sampling. Latin Hypercube is implemented in most, if not all, of the PSA software suites currently in widespread use. It proceeds by dividing the range of probable values of each parameter (say n parameters) in a given number (say m) of equally probable segments. This provides a matrix of $m \times n$ cells. However, instead of calculating the m^n possible combinations of parameter samples, the method proceeds by running precisely m cases, each of them using parameter samples belonging to different segments. In other words, samples for each case are taken in such a way that each row and each column of the cell matrix provides exactly one parameter value. Within each cell, a random sample is used to obtain the value. The results of the m runs are then statistically treated to obtain any percentile of the output uncertainty distribution.

6.4 Coupling between probability and dynamics

Several issues have been identified (see for instance [60]) concerning improvements in the quantification of core damage frequency as performed in current PSAs. As noted in previous sections, current PSA quantification methodologies are approximate in two respects, stemming from the need to obtain the MCS list prior to obtaining the value of the frequency. The first is the very process of construction of the MCS list, which, due to the huge amount of elements, has to be truncated so that it will contain only MCSs above a predetermined value. Secondly, even the frequency calculation of this truncated MCS list is not exact. The rule for obtaining the probability of the union of two sets with non-void intersection (equally valid for the frequency calculation), when recursively applied to a large number of sets, implies an exponential growth in the number of terms that make up the final probability (frequency) value. Binary Decision Diagrams were shown as a possible improvement in frequency quantification.

Other approximations exist within PSA, however. Most of the parameters in a PSA are composed of rates of occurrence that must be converted into probability. This is done by considering a mission time applicable to failure-to-run events and by surveillance and test intervals applicable to failure-in-stand-by events. Mission times are generally defined as the time a mitigating system has to operate to perform its safety function. The detailed assessment of this time will depend on the characteristics of the initiator and on the state of the plant equipment for each sequence, and bear strong dependencies with the plant dynamic evolution. General mission times are thus considered. These are typically of 24 hours extent, but may be reduced (e.g. in EDG operation) if granted by adequate analysis (in the example, off-site power restoration). However, considering 24 hours is also an approximation (conservative as it might be) and does not take into account other possible dynamic evolutions that may impact the probability of failure. Besides, dynamic interactions have also an impact in considering the operators' response times, which are intrinsically random, albeit driven by stimuli (control room alarms). The effect of this random time of response in the frequency quantification is not taken into account in current PSAs and needs some developments to be carried out.

Also significant is the time dependencies in the quantification of the probability of failure given maintenance, test and surveillance schedules. Maintenance schemes of trains within a system are often staggered to allow for at-power maintenance of systems subjected to technical specifications. These maintenance schemes imply different absolute times in the maintenance activities (although the intervals in between may be similar), providing a different time evolution of the probability of failure of the joint system. The combination of the different reliability functions in time produces a time profile of the risk

that is not generally taken into account, but that may be significant. Markov models can and should be used in this respect to obtain a better picture of the combined risk.

In addition to the above considerations, as indicated at the beginning of this chapter, the evaluation of the frequency of exceedance of a safety objective, requires to identify first the accident paths going beyond that objective, then to group them into sequences. Safety objectives are described in terms of range of values of safety variables such that, if the plant state is within those ranges, there is a non-negligible probability of unacceptable damage. These states are also denoted *damage states*. Note that, in general, there will be a different set of safety variables for each safety objective.

Since safety variables are functions of the plant process variables *during transients,* the key point to identify situations exceeding safety objectives is the evolution of the process variables along accident paths. Any plant transient states, including damage states, are the result of the plant evolution from a steady state, due to a set of events occurring at different times. This considerably reduces the number of transient states to be considered for evaluation of damage state frequencies. In order to characterize accident paths, the dynamic and reliability models used to represent the plant behaviour should describe:

1. The initial steady states that are possible prior to any of the faults considered as initiating events
2. The boundary conditions as required to limit the scope of the model and to model the initiating faults. These are given by a set of variables depending on the accident time. Safety system actuations may be included in the plant model or be modelled as boundary conditions (for instance a given safety injection flow).
3. The times at which the events of the sequence do occur or equivalent information to determine them.
4. The set of systems that may fail or not, which determine some of the events in the sequence. These systems will be associated to the sequence headers and their corresponding branching points in event tree sequences.
5. The sequence of possible stochastic phenomena, potentially altering the course of the accident (phenomena headers of an accident progression event tree (APET) in PSA level 2 for instance).

For a fixed sequence, items 4 and 5 are fixed, but there will be a lot of paths depending on the other items. Items 1 and 2 depend on the TH model and on the grouping of initiating events, and the final choice should result from an envelope analysis. Item 3 reflects the initiating criteria for reactor trip and safeguard actuations, or in other words, the impact of the automatic protection system and the emergency operating procedures as well as anything else involved in the decision making process for initiating protection measures. It is clear that protective measures should come on time, so to ensure adequate timing in between the events of the sequence is necessary to describe damage states. The implication of this for the exceedance frequency calculation is that merely identifying top events in static fault and event trees is not enough to identify a damage state. Additional consideration of the timing of the events during the accident is essential.

6.4.1 Treatment of the demand probability in traditional PSA

In traditional PSA, due consideration is given to the sequence delineation problem i.e. finding success and damage sequences relative to specific safety objectives, namely, safety limits of severe core damage and LER. As noted before, consideration of a sequence implies the assumption that the sequence safety functions will be *demanded* by all the sequence transient paths, i.e., that the corresponding safeguard

initiation signals or operator alarms are being activated. The delineation process may then be interpreted as taking the probability of the demand either one or zero for the whole set of transient paths with the same sequence headers. In addition, all of them are classified either as damage or success paths.

Provided no damage path is implicitly included in any success sequence, (a fact difficult to prove when considering the grouping of initial faults, initial conditions and boundary conditions of the grouped transients in every single sequence) this approach is conservative, but it may be nonetheless unrealistic, leading for instance to a wrong perception of dominant failure sequences whose frequency has been actually "inflated".

A complete quantification of the contribution of a sequence to the exceedance frequency of the safety objective can be grossly summarized as follows:

Damage sequence frequency (year^{-1}) =
frequency of the initiator (year^{-1})×
probability of the set of the sequence header fault trees (1/sequence demand)×
probability of the demand ×
fraction of sequence paths leading to exceedance of the safety objective.

but the last two terms are taken either 0 or 1 in the traditional analysis, while the first two terms have been extensively discussed in section 6.2 earlier.

However, if these approximations are too conservative, yielding unacceptable frequency numbers, additional headers (provided they can be proved to be demanded) may be used to further discriminate the damage path groups that may have been mixed together with an excessive number of success paths. Alternatively, modifications to the header success and failure criteria may be attempted, the header success criteria becoming sequence dependent. This approach is actually used for instance with regard to available time considerations for human actions.

Either way, it is necessary a detailed thermal-hydraulic analysis to show that the regrouping result is acceptable. This proof has the same purpose as the safety analysis of design basis accidents, but it may require additional runs. This is discussed in the next section.

6.4.2 Elements of PSA which include dynamic dependencies. Application to safety margins.

As indicated above, grouping of accident paths into event tree sequences depends on:

- The safety objective being analysed
- The sequence considered and its headers success or failure criteria.
- The initial and boundary conditions.

Typically, when the safety objective is that of the traditional PSA, and in order to prove the adequacy of the transient path grouping, the PSA-TH analysis hinges on **a portion** of the design basis safety analysis performed. Indeed, not all of the safety objectives of the safety study are PSA related, but only those for the so called *Condition IV* or *postulated* events. Nonetheless, reliance on accident analysis establishes a complex feedback among design assumptions, design transient analysis (and its consequences like Tec-Specs), sequence delineation and system success criteria with its corresponding fault tree modelling.

Even within the classical PSA scope, analyses supplementing the design basis ones are also performed in order to evaluate additional aspects or new headers beyond those already implicit in the design basis

transients. This is usually necessary at least when human actions are required during the sequence. Even when operator actions are considered in design basis analyses, their reliability is not quantified and, in order to calculate the sequence frequency, it is necessary to estimate the available time to perform the action. This refining process is commonly done with the aid of low detail "parametric" models and /or more detailed, best estimate TH codes.

It should be noted however that in the context of safety margins, the safety objectives corresponding to additional safety limits, like for instance those of *Condition II* and *III* events and, more generally, the extension to the risk space should be addressed. Thus, the scope of the frequency margin probabilistic analysis is larger, even if the probabilistic techniques used are the same. New sequences, success criteria, available times, etc, may be needed for the additional safety objectives.

The final result of this process is the detailed specification of the sequence fault trees for all the event trees to be quantified with the techniques of section 0. All of these dynamic elements then permeate the event trees and sequence header descriptions and models. For instance, header fault tree models may reflect some of these dynamic elements not only in their top event success criteria, but also in the boolean model itself. In this regard, *house* events are often used to represent sequence-specific boundary conditions, which are consequential to the sequence initiator and previous headers.

As a consequence, plant changes require a review of the plant PSA to ensure the consistency of the PSA models with the changes introduced that may affect any of these dynamic elements. If, in addition, a safety margin assessment is to be considered, one should extend the PSA model scope to the risk space and include the consideration of additional safety objectives. In order to make that extension in an efficient way, some new techniques may be helpful that are discussed next.

6.4.3 Some ideas to solve the dynamics/probability coupling in frequency margin calculations.

When extending the number of safety objectives to be analyzed, it may be inefficient to repeat the exceedance frequency calculation process once and again for each objective. Rather, it should be taken into account that these safety objectives are not totally independent and their exceedance frequencies are then correlated between themselves. For instance, radiological releases of outer barriers require at least partial loss of integrity of inner ones. So, limiting the frequency of exceedance of safety objectives related to an inner barrier will also contribute to bound that of an outer one, as this is the very purpose of the barrier philosophy.

In classical PSA, this principle translates in the so called binning process whereby for instance only sequences degrading the core (PSA-1 damage sequences) are considered in general as candidates for source terms (PSA-2). Although the traditional PSA is mainly looking at low frequency high radiological release sequences, this principle may be extended to the higher frequency lower damage range as well. For instance, in PWR´s, after a successful reactor trip, cooling degradation problems require the primary circuit coolant to lose the sub-cooling margin somewhere, so reaching saturation conditions. The same can be said of other critical safety functions, all of them necessary conditions for barrier degradation.

It is then of interest an approach able to link the exceedance frequencies of different safety objectives. For instance, able to correlate a barrier failure mode with those of prior barriers, and/or with the frequency of exceedance of required conditions for each of them. On the other hand, as grossly described in section 0 above, the classical probabilistic approach reduces in practice the calculation of safety objective exceedance frequencies to the quantification of initiating events and sequence headers. As shown in section 6.2.3, an underlying assumption of this approach is that the events follow a Markov stochastic process, so the analysis depends on the validity of this assumption and its implications.

One of those is that events may occur at any time with a given rate, and such that the frequency of entering a given state is independent on the time of entry. This assumption is reasonable in the long term time scale for random events, as for instance during the pre-accident period, but it is not so for the sequence of consequential events following an initiator. Extensions of Markov processes to relax these assumptions have been derived, and work is underway to apply them to real cases. On the other hand, these extensions also allow the probability of the demand, as well as the fraction of paths leading to exceedance of safety objective, to be more adequately addressed.

For instance, Markov extensions have been developed for cases where the transition rates depend on process variables, (theory of probabilistic dynamics, TPD). It has been shown that the classical event tree approach (i.e., setting the probability of the demand to 1 or 0) remains valid for sequences of events instantaneously triggered by setpoint crossing, with the additional assumption that a setpoint is deactivated immediately after its associated event has been triggered.

However, in some unfortunately frequent cases, there is a stochastic time delay since the activation of setpoints and/or they are not deactivated after the events. For instance, operators introduce delays in taking potentially different actions after alarms that may remain concurrently activated. In these cases, competing event mechanisms complicate the situation.

More generally, the same occurs whenever for the events to occur, some conditions ought to be fulfilled that depend on the accident paths followed. These conditions may persist after the events. A typical example is the occurrence of combustion phenomena only if flammability conditions are met, with delays potentially resulting from stochastic ignition conditions and with potential for multiple combustions if the flammability conditions persist. Those more general conditions (including setpoints as particular cases) may be considered as stimuli for the events. When accident paths reach those conditions, we speak of the paths “activating stimuli”.

Because stimuli activation conditions the events, the history of activations during the accident paths do matter in calculating the frequencies, and extensions of the Markov process equations accounting for these features are necessary. Those extensions constitute the so called *Stimulus Driven Theory of Probabilistic Dynamics* (SDTPD) [61]. It exhibits as a nice feature an explicit relation between the different exceedance frequencies in the terms explained above.

Indeed, SDTPD provides mathematical balances to calculate the probabilities per unit time of entering states with specified activated stimuli and correlate them with each other. In addition, in the calculation of the exceedance frequencies, the probability of the demand and the fraction of damage paths are not factorized but rather embedded in the activation of the stimuli. Exceeding safety objectives is a particular case of stimulus, so SDTPD has the potential for analyzing multiple safety objectives. Work is in progress to better relate the SDTPD theory with the classical probabilistic approach, so as to allow hybrid schemes to be used.

7. CONCLUSIONS

The industry is focusing on development and application of new licensing BEPU methods. The uncertainty analysis with random sampling of input parameters and nonparametric statistical tolerance limits for estimating the uncertainty of output parameters has become widely accepted. The response surface techniques and Monte Carlo sampling are still suitable, mostly for prediction of single value parameters like peak cladding temperature during LBLOCA. The existing BEPU methods seem mature enough for application while future research may focus on the codes with internal assessment of uncertainty. Nevertheless, realistic calculations with conservative input and boundary and initial conditions (the so-called best estimate bounding and realistic conservative approach) will continue in wide use, especially for risk space applications.

On the other hand, frequency calculations are essential ingredients of analyses in the risk space. Usual methods in current PSA show some limitations in accuracy and effectiveness, especially if they are being used in the risk space. However, they can be extended and/or complemented so as to be applied for analysis of multiple safety objectives where the influence of the dynamic state of the plant can be fully taken into account.References

8. REFERENCES

[1] IAEA, “Accident Analysis for Nuclear Power Plants”, Safety Report Series No. 23, International Atomic Energy Agency, Vienna, 2002.

[2] R. Herrero, J.M. Izquierdo, "Development of a computer tool for in-depth analysis and postprocessing of the RELAP5 thermalhydraulic code". Submitted to the USNRC for publication as NUREG/IA report.

[3] OECD/NEA, “Separate Effects Test Matrix for Thermal-Hydraulic Code Validation”, NEA/CSNI/R(93)14/Part. 1/Rev., Volume 1, Phenomena Characterization and Selection of Facilities and Tests, September 1993.

[4] OECD/NEA, “Separate Effects Test Matrix for Thermal-Hydraulic Code Validation”, NEA/CSNI/R(93)14/Part. 2/Rev., Volume 2, Facility and Experimental Characteristics, September 1993.

[5] Writing Group Committee of the PWG2, “CSNI Integral Test Facility Validation Matrix for the Assessment of Thermal-Hydraulic Codes for LWR LOCA and Transients”, CSNI Report 132/Revision 6, June 1995 (Restricted).

[6] IAEA, “Safety margins of operating reactors, Analyses of uncertainties and implications for decision making”, IAEA TEC-DOC-1332, Vienna, 2003.

[7] OECD/CSNI, “Report of a CSNI workshop on Uncertainty analysis methods, London 1-4 March 1994”, NEA/CSNI/R(1994)20, Vol. 1 and 2, OECD/NEA/CSNI, Paris, 1994.

[8] CSNI’s BEMUSE Phase I Report “Presentation a prioir of the uncertainty evaluation methodology to be used by the participants” [NEA/SEN/SIN/AMA(2005)1]

[9] USNRC, 10CFR50, “50.46 Acceptance criteria for emergency cooling systems for light water nuclear power reactors” and “App. K, ECCS evaluation models”, USNRC 1994.

[10] D. Bessette, “Initial and boundary conditions to LOCA analysis: An examination of the requirements of Appendix K”, ICONE-8, ASME, Baltimore, USA, April 2-6, 2000.

[11] Compendium of ECCS Research for Realistic LOCA Analysis, NUREG-1230, August 1988.

[12] USNRC, “Emergency Core Cooling Systems, Revisions to Acceptance Criteria”, Federal Register 53, 180, September 16, 1988.

[13] Technical Program Group: Boyack, B. E., Catton, I., Duffey, R. B., Griffith, P., Katsma, K. R., Lellouche, G. S., Levy, S., Rohatgi, U. S., Wilson, G. E., Wulff, W., and Zuber, N., “Quantifying Reactor Safety Margin Parts 1 to 6”, Nucl. Eng. Des., 119, 1990, pp. 1-117.

[14] Technical Program Group, “Quantifying Reactor Safety Margins”, NUREG/CR-5249, December 1989.

[15] OECD/CSNI, “Report on the Uncertainty Methods Study”, Report *NEA/CSNI/R(97)35*, Vol. 1 and 2, OECD/NEA/CSNI, Paris, 1997.

[16] USNRC and OECD/CSNI, “Proceedings of the OECD/CSNI Workshop on Transient Thermalhydraulic and Neutronic Codes Requirements held in Annapolis”, US NRC *NUREG/CP-0159* and OECD/CSNI Report *NEA/CSNI R(97)4*, Washington, DC, USA.

[17] OECD/CSNI, "Best-estimate Methods in Thermal Hydraulic Safety Analysis: Summary and conclusions of an OECD-CSNI Seminar", Report *NEA/CSNI/R(99)22*, Paris, 1999.

[18] OECD/CSNI, "Advanced Thermal-hydraulic and Neutronic Codes: Current and Future Applications", Report *NEA/CSNI/R(2001)9*, Paris, 2001

[19] A. Prošek, B. Mavko, "BEPU methods and combining of uncertainties", International meeting on updates in best estimate methods in nuclear installation safety analysis, BE-2004, November 14-18,2004, Washington, D.C., American Nuclear Society, 2004.

[20] A. Prošek, B. Mavko, "Response surface generation with optimal statistical estimator", J. of Mechanical Engineering, 46(1), pp. 14-23 (2000).

[21] B. Mavko, A. Stritar, A. Prošek, "Application of Code Scaling, Applicability and Uncertainty Methodology to Large Break LOCA Analysis of Two-Loop PWR", Nucl. Eng. Des., 143, pp. 95-109 (1993).

[22] A. Prošek, B. Mavko, "Evaluating Code Uncertainty - II: An Optimal Statistical Estimator Method to Evaluate the Uncertainties of Calculated Time Trends", Nucl. Technol., 126, pp. 186-195 (1999).

[23] W. T. Nutt, G. B. Wallis, "Evaluation of nuclear safety from the outputs of computer codes in the presence of uncertainties", Reliab. Eng. Syst. Safe., 83, pp. 57–77 (2004).

[24] F. D'Auria, W. Giannotti, "Development of a Code with the Capability of Internal Assessment of Uncertainty", Nucl. Technol., 131(2), pp 159-196 (2000).

[25] M. D. McKay, "Evaluating Prediction Uncertainty", NUREG/CR-6311, March 1995.

[26] USNRC, "Proceedings of the International Workshop on Uncertainty, Sensitivity, and Parameter Estimation for Multimedia Environmental Modeling", August 19-21, 2003, Rockville, MD, NUREG/CP-0187.

[27] B. Mavko, A. Prošek, "Thermal-hydraulic safety analyses supporting the steam generator replacement and uprating at Krško nuclear power plant", Journal of Mechanical Engineering, 2000, vol. 46, no. 4, 230-241.

[28] M. Trow, D.B. Newland, The Sizewell 'B' large LOCA uncertainty methodology, FED-Vol.223, Validation of System Transients Analyses Codes, ASME 1995.

[29] R. Ashley, N. Hollasky, M. Vincke, J. Vlassenbroeck, "Use of Best-Estimate Methods for Licensing Purposes in Belgium, International meeting on updates in best estimate methods in nuclear installation safety analysis", BE-2004, November 14-18,2004, Washington, D.C., American Nuclear Society, 2004

[30] J. Zhang, "The Tractebel Deterministic Bounding Approach to Accident Analysis", Proceedings of an OECD Exploratory Meeting of Experts on Best Estimate Calculations and Uncertainty Analysis, Aix-en-Provence, France, 13-14 May 2002, NEA/CSNI/R(2002)15, 2002.

[31] J. Zhang, S. Bosso, X. Henno, K. Ouliddren, C. R. Schneidesch and W. Van Hove, "Coupled RELAP5/PANTHER/COBRA Steam Line Break Accident Analysis in Support of Licensing Doel 2 Power Uprate and Steam Generator Replacement", International meeting on updates in best estimate methods in nuclear installation safety analysis, BE-2004, November 14-18, 2004, Washington, D.C., American Nuclear Society, 2004.

[32] H. Glaeser, "Large Break LOCA Uncertainty Evaluation and Comparison with Conservative Calculation, International meeting on updates in best estimate methods in nuclear installation safety analysis", BE-2004, November 14-18,2004, Washington, D.C., American Nuclear Society, 2004.

[33] J. Y. Sauvage, S. Laroche, "Validation of the Deterministic Realistic Method applied to Cathare on LB LOCA experiments", 10th International Conference on Nuclear Engineering (ICONE-10), Arlington, Virginia, April 14-18, 2002.

[34] M. G. Ortiz, L. S. Ghan, "Uncertainty Analysis of Minimum Vessel Liquid Inventory During a Small-Break LOCA in a B&W plant - An Application of the CSAU Methodology Using the RELAP5/MOD3 Computer Code", NUREG/CR-5818, EGG-2665, Idaho National Engineering Laboratory (1992).

[35] F. D'Auria, N. Debrecin, G. M. Galassi, "Outline of the Uncertainty Methodology Based on Accuracy Extrapolation", Nucl. Technol., 109, pp. 21-38 (1995).

[36] M. Y. Young, et al, "Application of code scaling applicability and uncertainty methodology to the Large Break LOCA", Nucle Eng Des. 186 (1-2), 39-52, 1998.

[37] J. Zhang, S.M. Bajorek, R. M.Kemper, M.E. Nissley, N. Petkov and L.H. Hochreiter, "Application of the WCOBRA/TRAC best estimate methodology to the AP600 Large Break LOCA analysis", Nucle Eng Des. 186 (1-2), 279-301, 1998.

[38] H. Glaeser, "Uncertainty evaluation of thermal-hydraulic code results", Proc. Int. Mtg. BE-2000, Washington, DC, November 12-16, American Nuclear Society (2000).

[39] H. Glaeser, "Large Break LOCA Uncertainty Evaluation and Comparison with Conservative Calculation", Best Estimate-2004: International Meeting on Updates in Best Estimate Methods in Nuclear Installations Safety Analysis, Washington, DC, November 14-18, 2004.

[40] C. H. Ban, S. Y. Lee, C. K. Sung, "Development and Application of KEPRI Realistic Evaluation Methodology (KREM) for LB-LOCA", Best Estimate-2004: International Meeting on Updates in Best Estimate Methods in Nuclear Installations Safety Analysis, Washington, DC, November 14-18, 2004.

[41] R. P. Martin, L. D. O'Dell, "AREVA's realistic large break LOCA analysis methodology", Nuclear Engineering and Design, 235, pp. 1713–1725 (2005).

[42] K. Muftuoglu, K. Ohkawa, C. Frepoli, M. Nissley, "Comparison of Realistic Large Break LOCA Analyses of a 3-Loop Westinghouse Plant Using Response Surface and Statistical Sampling Techniques", 12th International Conference on Nuclear Engineering ICONE-12, Arlington, Virginia, April 25-29, 2004.

[43] R. C. Borges, F. D'Auria, A. C. M. Alvim, "Independent Qualification of the CIAU Tool Based on the Uncertainty Estimate in the Prediction of Angra 1 NPP Inadvertent Load rejection Transient", 10th International Conference on Nuclear Engineering (ICONE-10), Arlington, Virginia, April 14-18, 2002.

[44] OECD/CSNI/SMAP, "Definition of Generalized Concepts of Safety Margins and Characterization of Safety Margin Sources", NEA/SEN/SINSMAP(2005)3, August 2005.

[45] IAEA, "Guidelines for Application of the Master Curve Approach to Pressure Vessel Integrity in Nuclear Power Plants", Technical Reports Series No. 429, March 2005.

[46] R. Ashley, M. El-Shanawany, F. Eltawila and F. D'Auria, "Good Practices for User Effect Reduction", NEA/CSNI/R(98)22, November 1998.

[47] S. N. Aksan, F. D'Auria and H. Städtke, "User Effects on the Transient System Code Calculations", NEA/CSNI/R(94)35, January 1995.

[48] K. Trambauer, "Computer and Compiler Effects on Code Results", NEA/CSNI/R(96)15, January 1997.

[49] J.M. Izquierdo, J. Hortal, L. Vanhoenacker, "Merits and limits of thermalhydraulic plant simulations - towards a unified approach to qualify plant models", Nuc. Eng. & Des. 145 (1993) 175-205.

[50] Roberts N. H., W. E. Vesely, D. F. Haasl, F. F. Goldberg, "Fault Tree Handbook", NUREG-0492, US NRC, Washington, 1981.

[51] IAEA, "Guidelines for Application of the Master Curve Approach to Pressure Vessel Integrity in Nuclear Power Plants", Technical Reports Series No. 429, March 2005.

[52] W. Vesely, J. Dugan, J. Fragola, J. Minarick, J. Railsback, Fault Tree Handbook with Aerospace Applications, National Aeronautics and Space Administration, NASA, 2002

[53] Čepin M., B. Mavko, A Dynamic Fault Tree, Reliability Engineering and System Safety, 2002; 75 (1): 83-91.

[54] S. Epstein, A. Rauzy, "Can we thrust PRA?", Reliability Engineering and System safety, 88, 195-205, 2005.

[55] I.A. Papazoglou, "Mathematical foundations of event trees", Reliability Engineering and System safety, 61, 169-183, 1998.

[56] B. Akers, "Binary Decision Diagrams. IEEE Transactions on Computers", 27(6):509–516, 1978.

[57] Henrik Reif Andersen, "An Introduction to Binary Decision Diagrams", http://www.itu.dk/people/hra/notes-index.html, 1997.

[58] Randall E. Bryant, "Graph based algorithms for boolean function manipulation", IEEE Transactions on Computers, 35(8):677–691, 1986.

[59] Antoine Rauzy, "A brief introduction to Binary Decision Diagrams", Journal Europŭen des Systumes Automatisŭs, 30(8):1033–1050, 1996.

[60] USNRC, "Issues and Recommendations for Advancement of PRA Technology in Risk-Informed Decision Making (NUREG/CR-6813)", April 2003.

[61] P. E. Labeau, J. M. Izquierdo, "Modeling PSA Problems - I: The Stimulus-Driven Theory of Probabilistic Dynamics", Nuclear Science and Engineering, 150(2), 115-139, 2005.