TOPSAFE

Dubrovnik, Croatia, 30.09 - 3.10.2008

TopSafe 2008

Transactions

Dubrovnik, Croatia
30.9. - 3.10.2008

HND

AEN
NEA

IAEA
International Atomic Energy Agency
Atoms For Peace

European Nuclear Society
Rue Belliard 65
1040 Brussels, Belgium
Phone + 32 2 505 30 54
Fax +32 2 502 39 02
E-mail ens@euronuclear.org
Internet www.euronuclear.org

ISBN 978-92-95064-06-5

These transactions contain all contributions submitted by 30 September 2008.

The content of contributions published in this book reflects solely the opinions of the authors concerned. The European Nuclear Society is not responsible for details published and the accuracy of data presented.

Licensing and Harmonisation

TOPSAFE
Dubrovnik, Croatia, 30.09 - 3.10.2008

Regulatory Challenges Posed by the "Best-estimate Plus Uncertainty" Methodologies

Rafael Mendizábal, Fernando Pelayo
Consejo de Seguridad Nuclear
Pedro Justo Dorado Dellmans, 11, 28040 Madrid, Spain
rmsanz@csn.es, fpl@csn.es

ABSTRACT

Realistic methodologies are gradually replacing the simpler and overconservative traditional ones in the realm of the deterministic safety analysis (DSA) of nuclear power plants. Such new approaches make use of realistic rather than pessimistic models and hypotheses, and must include uncertainty assessments of the important results, the term "best-estimate plus uncertainty" (BEPU) methodologies stemming from that fact. The safety acceptance criteria are correspondingly moving from a deterministic to a probabilistic shape. As a result, probabilistic definitions are currently being proposed for the safety margins, and statistical methodologies are now an essential part in the DSA toolkit. In this paper the main ideas about the DSA methodologies, and the differences between the conservative and realistic approaches, are described. The most widely used BEPU methodologies are based on Monte Carlo calculations performed with the predictive models, and feature order statistics method of uncertainty assessment (also known as Wilks method). In the present paper, such methodologies are described and discussed from a regulatory point of view, and insights obtained from the evaluation work conducted by the authors for Spain's regulatory authority are presented.

1 INTRODUCTION

Deterministic Safety Analysis (DSA) is one of the frameworks used in the design and safety evaluation of nuclear power plants (NPP). The risk posed by a NPP is described by the accidents which can occur therein, each one typified by its frequency and consequences. The DSA basically consists in assessing the damage level which is exceeded with a given frequency, and comparing it with a limit or acceptable value, whereas the Probabilistic Safety Analysis (PSA) has the complementary task of calculating the frequency of exceedance of a given damage level and comparing it with a limit or acceptable value.

The basis of the DSA consists in assessing the consequences of a group of selected transients or accidents, named Design Basis Transients (DBT) and defined as enveloping or bounding transients in the sense that their consequences (damage) are worse than those of the great majority of transients deriving from the same initiating event.

The consequences of the DBTs must be calculated using predictive models, and the results are compared to the safety limits. Nevertheless, as it is well known, the calculation processes introduce uncertainty in the results, for two main reasons:

(i) The inputs to the calculation (for instance, the conditions existing in the plant at the beginning and during the transient) are imperfectly known.

(ii) The predictive models used in the calculation are not perfect, because they are simplified views of the physical reality.

The conclusion is that the calculated consequences of a DBT have uncertainty, and this fact must be taken into account when checking the fulfilment of the safety criteria. In the safety sciences, a principle exists to deal with uncertainty: the risk must be assessed in a conservative (or pessimistic, or bounding…) fashion. In the DSA this means that the calculated consequences must be worse than the real ones with high confidence.

In this paper we will describe the formalism of DSA and distinguish between the different types of deterministic methodologies according to the type of predictive models and calculation hypotheses being used. The realistic (also known as BEPU) methodologies will be introduced, as an evolution of the traditional conservative ones. The most widely used BEPU methodologies are based in Monte Carlo analysis, and some challenges posed by them in the regulatory activities are described. Most insights have been obtained in the evaluation work performed by the authors for the Consejo de Seguridad Nuclear (Spain's nuclear authority).

2 THE FORMALISM OF DSA. CONSERVATIVE METHODOLOGIES

The DSA is based on calculations of accident consequences performed with predictive models. The models are deterministic, in two senses: first, they do not explicitly involve probabilities; second, they do not contain random number generators, so that two calculations with exactly the same input give the same results.

To fix some ideas let us suppose an accident or transient A deriving from an initiating event IE in a NPP and being simulated with a realistic and deterministic predictive model M, which can be viewed as a transformation from an input vector X into an output vector Y:

$$Y = M(X) \qquad (1)$$

It is assumed that the model M is composed by several submodels and correlations and the input vector X contains all the data which are needed by the model to perform the calculation of Y for the transient A, including parameters which describe the plant and the accident, initial and boundary conditions and model parameters. Most of these inputs correspond to physical magnitudes which have a real or true value, and are estimated by measure, control, calculation, expert elicitation…or combinations of them. Therefore, these inputs have uncertainty. It is the case of initial and boundary conditions, geometrical parameters,…, and also of the empirical parameters contained in the submodels and correlations of M, which are adjusted through comparison with real data.

On the contrary, there are other inputs which have no "true" value, and their existence shows the imperfection of the model. That is the case of the parameters related to the discretization process conducted for solving differential equations, such as time step and spatial node sizes. They are not properly uncertain parameters, but their presence introduces errors in the value of the outputs (i.e. deviation from their true value). And such errors are uncertain, because they are not perfectly known.

Therefore, the components of X can be roughly grouped in two categories:

1. Parameters representing real magnitudes
2. Parameters stemming from the imperfection of the model

The output vector Y includes the results of the calculation which are important from the safety point the view, especially those intervening in the acceptance criteria for the transient. According to our previous discussion, the outputs have uncertainty coming from two main sources: the uncertainty of the inputs, propagated through M, and the imperfection of M. In what follows we will suppose that fixed values are assigned to the parameters in the category 2, so as to give a conservative bias to Y. Then, all the uncertainty of Y is propagated from the inputs of category 1.

The uncertain magnitudes are classically described as random variables. In the sequel X will represent a multidimensional random variable.

We will focus on the simplest case, when Y is a scalar safety output, and further assume that the higher Y, the worse the consequences, so that Y has an upper safety limit L. The limit L is considered as a scalar, non-random magnitude, determined as a conservative (i.e. low) estimation of a damage threshold. This simple setting permits to lay down the main ideas about the deterministic analysis and the statistical methodologies.

Following [1,2], we define the probabilistic safety margin (PSM) of Y in A as:

$$PSM(Y;A) = PR\{Y < L / A\} \qquad (3)$$

, namely the probability of Y being under the limit L conditioned to the occurrence of the transient A. It is clearly a safety margin, because it measures the distance from Y to its "forbidden region" (from the safety point of view). The definition (3) is still valid in the case that L has uncertainty. Also, the definition is easily generalized when Y is a multidimensional vector (e.g when Y describes multiple failure modes of a safety barrier) [1,2]

The objective of DSA is to demonstrate that the PSM takes a high value, or, in other words, that, with a high enough probability, the safety limits are not violated. The procedure to achieve this goal has two steps:

1) A highly conservative value of Y, which we will name Y_{lic} (the subscript deriving from "licensing") is obtained
2) The safety acceptance criterion is stated as Y_{lic}<L

For obtaining Y_{lic}, the concept of Design Basis Transient (DBT) is used. In our simple case, given two realizations X_1 and X_2 of the input X, we will say that X_2 bounds or envelops X_1 (and write $X_2 \succ X_1$) whenever Y_2=M(X_2) is higher than Y_1=M(X_1):

$$X_2 \succ X_1 \quad \Leftrightarrow \quad M(X_2) > M(X_1) \qquad (4)$$

In mathematical terms, (4) defines an order relation, and the inputs to M can thus be ordered according to their bounding or enveloping character.

Given an initiating event IE in a NPP, a DBT for IE is an accident sequence deriving from IE and built in such a way that it bounds a majority of the sequences deriving from IE. The DBT is constructed by using the criteria of “defence-in depth”, for instance postulating some “additional failures” in safety systems that must cope with the accident (this means that some inputs are set to overconservative values) and furthermore choosing the time and space discretization schemes so that additional conservatism is introduced. Let us call XD the input corresponding to the DBT and YD≡M(XD). Then the following probability

$$PR\{XD \succ X\} \qquad (5)$$

which, according to (4), coincides with

$$PR\{YD > M(X)\} \qquad (6)$$

takes, by definition, a very high value (i.e. very close to 1). The probability in (5) represents the fraction of accidents deriving from IE and bounded by the DBT. The probability in (6) is an analogue to the PSM defined in (3), but with YD instead of L, and so it measures the smallness of the random variable Y≡M(X) with respect to the random variable YD. We call (6) the probabilistic analytical margin associated to the DBT, and obviously measures the DBT conservative character.

In summary, DBTs are defined as transients which bound a majority of transients with the same origin (initiating event), so that they keep a high analytical margin with respect to the safety output.

XD still has uncertain components. Thus YD has uncertainty, propagated from these inputs. A probabilistic safety margin can be associated to YD:

$$PSM(YD) = PR\{YD < L\} \qquad (7)$$

The bounding condition of the DBT implies that PSM(YD) is lower that PSM(Y).

The methodologies for performing the DSA can be classified according to their more or less realistic character. Here we will refer to two basic categories, the so-called conservative and realistic methodologies. The terms are a little misleading, because both of them use the DBT concept and so they are clearly conservative. The DBT is *a priori* built (i.e. before performing safety calculations), and the difference appears in the procedure for calculating Y_{lic}. In conservative methodologies, Y_{lic} is obtained by assigning fixed values to the uncertain inputs of XD. A worst case scenario is defined, in such a way that a number of important inputs (i.e. those influential on the results) are given conservative (even overconservative) values and the remaining, less important, inputs are kept in nominal or mean values. In this way, XD transforms into a non-random, very bounding input X_{lim} (limiting input) and $Y_{lic} = M(X_{lim})$. Therefore, pessimistic predictive models and hypotheses are used, and the very conservative condition of Y_{lic} justifies its calculation without uncertainty. Y_{lic} will be the figure-of-merit compared to the safety limit L.

3 REALISTIC METHODOLOGIES

In realistic or BEPU methodologies, the DBT is built similarly to the conservative ones. Some inputs are given conservative values (e.g. postulating additional failures). The time and space discretization schemes are chosen with a criterion of global conservatism. The main difference with the conservative approach lies on the use of realistic predictive models and the way in which Y_{lic} is obtained, through a statistical assessment of the uncertain variable YD, based on calculations of M with different realizations of XD. Y_{lic} is finally obtained as an estimate of a high quantile of YD. Therefore, in this case Y_{lic} is not calculated with a programmed input, but it is statistically estimated.

The conservative methodologies were absolute rulers over the deterministic realm for many years. With the increasing knowledge of the accident phenomenology in NPPs (mainly in the thermohydraulic and fuel behaviour fields) boosted by experimental and theoretical research programmes, the realistic analysis of accidents started to consolidate. The regulation had therefore to tackle the requirements to be imposed on the realistic methodologies.

In 1989 the USNRC released a new version of the rule 10 CFR 50.46 wherein the use of realistic methodologies was accepted to perform LOCA-ECCS analyses. In the Regulatory Guide 1.157 [3] the acceptable models for performing such analyses were described, and the acceptance criteria were given a probabilistic shape, so that the requirement was no more the strict compliance of the criteria, but the compliance with a high probability. In our simple framework, the traditional acceptance criterion for conservative methodologies:

$$Y_{lic} < L \qquad (8)$$

transforms into a probabilistic criterion for realistic methodologies

$$PR\{YD < L\} \geq Q \qquad (9)$$

where Q is a high (close to 1) value, imposed by the regulatory authorities.

Development and assessment of BEPU methods have been subject of extensive work within the nuclear safety community. The first realistic methodology, developed for LOCA analysis, was CSAU [4]. International efforts have promoted the development of uncertainty analysis methods [5,6]. Two basic approaches have been considered: i) based on uncertainty propagation through the predictive model (as described in section 2) and ii) based on the so-called “internal assessment of uncertainty”, which benefits from a direct calculation of the model error uncertainty using experimental data. In the present paper regulatory experience on the licensing of type i) methodologies is described.

The basic stages in a realistic or BEPU methodology of safety analysis are:

1) The most important inputs to the predictive model are selected, and its uncertainty is estimated. The result is a set of basic uncertainties.
2) The basic uncertainties are propagated through the model, to obtain the uncertainty of the safety outputs
3) The safety outputs are compared to their limits, and an estimation of the safety margin is obtained

4 DESCRIBING UNCERTAINTY

As we have already pointed out, the classical description of uncertainty is probabilistic, in such a way that an uncertain magnitude is represented as a random variable. From this point of view, the probability distribution of the variable completely describes its uncertainty. An uncertain magnitude V can be described by the cumulative distribution function, cdf, defined as:

$$F_V(v) \equiv PR\{V \leq v\} \qquad (10)$$

or by the probability density function, pdf, which is the derivative (when it exists) of the cdf:

$$f_V(v) \equiv F_V{}'(v) \qquad (11)$$

But uncertainty, in a more restricted way, can be described by:

- *A scalar parameter*, e.g. standard deviation or difference between quantiles
- *An interval* containing the value of the variable with a high probability.

If uncertainty is probabilistically described, it should be statistically estimated. On estimating uncertainty through random samples, the sample counterparts of the aforementioned descriptors are used, for instance the sample standard deviation or the so-called statistical intervals.

A statistical interval is, informally speaking, an interval which contains the true value of the magnitude with a high likelihood. The term *statistical* stems from the fact that the endpoints of the interval are statistics (i.e functions of the variable's sampled values). We will next focus on a specific type of statistical intervals, named tolerance intervals. First we will introduce the concept of coverage. Given a random variable V and an interval (L,U), we define:

$$W_V(L,U) \equiv F_V(U) - F_V(L) \equiv PR_V\{L < V \leq U\} \qquad (12)$$

as the coverage of V by (L,U). We also say that (L,U) covers V with a probability W_V(L,U).

A two-sided tolerance interval of level A/Q (where A and Q are both real numbers higher than 0 and less than 1) for the uncertain variable V is a statistical interval (L_T, U_T) covering a fraction higher than Q of the variable Y with a confidence level A:

$$PR_{L_T,U_T}\{PR_V\{L_T \leq V \leq U_T\} > Q\} = A \qquad (13)$$

It should be noticed that both L_T and U_T are random variables, dependent on the sample of Y values.

One-sided tolerance intervals are described by tolerance limits. Upper and lower tolerance limits with level A/Q for V are, respectively, statistics U_T and L_T such that:

$$PR_{U_T}\{PR_Y\{V \le U_T\} > Q\} = A \qquad (14)$$

and

$$PR_{L_T}\{PR_Y\{L_T \le V\} > Q\} = A \qquad (15)$$

It seems obvious that, when both Q and A are high values (i.e. close to 1), a two-sided tolerance interval is an adequate descriptor of a generic uncertain magnitude, because it covers a high fraction of the V values with a high statistical confidence. Nonetheless, the classification as “safety” of a magnitude affects the description of its uncertainty. For a safety magnitude having an upper (resp. lower) safety limit, the natural descriptor of uncertainty is an upper (resp. lower) tolerance limit. This seems quite logical, because the important values of the output, from the safety point of view, are those on the conservative side. For a safety magnitude like YD an A/Q upper tolerance limit will be used, A and Q being high values in the interval (0,1).

Tolerance interval endpoints and tolerance limits are statistically estimated, and thus they have statistical uncertainty, due to the finiteness of the random sample used in the estimation. So we have descriptors of the uncertainty which in turn are uncertain. This uncertainty of the uncertainty can be properly called metauncertainty, and has the property of tending to zero when the random sample size tends to infinity.

5 METHODOLOGIES BASED ON MONTE CARLO

The uncertainty propagation is a fundamental step in the BEPU methodologies, and the purpose of this paper is not to give a thorough survey of the propagation methods, but rather to refer to the methodologies based on Monte Carlo calculations and specially to those based on the propagation method that has become the most popular and widely used in the last years, namely the order statistics (OS) method, also known as Wilks method. The Monte Carlo method will be considered as directly applied to the predictive model M. Surrogate models, like the response surfaces proposed in the CSAU methodology [4], will not be treated in this paper.

5.1 Methods based on order statistics

The OS method is based on a pure Monte Carlo analysis of the magnitude YD=M(XD), wherein the uncertain inputs making up XD are randomly sampled so that a simple random sample of XD, ($XD_1,\ldots,XD_N$) is obtained. The model M is then run for the N sampled inputs and thus a simple random sample ($YD_1,\ldots,YD_N$) of the safety output YD is obtained. The hypothesis that YD is a continuous random variable with a continuous pdf will be adopted from now on.

The peculiarity of the OS method refers to the statistical analysis of the YD sample. The sampled values can be sorted ($YD_{1:N},\ldots,YD_{N:N}$) low to high, $YD_{1:N}$ and $YD_{N:N}$ being respectively the sample minimum and maximum. Then, the value $YD_{r:N}$ is called the r-th order statistic (OS) of the sample. Conventionally, statistics of order 0 and N+1 are respectively defined as the minimum and maximum of the complete YD range.

The usefulness of order statistics in uncertainty assessment stems from the fact that they can be used as endpoints of tolerance intervals for the uncertain variable. Let $YD_{r:N}$ and $YD_{s:N}$ two OS such that r<s. The coverage of YD by the interval ($YD_{r:N}$,$YD_{s:N}$) is:

$$W_{YD}(r,s) \equiv F_{YD}(YD_{s:N}) - F_Y(YD_{r:N}) = PR_Y\{YD_{r:N} \le YD \le YD_{s:N}\} \qquad (16)$$

The interesting property is that W_{YD}(r,s) has a well known probability distribution, namely the beta distribution with parameters s-r and N-s+r+1, and this is true whatever F_{YD} be [7]. This is the reason why the OS method is described as nonparametric or distribution-free. Then it is clear that:

$$PR\{PR_Y\{YD_{r:N} \le YD \le YD_{s:N}\} > Q\} = PR\{beta(s-r, N-s+r+1) > Q\} \qquad (17)$$

By comparison with (13) it is concluded that ($YD_{r:N}$,$YD_{s:N}$) is an A/Q tolerance interval for Y whenever

$$PR\{beta(s-r, N-s+r+1) > Q\} = A \qquad (18)$$

The probability distribution of the beta variable is codified in statistical packages and spreadsheets, so that the equation (18) can be implicitly resolved to find out pairs (r,s) giving the desired tolerance level. Actually, (18) has, in general, no solution for integer values of N, s and r, and thus it is replaced by the inequation

$$PR\{beta(s-r, N-s+r+1) > Q\} \ge A \qquad (19)$$

so that integer values are obtained fulfilling (19) while mimimizing the probability on the left hand side.

But, as already pointed out, the uncertainty of our safety output YD is more properly described by an upper tolerance level, rather than a two-sided interval. The expression (19) with r=0 reads:

$$PR\{beta(s, N-s+1) > Q\} \ge A \qquad (20)$$

that can also be expressed as

$${}_{1-A}beta(s, N-s+1) > Q \qquad \text{(20-bis)}$$

the left hand side being the (1-A) quantile of the beta variable. Integer values of N and s fulfilling (20) or (20-bis) while minimizing the respective left hand sides are such that $YD_{s:N}$ is an A/Q upper tolerance limit for YD. There is a minimum sample size N needed to obtain a tolerance interval or limit for a prescribed level A/Q. For instance, at least 59 samples are necessary to obtain a 95/95 tolerance limit.

In Wilks methodologies the licensing value Y_{lic} is finally obtained as an order statistic $YD_{s:N}$ from the YD random sample.

In figure 1 a schematic view of the safety outputs to the BEPU analysis is shown. The safety output Y transforms into YD when the DBT is considered. Y_{lic} is an upper tolerance limit for YD, covering a high quantile of YD with high confidence. Each safety output is depicted by a pdf. It is interesting to point out that Y_{lic} has metauncertainty; if the Monte Carlo sample size increases, the pdf of Y_{lic} will become narrower, whilst those of Y and YD will remain unchanged.

We have described the Wilks method for a single scalar magnitude. When considering multidimensional magnitudes the method becomes more complex to apply. For safety analysis the univariate version is enough, because there is actually a single scalar safety output, namely a Boolean index taking the value 1 when all the safety criteria are fulfilled and 0 otherwise. The multivariate version should be used in the process of validation of the predictive model [10].

5.2 Parametric Methods

The OS method uses a nonparametric inference about YD, and hence it is especially appealing when there is no *a priori* assumption about the probability distribution of YD. When there is information supporting the ascription of YD to a known family of probability distributions , for instance when the random sample of YD values fulfil a goodness-of fit test, statistical parametric methods can be used instead of OS. The most typical instance is when the YD data fit a normal distribution, or when they can be transformed to data that fit a normal distribution. In [8,9] expressions are given for normal tolerance intervals, usable as uncertainty descriptors. A normal upper tolerance limit for YD is obtained as

$$m_{YD} + k_{AQ}\, s_{YD} \qquad (21)$$

where m_{YD} and s_{YD} are respectively the mean and standard deviation of the YD sampled values. k_{AQ} is a coefficient depending on A, Q and N.

Contrary to the OS, the normal intervals do not require a minimum sample size to reach the tolerance level A/Q. As a counterweight to it, a small sample can be considered as insufficient to test the hypothesis of normality.

6 INTREPRETING AND EVALUATING MONTE CARLO METHODOLOGIES

When the regulator faces the task of evaluating a safety analysis methodology based on the Monte Carlo method, the three stages quoted in section 3 must be properly checked. The OS-based methodologies propagate the uncertainties by means of pure Monte Carlo calculations and the use of OS. This method has been worldwide accepted. Nevertheless there are points that the evaluation should focus on, roughly corresponding to the three aforementioned stages:

- Construction of the basic uncertainties
- Performance of the Monte Carlo calculations
- Interpretation of the results and calculation of safety margins

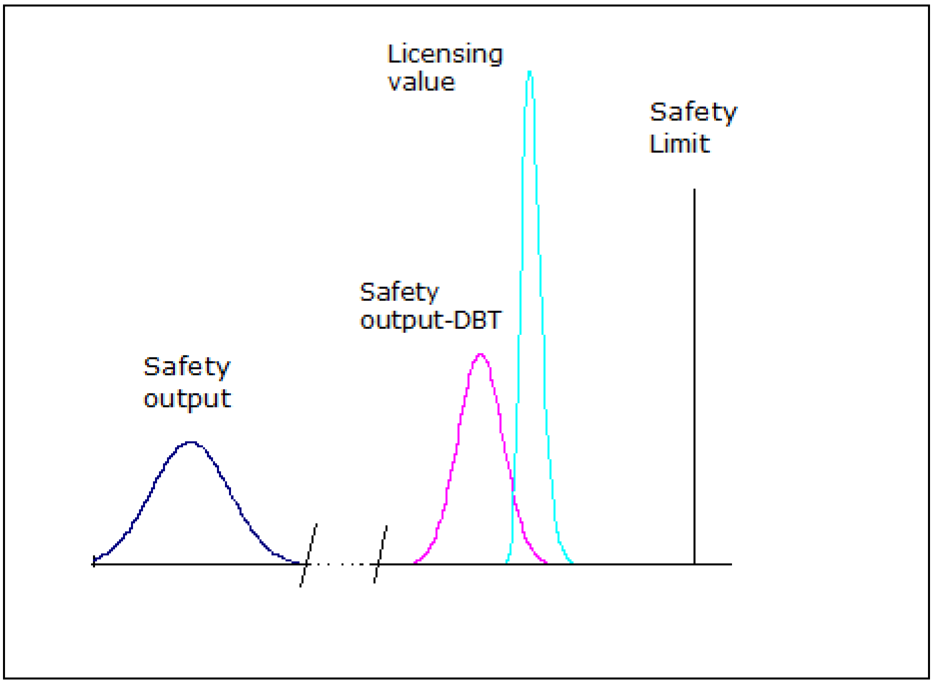


Figure 1: Safety outputs for a BEPU analysis

6.1 Checking basic uncertainties

The uncertainty of a safety output must not be underestimated, especially in the conservative range. Whenever all the uncertainty is propagated from the inputs, and the propagation method is sound, the interest is centred in the proper estimation of the input uncertainty, in such a way that it is nor underestimated in the conservative side.

Let us denote as Z an uncertain component of the vector XD (i.e. a scalar input to M). Different procedures exist in order to estimate the distribution function of Z, in the form either of pdf $f_Z(z)$ or of cdf $F_Z(z)$. When a random sample exists of values of the parameter, the data can be used to build an empirical pdf (a histogram) or an empirical cdf (ecdf), which is a stepwise function defined as:

$$F_Z^{emp}(z) \equiv fr(Z \leq z) \qquad (22)$$

i.e. the fraction of sampled data being lower or equal to z. The disadvantage of the histogram is that it depends on the data binning criterion; instead, the ecdf defined in (22) does not require any binning criterion.

But it is important to point out that a distribution function estimated with a finite sample has statistical uncertainty, that we have called metauncertainty, and when it is taken into account, the ecdf defined in (22) must be supplemented with confidence bands. These can be of two types:

- *Point-wise*: for each value z they contain the real $F_Z(z)$ with a prescribed confidence level
- *Joint*: they contain, with a prescribed confidence level, the whole real cdf curve

The cdf should then be estimated by means of a one-sided confidence band. For instance, if the conservative values of Z are the higher ones, a lower confidence band should be used, because it favours such high values.

Sometimes, the data are used to build a probability distribution belonging to a certain family (e.g, normal, lognormal, gamma, etc). In such cases, a statistical test should previously be conducted, keeping in mind that the fitting of distribution should be conservatively performed.

In fact, when data are really scarce, more drastic measures should be taken. For instance, sometimes only the range of the parameter is known, and then a possible choice is fixing the value of the parameter to a conservative value. In this case, the uncertainty of the parameter is really taken into account, but it finally contributes to the conservative bias of the prediction model rather than to the output uncertainty.

Another possibility is to introduce some expert opinion. For instance, the expert can recommend the use of a uniform distribution spanning the range of the parameter, hence assigning the same probability to all the values in a certain interval. In such case, the interval should be wide enough in the conservative direction. Other possibility is that the expert assigns to the parameter a known distribution function, for instance a normal distribution having as mean a nominal value and as standard deviation a certain percentage of the mean. The expert's assumptions must be properly justified

It is not unusual the truncation, for practical reasons, of the parametric distributions being used. For this procedure to be acceptable, the eliminated tail in the conservative side should be small enough.

6.2 Monte Carlo calculations

Once a random sample of inputs XD has been obtained, the predictive model M must be run for the different input realizations. This pure Monte Carlo analysis can be viewed as a binomial experiment (just like tossing N times a coin), the two outcomes being success (the safety criteria are fulfilled by the run output) and fail (some safety criteria are not fulfilled).

Some provision should be made about the runs failing to completion. In general, most of the failed cases can be successfully completed when rerun with a change in time step, or in some convergence criteria. If there are runs failing to completion even with such measures, the conclusion is that the predictive models have shortcomings, and such conclusion should be communicated to the experts in the model (developers, V&V team). If the experts believe that the shortcomings of the model in some isolated cases do not imperil the capacity to simulate the transients, then the strategy of obtaining a new random input to replace the one causing the failure could be acceptable. In fact a binomial model is being tested (from the probabilistic point of view) wherein only two results are accepted (namely success or fail in compliance of the safety criteria). The success probability, which is the probabilistic safety margin, is estimated through the number of successful runs and the total number of completed runs.

6.3 Interpreting the results

When the Wilks method is applied to a N-sized random sample of the uncertain variable YD, the minimum integer s satisfying (20) is obtained, so that $YD_{s:N}$ is an A/Q upper tolerance limit for YD. The safety criterion takes the form

$$YD_{s:N} \leq L \qquad (23)$$

The OS methodologies have a prompt interpretation in the realm of DSA, stemming from the definition of tolerance intervals. For a safety output as YD, nonparametric upper tolerance limits are obtained, covering a high quantile of the safety output with a high statistical confidence, and this fact (together with the bounding nature of the DBT) evidences the conservatism of the obtained Y_{lic} to be compared to the safety limit L.

But a more powerful interpretation can be done, in terms of probabilistic safety margins. The precise meaning of (23) is that at least s out of N random values of YD have fallen under the safety limit. A binomial experiment allows us to estimate the probability of the outcomes, for instance the probability of 'head' when tossing a coin. The Monte Carlo results allow us to estimate the probability of Y being under L, which is the PSM. Therefore, the use of the Monte Carlo method in the field of DSA not only permits to state that "enough safety margins exist", but to quantify such safety margin in terms of probability.

A clear relation exists between giving a tolerance limit for YD and giving a confidence limit for PSM(YD). In [2] it is mentioned that, when N Monte Carlo calculations are conducted and s of them give YD<L, a lower confidence limit with level A for PSM(YD) is the (1-A) quantile of the beta distribution with parameters s and N-s+1 (Clopper-Pearson limit). Comparing this statement with (20-bis) it is concluded that running N Monte Carlo cases, producing an A/Q upper tolerance limit $YD_{s:N}$ and checking that it is less than L, is equivalent to say that PSM(YD) is higher than Q with at least a confidence level A:

$$PR\{PR\{YD < L\} \geq Q\} \geq A \qquad (24)$$

The innermost probability in (24) refers to the uncertainty of YD; the outermost one refers to the metauncertainty stemming form the finiteness of the sample. (24) is the form assumed by the probabilistic acceptance criterion (8) when the metauncertainty is taken into account.

In [2] several methods for calculating probabilistic safety margins from random samples of safety outputs are gathered.

For instance, if N=105, then s=104 is the minimum solution of (19) with A=0.97 and Q=0.95, so that $Y_{104:105}$ is a 97/95 upper tolerance limit for YD. And if we confirm that $YD_{104:105} < L$, then it is concluded that PSM(YD) is higher than 0.95 with a confidence 0.97.

We introduced the concept of limiting output in connection with conservative methodologies. For BEPU methodology the definition is the same:

$$Y_{lic} = M\left(X_{lim}\right) \qquad (25)$$

In OS-based methodologies X_{lim} is obtained as the input giving rise to $YD_{s:N}$. According to the order relation between inputs defined in (4), the XD sample can be sorted low to high, $(XD_{1:N},\ldots,XD_{N:N})$ in such a way that $YD_{k:N} = M(XD_{k:N})$, k=1,…,N. Then it is clear that $X_{lim}=XD_{s:N}$, s being the minimum integer fulfilling (16). The conclusion is that the OS-based methods directly produce not only the licensing value, but the limiting output as well.

On the contrary, when the normal distribution is used for uncertainty propagation, the limiting output is not obtained as a direct by-product of the uncertainty assessment. The reason is that Y_{lic} is not obtained as an OS, but as a function, like (21), of the mean and standard deviation of the YD values.

In (6) we have defined the probabilistic analytical margin for YD, as a measure of the DBT conservative character. An analogous measure of the conservativeness of Y_{lic} with regard to YD can be defined. Let us suppose that a new random value of YD is sampled, additionally to the N previously sampled values. The probability that the new value is not higher than the s-th order statistic of the previous N-sized sample

$$PR\{YD_{N+1} \leq YD_{s:N}\} \qquad (26)$$

is a measure of the conservativeness of YDs:N with regard to YD. An advantage of the OS method is that the probability (26) can be easily calculated [7] and found to be

$$PR\{YD_{N+1} \leq YD_{s:N}\} = \frac{s}{N+1} \qquad (27)$$

In our previous example, with N=105 and s=104, the probability after (27) is 0.981.

There is an infinite number of pairs (s,N) of integer values such that $YD_{s:N}$ is an A/Q tolerance limit. But they have different degree of conservatism, described by (27). Y_{lic} is expected to be less conservative as N increases. In the limit, the metauncertainty disappears, and the OS tends to the Q quantile of YD:

$$lim_{N\to\infty}\, PR\{YD \leq YD_{s:N}\} = Q \qquad (28)$$

Then, when N increases the knowledge of the Q quantile of YD enhances. On the other hand, when N decreases the expected conservativeness of Y_{lic} increases

As described in 5.2, if the YD data pass some goodness-of-fit test, parametric methods can be used in order to obtain Y_{lic}. The normal distribution is the standard example. Normality tests are a special class of statistical tests wherein the null hypothesis is the normality of the analyzed variable. The convention exists of accepting the null hypothesis unless the sampled data show a clear discrepancy with it. The so-called p-value of the test is a measure of the agreement or compatibility of data and the null hypothesis. Sometimes a very low value of the p-value (e.g. >0.05) is admitted as sufficient to accept the normality hypothesis. This can lead to an underestimation of the uncertainty, for instance when the real distribution is heavytailed. When conducting this kind of tests for a safety magnitude, the default hypothesis should be non-normality rather than normality. In other words, the replacement of the nonparametric OS tolerance limits by normal ones should only be accepted if there is strong evidence of normality, including a high test p-value.

7 OTHER REGULATORY IMPLICATIONS

Whenever a new methodology is accepted for application in a safety case the implications in the regulatory frame must be assessed. Typically a revision of the Safety Analysis Report (SAR) will be issued where the analyses affected by the new methodology will be updated. As a result the limiting transient for a given safety limit may change. Also there may coexist within the SAR both methodologies, conservative and BEPU, applied to different set of transients. A careful analysis of the consistency of the analytical frame in the SAR must be conducted.

A special analysis should be made on the impact of the new method and the aforementioned analytical frame to the Technical Specifications (TS) of the plant. TS set limits on several components of X, which are operational parameters, defining a region in the X space where safe operation of the NPP is analytically supported and thus allowed by the regulator. In a simplified way, this means that any transient within the design basis has acceptable consequences provided that the input X is inside the TS acceptance region. The TS concept has been directly linked to the conservative methodologies of DSA, because they permit an easy checking of the safety acceptance criteria (using a single calculation, equation (6)) and therefore a quick exploration of the acceptance region boundaries. On the contrary, BEPU methodologies need N calculations in order to check the safety criteria (equation (24)), and perform a random sampling of the X space instead of looking for the boundaries of the acceptance region. A simplified procedure should imply analyzing a worst case scenario where the TS parameters are set to their analytical value in the input XD, and this would require a set of N Monte Carlo calculations additional to those performed for the input XD. In summary, the computational effort to check TS could soar up for BEPU methodologies.

A looser interpretation, in which the TS simply set limits on the ranges of some uncertain operational parameters, would not allow to state that operation in any point of the TS acceptance region is analytically supported. The interpretation of TS in relation with BEPU methods should be further studied

Another relevant issue regarding the regulatory perspective is the treatment of plant modifications and how the validity of the SAR is maintained. In the case of Monte Carlo methods it is important to determine when a complete reassessment must be made, and how to perform it. For performing the input's random sampling a set of pseudorandom numbers is use, using a random seed as starting point. If the safety analysis is repeated, the random seed of the base case can be maintained or it can be changed. The statistical inferences that can be performed in each case are different, and hence the regulator should pay attention to this "reseeding policy". The same situation would be apparent when errors are discovered in the methodology or the predictive models.

Last but not least, a decision has to be taken on the parameters included in the probabilistic acceptance criteria shown in expression (24), namely the level of coverage Q and of confidence A.

8 CONCLUSIONS

The increasing knowledge on accident phenomenology has promoted the use of realistic or BEPU methodologies. Those based in the use of Monte Carlo with order statistics for uncertainty propagation have become the most widespread. Such methodologies allow not only to state that "enough safety margins exist" but to quantify such safety margins in probabilistic terms (which are the really useful ones). The evaluation of a BEPU methodology must focus on the proper estimation of the basic uncertainties, which must not be underestimated, and on a right interpretation of the results

Parametric methods can be used as an alternative to the OS-based; the most typical are those based in the normal distribution. When testing normality, the default hypothesis should be the non-normality, so as to minimize the risk of underestimating the uncertainty.

An interesting point from the regulatory side is to study the relation between Technical Specifications and the BEPU methodologies.

REFERENCES

[1] J. HORTAL et al, "What does "safety margin" really means ?" . Accepted to ESREL 2008 conference. Valencia (2008)

[2] R. MENDIZÁBAL, "Probabilistic safety margins: definition and calculation". Accepted to ESREL 2008 Conference. Valencia (2008)

[3] U.S. Nuclear Regulatory Commission, Best-estimate Calculations of Emergency Core Cooling System Performance, Regulatory Guide 1.157 (1989)

[4] U.S. Nuclear Regulatory Commission, Quantifying Reactor Safety Margins – Application of the Code Scaling, Applicability and Uncertainty Evaluation Methodology to a Large-Break, Loss-of-Coolant Accident, NUREG/CR-5249 (1989)

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

[6] OECD/NEA/CSNI, "BEMUSE Phase III Report", NEA/CSNI/R(2007)4. Paris, 2007

[7] H. A. DAVID and H. N. Nagaraja, Order Statistics, 3rd Edition, John Wiley & Sons, Inc. (2003)

[8] G.J. HAHN & W.Q. MEEKER, Statistical Intervals. A Guide for Practitioners, Chapter 4, John Wiley & Sons, Inc. (1991)

[9] S. ZACKS, The theory of Statistical Inference, John Wiley & Sons, Inc. (1971)

[10] R. MENDIZÁBAL, "Order statistics methodologies and multiple outputs". Presented to the IAEA Topical Meeting on Advanced Safety Assessment Methods for Nuclear Reactors. Daejon, Korea (2007)

Accident Management Guidance and Individual Plant Accident Management Support - Recent IAEA Activities.

Suk Ho Lee, IAEA
George L. Vayssier, NSC Netherlands

Abstract

The IAEA is already long time involved in activities related to accident management. It has developed various documents on this subject, and also initiated a review service, where the accident management measures of an individual plant are reviewed.

Recently, the IAEA compiled a draft Safety Guide on Accident Management that comprises the main elements of such management in a complete and consistent way. It describes which steps should be taken in setting up an accident management program, from the conceptual stage down to a complete set of instructions - procedures and guidelines - to the plant operators.

Today's nuclear power plants have multiple barriers against the release of radioactive substances, plus a number of supportive systems that protect these barriers. There is a set of instructions, usually called Emergency Operating Procedures (EOPs), to deal with a large variety of credible events, both inside and outside the design basis. Nevertheless, there is a remote chance that these instructions are not successful, and that core damage will occur. In that case, plants still have capabilities to mitigate potential releases. The IAEA draft Safety Guide gives guidance on how such measures should be defined and how they should be executed.

The process is in a number of well-defined steps. First, the plant vulnerabilities for severe accidents (i.e. accidents with substantial core damage) are defined, as well as their timing. This gives a certain sequence of challenges to fission product boundaries. Then the plant capabilities to mitigate those challenges are researched. This leads to a number of possible strategies, which then are converted to mitigative measures. From there, procedures and guidelines are developed. Priorities are defined on the basis of the timing and magnitude of potential releases.

Major differences with the EOP-domain are that the plant status may be known only partially, the outcome of actions cannot always be predicted, and planned actions can even have severe negative consequences (e.g., ignition of hydrogen may lead to loss of containment). This complicates the decision making process. The IAEA draft Safety Guide gives guidance on how the evaluation and decision-making processes should be set up and where the authority should be placed.

A relatively new type of IAEA service in this field is the Review of the Accident Management Program (RAMP) of an individual plant. The objective of the RAMP is to assist at the utility and plant designer in preparation, development and implementation of effective plant specific accident management programme. However, assistance can also be provided to the regulatory body in reviewing of accident management programme. Such a review includes a one-week visit of a group of experts (about 5) to a nuclear site, a review of the relevant documentation, interviews with plant staff and, finally, discussion of findings and formulation of

recommendations. A guide has been prepared to structure this process. Three plants have been reviewed so far. These reviews have been received very well by the parties involved.

1. INTRODUCTION.

The IAEA has set up a series of documents that specify requirements and guidance for the design and operation of nuclear power plants (NPPs). Member States can use these as regulatory requirements and guidance in their national programs. Requirements are obligatory (i.e. ‘shall’ statements), guidance specifies recommendations how the requirements can be met (‘should’ statements).

The documents NS-R1 [1] and NS-R2 [2] specify the design and operations requirements, respectively; they require NPPs to also consider both design provisions and accident management procedures for severe accidents. The draft Safety Requirements [3] on Safety Assessment for Facilities and Activities states that the assessment of defence in depth is required to determine whether adequate provisions have been made at each of the levels of defence to identify accident measures to control severe accident conditions and to mitigate the radiological consequences of potential release. Before, the IAEA had already developed a number of documents for Member States to support them in establishing accident management at their plants. The Agency had compiled documents on the development of Emergency Operating Procedures (EOPs) [4] and on the implementation of accident management programs in NPPs [5], which latter document deals mostly with accidents beyond the design basis and severe accidents. The phenomenology of severe accidents and various analysis methods have been described in [6, 7]. Recently, a draft Safety Guide [8] has been compiled to give further guidance to the implementation of the requirements of [NS-R1], which is the subject of this article.

Today’s nuclear power plants have multiple barriers against the release of radioactive substances, plus a number of supportive systems that protect these barriers. The EOPs deal with a large variety of credible events, both inside and outside the design basis. Nevertheless, there is a remote chance that the EOPs are not successful, and that core damage will occur. In that case, plants still have capabilities to mitigate potential releases. The IAEA draft Safety Guide gives guidance on how such measures should be defined and in which way they should be executed.

The ultimate goal of accident management is to reduce risk in the unlikely case of a severe accident. Even if these are low probability events: ‘operators should never be placed for an accident that has not been previously analysed by an engineer’ - a paramount lesson from the TMI-2 event, as formulated by one of its operators.

2. STRUCTURE OF THE SAFETY GUIDE

The Guide has been developed in two parts:
Part 1 contains the basic principles, which are the ‘foundations’ of the program, i.e. fundamental characteristics that should be observed as core elements of the program.
Part 2 contains the technical and organisational elements of developing the AM-program, i.e. all work that must be done to finally arrive at a set of guidelines for use by plant personnel.

3. SETTING UP ACCIDENT MANAGEMENT GUIDANCE.

Accident management is a series of actions with the objectives:

1. to prevent a beyond design basis event to escalate into a severe accident,
2. to terminate the progress of core damage once it has started;
3. to maintain the capability of the containment as long as possible;
4. to minimize releases of radioactive material; and
5. to achieve a long term stable state.

The last four points constitute ‘severe accident management’ (SAM). The guidance in this field is usually called ‘severe accident management guidance / guidelines’ (SAMG).

Setting up a AMG-program for an NPP requires a number of steps in a top-down approach:

1. define the objectives, as described above.
2. define strategies to achieve the objectives
3. define measures to execute the strategies
4. develop procedures and guidelines for the actions to be taken by plant personnel

The process is illustrated in Fig 1.

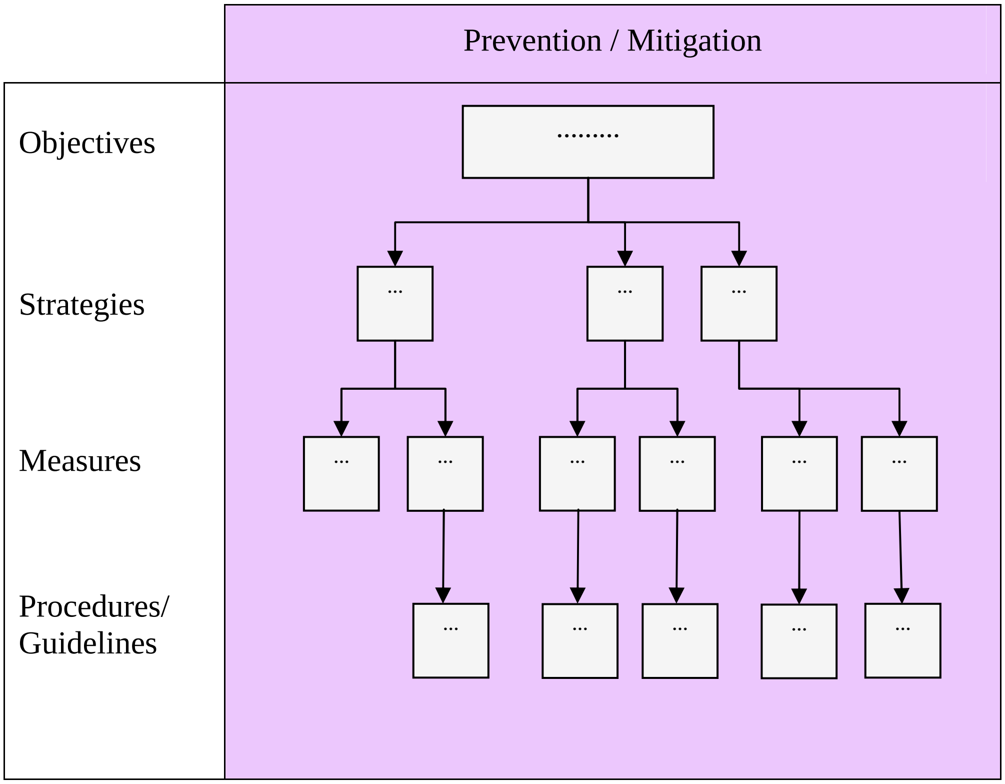


FIG. 1. Top down approach to accident management

4. CONCEPTUAL ELEMENTS

This section specifies some main principles, aspects of equipment upgrades, forms of the accident management guidance and roles and responsibilities. They are the basis for further development of the guidance. The text of this section is - mainly - a quote from the draft Guide and marked as such, where explanations / examples are here added in *italics* - they do not form part of the Guide. Paragraphs are not exact quotes, for reasons of brevity; numbering follows the numbering of this article, not that of the Guide.

MAIN PRINCIPLES

1. In view of the uncertainties involved in severe accidents, accident management guidance should be developed for *all physically identifiable challenge mechanisms* for which the development of accident management guidance is feasible; this should be performed largely independently of predicted frequencies of occurrence.

> *Arguments that certain plant damage states need no mitigation because of perceived /calculated low probability should, in principle, not be credited, as long as guidance for such states can be developed*.

2. Accident management should be *symptom based*, i.e. the strategies and the associated measures should be based on directly measurable plant parameters or parameters derived from these by simple calculations.

> *Strategies should not be developed on complex parameters such as peak clad temperature*

3. Accident management guidance should be set up in such a way that it is not necessary for the responsible staff to identify the accident sequence or to follow some pre-analysed accident

4. Accident management should cover at all modes of plant operation and also appropriately selected external events, such as fires, floods, seismic events and extreme weather conditions (e.g. high winds, extremely high or low temperatures, droughts) that could damage large parts of the plant. The accident management guidance should consider specific challenges posed by these events such as loss of the power supply, loss of the control room or switchgear room, and reduced accessibility to systems and components.

5. When developing guidance on accident management, consideration should be given to the plant’s full design capabilities, using both safety and non-safety systems, and including the possible use of some systems beyond their originally intended function and anticipated operating conditions and possibly outside their design basis.

EQUIPMENT UPGRADES

6. Design features important for the prevention or mitigation of severe accidents should be evaluated. Accordingly, existing equipment, and/or instrumentation should be upgraded or new equipment, and/or instrumentation should be added, if needed or useful for the development of a meaningful accident management program.

7. If a decision is taken to add or upgrade equipment and/or instrumentation, the design specification of such equipment and/or instrumentation should be such as to ensure appropriate independence from existing systems and preferably appropriate margins with regard to their use under accident and/or severe accident conditions.

8. The installation of new equipment or the upgrading of existing equipment should not remove the need for the development of guidance for the situation that such equipment fails, even if such failure has a low probability.

FORMS OF ACCIDENT MANAGEMENT GUIDANCE

Preventive domain

9. In the preventive domain, the guidance should consist of descriptive steps, as the plant status is known from the available instrumentation and the consequences of actions can be predetermined by appropriate analysis. The guidance, therefore, takes the form of procedures, usually called emergency operating procedures (EOPs), and is prescriptive in nature. EOPs cover both design basis accidents and beyond design basis accidents, but are generally limited to actions taken prior to core damage.

Mitigative domain

10. In the mitigative domain, uncertainties may exist both in the plant status and in the outcome of actions. Consequently, the guidance should not be prescriptive in nature but rather should propose a spectrum of potential mitigating actions and thus leave space for additional evaluation and alternate actions. Such guidance is usually termed severe accident management guidelines (SAMGs).

11. The guidance should contain a description of both the positive and negative potential consequences of proposed actions, including quantitative data where available and relevant, and should contain sufficient information for the plant staff to reach an adequate decision during the evolution of the accident.

12. The guidance should be sufficiently detailed to support the responsible staff in its deliberations and decisions in a high-stress environment, with a minimum chance to delete or overlook relevant information. The guidance should not be shaped in such a form and with such

detail that responsible personnel will tend to follow it verbatim, unless that is the intended type of action.

13. The overall form of the guidance and the selected amount of detail should be tested in drills and exercises. Based on the outcome of such drills, it should be judged whether the form is appropriate and whether additional detail or less detail should be included in the guidance.

ROLES AND RESPONSIBILITIES

14. Accident management guidance should be an integral part of the overall emergency arrangements at a nuclear power plant. The execution of the accident management guidance is the responsibility of the emergency response organization at the plant or the utility. Roles and responsibilities for the different members of the emergency response organization involved in accident management should be clearly defined and coordination among them should be ensured.

15. A specialized team or group of teams (referred to in the following as the technical support centre) should be available to provide technical support by performing evaluations and recommending recovery actions to a decision making authority, both in the preventive and mitigative domains. It should also provide appropriate input to the people responsible for the estimation of potential radiological consequences. For multiple teams, the role of each team should be specified.

16. The decision-making authority should be placed at an appropriate level commensurate with the complexity of the task and the potential for on-site and off-site releases. In the preventive domain, the control room shift supervisor or a dedicated safety engineer should be largely able to carry this responsibility, whereas a higher level of decision making is recommended in the mitigative domain.

5. PROCESS OF DEVELOPMENT OF AN ACCIDENT MANAGEMENT PROGRAM

The AM guide contains a full chapter on the process of setting up the accident management programme, outlined in 128 numbered paragraphs. Further technical detail which can be helpful is contained in references, such as [5]. The following subjects ate treated:

1 General remarks
2 Identification of plant vulnerabilities
3 Identification of plant capabilities
4 Development of accident management strategies
5 Development of procedures and guidelines
6 Hardware provisions for accident management
7 Role of instrumentation and control
8 Responsibilities and lines of authorization
9 Verification and validation
10 Education and training
11 Processing new information

12 Supporting analysis
13 Management system

Ad 1. General Remarks

This section addresses a.o. the selection of events to be considered. It describes the process of obtaining the events, not to exclude events because of assumed /calculated low probabilities, and also to check, at the end, whether indeed the important risk contributors are covered with means that indeed reduce risk. A PSA is helpful, in obtaining the events to be considered, but is not the only tool - other insights should be used as well, e.g. similar studies from other plants, operating experience and research on severe accidents.

After completion of the accident management guidance, it should be checked whether indeed all important accident sequences, in particular those obtained from the PSA, are covered, and whether plant risk is reduced accordingly.

Ad 2. Identification of plant vulnerabilities

A comprehensive set of insights should be obtained on the behaviour of the plant during a beyond design basis accident and severe accident; these should identify the phenomena that will occur and their timing and severity. In the severe accident domain, these insights are collected in the technical basis for severe accident management. This technical basis is often documented separately, as a collection of insights from where the AM program is developed.

The insights should be obtained using appropriate analysis tools. Also other inputs should be used, such as the results of research on severe accidents, insights from other plants and engineering judgment. Uncertainties in severe accident models and the assumptions made should be considered in developing the insights. Often, the plant PSA, if available, is used, but also other insights, as described, are important.

Ad 3. Identification of plant capabilities

All plant capabilities available to fulfil the safety functions should be investigated, including the use of non-dedicated systems, unconventional line-ups and temporary connections (hoses, mobile equipment) and use of systems beyond their design basis, up to and including the possibility of equipment damage. It should also be considered whether failed systems can be restored to service and, hence, can again contribute to the mitigation of the event. Where unconventional line-ups and temporary connections are identified, consideration should be given to adaptation of equipment necessary to use these capabilities.

Ad 4. Development of accident management strategies.

This is a complex matter. Although the principle elements of such strategies are relatively straightforward (e.g. depressurising the RCS), the strategies are interlinked and influence each other. Unlike in the preventive domain, strategies in the mitigative domain can also have negative consequences, which complicates the matter of prioritising and decision-making. As severe accidents evolve over a larger time frame, there should be time for evaluating positive and negative consequences. But for fast-developing scenarios, such time may not be available and the decision making process should account for it.
Strategies are not derived from a perceived underlying scenario, but from measurable parameters indicative of plant damage.

There should be a systematic evaluation of the possible strategies that can be applied, taking into consideration the evolution of the accident. In selecting and prioritising strategies, it should be noted that there is an increased importance of evaluation due to the presence of multiple potential negative impacts, and of increased levels of uncertainty in plant status and potential response to actions.

Special attention should be devoted to strategies that have both positive and negative impacts in order to provide the basis for a decision as to which strategies constitute a proper response under a given plant damage condition. An example is flooding the cavity, with the negative impact of the possible occurrence of a steam explosion.

Insights into the plant damage states in the evolution of the accident should be obtained wherever possible. They are helpful as they can help to select strategies, because some strategies can be effective in one plant damage state, but may be ineffective or even detrimental in another. In addition, such insights are relevant for the estimation of the source term and, if available, should be used for this purpose. Examples are: adding water to a core is generally beneficial; however, if it is done at the moment the fuel stack is still intact but the control rods have melted away, a large power spike may follow. If only a limited amount of water is available, injection may not cool the core, but just generate hydrogen. If the containment pressure is high, spraying it may be beneficial. However, it can also de-inert the containment atmosphere and cause hydrogen burns.

Priorities should be set between strategies, because possible strategies can have a different weight and/or effect on safety, and because not all strategies can be carried out at the same time. The basis of the selection of the priorities should be documented. The setting of priorities should include the consideration of support functions (vital auxiliaries such as power and cooling water).

Ad 5. Development of procedures and guidelines.

The strategies should be converted to procedures and guidelines, so as to make them suitable tools for the control room operators and their supportive organisation (Technical Support Centre). Elements of the procedures /guidelines are:

1. objectives and strategies;
2. initiation criteria;
3. the time window within which the actions are to be applied (if relevant);

4. the possible duration of actions;
5. the equipment and resources (e.g. AC, DC, water) required;
6. actions to be carried out;
7. cautions;
8. throttling and termination criteria;
9. monitoring of plant response.

The set of procedures and guidelines should include a logic diagram, which describes a sequence of relevant plant parameters which should be monitored and which are linked to the initiation / throttling / termination criteria of the various procedures and guidelines. The sequence should be in line with the priority of associated procedures and guidelines, as is described before.

Possible positive and negative consequences of proposed strategies should be specified in the guidelines, in cases where the selection of the strategies has to be done in the evolution of the accident. The technical support centre should check whether additional negative consequences are possible, and consider their impact.

Priorities should also be defined among the various procedures and among the various guidelines, in accordance with the priority of the underlying strategies. Conflicts in priorities, if any, should be resolved. The priorities may change in the course of the accident and, hence, the guidelines should call for selection of priorities to be reviewed at regular time intervals. The selection of actions should be changed accordingly.

The EOPs should be interfaced with the SAMGs, and proper transition from EOPs into SAMGs should be provided for, where appropriate. Functions and actions from strategies in the EOPs that have been identified as relevant in the mitigative domain should be identified and retained in the SAMGs.

Guidance should be developed to diagnose equipment failure and to identify methods to restore such failed equipment to service. The guidance should include recommendations on the priorities for restoration actions. In this context the following should be considered:

- the importance of the failed equipment for accident management;
- possibilities to restore the equipment;
- the likelihood of successful recovery if several pieces of equipment are out of service;
- dependence on the number of failed support systems;
- doses to personnel involved in restoration of the equipment.

Ad 6. Hardware provisions for accident management

In principle, each plant should develop SAMG irrespective of its hardware configuration. However, for certain functions, specific hardware may be useful or even needed. A list of such possible hardware is provided. Hardware modifications are always to be considered if it otherwise is not possible to develop a meaningful SAMG-program

Ad 7. Role of instrumentation and control

The plant parameters needed for preventive accident management measures and mitigative accident management measures should be identified. It should be checked that all these parameters are available from the instrumentation in the plant.

The effect of the environmental conditions on the instrument reading should be estimated and included in the guidance. It should be considered that a local environmental condition can deviate from global conditions and, hence, instrumentation that is qualified under global conditions may not function properly under local conditions. The expected failure mode and resultant instrument indication (e.g. off-scale high, off-scale low, floating) for instrumentation failures in severe accident conditions beyond the design basis should be identified.

Dedicated instrumentation that is qualified for the expected environmental conditions is the preferred method to obtain the necessary information. Where instruments can give information on the accident progression in a non-dedicated way, such possibilities should be investigated and included in the guidance.

Every key instrumentation reading from a non-qualified dedicated instrument that is used for diagnosis or verification should have an alternate method to verify that the primary reading (i.e. the reading from the dedicated instrument) is reasonable. Alternate instrumentation should be identified where the primary instrumentation is not available or not reliable. When an alternate means of obtaining a key parameter value cannot be identified, consideration should be given to upgrading or replacing the instruments in order to provide that alternate indication. Alternatively, other strategies that do not use this instrumentation should be developed.

The ability to infer important plant parameters from local instrumentation or from unconventional means should also be considered. For example, the steam generator level can be inferred from local pressure measurements on the steam line and steam generator blowdown lines.

The need for development of computational aids to get information where parameters are missing or their measurements are unreliable should be identified and appropriate computational aids should be developed accordingly.

Ad 8. Responsibilities and lines of authorization

Transfer of responsibilities and decision making authority from the control room staff to a higher level of authority should be made at some time point in an event that degrades into a severe accident, as decision making is highly complex in view of the uncertainties involved, and because it may involve actions with consequences beyond the information available in the control room or even at the plant. In the mitigative domain, the Technical Support Centre (TSC) should be charged with performing evaluation and recommending recovery actions to the decision-making authority.

This decision-making authority should be with a high level manager, here further denoted as the Emergency Director (ED). The ED holds the authority to decide on the implementation of accident management measures proposed by the technical support centre or, if needed, based on his own deliberation. The ED should have a broad understanding of the actual status of the plant and of other relevant aspects of the emergency response, including off-site effects. If there is any involvement of the regulatory authority in the decision-making, it should be defined how this is to be done.

An example of a typical layout of the main elements of the Emergency Response Organization (ERO) of a plant is shown in Fig. 2.

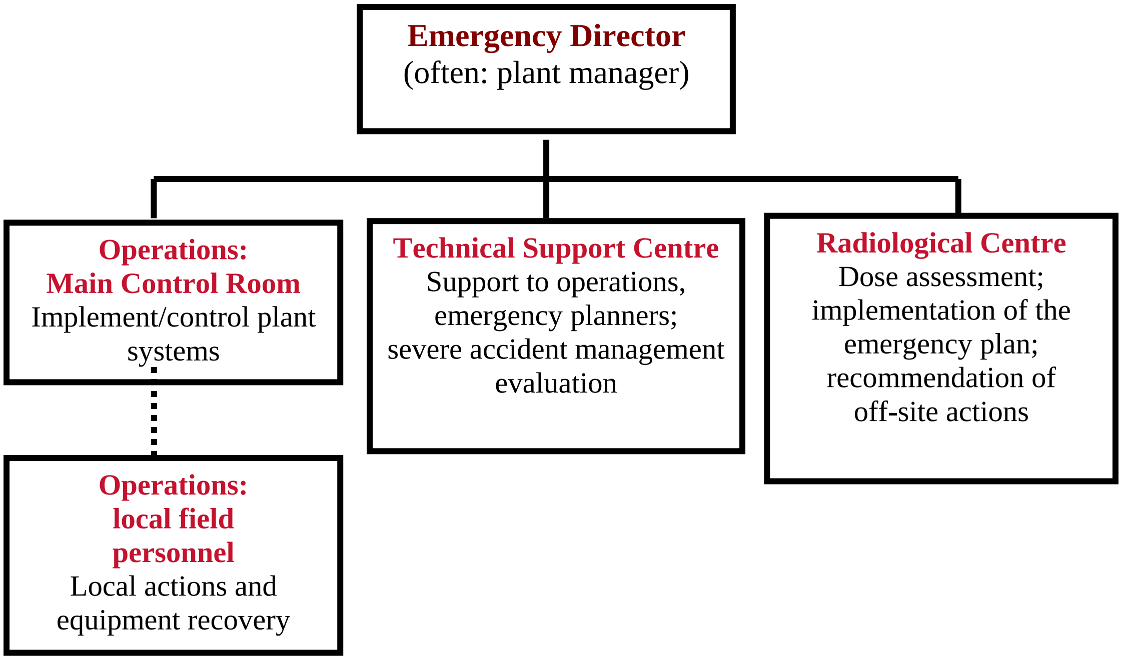

Emergency Director
(often: plant manager)
Operations:
Main Control Room
Implement/control plant systems
Technical Support Centre
Support to operations, emergency planners; severe accident management evaluation
Radiological Centre
Dose assessment; implementation of the emergency plan; recommendation of off-site actions
Operations:
local field personnel
Local actions and equipment recovery

FIG. 2. Typical layout of the main elements of the plant Emergency Response Organization

Criteria for activation of the TSC should be specified, and accident management measures should be carried out by the control room staff until the technical support centre is functional.

The rules for information exchange between the teams of the ERO should be defined. The flow of information between the TSC and the control room as well as from the TSC to other parts of the ERO, including those responsible for the execution of on-site and off-site emergency plans, should be specified.

The accessibility and habitability of the physical locations of the evaluator and implementer teams as well as of the emergency director under severe accident conditions should be checked and maintained. A widely applied arrangement is that the team of evaluators is located in the technical support centre room, and the team of implementers is in the control room of the plant.

Ad 9. Verification and validation

All procedures and guidelines should be validated. Validation is the evaluation that confirms that the actions specified in the procedures and guidelines can be followed by trained staff to manage emergency events

Possible methods to validate SAMG are the use of a full scope simulator (if available) or an engineering simulator or other plant analyser tool, or a tabletop method. The most appropriate method should be selected. On-site tests should be performed to validate the use of equipment. Scenarios should be developed, and they should describe a number of fairly realistic (complex) situations, which should require the application of major portions of the SAMGs.

Staff involved in the validation of the procedures and guidelines should be different from the staff that developed the procedures and guidelines.

Ad 10 - 13. Training; new information; analysis; management of AM program development.

The remaining items discuss the education and training of plant staff, and the processing of new information such as revision of the generic guidelines and new results of research in severe accidents.
Comprehensive guidance is formulated regarding the analysis needed and an example presented. Finally, the management of development of the am program is linked to applicable other IAEA documents.

6. PRESENT STATUS

The AM-Guide has been completed and approved by the NUSSC for collecting Member Sate comments. These have been processed and the Guide will now be considered by final approval by NUSSC and publication.

7. IAEA SERVICE: REVIEW OF THE ACCIDENT MANAGEMENT PROGRAM (‘RAMP’).

Apart from existing services such as OSART, IPSART, the IAEA has created a service called ‘Review of the Accident Management Program’ (RAMP) [9] at an NPP.

Objectives of the services can be summarized as follows:

1. to explain to licensee personnel principles and possible approaches in effective implementation of AMP based on experience world-wide;
2. to give opportunities to experts from the host plant to broaden their experience and knowledge in the field;
3. to perform an objective assessment of the status in various phases of AMP implementation, compared with international experience and practices; and
4. to provide the licensee with suggestions and assistance for improvements in various stages of AMP implementation.

The service consists of two parts, one for the analysis and one focussed on the implementation of the accident management program:

Review of Accident Analysis for Accident Management (RAAAM): this review is intended to check completeness and quality of accident analysis covering BDBA and severe accidents. The review should be typically performed prior to use of accident analysis for development of AMP. It is considered that 2 experts and 1 IAEA team leader in one-week mission can perform the review.

Review of Accident Management Programme (RAMP): this review of AMP, in particular appropriate prior to its implementation, is intended to check its quality, consistency and completeness. The review of accident analysis as described in the previous paragraph is a part of the overall review. It is considered that a group of 4 invited experts and one team leader (IAEA staff) during one-week mission will be capable to perform the task. Such composition of the team is sufficient, if detailed review of accident analysis as described in the previous bullet was done separately as a different task, or e.g. within the framework of review of level 1 or level 2 PSA study. If this is not the case, than two more experts should be included in the team to take care of the accident analysis.

At present, two full RAMP and one preparatory-RAMP missions have been completed. The IAEA is in contact with various Member States for further RAMP-missions.

8. CONCLUSIONS.

The IAEA has compiled extensive guidance on the development and implementation of accident management at an NPP. As such, it gives guidance on how to implement the requirements of [NS-R1]. Accident management is a set of actions to prevent a BDBA to escalate into a severe accident and, if not successful, to mitigate the consequences of such accidents.

The development of accident management guidance is a process with a number of dedicated steps in a top-down approach. First the objectives are defined, followed by the development of strategies to achieve these objectives. From the strategies, means are developed to execute the strategies. Finally, procedures and guidelines are set up, to give detailed guidelines on the actions to be taken on pant equipment.

The process of developing these guidelines is described in some detail. It has 13 elements, as described in sec. 5. It starts with a search for plant vulnerabilities, then it defines the plant capabilities. In defining these latter ones, use is made of all plant systems, also in a non-conventional way and, if needed, outside the design basis of the system. The role of instrumentation is discussed and possible hardware modifications are treated. In developing the guidelines, it is considered that many actions are not unique safety-oriented, but can have negative consequences as well.

As severe accident are complex events, appropriate evaluation and decision-making is required. Mechanisms to achieve this are described, e.g. the support by a Technical Support Centre and decision-making by a high-level authority, mostly the Emergency Director. The AM Guide discusses this item at length, in view of the importance of the issue.

The AM Guide further describes the process of verification and validation of the guidelines. Should new information arise, a process should exist to incorporate it into the guidelines.

Finally, it is described that IAEA has developed the service of Review of Accident Management Program (RAMP) at an NPP. This is a mission of about one week with 4 - 6 experts to a plant, and investigates the existing AM program in detail. Its objective is to further strengthen and improve the AM program. A number of RAMP missions have been performed in last years.

9. REFERENCES.

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Requirements, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Operation, Safety Requirements, Safety Standards Series No. NS-R-2, IAEA, Vienna (2000).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, draft Safety Requirements, IAEA, Vienna (in publication).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Review of Plant Specific Emergency Operating Procedures, Safety Reports Series No. 48, Vienna (2006).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Implementation of Accident Management Programmes in Nuclear Power Plants, Safety Report Series No. 32, IAEA, Vienna (2004).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Approaches and tools for severe accident analysis, Safety Report Series No. 56, IAEA, Vienna (2008).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, *Deterministic Analysis of Severe Accidents in Pressurized Heavy Water Reactors*, IAEA TECDOC No 5089, Vienna (2008).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Severe Accident Management Programme for Nuclear Power Plants, draft Safety Standards Series DS385, IAEA, Vienna.

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidelines for the Review of Accident Management Programmes in Nuclear Power Plants, IAEA Services Series No. 9, Vienna (2003).

TOPSAFE
Dubrovnik, Croatia, 1 - 3 October 2008
International Topical Meeting on Safety of Nuclear Installations

THE SGTR (STEAM GENERATOR TUBE RUPTURE) LICENSING EVOLUTION AND THE ASSOCIATED MODIFICATIONS FOR NUCLEAR UNITS IN BELGIUM

François Parmentier
Senior Engineer, thermalhydraulic & severe accidents group
Tractebel Engineering (Suez group)
Avenue Ariane,7. 1200 Bruxelles, Belgium
francois.parmentier@tractebel.com

Jean-Charles Delalleau
Safety manager, generation, Tihange
Electrabel (Suez group)
Avenue de l'industrie , 1. 4500,Huy, Belgium
jeancharles.delalleau@electrabel.com

ABSTRACT

All over the world, the Steam Generator Tube Rupture (SGTR) event has been a difficult and controversial subject of nuclear plant safety, at least for generation II plants. In some penalizing conditions, this event may lead to a direct radioactive release to the environment, by-passing both the Reactor Coolant System (RCS) and the containment barriers. From the time of the conception of generation II plants, several aspects have evolved. First of all, the event frequency has appeared to be higher than expected, because some SGTR events have really occurred, mainly due to corrosion of Steam Generators' (SG) tubes. Secondly, it became clear that besides the SG overfilling leading to liquid release, other phenomena could be possible, like the atomisation (small droplets of primary water escaping from SG's) of the break flow in case of low liquid level in the affected SG. Therefore, since the 90'ies, the Belgian Safety Authorities (BSA) requested to improve the situation of the plants in operation, and to provide a safety demonstration taking into account scenarios associated to these newly identified phenomena. After several years of efforts, 2007 has to be recognized as a milestone for the licensing, as an agreement has been finally reached between the Utility and the BSA. It consists in adopting different modifications enhancing both the prevention and the mitigation capacity of the plants. Complex and various supporting studies have demonstrated that the radiological impact of a SGTR occurring on any Belgian unit can be significantly reduced once these modifications are carried out. These are concerning Nitrogen-16 chains qualification, installation of control room operated motorized isolation valves upstream of the SG relief valves, reduction of the maximal iodine concentration during operation, reduction of the allowed primary to secondary system leak rate and improvement of the accident procedures. The fact that practically all the original steam generators have been replaced from 1993 until today, and the adoption of new chemical treatment of the secondary circuit (all volatile treatment), are major modifications reducing significantly the SGTR occurrence frequency. Finally, a specific training program helps the operators to react adequately and efficiently in case of any possible SGTR scenario. It must be underlined that this final agreement is the result of a fruitful collaboration between the Utility (Electrabel) and the Architect Engineer (Tractebel Engineering). Many experts have worked on the subject during a given period or even followed the entire project since its beginning.

1 INTRODUCTION

The Steam Generator Tube Rupture (SGTR) event is a design basis accident that must be taken into account for the licensing of PWR's. This accident is complex, with many particularities distinguishing it from other design basis events. Considering the three major safety functions defined by the IAEA [1] (capability to safely shut down, to remove residual heat and to limit radiological consequences), the SGTR has the potential to challenge each of them.

Firstly, the residual heat removal is a concern because there is a primary inventory loss that could lead to core melting.

Secondly, the control of the radiological release is maybe the most important concern characterizing the SGTR, because even without any core damage, there is a possibility to bypass all the three barriers (fuel, primary circuit, containment). The fuel cladding barrier is never perfectly leakproof and an iodine spiking, due to reactor trip, can lead to a significant activity increase in the primary coolant. The SGTR itself is a breach in the second barrier, while the opening of secondary relief valves allows release to the environment. In 1997 [2], the BSA (Belgian Safety Authorities) were considering the containment by-pass, and particularly the SGTR event, as a key point of future generation III plants.

Thirdly, the capacity to safely shutdown is also a concern recently highlighted again in the licensing of some generation III plants, because when primary and secondary pressures are similar, there is a possibility of back-flow that can cause a boron dilution and a reactivity rise in the core [3].

Even with design improvements that are included in generation III plants, the debates are still in progress.

Another particularity of this event is its relatively high occurrence frequency, since it has happened several times in the past operating experience of PWR's. Luckily these events have not lead to significant consequences, but this experience led to the observation of new phenomena, and to re-evaluations, in general showing that the SGTR risk was probably underestimated [4]. That explains the international pressure to re-evaluate the SGTR licensing of existing PWR's.

The present paper will treat the evolution of the international context, and in particular what has been required and achieved in Belgium to improve the safety of generation II PWR's. It is here supposed that the reader has a general knowledge on the SGTR scenario.

2 DESCRIPTION OF THE SGTR EVENT

The major causes of SG tube break can be the corrosion (different types), the wear, or the presence of a foreign object.

There are many different possibilities of SGTR scenarios, and a distinction should be made between realistic scenarios and scenarios resulting from a deterministic licensing approach using conservative initial and boundary conditions. Hereafter, an attempt is made to make a general description of what can happen after the initiating event, the figure 1 represents the primary and secondary pressure (one of the most important parameters) evolution.

The reactor can be initially at power or even in hot standby state. Regarding the radiological aspect, there is no risk of release to the environment if the primary coolant is perfectly clean and if the fuel cladding remains hermetical during the event. However, the primary coolant activity can be initially at the limit allowed by the technical specifications. In this situation, there is a continuous activity release through small cracks in the fuel rod cladding. This is the first barrier failure.

By definition, the initiating event is a SG tube break, somewhere between the tube plate and the apex.

From this time on, the Chemical and volumetric control system (CVCS) is not able to compensate the break flow, and the primary mass inventory begins to decrease, as well as the pressuriser level and the primary pressure. Regarding the radiological aspects, the initiating event is the second barrier failure.

If the reactor is at nominal power, the feedwater mass flow to the affected SG is controlled to maintain the narrow range level at the value corresponding to the SG's initial mass. Due to the break flow, the feedwater mass flow to the affected SG is lower than for the other two. With a reactor being initially in hot standby, the feedwater flow is small and the affected SG inventory will increase, this can be an important indication for the operator.

Even without any operator intervention, the reactor is tripped (if initially at power) on the low advanced pressuriser pressure signal. After that, the low low pressuriser pressure signal will start the safety injection.

From that time on, there is a stabilisation of the primary inventory and pressure, high pressure safety injection being able to compensate the break flow. This is a good factor for the core cooling, but not for the contamination of the secondary circuit that continues.

Many different hypotheses can be taken from the time of reactor trip, enhancing either the overfilling of the affected SG (risk of liquid releases), or it's emptying (risk of by-pass releases). A Loss Of Offsite Power (LOOP) can result from the grid perturbation after reactor trip, stopping primary pumps and normal feedwater pumps.

The turbine is also tripped and in case of unavailable condenser, the secondary pressure will increase until the actuation of a relief device (relief valve or safety valve). Regarding radiological aspect, this is the third barrier failure, and releases to environment begin.

For most plants, operator actions are necessary to reach a safe shutdown state. From the observation of activity in the secondary circuit using Nitrogen-16 (N-16) monitors), or abnormal SG level, the operator will identify the affected SG. The objective is firstly to isolate the affected steam generator (which is done by adjusting relief valve setpoint and closing the main steam isolation valve), and to control the level (which is done by auxiliary feedwater isolation if necessary). Thereafter, the operator cools down the primary circuit, via opening of the intact steam generator relief valves. This cool down is necessary to recover a sufficient subcooling margin to allow to depressurize the primary system without risk of massive boiling. This process requires to stop the safety injection pumps. A controlled state is reached when primary and secondary pressures match, terminating the break flow.

On the long term, the primary and secondary cooldown and depressurization are pursued until connection to the Residual Heat Removal system (RHR), in order to reach a safe shutdown state.

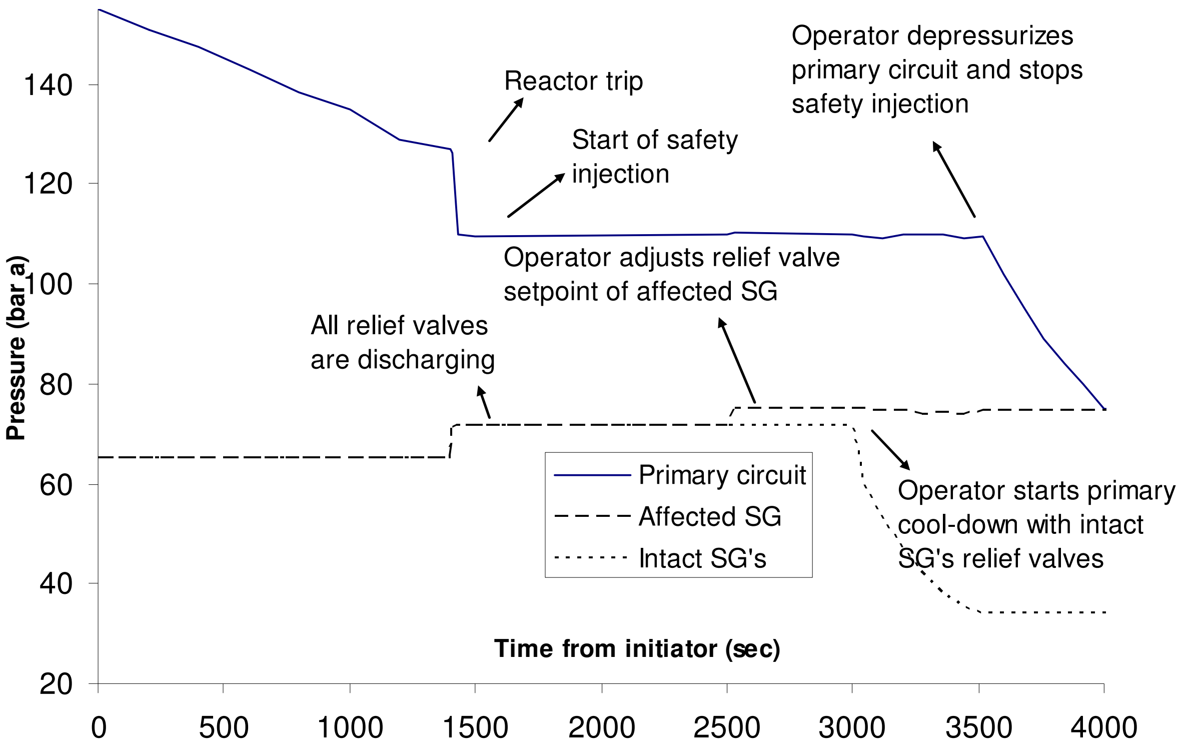


Figure 1 : typical pressures evolution during SGTR event (starting at Hot Full Power)

3 LICENSING EVOLUTION DUE TO THE US EXPERIENCE

Originally in Belgium, only the aspects of core melting and SG overfilling were investigated for the SGTR accident. Radiological consequences were evaluated considering the partitioning phenomenon, by which a fraction of the iodine in the liquid phase of the affected SG, is carried by the steam. A dilution of the break flow into the affected SG coolant was also assumed. By these two effects, the calculated radiological consequences were not important.

In the 80ies, two SGTR events occurred in the US. They both drew the attention of the NRC (Nuclear Regulatory Commission) and showed that these events were more than hypothetical and could have some unexpected characteristics:

- in 1982, Ginna event, during which an overfilling of the affected SG was observed. During this event, the SG safety valves opened 5 times, and failed to reseat twice. The radiological consequences were not important
- in 1987, North Anna event, with a break located at the top of the tube bundle.

Following this, NRC warned the industry [5] for a potential of non-conservatism in SGTR safety analysis for plants with inverted U-tube SG, using the following arguments:

- the North Anna tube rupture demonstrates that SG tube failure near the top of tube bundle cannot be excluded
- the tube uncovery can produce a direct path for fission product release
- for those plants where the steam generator tubes are thought to remain covered following tube rupture, the previously calculated safety analysis offsite dose might be exceeded

In order to better illustrate the situation, the following figure 2 shows the different possible release mechanisms:

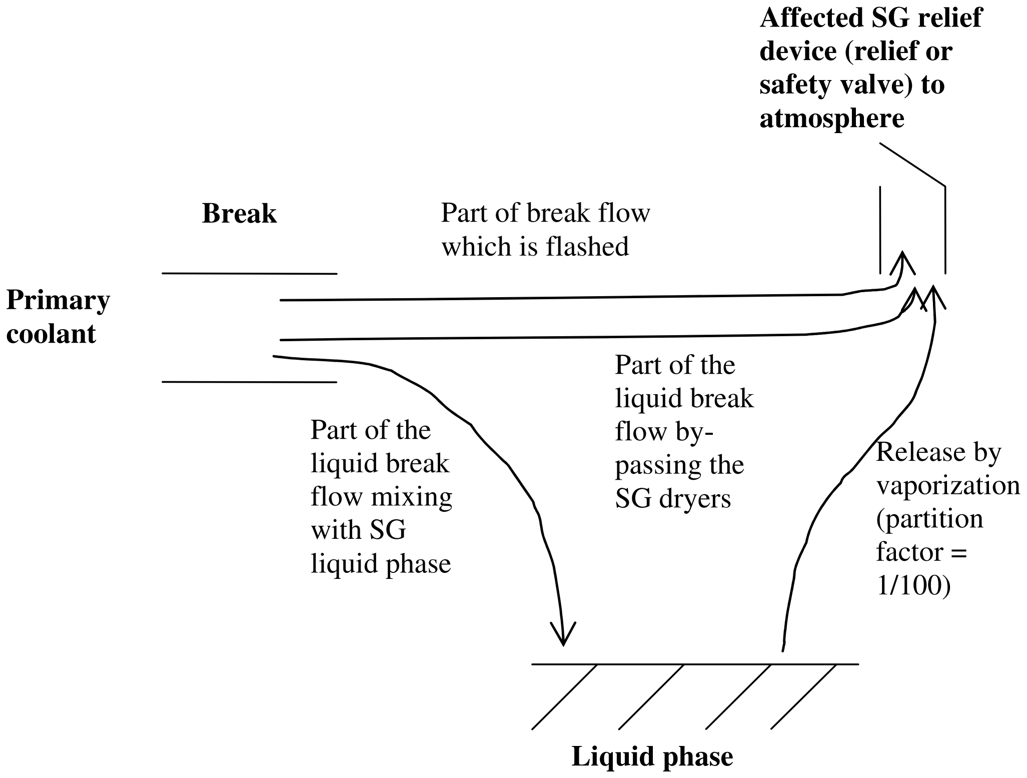

Affected SG relief device (relief or safety valve) to atmosphere
Break
Part of break flow which is flashed
Primary coolant
Part of the liquid break flow by-passing the SG dryers
Part of the liquid break flow mixing with SG liquid phase
Release by vaporization (partition factor = 1/100)
Liquid phase

Figure 2 : release mechanisms

Besides the possibility of SG overfilling and liquid releases, figure 2 shows the situation with a low liquid level in the affected SG (uncovered break). The break flow can be divided in three parts:

- the part of the break flow which is flashed (directly transformed into steam due to sudden depressurization)
- a first liquid part mixing with the SG water (liquid)
- a second liquid part composed of very small droplets (atomization) that can be carried out of the affected SG (steam dryer being not efficient for very small droplets)

At the relief device of the affected SG (relief or safety valve), three contributors of releases are possible:

- flashing, carrying the iodine primary activity
- partitioning, which is the affected SG liquid vaporization carrying a fraction (usually one hundreds) of the iodine in the liquid phase
- the by-pass (atomization), carrying the primary iodine activity

The response of the industry to the NRC requirement was an evaluation [6], using a model of primary water by-pass validated on a test facility. Moreover, a stuck-open relief valve was taken into account in the evaluation (not the case in the design basis). The report concluded that less than 1% of the break flow escapes through the open relief valve even when the break is uncovered. The report concluded that the contribution of this scenario to the global risk was negligible, and the design basis evaluations were still valid.

4 BELGIAN PUSGR PROGRAMS

After the SGTR events in US, the BSA reacted in 1989 by reclassifying the SGTR from class IV to class III according to ANSI 18.2, since an occurrence frequency lower than 10^{-2} event/year could not be justified anymore. As a result, a lower dose limit had to be respected.

The first Power Uprating and Steam Generator Replacement (PUSGR) in Belgium took place in 1992 for the Doel 3 unit, justifying the complete review of the Final Safety Analysis Report (FSAR). In particular, the SGTR event attracted the attention of the BSA in the safety review due to the following reasons:

- the degradation of the steam generators (addressed further in the document) was partially explaining the decision to launch this project
- the US experience as described before
- the Belgian experience, with the occurrence of an SGTR in Doel 2 in 1979

Therefore, despite the fact that the SG replacement was improving the situation, the requirements of the BSA regarding the new SGTR study were more stringent as compared to the design study:

- SGTR must be evaluated as a class III event, as required since 1989
- a stuck-open SG relief valve must be taken into account as possible single failure
- scenario with by-pass release must be considered

These requirements led to long and difficult discussions during the licensing process. The next PUSGR project in Tihange 1 (1995) had similar problems. Following these two difficult licensing situations, it appeared that the conclusions of the Belgian evaluations were not in accordance with the evaluation for US plants [6] since the scenario's that enhanced an uncovered break could lead to unacceptable consequences. The poor knowledge of the phenomena and the non adapted tools, were supplementary difficulties for a convincing safety demonstration.

In front of this situation, in agreement with the BSA, it was decided to create a SGTR generic project (i.e. concerning all 7 Belgian units) having as main objectives to deeply investigate and evaluate the consequences of an SGTR, mainly for scenario's leading to an uncovered break.

5 THE SGTR GENERIC PROJECT

Several tasks were defined in the beginning of the generic project in 1995, and they evolved in parallel. The work performed since then is quite important and described hereafter.

The Iodine-131 (I-131) is the most significant isotope regarding radiological impact. Therefore, it was fundamental to study its behavior during the SGTR calculations, going from the source term in the primary circuit, to the release to the atmosphere. First of all, a model of fission product transport was developed [7] and included into the RELAP5/MOD2 [8] input deck of a typical 3-loop Belgian nuclear unit. It consists in calculating the I-131 concentration in the primary circuit and in each SG, including all the release mechanisms described in figure 2.

The integration of the I-131 activity balance is performed for the 6 following systems starting from the break opening time:

- Primary without pressurizer
- Pressurizer
- Liquid phase of the affected SG
- Liquid phase of the leaking SG
- Liquid phase of the intact SG
- Condenser

For each of these systems, a I-131 balance equation is integrated, taking into account the incoming and outgoing flows with their respective activity, the source terms in the system and the radioactive decay. More details can be found in reference [7].

5.1 Spiking model

The Quantification of the source term of iodine in the primary circuit was a main task of the generic project.

The iodine spiking is a phenomenon during which the primary coolant activity in iodine is rising, following operational transients like scram, important load variation, or primary depressurization. Due to a poor understanding of this phenomenon, the first spiking model coming from the NRC in the 80ies was simple, expressing the fuel release rate (Bq/s) during the spiking as a multiple of the fuel release rate in normal operation*: R_0*.

The drawbacks of this model were the unspecified period of release and the absence of available iodine inventory. Its use was leading to very high and unrealistic activities (Bq/m3) in the primary circuit.

Therefore, for the SGTR generic project, a more efficient model was developed, starting from a sufficient comprehension of the key phenomena, as described hereafter.

Even with a good quality of fuel, fuel cladding cracks are always present. During an experience in which helium was injected in the space pellet-cladding, no iodine release was observed. It is thus supposed that iodine can be expulsed out of the fuel if water has first penetrated into the space pellet-cladding, through the existing cracks. In this space, iodine is supposed to be present in the form of a salt which is water soluble, and representing about 1% of the total fuel iodine inventory.

Moreover, a supplementary iodine inventory that originates directly from the pellets, can be released during the spiking:

- Due to the thermal shock between entering water and the pellets, that generates cracks in the pellets, forming a path for the iodine to escape
- Due to the decrease of pellets conductivity after oxidation with water, that generates higher temperatures in the pellets, enhancing iodine diffusion

This second contributor of iodine inventory is more important in case of fuel damage.

After a spiking, about 3 days of irradiation at full power are needed to recover half of the iodine inventory which is present in the space pellet-cladding.

Based on these observations, the new model can be build.

In a first step, an iodine *Inventory* (Bq) that can be released in the primary during the few hours after spiking initiation, is calculated, as function of $R_{0.}$ It has been verified that this model of inventory covers all the spiking phenomena that have been observed in the Belgian units during a long operation period.

R_0 is easily obtained because it is in equilibrium with the filtration rate of the CVCS system, imposing a given primary coolant activity. For a conservative evaluation in the SGTR analysis, this activity can be just at the limit authorized by the technical specifications at stable conditions (see later explanations on these limits), due to a pre-spiking occurring before the accident.

In a second step, the spiking itself is initiated at scram, releasing the remaining inventory (because not enough time to recover the total inventory), by the following relation:

$$R(t) = \frac{Inventory}{T} \cdot e^{-t/T} \qquad (1)$$

The acceptance of this model by the BSA was an important milestone of the project.

5.2 Atomization model

By lack of experimental data, the following simple and conservative model has been developed in accordance with the BSA. From figure 2, the fraction of the liquid break flow which is atomized and bypasses the dryers in the form of small droplets (carrying coolant activity out of the affected SG) depends on 2 thresholds:

- If the affected SG is not stratified (sufficient recirculation), which is considered to be the case before the scram, the by-pass fraction is 0.0001

- If the affected SG is stratified (which is the case after scram), the NLH (Net Liquid Height) value has to be calculated and represents the collapsed liquid level above the break location. If NLH is greater than 2 feet with uncertainties, the break is covered and the by-pass fraction is 0.01. Otherwise, the by-pass fraction is 0.3.

That explains the reason why the worst break location for scenarios enhancing the by-pass of the primary coolant, is at the top of the tube bundle.

5.3 Operator intervention timing model

As explained in figure 1, operator actions are necessary to reach a safe shutdown state following a SGTR event. For scenarios with uncovered break, the release is terminated when primary cool-down is initiated (except for a single failure with relief valve stuck open), because the affected SG pressure decreases and its relief valve closes. For the overfilling scenario, the primary-secondary pressure balance must be reached to terminate the break flow.

In order to defend a reasonably conservative timing, a new method has been developed, discussed and accepted by the BSA, specifically in the frame of SGTR generic project

The method consists in classifying all operator actions in five different types, each with its specific duration: opening of procedure, simple verification, verification with a judgment, simple action, complex action. This method requires characterizing the type of each operation action in one of the five categories that are proposed. For some of them, this interpretation can be discussed (especially when making the difference between simple and complex actions).

In a transient simulation, not all the operator's actions are necessarily simulated. Nevertheless, the delay and duration associated to these operators' actions have to be characterized and taken into account in order to obtain a realistic “time table”.

A first remark is that the procedures are specific for each unit (number and nature of steps to follow), and the “time table” is thus also specific. Unless a bounding approach is adopted, the plant specific accident procedures are thus directly linked with the safety assessment.

A second remark is the technical differences between plants: a simple action in one plant can correspond to a complex action in another plant.

An assessment of the proposed method has been made, performing different comparisons with simulator tests: WCAP simulator test results [9] using the standard Emergency Response Guidelines (ERG) procedures, simulator test results for Tihange 3 using the specific Tihange 3 E-0 and E-3 procedures, simulator test results for Doel 4 using the specific Doel 4 E-0 and E-3 procedures.

It appeared that the method covers the majority of the operator teams without being too conservative. The following example concerns some important actions that are simulated in the calculations for the overfilling scenario initiated at nominal power. Conservatively, the first evident sign for the operator that something is going wrong is the scram. The following events then take place:

- after 12 minutes, identification of the affected steam generator and going from E-0 to E-3 of the ERGs. Adjustment of the affected SG atmospheric relief valve setpoint.
- after 14 minutes, closing MSIV and by-pass valves
- after 16 minutes, checking the intact SG's level and keeping the level in a given range by a "switch on – switch off" feedwater system
- after 21 minutes, start of the Reactor Cooling System (RCS) cool-down by opening the intact SG relief valves.

The duration of the cool-down (about 15 minutes) depends on the RELAP model behavior, and is close to what is observed on simulator. The same occurs for the depressurization phase (about 10 minutes). From the scram to break flow inversion, the total duration is about 45 minutes.

5.4 Main results of generic evaluations

With all the detailed models described before, and with a RELAP input deck representing a typical 3-loops plant, calculations have been performed for three main scenarios that are summarized below.

Low water inventory and by-pass release

The reactor is initially at power. A break is simulated at the top of the tube bundle. Different possibilities of single failure have been examined and the most significant is the relief valve of the affected SG which remains stuck open after scram. The condenser is assumed unavailable. As aggravating failure, a LOOP is postulated at scram, leading to the coast-down of the primary pumps and of the SG feedwater pumps. It is the only scenario for which the radiological consequences are calculated.

Next figure 3 shows the importance of each contributor in the total release:

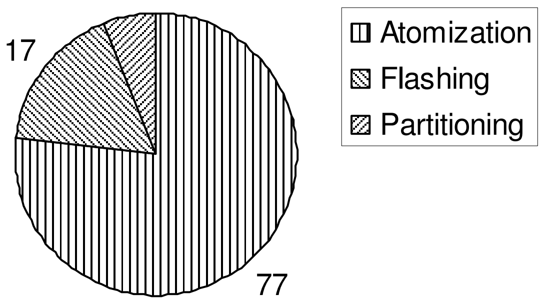


Figure 3 : contributors (% of total release)

The absolute value of release was slightly higher than the limits, and moreover, could only be terminated if the operator had the opportunity to isolate the stuck open relief valve. This result demonstrated the non applicability of the US evaluations [6] for Belgian licensing :

- due to different parameters influencing the results, as the smaller SG tube size, and the more important SG relief valve capacity. These differences completely change the affected SG mass balance and enhance the capability of SG emptying, increasing the risk of releases by atomization

- due to the stringent atomization model which is described in §5.2

It appeared that the difficulties encountered during PUSGR projects were confirmed, even using the very detailed models that were developed during SGTR generic project.

Anyway, this result was consistent with the European benchmark exercise realized in 1999 [4], concluding that bypass release mechanism could be an important contributor to risk, and that the prevailing licensing methodologies may in some cases be non-conservative.

Overfilling scenarios

The event was analyzed starting with reactor initially at full power, or at hot shutdown. A break is simulated at the base of the tube plate in order to maximize the break flow. SG level measurement error (for case at full power) and SG designer liquid inventory uncertainty, are added to enhance overfilling. For the case at power, the regulation of normal feedwater is considered as blocked at the initial position.

In both cases, an overflow of several tens of tons of liquid out of the affected SG was predicted. The major contributor of the affected SG overfilling is the break flow, demonstrating that the rapidity of the operator action is a key point.

Again for this scenario, difficulties were encountered, even using the operator intervention timing model described in §5.3.

6 FINAL AGREEMENT WITH BSA, SUPPORTED BY IMPROVEMENTS OF BELGIAN PWR UNITS

In 2007, a demonstration was performed in front of the BSA, regarding the reduction of the SGTR risk from the beginning of the SGTR generic project. Improvements concern both the prevention and the mitigation of the consequences. Some of the associated modifications are already performed, and others are planned on the short term. These are described hereafter.

6.1 Prevention improvements due to new steam generators, new chemical treatments and FME procedures

As mentioned in §4, despite the SG replacements in Belgium that improved gradually the situation, the requirements of the BSA regarding the new SGTR study were more stringent compared to the design study. This can be explained by the fact that there was no sufficient operation feedback and no sufficient reason to be more confident in new SG's.

The NRC has identified 10 SGTR events, all of them happened between 1975 to 1993, among them one in Belgium: Doel 2 in 1979. A remarkable point is that all these events happened in plants using SG's in Inconel 600 MA (Mill annealed).

In 2006, 10 years after the start of SGTR generic project, 13 years after the first SG replacement in Belgium, and 18 years after reclassification of SGTR event by the BSA, a new evaluation was made in the frame of the SGTR generic project. This evaluation was based on Belgian and international feedback and showed that the situation was significantly improved:

- the behavior of Inconel 690 or Incoloy 800 for new SG's appeared to be much better than the Inconel 600 regarding different types of corrosion phenomena
- the secondary circuit chemical treatment (all volatile treatment) was better than old treatment methods that led to corrosion
- procedures of Foreign Material Exclusion (FMA) applied for primary and secondary circuit, significantly reduced the probability of SGTR due to foreign object

For plants using SG's in Inconel 690 or Incoloy 800, the evaluation made counts about 1000 years of operation without any problem. Using a binomial distribution, it was demonstrated that:

- the frequency of 7 SGTR events per 10000 reactor-years is the most likely one
- there is 95% probability to have a frequency smaller than 3 SGTR events by 1000 reactor-years

Even considering that tomorrow, an SGTR event happens somewhere, the same evaluation shows slightly different results. In this case, there is more than 95% probability that the real SGTR frequency would be smaller than 5 events per 1000 reactor-years.

The situation is summarized in figure 4 below. Using the ANSI 18.2 classification as it is the case in Belgium, with the current conditions of operation (new types of SG, chemical treatment, FME procedures…) the SGTR event can be considered as a condition IV event. Even if the reclassification from condition IV to condition III that occurred in 1989 was justified, this is not the case anymore.

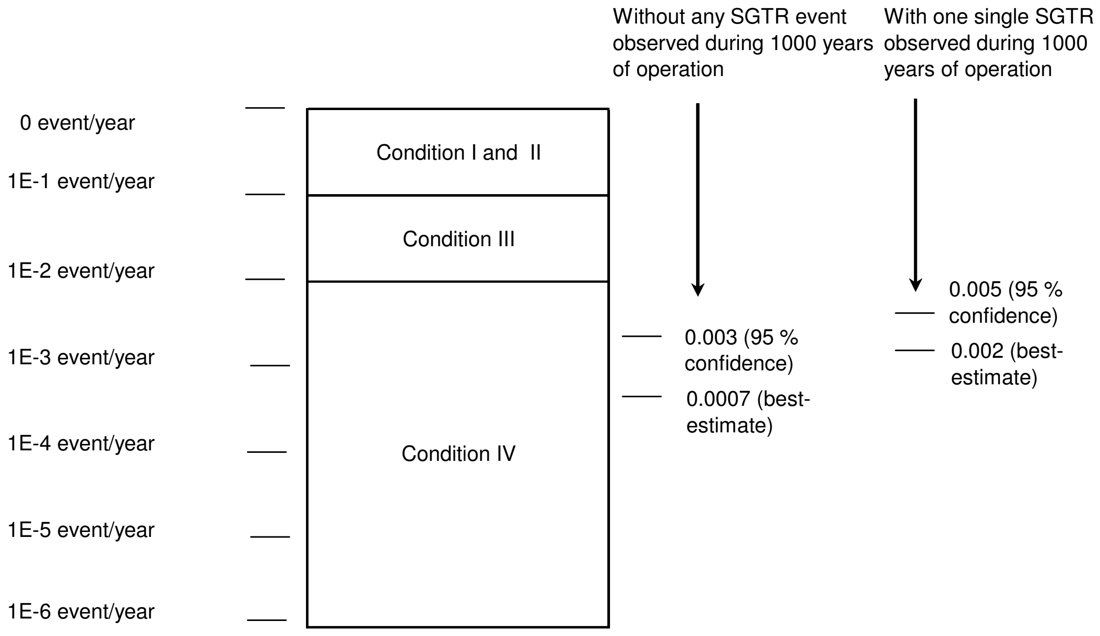


Figure 4 : SGTR classification following ANSI 18.2

As already mentioned; the first SG replacement in Belgium occurred 1992 (Doel 3). Since then, most SG's have been replaced on the Belgian units. Only Doel 1 is still equipped with its genuine SG’s (their replacement is planned for 2009). So far, no SG tube has been plugged in any new SG.

Since the beginning of the SGTR generic project, this is a significant improvement regarding prevention.

6.2 Prevention improvements regarding treatment of SG leakage

The current technical specifications allow a maximum primary to secondary leakage of 80 kg/h for each SG during power operation. The allowed leakage will be reduced to 24 kg/h in order to limit the likelihood of propagation of flaws to SG tube rupture. The alarm set-points on N-16 radiation monitors will also be reduced.

The training program for the licensed operators will be adapted in order to bring the proper response to an SG leakage.

6.3 Mitigation of consequences : qualification of the SG tube leakage monitoring

In §5.4 dealing with evaluations performed, it is supposed that the operator has an efficient indication to detect the accident and to identify the affected SG.

The continuous on-line N-16 radiation monitors provide for rapid detection and response to leakage. They allow the operator:

- to identify a SG tube leakage at an early stage and to take appropriate actions,
- to identify which SG is affected by a tube rupture and has to be isolated, according to the incident or accident response guidelines.

The N-16 chains are not effective at low power. Nevertheless, if a SGTR occurs at high power, the N-16 detection significantly reduces the overall operator response times when applying the accident procedures E-0 and E-3. The generic studies have shown that a shorter operator response time leads to the significant reduction of the radiological impact of the SGTR.

On the Doel units, the N-16 radiation monitors are located in safety-grade cabinets and receive a safety-grade power supply. Their output signals are sent to a safety-grade recorder in the control room.

On the Tihange units, the N-16 radiations monitors are not powered by a safety-grade power supply. Their output trigger an alarm in the control room but are not recorded.

The qualification level of the N-16 monitors will be improved on all units so as to ensure that their outputs are memorized and can be relied upon to ease the identification of a SGTR when applying E-0 and E-3 procedures.

Firstly, the Utility has charged the Architect Engineer to define for all units the required modifications to be carried out to reach the desired qualification level of N-16 radiation monitors. The modifications will be performed in a second phase currently in preparation.

6.4 Mitigation of consequences : remote controlled isolation of SG relief valve

As explained in §5.4 dealing with evaluations performed, the single failure applied on a stuck open relief valve led to unacceptable consequences, even considering an efficient isolation by the operator. However, this isolation could not be ensured on all Belgian plants.

As a consequence, on all Belgian plants, the SG relief valves will be provided with a qualified motor-operated isolation valve, capable of being remotely operated.

The electrical power supply to the isolation valve will be safety grade. For plants with a bunker, second level electrical power is also acceptable.

The remote controlled SG isolation valves will be subject to new technical specifications that can be added to the already existing specifications about the SG relief valves.

Some plants (e.g. Doel 4) already have the required isolation valve, but without the remote commands located in the main control room. Sending an operator to the bunker in order to perform isolation of a stuck-open relief valve takes about 1 minute, which is acceptable.

This modification has been carried out in 2006 on Tihange 2 and 3.

All Belgian units are thus today consistent with the SGTR generic evaluations.

6.5 Mitigation of consequences : improvement of emergency response guidelines and licensed operator training

The following modifications have been introduced in ERG procedures in Doel and Tihange. At an early stage in the procedures, the operator is explicitly asked to pay attention to the narrow range level and feed-water flow of the affected SG. Early contingency actions are asked should, for some reason, the SG level be out of control:

- isolation of Main Feedwater (MFW), Auxiliary Feedwater (AFW) and Emergency Feedwater (EFW) in case of uncontrolled SG overfilling,
- isolation of the SG relief valve in case of uncontrolled SG draining by a stuck-open SG Relief Valve.

Specifically for the Doel units :

- the operator is asked to use the (recorded) N-16 indications to identify a SGTR,
- the subcooling target at the end of the cooldown phase has been lowered from 30°C to 20°C so as to reduce the delay needed to resume the subcooling target and bring the RCS pressure to the affected SG pressure.

On the Tihange units, the use of the N-16 indications to identify a SGTR will be added to the procedures once these indications are adequately qualified.

Training program for licensed operators will be adapted in order to (continuously) clarify their knowledge and understanding of:

- the physical phenomena that influence the radiological impact of a SGTR,
- the purpose and impact of above mentioned system and technical specifications modifications,
- the proper response according to each leakage or SGTR possible situation,
- the usage of incident procedures as well as emergency response guidelines.

As the Hot Zero Power (HZP) scenario of the overfilling (in §5.4) was also sensitive, the future simulator training will also focus on the HZP case and not only on the Hot Full Power (HFP) case.

6.6 Mitigation of consequences : reduction of the technical specifications limits on primary specific activity

The technical specifications limit the allowed primary activity, for both steady state (equilibrium) and transient situations. These limits are expressed as the specific activity of the isotope I-131.

The Utility intends to reduce the radiological impact of a SGTR by adopting for all Belgian units reduced and uniform activity limits:

Table 1

Unit	**Current TS activity limit GBq/t I-131 alone equil. / trans.**	**New TS activity limit GBq/t I-131 alone equil. / trans.**
Doel 1/2	0.65 / 3.75	unchanged
Doel 3	9.11 / 253.85	1.80 / 18.00
Doel 4	2.80 / 28.46	1.80 / 18.00
Tihange 1	14.23 / 40.38	1.80 / 18.00
Tihange 2	7.69 / 40.00	1.80 / 18.00
Tihange 3	4.46 / 38.46	1.80 / 18.00

The activity limits of Doel 1/2 have already been significantly reduced after SG replacement carried out on Doel 2. The main reason was the non applicability of the SGTR generic evaluations for a 2 loop plant (see §5.4).

For all the units, it was demonstrated to the BSA that the radiological consequences of the scenarios examined in §5.4, were reduced quasi proportionally.

The new technical specifications will progressively be adopted by the Utility.

7 CONCLUSIONS

The licensing of the SGTR event has evolved from the conception of generation II plants until today, both due to the occurrence of the event, and to the consideration of new phenomena. In Belgium, difficulties have led to the creation of the SGTR generic project in 1995, in which different tasks were defined in order to deeply investigate the subject. Using the RELAP code, a model of fission product transport was specifically developed. Moreover, precise models were also developed for the spiking, the atomization, and the timing of operator intervention. The last step of this work was a final evaluation using all these models.

For the scenarios enhancing SG overfilling, with the entire conservative initial and boundary conditions, it appeared that the affected SG overfilling is very difficult to avoid, particularly in HZP. However, this situation is less frequent than HFP.

For the scenarios enhancing low water inventory and bypass release, there remains an important uncertainty on the atomization model that was very conservative for the evaluations.

The radiological consequences of all scenarios are limited with the adoption of new technical specifications limits on primary specific activity. This modification is an important challenge for the Utility, which is consistent with the objectives of the Institute of Nuclear Power Operations (INPO) regarding the fuel integrity : “0 failures by 2010”.

During the last 15 years, important efforts were made in the frame of SGTR generic project, in various areas regarding studies and modifications on site, concerning both the Utility and the Architect Engineer, working together to find a solution.

The final agreement with the BSA in 2007 is the demonstration of the success of this work.

8 REFERENCES

[1] IAEA safety glossary, 2007

[2] "TSO study project on development of a common safety approach in EU countries for large evolutionary PWR's" : ICONE5-2160 (Nice, 1997)

[3] "EPR : Steam Generator Tube Rupture analysis in Finland and in France" EUROSAFE 2006.

[4] "Benchmark exercise on the probabilistic safety assessment of steam generator tube rupture radiological releases" European Commission, Nuclear science and technology, Report EUR 18550, 1999

[5] U.S. Nuclear Regulatory Commission : "Steam Generator Tube Rupture Analysis Deficiency", IN 1988-31, May 25, 1988

[6] WCAP 13132 : "The effect of steam generator tube bundle uncovery on radioiodine release", January 1992

[7] "Coupled calculation of the radiological release and the thermal-hydraulic behaviour of a 3-loop PWR after a SGTR by means of the code RELAP5" : Nuclear Engineering and Design 177 (1997)

[8] RELAP5/MOD2 code manual, NUREG/CR-4312, 1985

[9] WCAP-14996 "ERG Operator Response time assessment program : final report" : 1997

TOPSAFE
Dubrovnik, Croatia, 30.09 - 3.10.2008

NPP Safety In Ukraine: Recent Developments and Trend

G. Gromov, O. Sevbo, S. Sholomitsky
State Scientific and Technical Center on Nuclear and Radiation Safety (SSTC)
Str. Stusa 35/37, Kiev, Ukraine
ppmaster@iptelecom.net.ua

ABSTRACT

Significance of nuclear power industry in the Ukrainian fuel and energy complex continually increases. Nuclear energy development program has envisages construction of more than 10 new power facilities during next 20 years. It should be noted that for new nuclear power plants (NPP) more strict requirements for safety (comparing to existent NPPs) are established. The safety has to be ensured by means of NPPs proper siting, design, construction and commissioning, followed by the proper management and operation of the plant.

International and national researches show that the design and operation of existent NPPs meet internationally approved safety principles. However, understanding significance of safety, existent plants promote activities to meet safety requirements for new NPPs. These activities include (but are not limited) such directions, as periodic safety review and life extension/management for older plants, safety upgrade program (for all plants), continuous enhancement of operational safety and implementation of quality assurance system. This paper presents an overview of current trend in the development of these directions.

In particular, in order to meet national requirements, both the Utility and Regulatory Authority undertake activities on NPP modernization using both deterministic and probabilistic justifications. Adopted approach allows increasing safety by more effective use of efforts and means for elimination of safety deficiencies; increase regulatory efficiency; and reduce licensee undue burden while maintaining required safety level. This paper summarizes the main insights and recent results of realization of Safety Upgrade Program on NPPs in Ukraine.

1 INTRODUCTION

Currently four nuclear power plants (NPP) with 15 nuclear reactors of WWER type produce more than 50% electricity in Ukraine. The initial design of these plants and their safety has been continuously improved over the years by taking into account the feedback from operational experience. It can be considered that the safety of these NPPs designed to earlier standards is sufficient. Furthermore, the Utility promotes activities to meet more strict safety requirements for future plants. However, the plants (both future and existing NPPs) must meet a difficult challenge: to be both safe and economically competitive. The way to achieve competitiveness includes (a) enhancement of safety by modification of design / operation and (b) application of risk-informed techniques in decision making process of both the Utility and Regulatory Authority. This paper deals with trends and issues in the development of these directions in Ukraine.

2 SAFETY OF NUCLEAR POWER PLANTS

International and national researches (specifically, safety analysis reports for each type of WWER in Ukraine) show that the design and operation of existent NPPs meet internationally approved safety principles. However, understanding significance of safety, the Utility intends to ensure that operating NPPs maintain safety level comparable to the plants designed and constructed today. To attain this goal, Utility needs, among other aspects, a stable regulatory system that should not be excessively conservative. In order to achieve a stable regulatory system, new regulatory rules must be carefully considered. The rules should be such that Utilities can use their resources for those improvements which are essential to safety rather than on items which are less important, and only marginal to safety. Therefore, the rules should quantitatively define the safety goals. Top level regulatory document, [1], renewed in 2008, numerically defines the safety goals for operating and future NPPs. These goals (as well as the whole document) are consistent with the IAEA safety standards. As a most effective tool in evaluating and comparing NPP safety against safety goal, probabilistic approach is used. Activities in this field are described is Section 3.

To meet safety requirements for future NPPs, the Utility undertakes the efforts, which include (but are not limited) realization of measures developed under periodic safety reviews, implementation of safety upgrade program, and continuous enhancement of operational safety.

2.1 Periodic Safety Review

Regulatory documents, Refs. [1] and [2] require that each power unit of each NPP must perform periodic safety review (PSR) with periodicity of 10 years. The main purposes are to evaluate current level of safety, and to assess whether NPP designed to earlier standards can maintain an adequate safety level, to satisfy operating safety standards and rules. Moreover, it is necessary to conduct PSR to clearly identify any deficiencies in defence in depth, followed by a modernization program so that all barriers can be timely reinforced.

The Utility has developed guide (see Ref. [3]) on contents and structure of report on periodic safety review. At the first stage, Ref. [3] provides requirements for older units, commissioned at 1980-1982 years (Rivne NPP Units 1 and 2; South Ukraine NPP Unit 1). Taking into account experience from conducting PSR for these three units, PSR requirements for other NPPs will be refined.

PSR report should provide real status and prognosis for each safety factor for a period to the next PSR or to the expiration of NPP life time. List of evaluated safety factors should include the following: (1) design; (2) current technical condition of systems and components; (3) equipment qualification; (4) aging; (5) analysis of internal and external hazards; (6) deterministic safety assessment; (7) probabilistic safety assessment; (8) operational safety; (9) management and control; (10) operational documentation; (11) human factors; (12) experience feedback from other plants of similar design and scientific researches; (13) emergency preparedness; and (14) environment impacts. One of the important results from PSR will be NPP modification program that includes measures which are necessary for compliance with more modern regulatory requirements and international good practices; and aging management measures. The measures should be developed taking into account for operating experience, maintenance history, aging, and severe accident analysis. Both deterministic and probabilistic approaches should be properly combined to achieve a more balanced modification program.

Probabilistic safety analyses (PSA) have become an important part of PSR. From one hand, during PSR should be determined to what extent the existing PSA remains valid as a representative model of the plant when the following aspects have been taken into account:

changes in the design and operation of the plant; new technical information; current methods; and new operational data. From other hand, according to the extent of PSA (i.e., completeness), PSAs can be used to evaluate proposed (under PSR) modifications. It is understood that to keep the PSA as an effective tool, it has to be maintained in a living status in the sense that it should be updated to reflect plant conditions at any given time.

According to regulatory document [2] and guide [3], the first PSRs in Ukraine will be used to support justifications of lifetime extensions for RNPP Units 1 and 2 and SUNPP Unit 1. Currently, there is no international experience (or experience is very limited) in conducting of such type PSR (up-to-now PSRs were applied mostly for recovery of design basis, or for licence renewal). So, it is believed that performing PSRs for older units in Ukraine will provide a good experience and valuable results for justification of lifetime extension and for further development and enhancement of safety not only for Ukraine, but for all countries where lifetime extension issue becomes actual.

2.2 Safety Upgrade Program

In 2005 the Ukrainian Government has approved the Complex Program of the NPP modification and safety improvement, Ref. [4]. The Program includes safety enhancement areas and associated safety measures developed using information on risk from safety analyses, considering qualitative and quantitative outcomes from PSA. The main goal is to further enhance safety of the Ukrainian NPPs to account for enforcements in regulations and best current practices in rational and the most efficient way.

Each safety enhancement area contains a number of safety measures for each type of WWER reactors. PSA informed areas are presented below. In addition to PSA-informed areas, Safety Upgrade Program includes areas identified based on international recommendations/ advanced international experience, deterministic safety analysis etc. Table 1 shows total number of areas / measures for each type of reactors operating in Ukraine.

Table 1 Safety upgrade areas

	SAFETY UPGRADE AREAS								
	Area 1: LOCA from primary to secondary side	Area 2: Dependent and common cause failures	Area 3: Secondary heat removal	Area 4: Pressurized thermal shock	Area 5: Primary heat removal and pressure control	Area 6: Containment reliability	Area 7 : Emergency power supply	Area 8: EOI and emergency preparedness	Area 9: Safety analyses
Basis for area	PSA insights	PSA insights	PSA insights	IAEA recom-mendations	PSA insights	IAEA recom-mendations	PSA insights	IAEA recom-mendations	Regulatory requirements
Number of measures for WWER-440	11	7	5	6	10	5	4	13	5
Number of measures for WWER-1000 “small series”	12	9	3	6	12	4	4	13	5
Number of measures for WWER-1000	10	4	6	7	7	5	6	13	5

Table 1 depicts 9 safety upgrade areas covered in Ref. [4]. The brief description of PSA informed areas is provided below.

2.2.1 PSA informed areas

Area 1 “Medium LOCA from primary to secondary side”. This initiating event is the most complex for control and has a most impact into the CDF (and large release frequency, LRF) values. This is because of IE diagnostics is difficult, emergency control is complicated for personnel, time available for decision making and actions performing is limited with coolant inventory for make-up, probability of steam dump valves (SDV) on affected steam generator (SG) non-closing after opening is high (taking into account for SDVs presence, which are not qualified for operation on a steam-water mixture), and as a consequence containment bypass, irretrievable loss of coolant and radioactive materials release into the environment are possible. Safety issue realization implies the complex of tasks including: (a) preventive measures which decrease the probability of primary to secondary circuit leakage occurrence (use of 100% non-destructive monitoring of SG manifold metal and welded splices, implementation of adequate water-chemical mode, etc) and constrain the leakage rate; (b) organization measures directed on the emergency preparedness by the way of: revision of the emergency procedures aimed on leakage localization within the affected SG, prevention of containment bypass and excluding or minimization of the radioactive release into environment under leakage; and personnel training using the full-scale simulator; (c) plant modifications directed on expansion of safety systems capabilities to overcome given accident and to facilitate the personnel tasks on emergency control.

Area 2 “Dependent and common cause failures”**.** Measures of this area are directed on reducing multiple malfunctions of equipment due to dependent failures and common cause, such as: (a) spatial interactions (steaming, spraying, piping whip, steam and water jet impingement) resulted from high energy line breaks; (b) internal flooding and fires; (c) blasted insulation due to LOCA inside containment.

Area 3 “Secondary heat removal”**.** For this safety function the following safety deficiencies were identified: (a) SDVs availability is not ensured under the steam-water mixture outflow; (b) some of existing components may be used only for limited number of accident modes, that significantly decrease redundancy and consequently the safety function reliability. Safety analyses showed, for example, that for ensuring SG feeding from the auxiliary feedwater pumps the intersystem dependencies are not balanced and have not enough redundancy.

Area 5 “Primary heat removal and pressure control”. This area is directed on implementation of primary heat removal in feed and bleed mode. This method is well known and effective mode which applies to prevent the reactor core damage under emergency situations. List of measures includes: changes in systems design and construction, modifications of operational and emergency procedures. List of modified systems includes pressurizer pilot operated relief valves, high pressure and low pressure injection systems, instrumentation and control.

Area 7 “Emergency power supply”**.** Measures under this area are associated with total station blackout. Under total blackout core damage will occur in few hours. If the external grid is restored during this time interval, the potential exists to prevent the core damage, if the NPP will be timely switched on to the restored grid. Availability of batteries is the important condition for providing that after external power supply recovery the front-line systems may be powered. In a case of batteries complete exhausting, switching on to the external grid becomes more complicated, while this possibility still remains under condition if batteries of open switchyard are available.

2.2.2 Safety areas ranking

It was decided that implementation of safety measures will be performed by step-by-step procedure, taking into account their safety efficiency. Currently, the Utility activities in this field are directed on prioritisation of safety measures and areas using probabilistic safety assessments. Brief description of risk-informed techniques in decision making process is provided in Section 3.

Regulatory guide (Ref. [5]) establishes methods for prioritization, qualitative and quantitative ranking criteria, as well as, requirements for PSA technical quality for such application. Quantitative ranking criteria according to regulatory guideline are shown on Table 2.

Table 2 Ranking criteria for safety measures/issues

Category name	**Criterion,** ΔCDF_i **1/year**	**Criterion,** ΔLRF_i **1/year**
Category 0: Insignificant influence on the NPP safety level.	<1E-07	<1E-08
Category I: Low influence (importance) on the plant safety	<1E-06	<1E-07
Category II: Medium influence (importance) on the plant safety	<1E-5	<1E-6
Category III: High influence (importance) on the plant safety	<1E-4	<1E-5
Category IV: Very high influence (importance) on the plant safety	>1E-04	>1E-05

Prioritisation of safety areas/measures for new units (KhNPP Unit 2 and RNPP Unit 4) is near completion, while for ZNPP Unit 5, SUNPP Unit 1 and RNPP Unit 1 prioritization process is underway. Preliminary ranking of the safety areas for different reactors, and change in CDF, based on probabilistic analyses, are shown in Table 3.

Table 3 Preliminary ranking of the safety upgrade areas

Safety area	**WWER-1000/302**		**WWER-1000/320**	
	Rank	**Potential to CDF decrease,** ΔCDF_i	**Rank**	**Potential to CDF decrease,** ΔCDF_i
Area 1 "LOCA from primary to secondary side"	III	2.4E-05	III	2.2E-05
Area 2a "Dependent and common cause failures - ECCS sump issue"	II	7.5E-06	II	2.9E-06
Area 2b "Dependent and common cause failures - Control systems issue"	I	2.5E-07	I	2.5E-07

Safety area	WWER-1000/302		WWER-1000/320	
	Rank	Potential to CDF decrease, ΔCDF_i	Rank	Potential to CDF decrease, ΔCDF_i
Area 2c "Dependent and common cause failures - Spatial interactions issue"	III	3.2E-05	II	2.4E-06
Area 3 “Secondary heat removal"	II	3.6E-06	II	6.8E-06
Area 4 "Cold overpressure"	I	1.0E-07	II	4.6E-06
Area 5 “Primary heat removal and pressure control	II	3.6E-06	II	2.6E-06
Area 6 "Containment reliability"	II	N/A	II	N/A
Area 7 “Emergency power supply	I	4.2E-07	II	9.6E-06
Area 8 "EOI and emergency preparedness"	III	1.0E-05	III	4.0E-05
Area 9 "Safety Analyses"	N/A	N/A	N/A	N/A

Figure 1 illustrates tentative decrease in total CDF as result of fulfilment of measures under safety upgrade program.

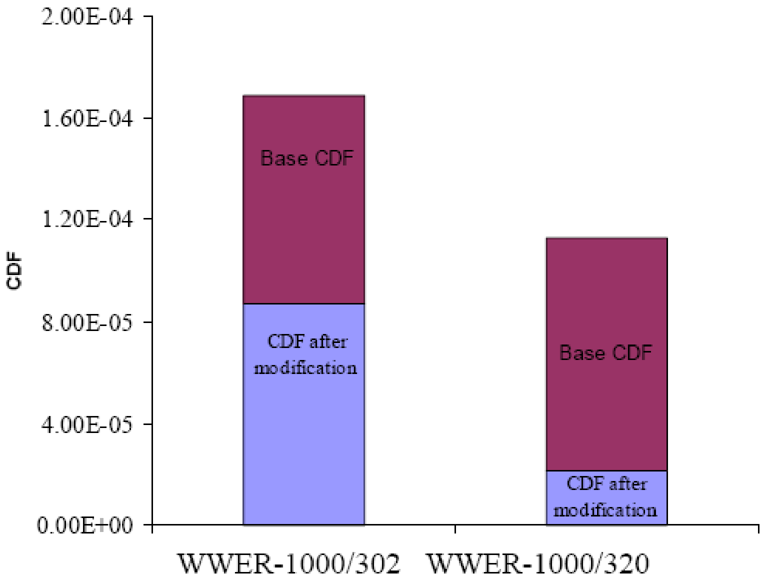


Figure 1 CDF due to realization of safety upgrade program

Industry activities on realization of safety upgrade program and continuous enhancement of operational safety will further decrease CDF estimates.

3 RISK-INFORMED TECHNIQUES IN DECISION MAKING PROCESS (RIDM)

To ensure that NPPs are both safe and economically competitive, the Utility and Regulatory Authority take efforts on implementation of risk-informed techniques in decision making process. Activities on RIDM are covered by Policy decisions, Ref. [6], and Implementation Plan, that was approved by Utility and Regulatory Authority in 2003. Adopted approach allows increasing safety by more effective use of efforts and means for elimination of safety deficiencies; increase regulatory efficiency; and reduce licensee undue burden while maintaining required safety level

It was found that balanced use of PSA technique and methods to improve NPP safety jointly with the deterministic approaches supports making of well-founded regulatory decisions on NPP safety. However, whether risk informed regulation is of benefit to Utilities depends to a large extent on the common understanding developed with the Regulatory Authorities. Since PSA development imposes a considerable burden, in terms of the human and financial resources that need to be expended, it is very important to clearly define what is expected from the Utility and how the results will be used. The counter parties try to develop common understanding through wide discussion of RIDM and development of a suitable regulatory framework. To achieve common understanding, a discussion framework was established through interagency coordination board. The board is advisory organ on RIDM for both Regulatory Authority and Utility. The coordination board consists of senior engineers and managers representing Regulatory authority and their technical support organizations, the Utility, NPPs and design organizations. Place of the board in organizational structure is illustrated on Figure 2.

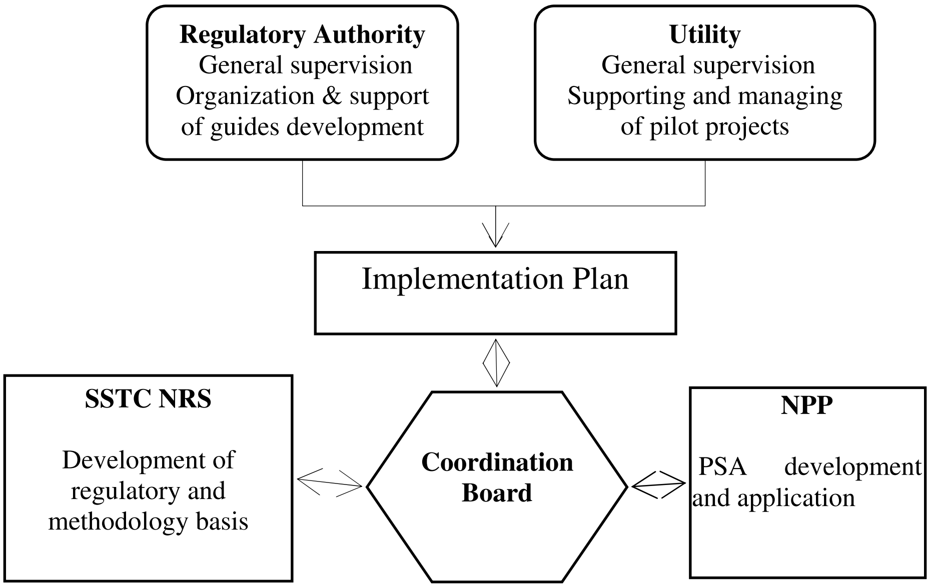


Figure 2**:** RIDM Organizational structure

The following responsibilities are imposed to the coordination board: General organizational oversight and coordination of works envisaged by the Implementation Plan; wide discussion and development of recommendations in order to: (a) resolve actual technical issues; (b) form a common industry policy in the area of RIDM; (c) analysis and evaluation of experience, updating of plans and schedules, upgrading the Implementation Plan. The first results of coordination board meetings have involved wide discussion and approval of general regulatory document on risk-informed regulation, see [7]; introduction of new projects on PSA application; rescheduling of pilot projects, etc.

Top level regulatory document, [1] numerically defines the safety goals (core damage frequency and large release frequency) for operating and future NPPs. Based on these targets, general regulatory document, Ref. [7] proposes risk acceptance criteria for RIDM. The criteria are stated in terms of risk metric (CDF; LRF) and change in risk metric due to plant upgrade. Depending on relation between base risk metric and change in risk metric, regulatory body makes decision on allowance of plant upgrading and necessity for compensatory measures. For example, if base CDF is less than 1.0E-04, the plant upgrade can be permitted, on conditions that: change in CDF is small; no degradation of defence in depth; and compensatory measures are considered. In the RIDM context, the criteria of [4] should be interpreted as targets. They are intended to provide an indication, in numerical terms, of proposed changes acceptability. Criteria are intended for comparison with a full scope (including internal and external events, full power, low power and shutdown) assessment of the risk metric. Illustration of criteria is shown on Figure 3.

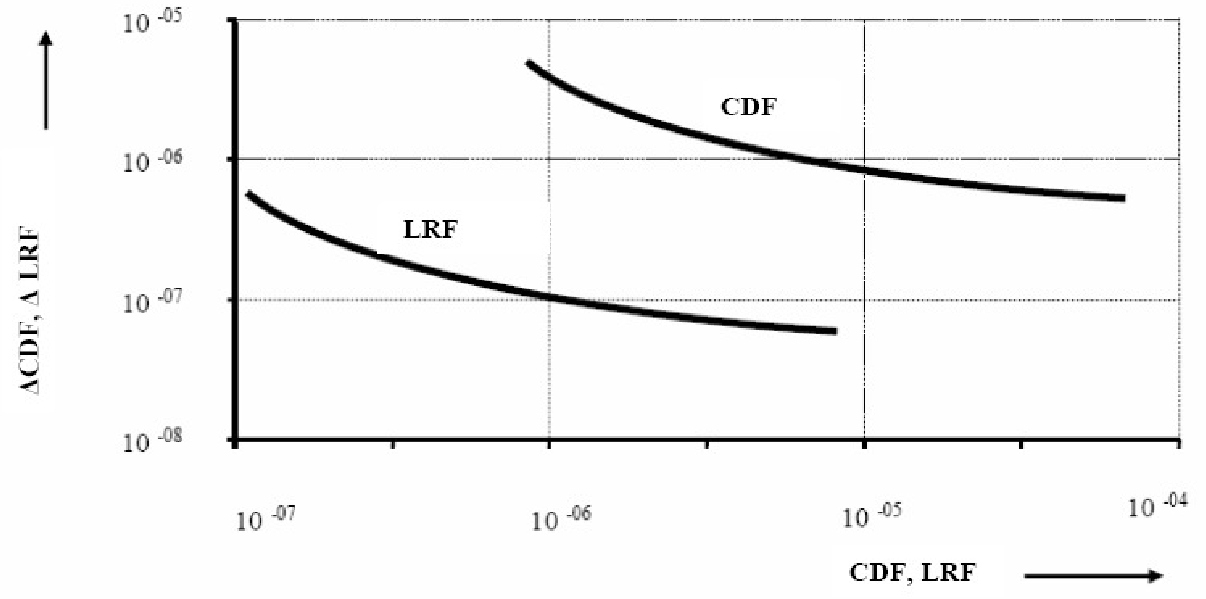


Figure 3: Risk Acceptance criteria

The plant upgrade can be permitted if base CDF and LRF are consistent with the safety goals, on conditions that: changes in CDF and LRF are satisfactory in numerical terms; and compliance with such engineering safety principles is ensured as (a) consistency with the defence in depth philosophy should be maintained; (b) sufficient safety margins should be ensured; (c) impact of plant modification on safety should be monitored; and other.

To ensure PSAs of high quality to support RIDM, from one hand, the Utility involves high-professional engineering support organizations to develop internal guidelines on PSA and prepare full-scope PSA. From other hand, the Regulatory Authority develops regulatory requirements to PSA and PSA applications and provides regulatory review services for associated reports developed by the Utility. Recent regulatory requirements include guideline on Living PSA, guideline on PSA Level 2, guideline on evaluation of safety measure/issues, and other. The development of procedures and technical guidelines assumes using advanced international experience. In this respect, international workshops, forums, etc. are especially valuable as opportunity for transferring to Ukraine the advanced technologies, best regulatory practices and experiences in PRA field.

According to regulatory requirements, PSA used for NPP licensing must be full scope PSA. The Utility undertakes efforts on gradual development of full scope PSAs for each plant through a logical step by step procedure. Three pilot units, which represent three types of WWER reactors (Unit 1 of South Ukraine NPP - WWER-1000 of “small series”, Unit 5 of Zaporizhzha NPP – ‘serial’ WWER-1000 and Unit 1 of Rivne NPP - WWER-440) operating in Ukraine, have developed safety analysis reports with full scope PSA chapters. New units (Unit 2 of KhNPP and Unit 4 of Rivne NPP) also have completed full scope PSAs. PSA for other 10 units in Ukraine will be developed by adaptation of PSA models and documentation from pilot units to non-pilot units of similar design. Scope and degree of adaptation depend on differences in design, construction, procedures, operational practice and experience between NPPs. To a certain extent, adaptation can be considered as harmonization of PSA. Expected results of this process will be estimated level of overall safety for each power unit in such way, that the differences in PSA results can by explained only by differences between units, not by differences in PSA teams, methods and approaches.

To realize adaptation procedure in justifiable and consistent way, a standardized approach was developed, which was approved by SNRCU and Utility in 2007.

Based on established infrastructure for PSA application, the Utility and Regulatory Authority proceed now with practical use of PSA and PSA applications. Ongoing activities in this field are associated with:

(a) evaluation and prioritization of safety areas/ safety upgrade measures (all NPPs);

(b) optimization of test, maintenance and repair procedures (e.g. SUNPP Unit 1, ZNPP Unit 5);

(c) using PSA together with full scope simulator trainings to improve operator training programs and enhance human reliability, and to evaluate and improve emergency operating procedures (e.g., SUNPP Unit 1); Main insights show that integral evaluation of accident progressions provides important information on the benefits and drawbacks of various operations in abnormal plant states; and there is significant potential for safety increase due to improvement of EOP and more efficient use of full scope simulator at NPP.

(d) introduce compensatory measures to decrease safety deficiencies (e.g. for turbine hall issue at RNPP Units 1 and 2).

Further industry activities on RIDM are connected with risk-informed in-service inspection; prioritization of regulatory inspections; precursor analysis, etc.

4 CONCLUSIONS

Permanent safety improvement activities at Ukrainian NPPs provide considerable enhancement of safety level. However, potentials for safety increase are not exhausted. Ukrainian Nuclear Regulatory Authorities and Utility promote use of PSA and PSA application as advanced tools that complement traditional methods and facilitate decision making on the safety. Enhancing safety and efficiency of NPP operation is especially important for Ukraine, with 50% share of nuclear power in total energy production. Pilot PSA applications have demonstrated their efficiency for regulatory tasks and for Utility. There is a need in further strengthening the regulatory framework and technical basis for practical use of RIDM.

REFERENCES

[1] General Provisions of Safety, NP306.2.141-2008, Kiev (2008).

[2] General requirements on extension of lifetime of NPPs by results of periodic safety review», NP 306.2.099-2004, Kiev (2004)

[3] “Requirement to content and structure of report on periodic safety review of operating NPPs”, PL-D.0.08.388-06

[4] ENERGOATOM, State Nuclear Regulatory Committee of Ukraine, “Complex Program of the NPP Units Modification and Safety Improvement”, Kyiv, (2006).

[5] State Nuclear Regulatory Committee of Ukraine “Requirements on using probabilistic methods for prioritezation of safety issues”, Revision 1, Kyiv (2008).

[6] State Nuclear Regulatory Committee of Ukraine, Decision of the Board of State Nuclear Regulatory Committee of Ukraine, № 9 , «Implementation of risk assessments in regulation of nuclear facilities safety», Kyiv (2001).

[7] G. Gromov, I. Lola, O. Sevbo, “General regulatory document on risk-informed regulation”, Kyiv (2004).

TOPSAFE
Dubrovnik, Croatia, 30.09 - 3.10.2008

Exploitation of BEPU Approach for Licensing Purposes

C. Camargo, R. Galetti,
C/O Prof. F. D'Auria - University of Pisa
Via Diotisalvi, 2 56123 Pisa, Italy
camargo@cnen.gov.br, regina@cnen.gov.br

F. D'Auria,
University of Pisa
Via Diotisalvi, 2 56123 Pisa, Italy
dauria@ing.unipi.it

O. Mazzantini
NA-SA
Arribenos 3610 C1429BKQ – Ciudad de Buenos Aires, Argentina
oscarmazzantini@arnet.com.ar

ABSTRACT

Best estimate codes supplemented by uncertainty evaluation (i.e. BEPU = Best Estimate Plus Uncertainty) achieved a suitable maturity and can be applied to the licensing process of water cooled nuclear power plants. The Final Safety Analysis Report (FSAR) constitutes the key element for demonstrating the safety of a nuclear power plant. Thus BEPU approach is relevant to the FSAR.

The present paper deals with a proposal to apply a BEPU approach to the FSAR of Atucha-2 PHWR (Pressurized Heavy Water Reactor) now in construction in Argentina with operation start expected in 2010. Atucha-2 is a vessel type two loop KWU-Siemens-AREVA plant with vertical core channels and hydraulically separated moderator and coolant circuits.

The following key aspects are at the basis of the possible application of the BEPU approach in the Atucha-2 licensing process:

- The accident classification: the standard distinction between Anticipated Operational Occurrences, Design Basis Accident and Beyond Design Basis Accident is considered. However, different assumptions are proposed for the analysis of selected transients belonging to individual classes.
- Conservatism is embedded into the reactor design including protection system and related set-points; furthermore, conservatism can be added in the analyses through the proper choice of boundary and initial conditions or by (typically) preventing redundant trains of emergency core cooling systems (ECCS) from contributing in recovering the plant safety functions.
- A best estimate analysis of phenomena expected in the concerned class of transients implies the coupled application of system thermal-hydraulics, computational fluid dynamics and three-dimensional neutron kinetics computational tools other than structural mechanics codes. The demonstration of suitable qualification for the computational tools constitutes a challenge for the present approach.

1 INTRODUCTION

The Atucha-2 nuclear power plant is designed to produce 745 MW of electrical power, with a pressurized heavy water cooled and moderated reactor (PHWR). The Atucha-2 Construction License was issued in July 1981, upon a previously submitted Preliminary Safety Analysis Report (PSAR) [1], basically fulfilling the requirements on Safety Analysis Reports, established by IAEA standard [2], although its format has been prepared in accordance with a largely adopted US standard [3].

Consistent with the fundamental radiation protection objective, the Argentinean regulatory standard AR 3.1.3 [4] establishes a criterion which provides an upper limit for the radiological impact for nuclear power plant operation (restriction of radioactive releases), including the consideration of the complete spectrum of accidents and the correspondent probabilities of occurrences. Additionally, this standard requires a probabilistic safety analysis to support the acceptability of the design of a nuclear power plant.

During the period between 1977 and 1994, significant progresses have been observed in the activities of design finalization, components fabrication and of the erection of structures and buildings. The established licensing compromises have been strictly observed and are embedded in the Atucha-2 safety design concept.

Despite the fact that the licensing procedure in Argentina follows basically a probabilistic approach, a deterministic safety analysis must also be submitted. With the exclusion of the maximum credible accident from the range of the design basis spectrum for Atucha-2, a break size of ten percent on reactor coolant pipe (0.1 A) was recognized [5] as the basis for fulfilling traditional regulatory requirements.

After a long period of delay, a decision was taken to resume the construction, and to bring the plant into operation until the year 2010. Consequently, strong demands have been derived for design finalization, including the issuance of a Final Safety Analysis Report (FSAR). To this aim, a twofold strategy is foreseen: the original safety design philosophy must be preserved, and recent advances in nuclear safety technology should be incorporated, as long as possible.

Significant progress has been observed in areas of the nuclear safety field, in the last twenty years. Many of them are related to improvements in the ability to predict plant behavior during normal and accident conditions. Evolution of analytical models, supported by comprehensive experimental efforts made available powerful computational tools which provide support for detailed calculation on relevant phenomena for nuclear reactor dynamics.

Within the framework of Atucha-2 project finalization, NA-SA (Nucleoeléctrica Argentina Sociedad Anónima) and Unipi (University of Pisa) have signed an agreement for supporting activities in the area of deterministic safety analysis methods. Separate efforts are also undertaken in the area of probabilistic safety analysis, which are, however, out of the scope of this paper.

Derived from the connected probabilistic approach, the double ended guillotine break is considered as a beyond design basis scenario. Nevertheless, the demonstration of the design capability to overcome this event has still a relevant role in the safety performance evaluation. For this aim, however, currently used conservative approach for safety analysis may not be sufficient to guarantee that safety margins still exist. Quantification of available safety margins seems to be an adequate strategy.

2 OBJECTIVE AND SCOPE

This paper aims at to describe a comprehensive and modern methodology proposed for performing the deterministic safety analysis to be included in the chapter 15 of the Atucha-2 Final Safety Analysis Report. Such analyses provide the basis to determine the plant limiting conditions for operation, limiting safety system settings, and design specifications for safety-related components and systems, as well as the deterministic technical basis for the demonstration of the existence of adequate protection of public health and safety.

The proposal has been developed starting from the original SIEMENS methodology planned to be used for accident analysis [6], but further enhanced to comprise the use of modern best estimate computer codes and methods, including evaluation of uncertainty in the calculated results (Best Estimate plus Uncertainties or BEPU approach). It follows well established safety practices, but also includes some advanced solutions compatible with the state of the art in the field of nuclear reactor safety.

The proposed approach has been built to cover the design basis spectrum of events, but it was intentionally extended to address additional safety relevant events beyond design basis, including the double-ended guillotine break (DEGB) loss of coolant accident (LOCA).

The acceptance criteria adopted for these analyses are of deterministic nature, even for radiological consequences associated to the events.

The application of the proposed methodology does not include, however, the analysis of severe accidents, by recognizing the complementary role of probabilistic safety analysis and by understanding that related issues are to be addressed by an independently and separately performed study under NA-SA responsibility.

3. PROPOSED BEPU APPROACH

The event sequences postulated in the design of the plant are analyzed to demonstrate that in operational states, on the occurrence of a design basis accident and, to the extent practicable, on the occurrence of some selected accident conditions that are beyond the design basis accidents, the following three fundamental safety functions are performed:

- Safe shutdown and long term subcriticality
- Residual heat removal
- Limitation of radioactive releases.

The proposal follows well accepted design philosophy for nuclear power plants, which recognizes the principle that plant states which could result in high radiation doses or radioactive releases are of very low probability of occurrence, and plant states with significant probability of occurrence have only minor or no radiological consequences. Postulated initiating events (PIE) are grouped according to their anticipated probability of occurrence in anticipated operational occurrences (AOO), design basis accidents or selected beyond design basis accidents (SBDBA).

The third event category is proposed to address specific scenarios beyond design basis, including DEGB LOCA and ATWS. Accident conditions which stand out of these ranges of probabilities should be treated separately, through the probabilistic safety analysis.

The approach takes credit of the concept of evaluation model (EM), and comprising three separate possible modules depending on the application purposes:

- For the performance of safety system countermeasures (EM/SA)
- For the evaluation of radiological consequences (EM/RA)
- For the review of components structural design loadings (EM/CA).

All selected scenarios are grouped in a classical nine families of events, already established within the scope of the PSAR, where each family covers events with similar phenomena.

For the FSAR Chapter 15 analyses, and for each category of events, the results of the analyses will be assessed in terms of the fulfilment of safety functions which are graded according to the expected frequencies of occurrences for the correspondent PIE.

To keep a consistently flat risk profile over the entire spectrum of AOO and DBA, the more frequent the event is, the less tolerable its consequences are. In this sense, acceptance criteria are selected for different event categories, for safety parameters as fuel and cladding temperatures, departure from nucleate boiling ratio (DNBR), primary circuit pressure, containment pressures, and total effective dose equivalent (TEDE).

To start analyzing typical events scenarios for the chapter 15 of an FSAR, evaluation models rely mostly on system thermal hydraulic codes (as for EM/SA) to solve the transport of fluid mass, momentum and energy throughout the reactor coolant systems. The extent and complexity of the physical modes needed to simulated plant behavior are strongly dependent of the reactor design and of the transient itself.

For some scenarios, or regarding some analysis purposes, the system thermal hydraulic code may, for example, be complemented by (or coupled with) a three-dimensional neutron kinetics code or the reference model may need an expansion to include a detailed simulation of controls and limitation systems which play a relevant role for determining the plant response.

For the scope of the proposed approach for accident analyses, the complexity of the evaluation model may range from a simplified qualitative evaluation (EM/QA) to a complete combination of the three possible modules (EM/SA + EM/RA + EM/CA).

Additionally to the computers codes and the selection of modelling options, the established procedures for treating the input and output information are also recognized as comprising key parts of the evaluation model. The adopted procedures to select initial and boundary conditions, which follows the original design safety philosophy, are of particular importance for supporting the regulatory acceptability of the results provided by the EM.

As the foreseen use of this EM is for licensing purposes, it is necessary to evaluate the suitability of conservative assumptions or to adopt best estimate approaches with the quantification of uncertainties.

Suitability of conservatism should be understood as addressing the issue of “how conservative is conservative enough”. Alternatively, when a best estimate approach is adopted, then realistic assumptions will be input to best estimate models, conducting to realistic estimates for plant behavior. In these cases, licensing applications demand the quantification of uncertainties in the calculated results to ensure that safety margins are still available. For the scenarios were the conservative assumptions may provide enough safety margins, the proposal includes a criterion to determine the need for uncertainty calculations. Typically, SBDBA will involve quantification of uncertainties. It is a relevant part of the proposed approach for accident analyses, the application of a comprehensive method for estimate uncertainties.

The figure 1 shows a simplified flowchart with the steps followed by the proposed approach.

Starting from the selection of the event to be analyzed, after establishing the purposes for the analysis, EM requirements are derived from the identification of event-related phenomena.

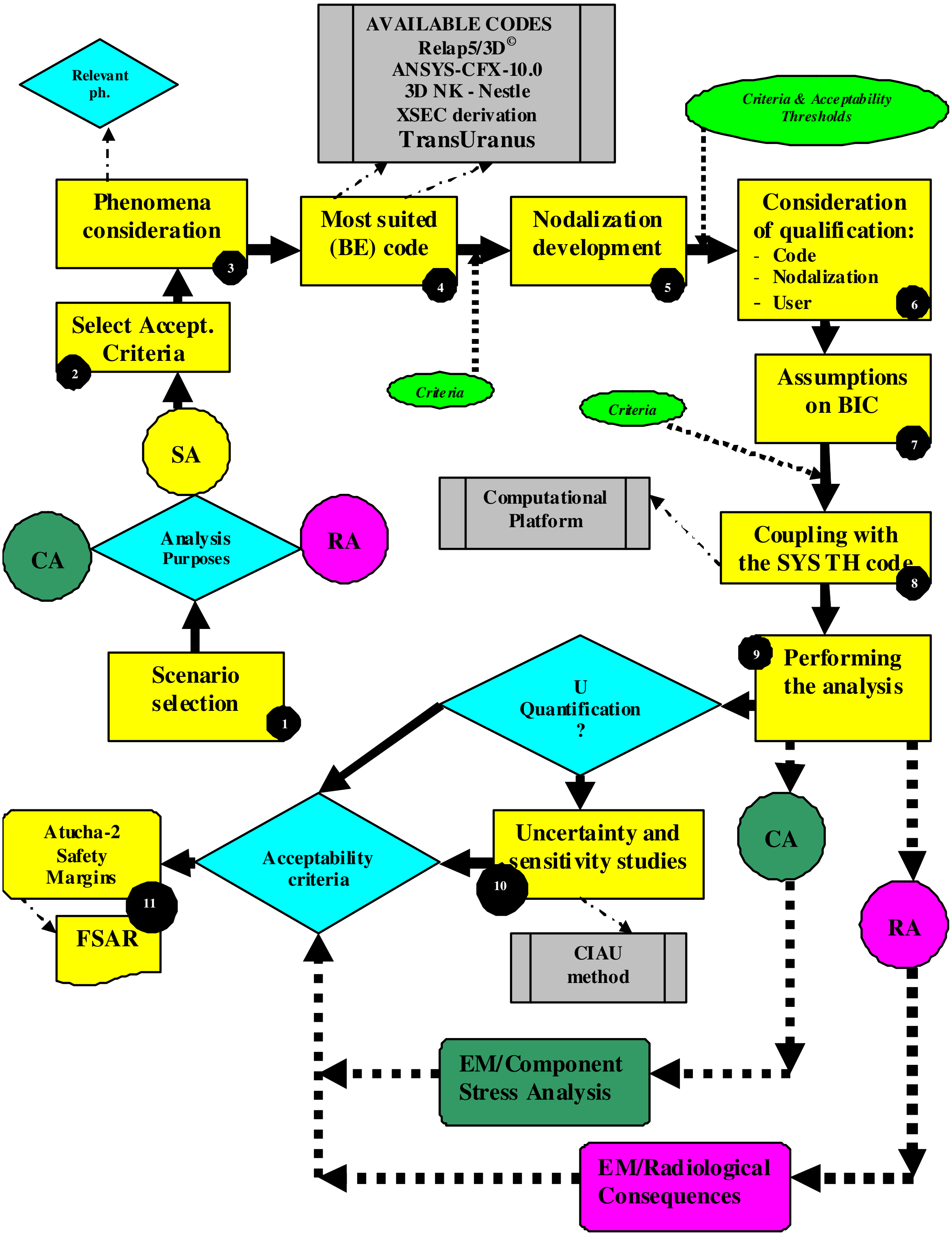


Figure 1: Simplified flowchart for the proposed BEPU approach to be applied for Atucha 2 accident analysis

The two main aspects which have been considered for developing the evaluation model with the ability of adequately predict plant response to postulated initiating events are intrinsic plant features and event-related phenomena characteristics.

For the two modules EM/SA and EM/CA, the first set of requirements for the evaluation model is imposed by the design characteristics of the nuclear power plant, its systems and components. Requirements on the capability of simulating automatic systems are of particularly importance for anticipated operational occurrences, in which control and limitation systems play a key role on the dynamic response of the plant. For evaluation of radiological consequences, the EM/RA module has demanded additional appropriate site-related features to be built in.

The third set of requirements is derived from the expected evolution of the main plant process variables and the associated physical phenomena. For the proposed approach, this is performed through the process of identifying the Phenomenological Windows (PhW) and the Relevant Thermal-hydraulic Aspects (RTA). The relevant timeframe for the event is divided into well defined intervals when the behaviour of relevant safety parameters is representative of the physical phenomena.

For the adequate simulation of the identified phenomena, computational tools were selected from those which have previous qualification using an appropriate experimental data base. Satisfactory qualification targets provide basis for acceptability of the postulated application.

For the proposed approach, with the full scope of application of best estimate plus uncertainty quantification (BEPU), a pre-requisite is the availability or the support of the most advanced-qualified computational tools. This comprises a key feature of the proposed approach: all computer codes which have been selected are the best codes available in the market.

For most event scenarios, the single purpose evaluation model EM/SA may be necessary and sufficient to be developed. In this sense, the availability and the application of qualified system thermal-hydraulic code (SYS TH) and reliable uncertainty methodology (UM) should be the minimum requirement.

Additionally, depending on the specific event scenario and on the purpose of the analysis, it is necessary the availability of calculational methods that are not embedded in the SYS TH code, as for burst temperature, burst strain and flow blockage calculations. This may imply an evaluation model EM/CA composed by a fuel rod thermal-mechanical computer code.

For the present proposal, the first selected computational tool would usually comprise a qualified SYS TH code with proven availability of models capable of simulating each individual phenomenon expected to occur during the safety relevant scenarios.

The second selected computational tool, for a minimum requirement scope, is an uncertainty methodology (UM) tool that has been qualified by a comprehensive regulatory body peer review process and by international scrutiny evaluation through participation on projects like OECD/NEA/CSNI Uncertainty Methodology Study [7] and BEMUSE [8-10].

For some specific event scenarios, model requirements derived from identified phenomena may demand for the use of computational tools that have capabilities not available to system code and that allow the 'best' simulation of the phenomena expected to be relevant for the safety demonstration of the concerned system.

Two typologies of codes are used as support for application in some accident scenarios. Geometric complexities of the Atucha-2 primary system and three-dimensional mixing phenomena within the reactor vessel play relevant role in the safety performance. In this sense, selected set of codes may involve a coupled SYS TH code with 3 dimensional neutronic capabilities or a coupled use of computational fluid dynamics tool. In the present case, the local (three-dimensional in nature) effects principally of channel voiding and of boron upon the reactivity justify the use of coupled techniques. Currently, qualification of CFD codes is a very active field (see e.g. [17,18,19]). When it comes to licensing, CFD codes are used mainly as supporting tools (e.g. [16]). Recent works draw attention to quality assurance in CFD applications for reactor safety analysis ("Best Practice Guidelines", [20]).

Qualified code and qualified uncertainty method imply qualified interfaces between the code and the simulated systems (this is called nodalization in the case of thermal-hydraulic system code) and qualified group of users, where:

- Qualified code-input data set or nodalization implies fulfilment of qualitative and quantitative acceptance criteria, separating nodalization development, achievement of steady state and transient analysis.
- Qualified group of code users should be available for the selected SYS-TH code. This implies the documented consideration of recommendations included in internationally agreed documents, e.g. references [11] to [13].
- Qualified UM input data set and UM users. Although internationally recognized as an open issue, (e.g. as discussed in ref. [10]), and with main concern being regarding the identification the input uncertain parameters and their range of variation, for the present approach this problem is not applicable, as an internal assessment of uncertainty capability is available.

4. ASSUMED BOUNDARY AND INITIAL CONDITIONS

To build a complete and detailed EM for a particular plant and event, properly selected code options, boundary conditions, and temporal and spatial relationships among the component devices, code input specific data set are derived.

The strategy for the analyses follows the original design safety approach [6]. Plant behavior is investigated under design basis specific predetermined operational states and accident conditions, as well as for some selected beyond design basis conditions, applying a specific set of rules to provide enough insurance (as per regulatory requirements) on design adequacy.

Basically, for each event to be analyzed two complementary scenarios are investigated:

A. Realistic Case – in a first step, the realistic sequence of events is calculated under normal (best estimate) conditions for which all systems which did not fail as a consequence of the postulated initiating event are assumed to be available. Additional failure assumptions in case of normal conditions are not postulated.

B. Conservative Case - Regarding the fact that additional failures are conceivable or have to be postulated according regulations, in addition to the normal case, and as a second step of calculations, a conservative case of each respective event is also analyzed.

As a general assumption for conservative cases of accidents, it is assumed that, beyond the postulated situation of a subsystem being repaired, when a safety system is needed, there will be a single failure (random failure) in one of the safety devices.

Failure assumptions for control, limitation and reactor trip are also postulated to achieve a sufficient level of conservatism in the analysis of AOO and DBA.

The evaluation of these conservative cases shall demonstrate that measures of reactor protection system and safety grade systems are available (n+2 prove) for event control and for the successful performance of the correspondent subsidiary safety functions.

The realistic case calculations are performed to demonstrate that anticipated operational occurrences will not escalate into accident conditions and that, as a rule, there is no need for safety-grade system to operate. Reactor trip is possible, and even necessary, in some cases.

For the proposed approach, the analyses of the events are performed, both the realistic and the conservative cases, starting from the same set of nominal parameter values (e.g. temperature, pressures) corresponding to that power level for which the analyses are performed. For example, some reactivity transients are analyzed for 0% power level, although most of the cases are analyzed for 100% power level. Deviations of the plant parameters from their rated setpoints are, in general, not considered.

For AOO with postulated additional failures, an escalation into an accident condition is also conceivable under certain circumstances (such as the coincident failure of the reactor power limitation system and a control system). Analyses of AOO for conservative conditions are conducted to demonstrate that, despite additional system failures, the next level of acceptance criteria (that means for DBA) is met due to the action of safety systems (reactor protection system, engineered safety features).

By contrast, for design basis accidents, the realistic case is calculated only to show the expected behavior of the plant, with all safety systems countermeasures providing enough margins to the applicable acceptance criteria. In the conservative case, it is necessary to demonstrate the effectiveness of the safety system, with credit taken only for those systems or system redundancies which may deterministically be taken as available for mitigation of the consequences of the event.

For beyond design basis accidents, measures are foreseen to mitigate their consequences. These measures are introduced under consideration of achieving a reasonable balance between the engineering effort and its achievable risk reduction. They are event specific actions using design margins of the plant.

Anticipated transients without scram (ATWS) are analyzed only for the normal case, which means best estimate conditions, to demonstrate that due to common acting of all available systems using thereby design reserves of the plant, the subsidiary safety functions of heat removal and long term subcriticality of the reactor are ensured.

For extended spectrum of LOCA recognized as SBDBA, or extremely low probability scenarios, only best estimate cases are evaluated. As additional system failures are not required to be postulated, to quantify the available safety margins, regarding the same acceptance criteria as for DBA, involved evaluation model uncertainties are quantified.

For extended spectrum of loss of coolant accidents (from 0.1 to 2A break sizes), the use of a systematic approach which quantifies the uncertainty (BEPU) supports the demonstration of the existence of margins to the safety limits of the activity barriers.

5. UNCERTAINTY QUANTIFICATION – CRITERIA AND METHOD

In principle, whenever a best estimate method is applied for licensing purposes, uncertainty quantification is needed. For the present proposal, as a realistic conservative approach, it should include uncertainty quantification. Nevertheless, due to the conservatism embedded in some assumptions, and due to efficient safety performance of limitation and protection systems, in many cases there is no real need for such calculations. The proposed BEPU approach derived a non-safety related criterion to decide upon the need for performing uncertainty calculation. Whenever the safety parameter, as calculated by the evaluation model, comes within an established range or distance from the limit value, the uncertainty in the calculated results is quantified (BEPU). For any case, however, such calculation may be performed, and specific additional demands from the regulator may be fully addressed.

The application of acceptance criteria is also addressed for SBDBA, but with the need to determine the available safety margins, the uncertainties are always quantified.

For the proposed methodology, all events in the category SBDBA and some events in the DBA category will be analyzed with the full scope of the BEPU approach.

This is particularly valid for the evaluation model module developed for performing safety systems analyses (EM/SA). Usually, radiological consequences and component stress analyses follow well established conservative and deterministic procedures. In this sense, the correspondent evaluation modules (EM/RA and EM/CA), in principle, will not include uncertainty methods.

For the EM/SA, however, uncertainty analyses are performed to confirm that the combined code and application uncertainty is less than the design margin for the safety parameter of interest when the code is used in a licensing calculation. Examples of safety parameters are peak cladding temperature (PCT), cladding oxidation thickness and departure from nucleate boiling ratio (DNBR).

The internal assessment of uncertainty is a relevant capability for thermal-hydraulic system codes. This consists of the possibility of obtaining proper uncertainty bands each time a nuclear power plant scenario is calculated. At the basis of the derivation of the code with (the capability of) internal assessment of uncertainty (CIAU), there is the uncertainty methodology based on the accuracy extrapolation (UMAE), although other uncertainty methodologies can be used for the same purpose.

The UMAE method [14] focuses not on the evaluation of individual parameter uncertainties but on the propagation of errors from a suitable database calculating the final uncertainty by extrapolating the accuracy from relevant integral experiments to full scale NPP.

The basic idea of the CIAU [15] can be summarized in two parts, as per Figure 2:

- Consideration of plant status: each status is characterized by the value of six relevant quantities (i.e. a hypercube) and by the value of the time since the transient start.
- Association of an uncertainty to each plant status.

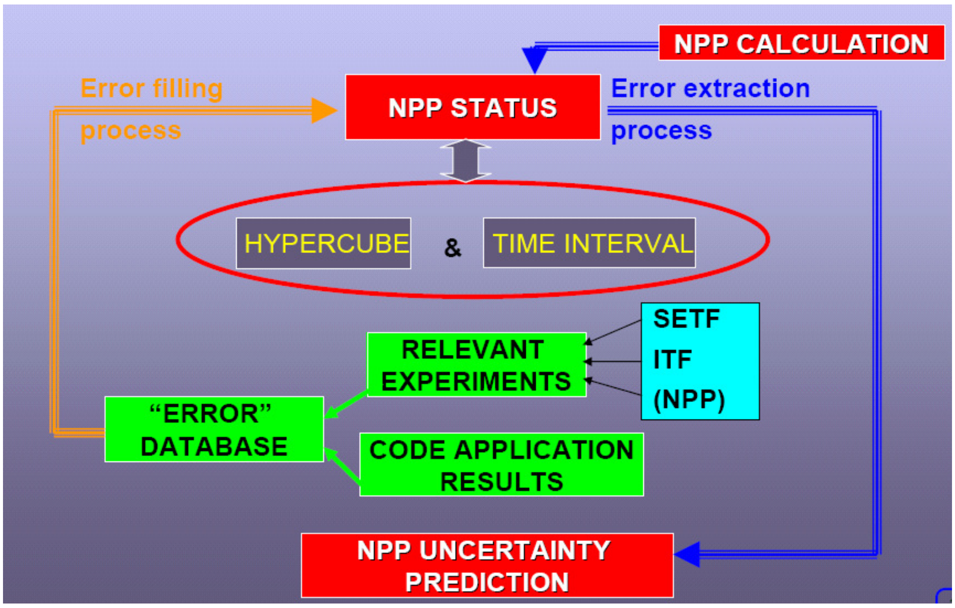


Figure 2. – Outline of the basic idea of the CIAU method.

In the case of a PWR the six quantities are: 1) the upper plenum pressure, 2) the primary loop mass inventory, 3) the steam generator pressure, 4) the cladding surface temperature at

2/3 of core active length, 5) the core power, and 6) the steam generator down-comer collapsed liquid level. These quantities are also considered in the large break LOCA analysis of Atucha-2 [21], a PHWR.

A hypercube and a time interval characterize a unique plant status to the aim of uncertainty evaluation. All plant statuses are characterized by a matrix of hypercubes and by a vector of time intervals. Let us define Y as a generic thermal-hydraulic code output plotted versus time. Each point of the curve is affected by a quantity uncertainty (Uq) and by a time uncertainty (Ut). Owing to the uncertainty, each point may take any value within the rectangle identified by the quantity and the time uncertainty. The value of uncertainty, corresponding to each edge of the rectangle, can be defined in probabilistic terms.

The idea at the basis of CIAU can be made more specific as follows: the uncertainty in code prediction is the same for each plant status. A Quantity Uncertainty Matrix (QUM) and a Time Uncertainty Vector (TUV) can be set up including values of Uq and Ut derived by an uncertainty methodology.

REFERENCES

[1] Atucha-2 Preliminary Safety Analysis Report (1981).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY Safety Guide N^{o}50 SG-G2, withdrawn.

[3] USNRC Regulatory Guide 1.70: “Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants LWR Edition”, Revision 3 (November 1978).

[4] CNEA/KWU Protocol of Understanding (November 1977).

[5] Reunion de Directorios entre NA-SA y ARN, celebrada el dia 18 de septiembre de 2007 (Meeting between Argentinean Nuclear Regulatory Body and utility NA-SA, dated September 18 2007).

[6] BORDIHN et. al.: Initial and Boundary Condition for Accident Analyses, SIEMENS Work Report KWU NA-T/1995/011, Restricted, Erlangen (24.Feb. 1995).

[7] T. WICKETT (Editor), F. D’Auria, H. Glaeser, E. Chojnacki, C. Lage (Lead Authors), D. Sweet, A.Neil, G.M. Galassi, S. Belsito, M. Ingegneri, P. Gatta, T. Skorek, E. Hofer, M. Kloos, M. Ounsy, J.I. Sanchez – “Report of the Uncertainty Method Study for advanced best estimate thermal-hydraulic code applications”, Vols. I and II OECD/CSNI Report NEA/CSNI R (97) 35, Paris (F) (June 1998).

[8] A. PETRUZZI, F. D'Auria, J-C. Micaelli, A. De Crecy, J. Royen – "The BEMUSE programme (Best-Estimate Methods – Uncertainty and Sensitivity Evaluation)" Int. Meet. on Best-Estimate Methods in Nuclear Installation Safety Analysis (BE-2004) IX, Washington D.C. (US) (Nov. 14-18, 2004), ANS copyright © 2004.

[9] A. PETRUZZI, F. D’Auria, A. De Crecy, et al., “BEMUSE Programme. Phase 2 report (Re-Analysis of the ISP-13 Exercise, post test analysis of the LOFT L2-5 experiment),”

OECD/CSNI Report NEA/CSNI/R(2006)2 (June, 2006), JT03210882, Paris, France, OECD 2006, pages 1–625.

[10] OECD NEA/CSNI – "BEMUSE Phase III Report – Uncertainty and Sensitivity Analysis of the LOFT L2-5 Test", NEA/CSNI/R(2007)4 (May 2007).

[11] S. N. AKSAN, F. D'Auria, H. Staedtke, "User Effects on the Thermal-hydraulic Transient System Codes Calculations". *Nucl. Eng. Des*., 145, 1&2, (1993), OECD/CSNI Report NEA/CSNI R (94) 35, Paris (F) (January 1995).

[12] R. ASHLEY, M. El-Shanawany, F. Eltawila, F. D'Auria, "Good Practices for User Effect Reduction", OECD/CSNI Report NEA/CSNI/R(98)22, Paris (F) (November 1998).

[13] F. D'AURIA – "Proposal for training of thermal-hydraulic system codes users", IAEA Specialist Meeting on User Qualification and User Effects on Accident Analysis for Nuclear Power Plants - Vienna (A) (August 31-September 4 1998).

[14] F. D'AURIA, N. Debrecin, and G.M. Galassi, "Outline of the uncertainty methodology based on accuracy extrapolation," *Nuclear Technology*, vol. 109, no. 1, pp. 21–38 (1994).

[15] F. D'AURIA, W. Giannotti, "Development of a Code with the Capability of Internal Assessment of Uncertainty", Nuclear Technology, Vol. 131, pp 159-196 (2000).

[16] European Commission – Europeaid Cooperation Office, TACIS Project R2.02/02, "Development of safety analysis capabilities for VVER-1000 transients involving spatial variations of coolant properties (temperature or boron concentration at core inlet)", Terms of Reference.

[17] EURATOM 6th FP, NURESIM Integrated Project, Annex I – Description of Work (December 2004).

[18] U. ROHDE et al., FLOMIX-R Project – Final Summary Report, European Commission, 2003.

[19] M. SCHEUERER et al., ECORA Project - Condensed Final Summary Report, European Commission (March 2005).

[20] J. MAHAFFY et al., Best Practice Guidelines for the use of CFD in Nuclear Reactor Safety Applications, NEA/CSNI/R(2007)5 (May 2007).

[21] F. D'AURIA et al.: DEGB LBLOCA (2 x 100% Break in CL) in Atucha-2 NPP, DIMNP NT 628 (08) – rev. 1, March 08.

TOPSAFE
Dubrovnik, Croatia, 30.09 - 3.10.2008

Cultural And Organizational Factors Leading To Major Events

Lorenzo G.A. van Wijk, Richard H. Taylor, John H.R. May
University of Bristol
Department of Civil Engineering, Safety Systems Research Centre
Queen's Building - University Walk, Bristol BS8 1TR, United Kingdom
Lorenzo.van-Wijk@bristol.ac.uk, Richard.Taylor@bristol.ac.uk, J.May@bristol.ac.uk

ABSTRACT

More than ten events from a range of industries (e.g. nuclear, petrochemical, transport) on a worldwide basis, including several recent nuclear events, have now been analysed in detail. The work has allowed common organisational and cultural factors to be identified, from leadership issues to operational cultural issues and the impact of commercial pressures. It is argued that if these are recognised and addressed, the risks of further events might be reduced. These common factors will be presented and discussed in the paper.

In addition, organisational objectives and specific supporting question sets have been generated against the above identified key factors with the intention that operating organisations and regulators can carry out assessments of the vulnerability of organisations to these complex ‘organisational accidents’. The aim of continuing research is to develop a software tool capable of addressing organisational vulnerability. Approaches to structuring such a tool are discussed.

Keywords: organisational safety culture, systems, processes, evidence, risk, vulnerability.

1 INTRODUCTION

Major accidents in the nuclear industry are rare, not least, because significant effort has been spent on designing and operating plant to minimise the risk of such events. Nonetheless, in the last decade there have been several lesser incidents and ‘near-hits’ which provide further learning to continue the process of risk reduction. Some of this learning relates to technical and procedural issues. However, maintaining high levels of safety requires also the understanding of causes involving more deep-seated and complex issues relating to organisational and cultural shortcomings.

The nuclear industry is not alone in having to deal with such issues in order to ensure continuing high levels of safety. Parts of the chemical/petrochemical, transport and civil engineering industries also have to operate to high standards and pay great attention to such issues. There have been several significant events in these sectors over the last decade or so, from which we can collectively learn.

In a previous study carried out as part of an internal BNFL project, five major accidents were studied including one nuclear related event (the JCO criticality accident in Japan in 1999) [1]. The findings on the organisational and cultural causes of these events and some preliminary conclusions attracted interest in the nuclear industry and beyond. Understanding such 'organisational' accidents has also become of growing interest in industry and among regulators following more recent events such as the BP Texas City oil refinery disaster.

The present paper involves a deeper study of ten events (including three of those from the BNFL study). A description of the identified issues is the main subject of this paper. It should be emphasised that in discussing these and other events we have drawn on the findings of reviews and Inquiries. We have attempted to do this in a spirit of learning and it is not our intention to establish blame or to criticise organisations or individuals. In each case, the organisations involved were subject to pressures and difficulties (many of which we attempt to identify).

One important finding of the BNFL study was that when considering organisational and cultural causes, similar issues appear to surface whatever the nature of the event or the industrial sector involved. Such a recurrent and repetitive pattern was again revealed across all the ten events studied in this research. This is important because it provides an opportunity to address such issues generically and to develop tools for diagnosis and action which might provide further opportunities to reduce risks in a wide range of circumstances. This will be relevant to organisations themselves seeking to improve safety, particularity in a nuclear or process safety context but also to regulatory bodies.

A wider discussion of these issues and the development of diagnostic question sets is an important first step. A longer term objective of the current research is to attempt to develop a 'vulnerability tool' which attempts to structure the issues and gain clearer systems insight. The tool to be developed will be rooted in previous work at the Safety System Research Centre (SSRC) in the modelling of complex systems [2]. Also important objective will be to make such a tool. Some preliminary approaches to modelling this are outlined in the final section of this paper.

2 THE FINDINGS FROM TEN EVENTS

To illustrate the relevance of organisational safety culture failings and its implications from a safety point of view, ten events have been studied in some depth. The current work, has used a similar methodology to that described in Taylor and Rycraft [1]. This in turn was broadly based on the approach to such accidents developed by Turner [3], Blockley and Pidgeon [4] and Reason [5]. The ten events studied were:

1) Port of Ramsgate walkway collapse (UK, September 1994) [6];
2) Heathrow Express NATM tunnel collapse during construction (UK, October 1994) [7];
3) Longford gas plant explosion (Australia, September 1998) [8, 9, 10];
4) Tokai-mura criticality accident (Japan, September 1999) [11];
5) Hatfield railway accident (UK, October 2000) [12];
6) Davis Besse pressure vessel corrosion event (USA, February 2002) [13];
7) loss of the Columbia Shuttle (USA, February 2003) [14];
8) Paks Nuclear Plant fuel cleaning event (Hungary, April 2003) [15, 16];
9) Texas City oil refinery explosion (USA, March 2005) [17, 18, 19];
10) loss of containment at the THORP Sellafield reprocessing incident (UK, April 2005) [20].

Organisational and cultural findings contributing to each event were assembled from the published reports for each of the ten cases studied. The analysis revealed strong similarities between the findings. As a step in the development of a 'vulnerability tool', these have been grouped under eight generic/key headings. The main areas identified and discussed in more detail below are:

1. leadership issues;
2. operational attitudes and behaviours (operational 'culture');
3. the impact of the business environment (often commercial and budgetary pressures);
4. oversight and scrutiny;
5. competence and training (at all levels);
6. risk assessment and risk management;
7. organisational learning;
8. communication issues.

These issues were relevant to nearly all of the events studied. In addition, several (but not all) of the events had specific learning relevant to external regulation and to the interface with contractors. More detailed questions sets based on the identified issues have been developed and these will be used as an input to the vulnerability tool. These issues will be addressed in the final project report.

2.1 Leadership

Weak/ineffective leadership is considered by the authors to be the most fundamental issue leading to most of the events analysed. Specific issues include the following:

- The need for commitment to nuclear/process safety from 'the top' and the communication of this as a core value to the workforce in a compelling and intelligible way, such that the priority attached to this in the organisation is beyond question.
- A requirement for a strong understanding of operational 'reality' obtained from high leadership visibility and a questioning attitude about matters as they really are, rather than encouraging the transmission upwards primarily of 'good news'.
- A sufficient understanding of nuclear/process issues so that information received and decisions taken can be considered in an informed way and properly integrated in the business decision making process.
- The development of clear organisational structures, which minimise complexity. This also ensures clarity about roles and responsibilities. It also facilitates good communication and minimises the existence of 'silos' which can reduce team working and learning.
- The need to ensure that the organisation maintains its capability as the 'controlling mind' and is an intelligent customer for services that it buys in, with an understanding of the role of licensee or equivalent.
- Ensuring that there is an effective safety management system (SMS), that this is supported by a strong safety culture and that 'policy' is translated into operational requirements and procedures in such a way that the users of the SMS understand the basis of requirements and receive help and advice, where necessary, in implementation. In particular there is a need for a clear and well-understood 'balance' between requirements from the 'centre' and discretion given to operational units.
- The need for sufficient information effectively to monitor and review performance – for example, reviewing on a regular basis a suitably detailed range of performance

indicators for nuclear/process safety which contain leading as well as lagging parameters. This is further discussed in section 2.6.

- The existence of processes which recognise the importance of nuclear/process safety issues and integrate these with decision making about other aspects of business performance. Issues relating to nuclear/process safety must always be given sufficient prominence (e.g. when compared to the review of financial and commercial performance).
- The existence of an approach to communication which transmits key expectations and issues to the workforce and which encourages and facilitates feedback which is then used to drive improvement. An effective system allows key messages to be cascaded into the organisation in a suitable form and thus ensures that the 'right messages are received by the right people at the right time'.
- The enabling of processes and systems which ensure that risks are properly assessed and reviewed and that this is done in such a way that independent challenge is welcomed, that learning is encouraged and shared and that there is clarity about priorities backed by adequate resources. When actions are taken to address risks it is essential that leaders confirm that these have been satisfactorily implemented.
- An awareness by leaders of the nuclear/process safety risks which they are managing and a recognition that when commercial and other pressures require organisational changes to be made, this is done after carefully considering the effect on these risks and adequate resources are available to manage them.

2.2 Operational attitudes and behaviours

Analysis of the events studied has provided many examples of issues which are brought together under this broad heading.

- Poor quality procedures (sometimes not reflecting risk assessment or safety case findings) and/or failure to comply with them – in particular, a failure to distinguish between 'what is written and what is done'. This led to 'workarounds', violations and/or the development of informal procedures.
- Failure to ensure that operators have a sufficient understanding of the risks that procedures and instructions are designed to control. In some cases, the workforce had not received sufficient training on nuclear/process risks and there was a false belief that the control of industrial safety risks (e.g. slips, trips and falls) would necessarily lead to good performance across the spectrum of safety risks.
- Significant attention needs to be given to the vital role of first line supervisors in both setting standards and challenging unacceptable practices.
- Failure to encourage a questioning attitude and constructive challenge allows the development of mindsets. In some cases this resulted in important risks being 'normalised' and risks being taken on a habitual basis by default. In such cases, risks which were once identified as significant and worthy of particular attention became neglected because they did not lead to major problems.
- The need to ensure that there is 'conservative decision making' such that nuclear/process issues are always given sufficient attention and priority. This is particularly relevant in cases where novel processes are being used or in the case of 'new plant culture' – the view that a new plant or process at the cutting edge of technology is unlikely to fail. It can also be important, however, where a process has become familiar and operators are no longer sufficiently cautious.

- Failure to address issues of complacency/overconfidence often arises from a view that the organisation has ‘always done it this way’. In some cases the organisation had previously been successful but unrecognised organisational drift then led to degraded performance.
- Poor communication, particularly at shift handovers or between engineering/specialists and operational staff, were factors in several events.
- A willingness to operate with equipment which is in an unacceptable condition or in a working environment which is conducive to poor quality in operations.
- A failure to encourage and involve individuals and teams in identifying improvement opportunities and ‘challenging’ poor standards.
- Weaknesses in providing sufficient capability in recognising and dealing with abnormal events and/or recurring issues. This was exemplified in several events by a failure to understand the significance of alarms, to deal with information overload and to seek assistance when issues had escalated beyond normal operations.
- The development of inappropriate patterns of work with casual transfer of roles and in some cases the working of long hours leading to fatigue and possible deterioration in the ability to make important decisions.

2.3 Business environment

Nearly all of the events studied arose against a background of significant commercial and/or operational pressure. In any organisation there is always a balance to be struck between the pressures of production/delivery and the achievement of acceptable levels of safety performance. It is when the balance leans towards an emphasis on achieving commercial results at the expense of safety that danger arises. The following are among the specific issues which have arisen:

- A failure to consider the nuclear/process safety implications of changes to the organisation in terms of either people or other resources, sometimes because required changes are perceived as urgent and sometimes because there is insufficient analysis to make leaders and managers aware of the implications of the change.
- In some cases, business decisions from ‘above’ have overburdened plants so that they have been overloaded with initiatives and requirements. This has led to a loss of direction and sense of priority. More specifically, personnel have regarded changes as ‘flavour of the month’ and commitment and trust has been lost. Loss of direction was sometimes exacerbated in cases where there were very rapid changes in the composition of the leadership team.
- In organisations where resource reductions become the norm (e.g. cost cutting in continuing attempts to restore profitability in the face of changing market conditions), ‘salami slicing’ of resources has taken place without the review of the cumulative impact of such changes on nuclear/process safety.
- Where new facilities are acquired, this can lead to positive steps to improve the material condition and people-related issues at the facility. Sometimes, however, the fact that infrastructure is in a relatively poor state is not fully recognised and acted upon and it is allowed to deteriorate further with the new owners unwilling or unaware of the need to seek substantial improvement.
- Commercial and ‘political’ pressures have led to organisations outsourcing or passing substantial safety related responsibilities and competences to contractors often in order to minimise costs. This can result in a loss of clarity about accountabilities, a failure of the contracting organisation to maintain its competence

as an informed and intelligent customer and in some contexts, to abrogate its responsibilities as a licensee/duty holder.

- Incentives have sometimes been introduced which fail to take account of nuclear/process safety issues and which concentrate on financial or quality-related issues – sometimes with a negative impact on safety. Where such incentives are introduced, it is important to examine the potential impact of these and introduce balancing requirements or incentives to give safety sufficiently high priority.
- Changes in the business environment which have led to processes or plant becoming neglected. The 'orphan plant' issue, as exemplified by the Tokai-mura accident, illustrates the potential of this as a factor in events. In this case there was an apparent lack of 'ownership' of a peripheral plant which was not in the mainstream of the organisation's business. A similar issue relates to 'organisational drift'. In this case, a once 'high performing' plant deteriorates and standards drop whilst leaders and regulators fail to notice and continue to act as though the plant has retained its previous high standards.

2.4 Competence

Most of the events studied have shortcomings in competence as an issue. The following issues have been identified from the events studied:

- In some events, there was a gradual erosion of competence and a lack of process-related knowledge. This was not identified because of a failure to review competencies for nuclear/process safety on a regular and systematic basis – particularly during or following major organisational change. This relates to positions at all levels in the organisation and often includes contractors.
- There is a need to ensure that senior managers and organisational leaders have sufficient understanding of the risks which they are seeking to manage and to ensure that the consequences of failing to do so has been highlighted.
- Some events studied highlighted the need for front line staff and their supervisors to have a greater understanding of nuclear/process safety risk and an ability to recognise when abnormal and potentially dangerous situations are developing. In these situations they need to be able and willing to draw on competent specialist support.
- In some events, training was superficial and based on a 'tick box' approach without adequate planning, assessment and direct personal support to ensure a deeper understanding of principles and the underlying issues.
- Technical competence is vital but issues relating to non-technical capabilities such as communication, team working and issues relating to safety culture (such as the need for a questioning attitude and the importance of reporting and learning from events and precursors) in some cases did not receive the necessary attention.

2.5 Risk assessment and management

This area has again been highlighted by almost all of the events studied and includes a wide range of issues from the strategic to the specialist, through to the assessment and management of risks in day-to-day operations. The specific issues from the events studied include the following:

- Failure to have in place an overarching process by which nuclear/process safety risks can be assessed and minimised. For some of the events studied, the organisations had no systematic process to identify and prioritise the risks and their response to them. In some cases they were overwhelmed by competing priorities such that the key risks did not receive the attention they deserved.

- In other cases, the organisations had drifted into a mindset or state of complacency as a result of previous good performance and/or excellence. This meant that emerging and (in some cases) long-standing nuclear/process safety risks were not identified or were not seen to be significant. Where they were recognised, they were 'normalised' and actions were sometimes inappropriate or ineffective, with no check on their effectiveness.
- In several cases, there was a lack of rigour in assessing risks, developing a suitable safety case, ensuring that issues were reflected in operational procedures and that these were then adequately controlled.
- Mechanical integrity programmes and related inspection programmes were not maintained and remedial actions prioritised.
- Important technical findings, such as good practices identified in Hazops and safety reviews, were deferred (sometimes for budgetary reasons).
- Indicators associated with abnormal conditions (e.g. alarms and data trends) were not systematically addressed in several cases, particularly during start-ups and shut-downs.
- There was no recognised and useable process for assessing the effects of organisational and, in some cases, technical changes on nuclear/process safety.

2.6 Oversight and scrutiny

When failures occur in systems and /or as a result of a weak organisational culture, this can be put right before a major failure occurs by oversight systems designed to alert different layers of the organisation to the deficiencies. Failures in oversight were (perhaps unsurprisingly) a common feature of all of the events studied. The following specific issues were identified:

- A failure to have in place a hierarchical, layered system of checks and balances. In some cases there was only a conventional audit process - often solely within the line and consequently lacking clear independence. In some cases this did not look beyond paper systems and did not identify failures to comply and deficiencies in the underlying safety culture.
- Oversight processes were sometimes ineffective because they were either poorly resourced, reports and feedback were not given sufficient weight and/or were not the subject of sufficient questioning by the recipients of the reports. This was sometimes reinforced by a 'good news culture' in which unpalatable aspects were not highlighted or acted upon.
- In some cases, information being fed up to senior leaders was aggregated such that weaknesses relating to particular plants or functions could not easily be identified and addressed. On occasions, also, there was a failure to prioritise remedial actions and then to check that actions had been carried out and had achieved the desired outcome.
- Early warning of emerging issues can most effectively be identified in the oversight process if key measures and issues are integrated. Thus it is not sufficient to rely just on performance indicators. An effective system uses these together with audit findings, event reports and through the commitment of senior leaders to question safety performance systematically to the same depth and intensity to which financial

and project related programmes would usually be scrutinised - for example through regular face-to-face scrutiny meetings between leaders and their direct reports. In few of the events studied, did leaders appear to exercise a formal, integrated process.

- Safety Departments (which might be expected to provide independent authoritative advice) were not sufficiently resourced or competent and/or did not have sufficient authority to stop potentially unsafe operations.
- In several of the events studied, organisations had once been strong performers with a good reputation, but this had gradually eroded without the organisation being aware of this. This 'organisational drift' is often an important precursor to organisational accidents.
- Failure to detect weaknesses in nuclear/process safety performance also arose from the lack of suitable nuclear/process safety metrics. In some cases over- reliance was placed on metrics relating to personnel/industrial safety and it was wrongly assumed that successful performance in these areas of safety would 'guarantee' excellence in nuclear/process safety. In nearly all cases suitable metrics relating to nuclear/process safety were not available or contained only lagging indicators.
- There was evidence in many cases that leadership teams at the top of the organisation were unaware of the reality of safety shortcomings at plant level. Findings were not always questioned, in some cases probably because of a lack of expertise at this level about the nuclear/process safety issues involved but, in some cases, because it appeared that the needs of the broader business agenda did not 'align' with the information being made available through the oversight processes.

2.7 Organisational learning

For most of the events studied there had been previous events from which there was suitable learning available. If this had been acted upon, the event would not have occurred. The following issues were identified:

- There sometimes did not appear to be an effective system for event reporting particularly in relation to nuclear/process safety. Reporting was poor for a variety of reasons, including apparent concerns from staff that their reports would not be part of a 'just' or 'blame free' response, that bad news would not be welcome at more senior levels, that there was insufficient knowledge to recognise precursors and/or that there was simply a culture of mistrust and/or complacency which did not encourage open reporting.
- Previous events had not been investigated on a systematic basis. This was reflected in a failure to investigate some events at all and in other cases there was a failure to consider root causes. Learning from events was often not shared within the organisation or beyond as part of an effective OEF programme.
- In many cases there were historical events which provided significant learning opportunities. Some of these had happened in the organisation and others were from other companies within the same industrial sector. Where these had been recognised as learning opportunities, they had often faded in significance within the corporate memory or improvement actions taken had not been tracked, completed or carried out effectively.
- Members of the workforce were sometimes not aware of the risks being run through poor practices or failed equipment. For many of the events studied there appeared to be little evidence that organisations were actively encouraging the workforce to

become involved in improvement activities in the area of nuclear/process safety as individuals or as teams.

- The existence of ‘organisational silos’ also meant that important knowledge which might have minimised the risk of the resulting event was not transferred. There was, for example, a failure to transfer learning between engineering or technical staff and operations staff or to share learning with contractors.

2.8 Use of contractors

The impact of contractors and their control by the contracting organisation was an important factor in about half of the events studied. Identified issues included:

- A gradual loss of control with more and more responsibility being ceded to contractors and without the contracting organisation always being aware of its failure to retain the necessary control.
- In doing this, the contracting organisation sometimes lost competence (or failed to develop the necessary competence) and was thus unable to determine whether the contractor was carrying out its operations safely and/or with an acceptable safety culture.
- In some cases the contractor was more aware of an emerging issue than the contracting organisation. However, failures of communication, a lack of competence or commercial and other pressures, meant that advice from the contractor was not acted upon.
- Contractors were in some cases the subject of contracts which did not properly reflect the importance of safety as part of their role. Incentives to complete on time and to cost sometimes reinforced this.

2.9 Communication

Communication issues enter into all events in one form or another. Relevant issues were:

- Failure of communication between leaders and the workforce about the high priority to be attached to nuclear/process safety. Where communication had occurred it was often based on written systems and the element of personal commitment shown in good face to face communication had been lost. This was also often not a two way process with leaders failing to ask the workforce about the real operational issues affecting nuclear/process safety.
- Breakdowns of communication occurred between contracting organisations and their contractors.
- Breakdowns of communication occurred between operational staff and those providing engineering and/or technical support.
- The existence of organisational ‘silos’ where communication was only channelled through certain routes and where communication between individuals and teams was outside the norms of organisational behaviour.
- In several events, there was evidence of a breakdown of communication at critical points in the progression of an event. A particular example was breakdown in communication at shift handover. In some cases this involved the failure to use an existing procedure, whilst in others, communication was generally carried out within an informal setting and was not subject to a formal process requirement.

- Failure of communication with other organisations, particularly in terms of improvement ideas and the sharing of learning, was an important element in some of the events studied. Many of the organisations involved had developed a 'closed' culture in which communication in a spirit of questioning and learning from others was no longer a practice which was supported and encouraged.

2.10 External regulation

Regulatory bodies provide a vital safeguard in acting as a last line of defence in providing oversight. When effective, they can also provide a stimulus to the achievement of good practice and enable organisations to realise that complacency, organisational drift or overconfidence is becoming a danger.

Many of the issues discussed above are applicable to the regulatory body (e.g. leadership, competence, organisational learning and review and oversight of the regulator's own role). Commercial pressures may also be significant both in terms of the level of resource available to regulators and the need for them to challenge the development of an unhealthy business environment in which safety is not being given an acceptable degree of priority. This is difficult because it may sometimes mean challenging the safety implications of broader (e.g. government) policy when this is likely to have a negative impact on safety.

Issues relating to external regulation which arise from the events studied include the following:

- For most of the events studied, the striking finding in relation to external regulation was its absence or weakness. In some cases there was an inadequate inspection regime (e.g. Tokai-mura), in other cases the regulator appeared to trust the judgement of the operator/licensee rather more than was justified (e.g. Paks and Davis Besse). In several instances, the relationship between the parties may have become too 'comfortable'. This was particularly highlighted in the case of 'good performers' such as Davis Besse, where scrutiny was reduced but where subsequently performance appeared to have declined.
- In addition to general inspection of plant and awareness about overall plant condition and culture, the events highlight the significance of regulators being aware of major emerging engineering developments on which focussed scrutiny may be required.
- The need for regulators to take a view on the capability of the organisation as a whole in the context of such issues as leadership commitment, safety culture, the management of change, the role of contractors, the impact of the business or 'political' environment (as discussed above) and evidence of 'organisational drift'. These are difficult issues which require significant judgement but are the 'seeds' out of which many of the events studied have grown. They are not always part of standard regulatory procedures and practice, but regulators need to ensure that they have the remit and ability to 'test' such issues.
- At a more practical level, for some events there had been regulatory involvement in the emerging issue but insufficient follow up of the actions taken by the operating organisation.
- Several of the events have pointed to the need for regulatory bodies to improve their own internal communication and thus to integrate better the knowledge which was available in the organisation. This appeared to be a particular issue between technical specialists and inspectors who had to agree priority actions with the operating organisation.

- Finally, some of the events pointed to shortcomings in the regulatory framework. An obvious case was the need for a safety case/permissioning regime in the State of Victoria at the time of the Longford accident. A further issue may also attach to the need to identify 'orphan' plant or areas of risk which are currently not regulated to a level that their safety significance might suggest is appropriate.

3 PROCESS MODELLING

The key areas identified in section 2 emphasise how safety performance of a whole system (e.g. an organisation) is affected by both technical and human factors. It can be a very challenging task to assess safety performance in a way that allows a view to be developed of the 'big safety picture' in a clear and transparent way. Also, it is particularly difficult to capture the rationale behind the reasoning. This section investigates tools to support and help to analyse these relations.

It is suggested that a systems methodology such as that set out by Blockley and Godfrey in their book 'Doing it Differently' [21], can provide structure and form the basis of a new software tool to help to achieve this. In particular, a modelling technique known as hierarchical process modelling (HPM) offers a new approach to safety assessment [22]. Such an approach describes a complex process at different levels of definition and contains a rich analysis of the connectivities between different parts of the system under study. HPM is currently the subject of further research with the aim of building a tool to assess organisational safety and safety culture within an organisation, based on issues such as those discussed in Section 2 above and associated evidence gathered from inspections/questionnaires etc.

The following sections provide insight into the different concepts involved in the systems methodology and how they can be used in practice. These concepts are holons, interval probability (Italian Flag) and the hierarchical process model.

3.1 The need for a holistic approach

Assessing the safety performance of the whole system requires a holistic approach, addressing all factors such as technical systems, safety management systems, organisational safety and leadership. The approach must assess individual components of the system but also the interactions between those components.

As a tool for analysing this process, traditional reductionism has proven useful when addressing well defined physical systems but does not work well for human driven systems. In contrast, HPM is a holistic approach, capable of modelling key emergent system properties and has advantages over the traditional reductionist approach. Using hierarchical abstraction, a complex process is described at different levels of definition, as are the connectivities between different parts of that process. Also, it provides an opportunity to integrate all of these parts, both 'hard' and 'soft', within one unified framework [23].

3.2 A need for a hierarchical process model

HPM provides a detailed understanding of the top-process (i.e. the highest level process that defines the purpose of the activity) in terms of the factors that lead to the success of that process. The hierarchy elaborates these factors in increasing levels of detail. This improves transparency by enabling stakeholders to walk through the model and understand how lower level processes affect the performance of higher level processes, allowing them to discuss, elicit, evaluate and update parts of the process model. It also facilitates a 'whole view' of the safety system. This will enable those responsible, whether within an operating organisation or regulatory body, to demonstrate or identify deficiencies in safety performance with greater confidence and clarity and to justify action and eventually address process safety issues which if not addressed could be precursors to events as those studied as part of this research project.

3.3 Defining a process holon

In HPM, processes are described in terms of holons. A process holon is a well-described characterisation of a process. A high level process is described as an interacting collection of lower level process holons. A holon is usually viewed as an activity which is 'a way of getting from where you are to where you want to be'. A holon can identify both 'hard' as well as 'soft' processes and is therefore useful for complex problems involving human components.

A process holon is defined by its name and a set of attributes that define the success of the activity. The name is in a phrase form which describes what the objective of the owner of the process is. The owner is responsible and accountable for attaining the purpose successfully. The attributes of the process formed by asking six fundamental questions: 'what', 'where', 'who', 'when', 'how', and 'why'. These key questions are used to provide the evidence to support judgements regarding the success of the process.

3.4 Modelling uncertainty

It is seldom possible to present the conclusions of a safety analysis with absolute certainty. It can be difficult to obtain objective quantitative data in support of conclusions, as is often the case in assessment of safety culture or human factors. One of the greatest difficulties of safety performance assessment resides in the treatment of evidence or data which might be uncertain, incomplete, inaccurate or inconsistent (or even simply missing). Because uncertainty is often unavoidable, it is important to help safety analysts to manage it within an appropriate, well founded reasoning framework. Several mathematical approaches exist to quantify uncertainty and have been discussed in various sources [24, 25]. One such approach is Interval Probability Theory [26, 27]. This can be used to handle in a simple way, fuzziness, incompleteness and randomness and has been found to be particularly appropriate for managing uncertainty in an HPM.

3.5 Performance measurement in HPM

The 'state' of an HPM process holon and its progress towards eventual success are defined in terms of performance measures, referred to in this context as Performance Indicators (PIs). PIs are derived from a variety of sources ranging from measurements, inspection documents and model calculations to expert elicitation. The degree of success of a process is determined by comparing the values of its PIs to target values and the results are used to assess process performance. The values of all the PIs for a single process are combined into an 'Italian Flag' (green-white-red) diagrammatic representation to visualise process performance. This allows non-experts to get a 'feeling' of how well a process is performing without knowing all of the technical and non technical details.

3.6 A simple hierarchical process model example

The theoretical ideas discussed above are under development as part of this project to design and build a practical vulnerability assessment tool. This work is not complete and is not possible yet to provide a developed organisational safety assessment, but a simple example is provided to demonstrate the key elements of the methodology. One top process and four sub processes are shown in Figure 1.

The sub processes H_1 'Having good safety leadership', H_2 'Containing both risks and hazards', H_3 'Having commercial growth without reducing organisational safety' and H_4

‘Having good communication’ are linked to the top process H_0 ‘Maintaining a high level organisational safety performance’. The arcs are directed from the sub processes to the top process indicating that success in all the sub processes is necessary and sufficient for the success of top process H0. More specifically, the arcs reflect the necessity (N) and sufficiency (S) relationship existing between each sub process and the associated top process. These N/S relationships are given values on a [0, 1] interval to model the relative importance the sub processes.

Performance evidence is acquired at the level of processes H_1, H_2, H_3 and H_4. The effect of this evidence on the top level process is modelled by developing an Italian Flag associated with each of H_1, H_2, H_3 and H_4. These flags are derived from the PIs associated with H_1, H_2, H_3 and H_4. Each Italian Flag bar represents an interval probability statement summarising the degree of success of a process. The performance of H_0, represented by its Italian Flag, is calculated from the Italian Flags assigned to the sub processes, and the S/N links. It is also possible to define a local PI for the top process. Comparing the Italian Flag from this with the propagated ones enables the process owner to highlight possible situations of conflict.

The amount of white in a flag indicates the level of uncertainty in assessing the success of the process. A wide white band would be an indication that, in the case of H_0 for example, an operating organisation or regulatory body needs to undertake further evidence collection in order to reduce the amount of uncertainty associated with the success of the process. Similarly, green indicates positive evidence in support of success and red indicates evidence in support of failure. The process model provides the opportunity to examine how the component parts of the flag for a process are computed thus offers key insight into the causal factors that determine the (success) of a process.

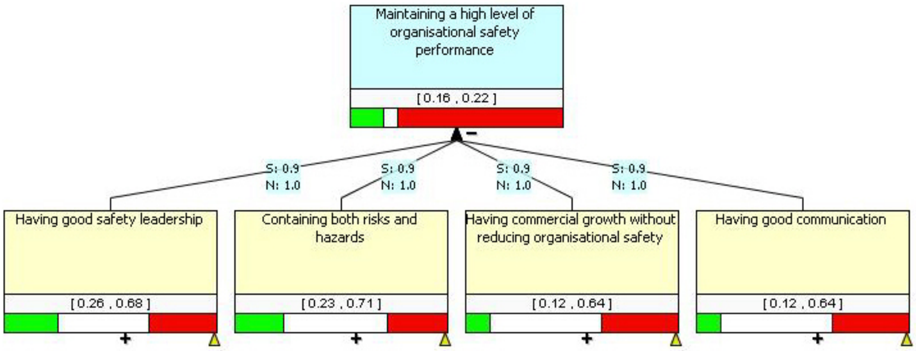

Maintaining a high level of organisational safety performance
[0.16 , 0.22]
–
S: 0.9
N: 1.0
S: 0.9
N: 1.0
S: 0.9
N: 1.0
S: 0.9
N: 1.0
Having good safety leadership
[0.26 , 0.68]
+
Containing both risks and hazards
[0.23 , 0.71]
+
Having commercial growth without reducing organisational safety
[0.12 , 0.64]
+
Having good communication
[0.12 , 0.64]
+

Figure 1: A hierarchical process model representing a top process with its four sub processes.

4 CONCLUSIONS

Detailed study of the reports into the recent major events across a range of industries (including several events in the nuclear industry) has allowed a range of organisational and cultural factors to be identified which seem to be common precursors to the events. It is believed that if operating organisations can develop a better understanding of these issues and a ‘vulnerability tool’ can be developed to assess the ‘health’ of organisations with respect to these factors, it may be possible to reduce the risks of so-called ‘organisational accidents’.

This paper has reviewed the issues identified for the events studied and categorised them under broad headings. A question set is being drawn up, based on the identified issues, which should be helpful in enabling regulators and operators to assess performance.

However, it is believed to be important that process modelling based on a 'systems thinking' approach should be developed in order to structure, clarify and potentially 'measure' organisational vulnerability with an appreciation of the uncertainties involved. The paper has presented some approaches which have been developed by the SSRC at the University of Bristol and describes some of the concepts and how in outline these might be combined with the identified issues to provide a hierarchical process model as part of a structured holistic approach to assess the impact of the complex, wide-ranging factors involved.

ACKNOWLEDGMENTS

This work is part of a substantial project being carried out at the Safety Systems Research Centre at the University of Bristol, with funding from the UK Nuclear Installations Inspectorate (NII) for the first stage work and initially from British Nuclear Fuels (BNFL plc). The authors are grateful to these organisations. In particular, the authors wish to thank David Blockley, Helen Rycraft, Sarah Peck for their input to discussions during the development of this paper.

REFERENCES

[1] R. H. Taylor, H. S. Rycraft, 'Learning from disasters', IAEA Conference on Topical Issues in Nuclear Installation Safety, Beijing- China, (October 2004).

[2] L. G. A. van Wijk, D. I. Blockley, 'A Systems Approach for Assessing Non Nuclear Proliferation', Systems Analysis for a More Secure World: Application of System Analysis and RAMS to Security of Complex Systems, Ispra, Italy, 25th-26th (October 2005), ESReDA Conference, Systems Analysis for a More Secure World, pp. 221-232, (2006), ISSN: 1018-5593, ISBN: 9279012282.

[3] B.A. Turner, N.F. Pidgeon, Man-Made Disasters, Butterworth-Heinemann Ltd; Oxford, UK, (7 April 1997), ISBN-10 0750620870.

[4] N. F. Pidgeon, B. A. Turner, D. I. Blockley, The use of Grounded theory for conceptual analysis in knowledge elicitation, *International Journal of Man-Machine Studies*, Volume 35, Issue 2, pp. 151-173, (August 1991).

[5] J. Reason, Managing the risks of organizational accidents, Ashgate, Aldershot, UK, (15 Dec 1997), SBN-10 1840141050.

[6] Health and Safety Executive, Walkway collapse at Port Ramsgate: A report on the investigation, (2000).

[7] Health and Safety Executive, Collapse of NATM tunnels at Heathrow Airport. A report on the investigation by the HSE into the collapse of New Austrian Tunnelling Method (NATM) tunnels at the Central Terminal Area of Heathrow Airport on 20/21 October 1994, (2000).

[8] A. Hopkins, Lessons from Longford: the Esso Gas Plant Explosion, CCH Australia Limited, May (2000), ISBN 1864684224.

[9] Royal Commission, The Esso Longford gas plant accident: Report of the Longford Royal Commission, Department of Premier and Cabinet, Act Number 42/99, Parliament of Victoria, Melbourne, Australia, (1999), ISBN 0731138589

[10] State Coroner Victoria, Inquest into the deaths of Peter Brubeck Wilson and John Francis Lowery and the fire at Longford Gas Plant Number 1, Coroner's Case Number 2907/98, Melbourne, Australia, (2002).

[11] International Atomic Energy Agency, Report on the preliminary fact finding mission following the accident at the nuclear fuel processing facility in Tokai-mura, Japan, Vienna – Austria, (1999).

[12] Office of Rail Regulation, Train Derailment at Hatfield: A Final Report by the Independent Investigation Board, (July 2006).

[13] U.S. Nuclear Regulatory Commission, Davis-Besse Reactor Vessel Head Degradation Lessons-Learned Task Force Report (2002).

[14] Columbia Accident Investigation Board, Report Volumes 1-6, Printing and Distribution by the National Aeronautics and Space Administration and the Government Printing Office Washington, D.C., (August 2003).

[15] International Atomic Energy Agency, Report of the Expert Mission conducted under IAEA Technical Co-operation Project HUN/9/022 Support for Nuclear Safety Review Mission, ‘To Assess the Results of the Hungarian Atomic Energy Authorities Investigation of the 10 April 2003 Fuel Cleaning Incident at Paks NPP, (2003).

[16] Hungarian Atomic Energy Authority Report to the Chairman of the Hungarian Atomic Energy Commission on the Authority’s investigation of the incident at Paks Nuclear Power Plant on 10 April 2003 (Identification number of the event: 1120), (May 2003).

[17] BP Report, Fatal Accident Investigation Report - Isomerisation unit Explosion Final Report, Texas City, Texas, USA, (December 2005).

[18] US Chemical Safety Hazards Investigation Board, Investigation Report: Refinery Explosion and Fire, Report No. 2005-04-I-TX, (March 2007).

[19] The Report of the BP U.S. Refineries Independent Safety Review Panel, (January 2007).

[20] Health and Safety Executive, Report of the investigation into the leak of dissolver product liquor at the Thermal Oxide Reprocessing Plant (THORP), Sellafield, notified to HSE on 20 April 2005, (2005).

[21] D. I. Blockley, P. Godfrey, Doing it differently, Thomas Telford Books, London, (2000), ISBN 0727727486.

[22] J. P. Davis, J. W. Hall, A software-supported process for assembling evidence and handling uncertainty in decision-making, *Decision Support Systems*, V. 35, pp. 415- 433, (2003).

[23] P. Checkland, Systems Thinking Systems Practice, John Wiley & Sons, (July 1999), ISBN-10 0471279110.

[24] H. Jeffreys, Theory of Probability, Oxford University Press: Clarendon Press, (1998), ISBN 0198503687.

[25] R. C. Jeffrey, The Logic of Decision, University Of Chicago Press, (1990), ISBN 0226395820.

[26] W. C. Cui, D. I. Blockley, Interval probability theory for evidential support, *International Journal of Intelligent Systems*, V. 5, pp. 183-192, (1990).

[27] J. W. Hall, D. I. Blockley, J. P. Davis, Uncertain inference using interval probability theory, *International Journal of Approximate Reasoning*, Vol. 19, pp. 247-264, (1998).

TOPSAFE
Dubrovnik, Croatia, 30.09 - 3.10.2008

A NEW METHOD TO RESPECT THE REAL STATE OF KNOWLEDGE ON UNCERTAINTIES IN THE EVALUATION OF SAFEY MARGINS

J. Baccou and E. Chojnacki
Institut de Radioprotection et de Sûreté Nucléaire,
BP3, 13115, Saint Paul-les-Durance, France

Corresponding author *J. Baccou,* jean.baccou@irsn.fr

ABSTRACT

This paper is devoted to some recent developments in uncertainty analysis methods of computer codes used for accident management procedures in nuclear industry. A quick overview on current practices as for uncertainty methodology is first given with a special attention devoted to the probabilistic modelling which is the most classical approach currently used by analysts. It turns out that despite its attractiveness relying on a simple implementation and convenient available tools to study the statistics of the code response, probability theory does not provide satisfactory results for uncertainty quantification in presence of incomplete knowledge or when the uncertainty is not only of aleatory nature. Therefore, a new approach, called the RaFU method, is introduced to avoid the subjectivity which may exist in the choice of a single probability distribution when it is not justified. Finally, an application of the RaFU method to uncertainty analysis of a LBLOCA transient (LOFT-L2-5) is given and a comparison with probability-based methods is provided as well. This application has been performed in the framework of the BEMUSE OECD project.

1 INTRODUCTION

Best estimate computer codes are increasingly used in nuclear industry for the accident management procedures and have been planned to be used for the licensing procedures. Unlike conservative codes, they attempt to calculate accidental transients in a more realistic way. Therefore, it becomes of prime importance, in particular for the French Institut de Radioprotection et de Sûreté Nucléaire (IRSN) in charge of safety assessment, to know the uncertainty on the results of such best estimate codes.

A large majority of uncertainty analysts uses uncertainty methodologies based on a probabilistic modelling and Monte-Carlo simulations to propagate the uncertainties through their computer codes. However, the two following limitations can reduce the efficiency of such an approach and deteriorate the relevance of the decision-making process:

- These methods require a lot of knowledge to determine the probability law associated to each uncertain parameter and all the possible dependencies between the uncertain parameters. In practice, such information is rarely fully available.
- Working within the probability theory framework implicitly assumes that all uncertainties are aleatory (i.e. due to the natural variability of an observed

phenomenon). In practice, uncertainties can arise from imprecision (a variable has a fixed value which is badly known due to the lack of data, knowledge or experiment).

Therefore, recent works have focused on new methods able to avoid the subjectivity which may exist in the choice of a single probability distribution in presence of incomplete knowledge or when uncertainties are due to imprecision. Existing methods are often computationally costly and are thus applicable to relatively simple models, which limits the efficiency of such approaches in fields (such as nuclear safety) where models can be very complex and where computational costs have to be taken into account.

We propose in this work a new numerical treatment of such methods based on Monte-Carlo sampling techniques which reduces the computational cost and can be applied to complex models. Moreover, by using notions of order statistics, our method proposes a way to estimate the numerical accuracy of the results. The key point of our work mainly consists in setting some decision step before the uncertainty propagation, whereas usual methods postpone this step after the propagation.

Section 2 gives to a quick overview on current practices as for uncertainty methodology with a special attention devoted to the classical probabilistic modelling. Since it will become clear that this approach does not provide satisfactory results in many cases , we introduce, in Section 3, our new method, called the RaFU method. It allows to work within an unified framework to take into account the nature of uncertainty sources and to properly represent the real state of knowledge on uncertainties. It leads also to a numerical implementation ensuring a minimal computational cost. Finally, in the framework of the BEMUSE OECD project, an application of the RaFU method to uncertainty analysis of a LBLOCA transient (LOFT-L2-5) is given in Section 4 and a comparison with probability-based methods is provided as well.

2 UNCERTAINTY ANALYSIS AND CURRENT PRACTICES

2.1 Main steps of an uncertainty analysis

Uncertainty analysis methods are performed in four steps:

Step 1: *Identification of uncertain parameters*
All important factors affecting the model results must be identified. These factors are generally referred to as the “uncertainty sources” or as the “uncertain parameters”.

Step 2: *Quantification of the knowledge about uncertain parameters*
The available information about uncertain parameters is formalized. The uncertainty of each uncertain parameter is quantified. If dependencies are known between uncertain parameters (or classes of uncertain parameters) and judged to be potentially important, they also need to be specified.

Step 3: *Propagation of uncertainties through the computer code*
The propagation requires, except for very simple computer codes, a coupling between the code and a statistical software.

Step 4: *Treatment and interpretation of the code responses*
The code responses are used to get quantitative insights regarding the output variable.

For example, in risk studies, the main concern is to estimate the likelihood of the code response to be above a critical value.
When performing practical studies, the two following requirements have to be respected in order to guarantee a relevant uncertainty evaluation:

- The method has to respect the state of knowledge in the quantification of the information about uncertain parameters (Step 2 in the sketch of the uncertainty propagation methods).
- The method has to lead to a tractable algorithm for uncertainty evaluation (Step 3 and 4 in the sketch of the uncertainty propagation methods) i.e with a reasonable computational cost.

A classical method for uncertainty analysis is the one based on the probabilistic approach. This modelling, as well as its advantages and limitations are recalled in the following section.

2.2 Probabilistic Modelling

2.2.1 Construction of the probabilistic modelling

Here, we specify Steps 2, 3 and 4 within the probabilistic modelling:

Quantification of the knowledge about uncertain parameters

The uncertainty of each uncertain parameter is quantified by a probability density function (pdf). If dependencies between uncertain parameters are known and judged to be potentially important, they are quantified by correlation coefficients.

Propagation of uncertainties through the computer code

The numerical estimation is obtained thanks to Monte-Carlo simulations ([1]). In Monte-Carlo simulation, the computer code is run repeatedly, each time using different values for each of the uncertain parameters. These values are drawn from the probability distributions and dependencies chosen in the previous step. In this way, one value for each uncertain parameter is sampled simultaneously in each repetition of the simulation. The results of a Monte-Carlo simulation lead to a sample of the same size for each output quantity.
The advantage of Monte-Carlo methods with respect to deterministic uncertainty analysis methods (i.e. that do not involve stochastic or statistical approaches) is that the combination of uncertain parameters values are performed in such a manner that they allow to quantify the likelihood of any combinations of parameter values.

Treatment and interpretation of the code responses

Using the central-limit theorem ([2]), the output sample is used to get any typical statistics of the code response such as mean or variance and to determine the cumulative distribution function (CDF). The CDF allows to derive the percentiles of the distribution (if X is a random variable and F_X its CDF, the α-percentile, $\alpha \in [0;1]$, is the deterministic value X_α such that $F_X(X_\alpha)$=Proba($X \le X_\alpha$)=α). Its estimation is crucial for safety assessment since the CDF allows to estimate whether the code response can exceed a critical value.
A simple and robust way to get information on the CDF is to use order statistics ([2]). The principle of order statistics is to derive statistical results from the ranked values of a sample. If $X=(X^{(1)},\ldots,X^{(L)})$ denotes the output sample, the key idea is that the cumulative distribution of

$X^{(k)}$, $F_X(X^{(k)})$, follows the Beta law $\beta(k,L-k+1)$ which does not depend on the distribution of X. Therefore, it is possible to derive confidence intervals for any percentiles directly from the sample values without having to determine the probability distribution of the random variable. This relevant result is very popular in the safety assessment community. It is often used in two ways: when the sample size is fixed, it provides the numerical accuracy (due to the finite sample size) associated to the estimation. It also gives for a fixed numerical accuracy the minimal sample size (and therefore the minimal number of computer runs) to perform in order to reach this accuracy. The connection between accuracy and minimal sample size is often quoted as the Wilk's formula.

2.2.2 Advantages and limitations of the probabilistic approach

The probabilistic model is simple to implement thanks to the uncertainty propagation by Monte-Carlo simulations. Moreover, the use of order statistics provides both simple and robust estimators of percentiles for any output quantities without using response surfaces or fit tests. However, it assumes that each uncertain parameter can be modeled by a random variable (i.e the uncertainty is due to the natural variability and cannot be reduced by the arrival of new information, it is referred to "aleatory uncertainty" in the sequel). This is not true in many applications:

- When the uncertain parameter is measured through an experimental design leading to systematic errors, a pdf is not adapted to the modelization of such uncertainties which are due to imprecision instead of variability.
- Even in the case of random uncertain parameters, choosing an unique pdf and specifying all the possible dependencies between the uncertain parameters is not always affordable since the knowledge related to uncertainties is often incomplete. In practice, following a principle of minimal information, the engineers select an uniform distribution as pdf when only the uncertainty range of the parameter is known and take an independence assumption between two uncertain parameters for granted when no information is known about their dependencies. Uniformity means equiprobability of any values within the uncertainty range which is not justified when knowing only the uncertainty range. Independence implies that it is unlikely to have simultaneously extreme values between random variables and often leads to uncertainty compensation. Therefore, these assumptions do not lead to conservative results and do not meet the precautionary principle when poor information is known.

One speaks about epistemic uncertainty when the choice of a single pdf cannot be assumed or known. This type of uncertainty can be reduced by increasing the state of knowledge.

Therefore, it comes out that the probabilistic modelling is not tailored to handle all the practical issues coming from safety assessment applications. It may lead to an unjustified reduction of the final uncertainty of the model response and affect the decision-making process in risk studies. Indeed, in the worst case, because of such an artificial reduction, the decision maker could underestimate the risk and accept a too high level of risk but a more relevant quantification of uncertainties (i.e another choice of pdf and dependency assumption or another modelization to take into account imprecision) would have shown that the code response is likely to exceed the critical value. For safety reason, it becomes of prime importance to provide a new methodology that gives the engineer a tool to measure the impact of a misleading modelization of uncertainty due to poor knowledge.

Therefore, we propose in the rest of this paper a new method for uncertainty evaluation (called the RaFU method). It allows us to mix different kinds of knowledge representation in order to respect the available information about uncertain parameters and about the nature of their uncertainty. It also integrates an efficient numerical strategy to reduce the computational cost to its minimum.

3 THE RAFU METHOD

We describe in the sequel Steps 2, 3 and 4 within the RaFU modelling.

3.1 Quantification of the knowledge about uncertain parameters

The RaFU ([3]) method allows to handle two kinds of uncertainties: aleatory and epistemic uncertainties. As mentioned previously, aleatory uncertainty is due to the natural variability or randomness of an observed phenomenon. This kind of uncertainty cannot be reduced by new information and its modelling by a pdf is well appropriate. Epistemic uncertainty is due to imprecision or lack of knowledge and thus can be reduced by the arrival of new information. It can come from systematical error such as measurement error but also from the scarcity of information about random phenomena that prevents from choosing an unique pdf for the uncertainty modelization. Possibility theory ([4]) provides an attractive framework to quantify this second type of uncertainty. A possibility distribution is well fitted to the situation where a given variable has a fixed value but badly known. Moreover, if π denotes a possibility distribution, it induces the set of probabilities $P_\pi = \{P / \forall A, P(A) \le \sup_{x\in A} \pi(x)\}$, which is particularly well fitted to represent a badly-known random phenomenon due to an incomplete state of knowledge. In this sense, a possibility distribution can be seen as a model of partial probabilistic information. For example, it can be proved that the probability set induced by a trapezoidal possibility distribution (Figure 1, right) contains all the probabilities with the same core (i.e the most likely values are located in the same interval, [2;4] in our example) and the same support ([1;7]). In other words, if the uncertainty attached to a parameter P is summarized by its range of variation ([1;7]) and an interval of values within this range that P is more likely to take ([2;4]), then the trapezoidal possibility distribution of Figure 1, right, can be chosen for uncertainty quantification. Similarly, the set of pdfs induced by triangular possibility distributions (Figure 1, left) contains all the pdfs with the same mode (i.e. the same most likely value, 3 in our example) and the same support ([2;4]). It is therefore well fitted when the information related to P is its range of variation ([2;4]) and its nominal value (3).

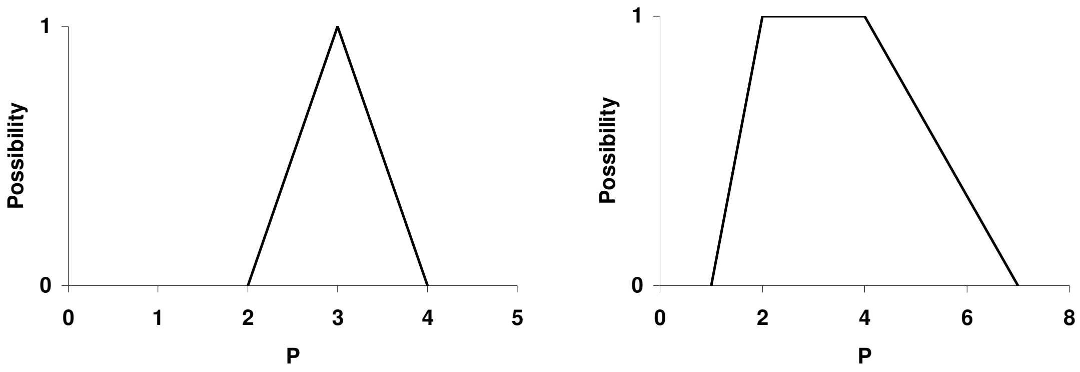


Figure 1: Example of possibility distributions. Left, triangular possibility, right, trapezoidal possibility.

It turns out that the possibility theory is a convenient way to quantify epistemic uncertainty but it can lead also to unrealistic uncertainty margins when, in the case of aleatory uncertainty, enough information is available to select an unique pdf. Therefore, our method allows the analyst to select a probability distribution or a possibility one with respect to the amount of information about uncertain parameters and to the nature of uncertainty. This is achieved by working in an unified framework for probability and possibility called the theory of evidence ([5]). In the same way that the probability theory assigns weights to the different values taken by each uncertain parameter (for example all the points within the core of the trapezoidal distribution), the idea of the theory of evidence is to put weights on subset of values (and not necessarily on single values) such as intervals.

A remaining crucial question concerns the choice (and the simulation) of dependencies between uncertain parameters. Indeed, the classical independence assumption that is taken when few information about dependencies is available is not always justified. It can lead to compensate uncertainties and can affect the uncertainty margins. Based on precautionary approach, it becomes important to allow uncertainty accumulation if there is no information about compensating effect. This can be achieved within the RaFU method thanks to a special propagation strategy.

Therefore, our new method is derived to allow the engineer to answer independently to these two following questions:

- *Probability or possibility?*

In the case of epistemic uncertainty, possibility distributions are used in order to relax assumptions currently made on the choice of the pdfs associated to some uncertain parameters. For aleatory uncertainty, specific pdfs can also be used if a substantial amount of information is available, limiting the over-conservatism encountered in standard interval calculations.

- *Compensation (independence) or accumulation of uncertainties (ignorance of dependencies)?*

When the amount of information to ensure compensating effects is sufficient, one might assume independence whereas simulate uncertainty accumulation in the case of poor information.

3.2 Propagation of uncertainties through the computer code and treatment of the responses

The propagation is based on an extension of Monte-Carlo simulations and therefore first requires a sampling of random (aleatory uncertainty)/badly-known (epistemic uncertainty) variables. Note that sampling a random variable gives a value (Figure 2, left) (as in classical Monte-Carlo simulations). As for badly-known variables, the sampling (Figure 2, right) is performed on the possibility distributions associated to each variable. We focus in this work on convex possibility distributions which are the most encountered in practical studies. Therefore, sampling badly-known variables leads to a set of nested intervals called α-cuts (a set of nested intervals $\{I_\alpha, 0 \leq \alpha \leq 1\}$ satisfies $\forall \alpha \in]0;1[$, $I_1 \subset I_\alpha \subset I_0$).

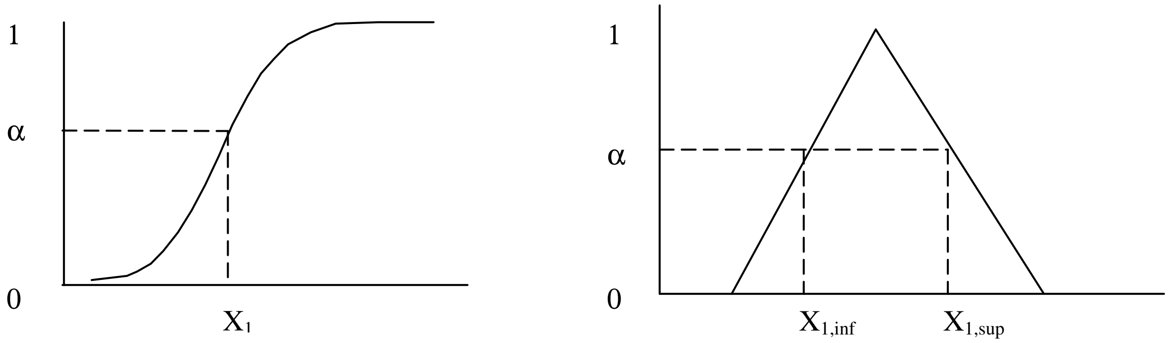


Figure 2: Sampling probability (left) and possibility (right) distributions.

It is therefore similar to performing Monte-Carlo simulations on intervals (i.e. calculations are performed with values at the extreme of each sampled interval). Monte-Carlo techniques offers also an attractive framework for the simulation of dependency. More precisely, for uncertainty compensation, the sample is constructed by randomly combining values/intervals drawn from probability/possibility distributions. When assuming uncertainty accumulation, this combination is performed at the same confidence level. Since both probability and possibility are used to model parameters, the output of the computer code is no more a random variable but a random fuzzy variable. This also implies that the uncertainty derived by this methodology cannot be summarized by a pdf (or a CDF) but by a pair of lower and upper CDFs, $[\overline{F},\underline{F}]$, called probability boxes ([6]). The difference between these CDFs comes from the lack of knowledge modeled by possibility distributions.

There exist many recent works that handle, like the RaFU method, both aleatory and epistemic uncertainties and derive a pair of CDFs. Among them, one can mention the work of Ferson and Ginzburg ([7]) and Baudrit *et al* ([8]) that propose a post-processing technique to extract the relevant information from the resulting random fuzzy variable. Up to now, they concern very simple models or are computationally costly, which limits their efficiency in fields such as nuclear safety where computational cost has to be taken into account.
On the contrary, the RaFU methodology integrates a computational cost reduction strategy. The underlying idea is that in many studies, analysts are interested in some particular statistical summary (such as α-percentiles) which can be evaluated without building the whole random fuzzy variable. Since the RaFU propagation can be seen as an extension of Monte-Carlo simulation to the theory of evidence framework, each statistical quantity of interest is directly estimated using standard results coming from the probabilistic modelling. Moreover, one can exploit convergence theorems to derive the numerical accuracy associated to the limited sample size. The computational cost reduction strategy of the RaFU is then to set a decision step before propagating uncertainties and leading to an optimal (in term of number of code runs) sampling. More precisely, the RaFU method is pre-defined by a triplet of parameters $(\gamma_S,\gamma_E,\gamma_A)$ specified by the analyst:

- Parameter γ_S is related to the aleatory uncertainty. It provides the statistical quantity the analyst is interested in (usually α-percentiles in safety studies).
- Parameter γ_E is related to the epistemic uncertainty. It determines how α-cuts are drawn from possibility distributions.
- Finally, parameter γ_A measures the desired numerical accuracy on the final result. In the case of α-percentile estimation, γ_A comes from the use of order statistics.

According to the analyst, the RaFU method then determines the minimal sample size and the nature of the required sampling to build the wished response. Number of calculations is thus reduced to its minimal number, in accordance with the analyst's choice. Moreover, computational cost can be easily evaluated, allowing the analyst to eventually revise her/his choices before uncertainty propagation. It is also possible for her/him to provide the maximal number of code runs that can be made and the RaFU method will derive the numerical accuracy that can be reached.

Let us come back in detail on the sampling procedure that plays a key role in the implementation of the RaFU method once the triplet (γ_S,γ_E ,γ_A) has been chosen by the analyst. This procedure is fully specified in the following example:

Let $P_1,...,P_N$ be the N uncertain parameters (identified by a preliminary sensitivity analysis for example) of a computer code. We denote by T the output variable and for sake of simplicity, T is assumed to be monotonous increasing with respect to $P_1,...,P_N$. Moreover, we consider that, according to expert's judgement for example, the uncertainty associated to $P_1,...,P_k$, $k < N$, is aleatory (i.e. quantified by a pdf) whereas the uncertainty related to $P_{k+1},...,P_N$ is of epistemic nature (i.e. quantified by a possibility distribution). Once the analyst has chosen the triplet (γ_S,γ_E ,γ_A), the sampling procedure is performed in three steps:

- Generate L samples $X^{(i)} = (P_1^{(i)},...,P_k^{(i)})$, $i = 1,...,L$, for the k first random variables according to the identified pdfs and the dependencies between uncertain parameters (L denotes here the number of samples chosen by the analyst or associated to the selected numerical accuracy, γ_A, to reach).
- Associate to each $X^{(i)}$ one sample of intervals corresponding to the N-k badly known variables P_{k+1},…,P_N and denoted $I^{(i)} = ([\underline{P}_{k+1}{}^{(i)}, \overline{P}_{k+1}{}^{(i)}],...,[\underline{P}_N{}^{(i)}, \overline{P}_N{}^{(i)}])$. Each sample is constructed according to the identified possibility distributions and to the sampling strategy of epistemic uncertainty represented by Parameter γ_E.
- Propagate the two sets of samples $\underline{S}^{(i)} = (P_1^{(i)},...,P_k^{(i)}, \underline{P}_{k+1}{}^{(i)},..., \underline{P}_N{}^{(i)})$ and $\overline{S}^{(i)} = (P_1^{(i)},...,P_k^{(i)}, \overline{P}_{k+1}{}^{(i)},..., \overline{P}_N{}^{(i)})$ $(i = 1,...,L)$ through the computer code and get the two corresponding output samples $(\underline{T}^{(1)},...,\underline{T}^{(L)})$ and $(\overline{T}^{(1)},...,\overline{T}^{(L)})$.

Figure 4 displays a flowchart of the RaFU method.

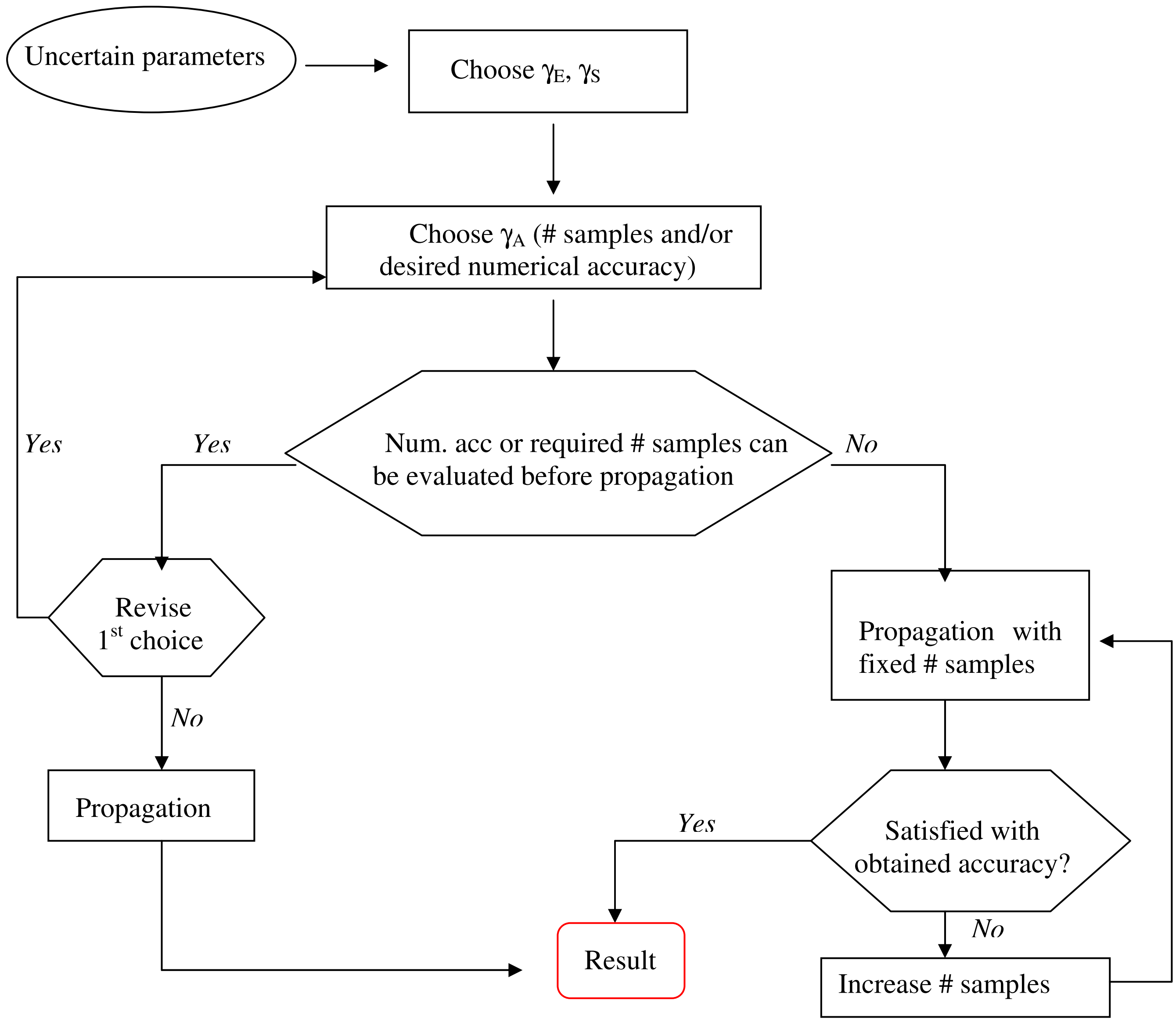

Uncertain parameters
Choose γ_E, γ_S
Choose γ_A (# samples and/or desired numerical accuracy)
Num. acc or required # samples can be evaluated before propagation
Yes
Yes
No
Revise 1st choice
No
Propagation
Propagation with fixed # samples
Satisfied with obtained accuracy?
Yes
No
Result
Increase # samples

Figure 4: Flowchart of the RaFU method.

4 APPLICATION OF THE RAFU METHOD TO UNCERTAINTY ANALYSIS OF A LBLOCA TRANSIENT (LOFT-L2-5)

4.1 Description of LOFT L2-5

The Loss-of-Fluid Test (LOFT) facility (Figure 5) simulated the major components and the system responses of a commercial PWR during a loss-of-coolant accident (LOCA). The core was a semi-scale one with an active height of 1.70m. The experimental assembly included five major subsystems which were instrumented such that system variables can be measured and recorded.The L2-5 experiment has been successfully completed on June 16, 1982 in the LOFT facility at INEL (Idaho National Engineering Laboratory). This experiment simulated a guillotine rupture of an inlet pipe in a pressurized water reactor with a true nuclear core. The experiment L2-5 was initiated, after operating the reactor at 36.0 MW for 40 effective full power hours to build up a fission decay product inventory, by opening two quick-opening blow-down valves upstream a blowdown suppression tank simulating the reactor containment behavior.

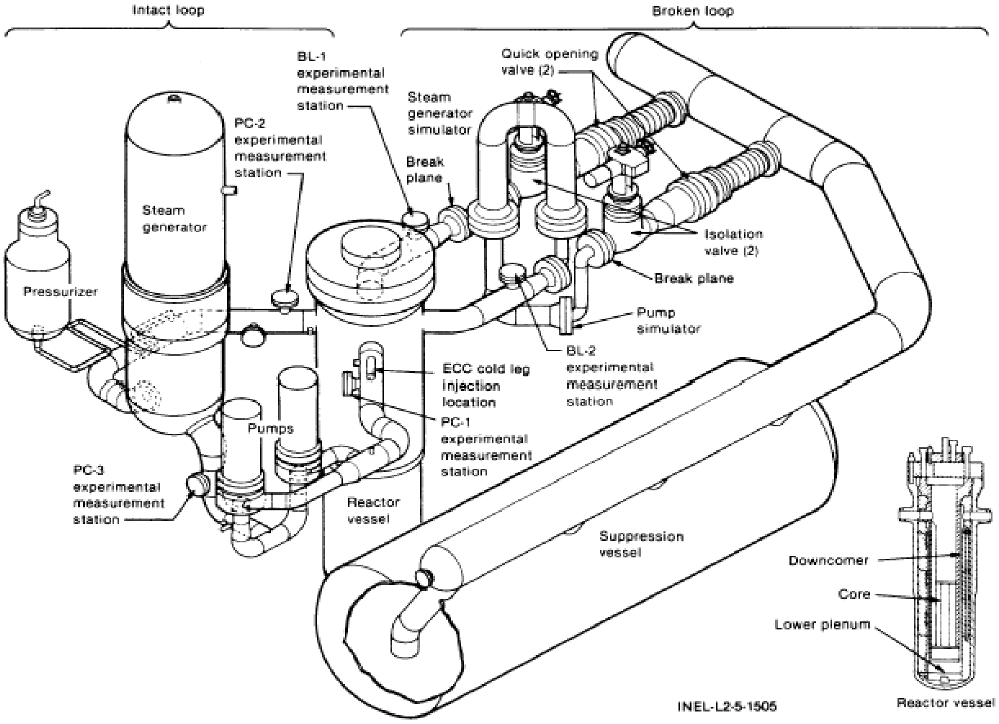

Intact loop
Broken loop
BL-1 experimental measurement station
Quick opening valve (2)
Steam generator simulator
PC-2 experimental measurement station
Break plane
Steam generator
Pressurizer
Isolation valve (2)
Break plane
Pump simulator
BL-2 experimental measurement station
ECC cold leg injection location
PC-1 experimental measurement station
Pumps
PC-3 experimental measurement station
Reactor vessel
Suppression vessel
Downcomer
Core
Lower plenum
INEL-L2-5-1505
Reactor vessel

Figure A-1. Axonometric projection of LOFT system.

Figure 5: View of the experimental LOFT system

Since the L2-5 experiment, several computations have been conducted to simulate the behavior of the LOFT system and to compare with experimental results. Among them, one can mention the OECD/CSNI program on Best Estimate Methods for Uncertainty and Sensitivity analysis (BEMUSE) whose goal is to apply uncertainty methodologies to a Large Break Loss Of Coolant Accident (LB-LOCA transient) performed on an integral test facility [9].

4.2 Uncertain parameters

After sensitivity analysis, a list of 27 uncertain parameters (Table 1) has been proposed by IRSN. Table 1 provides also the available information related to the range of variation and the nominal value associated to each parameter.

Table 1: the 27 most influential uncertain parameters identified by IRSN.

N°	Phenomenon	Nom. value	Range
1	Critical heat flux		[0,8 ; 1,2]
2	Interface to liquid heat flux - flashing		[0,05 ; 1]
3	Interface to liquid heat flux - ``Shah" correlation	1	[0,1 ; 6]
4	Interface to liquid heat flux - stratified flows	1	[0,3 ; 3]
5	Minimum stable film temperature	1	[-42 ; 60]
6	Interface to liquid heat flux - turbulences induced by injection	1	[0,3 ; 3]
7	Interface to liquid heat flux - droplet flows standard model	1	[0,3 ; 3]
8	Condensation by injection of under-saturated water	1	[0,5 ; 2]
9	Vapor wall heat flux - vaporization, Vapor wall heat flux - condensation	1	[0,5 ; 2]
10	Interfacial friction - annular flows	1	[0,5 ; 2]
11	interfacial friction - stratified flows	1	[0,5 ; 2]
12	Liquid-wall friction	1	[0,8 ; 1,9]
13	Interfacial friction downstream quench front	1	[0,29 ; 3,4]
14	Vapour-wall friction	1	[0,8 ; 1,9]
15	Interfacial friction (churn-bubble flows) in pipe geometry	1	[0,2 ; 10]
16	Interfacial friction (churn-bubble flows) in assembly geometry	1	[0,6 ; 1,8]
17	Interfacial friction (churn-bubble flows) in annular geometry	1	[0,5 ; 2]
18	Vapour-wall heat transfer (forced convection regime)	1	[0,5 ; 2]
19	Vapour-wall heat transfer (natural convection regime)	1	[0,5 ; 2]
20	Film-boiling (Berenson/Bryce) Standard model	1	[0,15 ; 6,5]
21	Interface-wall heat transfer downstream quench front	1	[0,5 ; 2]
22	Liquid-wall heat transfer (nucleate boiling) Standard model	1	[0,5 ; 2]
23	Liquid-wall heat transfer Laminar/turbulent forced convection	1	[0.8 ; 1,2]
24	Fluid-wall heat transfer (2D conduction near quench front)	1	[0,5 ; 2]
25	Droplets fall velocity	1	[0,5 ; 2]
26	Bubbles rise velocity	1	[0,4 ; 5]
27	Phases distribution coefficient in volumes	1	[0,85 ; 1,15]

If we choose a probabilistic modelization, the state of knowledge does not allow to identify an unique probability law to represent the uncertainty attached to each uncertain parameter. According to Table 1, only the support (i.e. the range of variation) and the mode (i.e. the nominal value) can be derived. Therefore, the partial probabilistic modelling of the RaFU framework turns out to well fitted to this situation. In the next section, we propose several numerical tests to illustrate the capabilities of the RaFU method. Our goal is here to show how it can provide robust margins to the assumptions related to the choice of an unique pdf in classical Monte-Carlo simulations. The question of computational cost is also fully detailed in the sequel.

4.3 Numerical tests

We focus on the uncertainty analysis of the first peak cladding temperature (PCT) of a hot rod in a hot channel. A preliminary study performed within the probabilistic framework has shown that selecting the three most influential uncertain parameters (i.e. Parameters N°12, 18 and 20 in Table 1) leads to very similar uncertainty margin estimations as in the case of 27 parameters. Therefore, we only consider in these numerical tests the 3 most influential ones. However, the RaFU method is not limited to small numbers of uncertain inputs and can be applied in higher dimension. In order to show the capability of our approach, the uncertainty attached to PCT is estimated using both probabilistic and RaFU modellings. In the first series of tests, we assume that for computational cost reason, the analyst intends to build a sample of fixed size and we compare both probabilistic and RaFU methods in term of capability to represent uncertainty according to the real state of knowledge. In the second one, we focus on the numerical treatment of the RaFU approach and show how it can drastically reduce the computational cost associated to existing methods handling both aleatory and epistemic uncertainties such as [7] and [8]. In every test, the computer code is CATHARE V2.5 mod 6.1 ([10]). The statistical treatment is performed with the software SUNSET ([11]) developed by IRSN.

4.3.1 First series of tests

Uncertainty quantification

As mentioned in Section 4.2, due to the lack of information, there exists several suitable families of pdfs to modelize the uncertainty attached to each parameter. When only the support (i.e. the range of variation) is known, an uniform probability distribution (Figure 6, left) is classically chosen: it corresponds to a minimal state of knowledge. It assumes that each value in the support is likely to be taken by the uncertain parameter. When the support and the mode (i.e. the most likely value or the nominal value in our study) are known (which is the case for many parameters of Table 1), the previous modelization does not emphasize that one particular value within the support (i.e the mode) is more likely to be taken. Therefore, analysts often switches to histogram distributions with the 50%-percentile for the nominal value (Figure 6, right). This is this last type of law that is considered in the sequel.

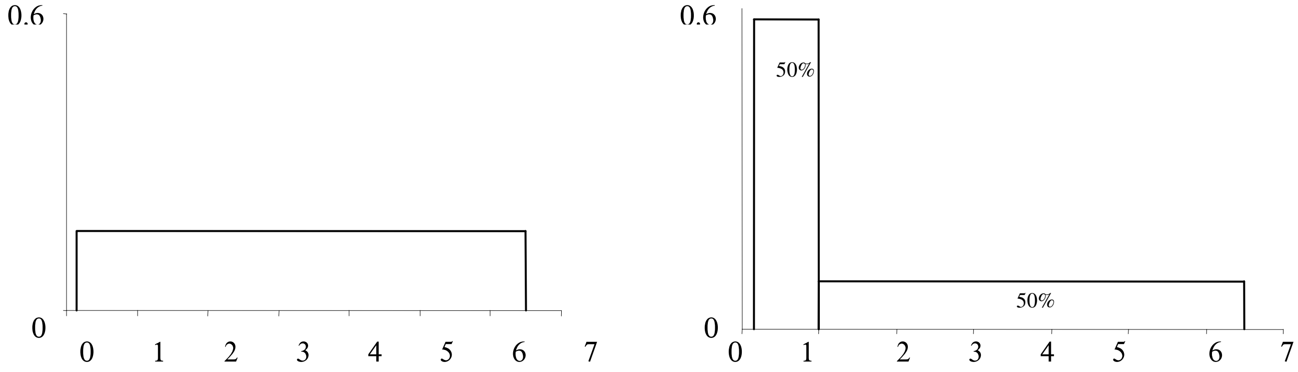


Figure 6: Uniform (Left) and Histogram (right) probability distributions.

Within the RaFU framework, each uncertain parameter follows a triangular possibility distribution (Figure 1, left). Note that the family of pdfs encoded by each triangular possibility encompasses the histogram distribution chosen in the previous modelization.

The probabilistic and RaFU modelings are compared assuming first uncertainty compensation then uncertainty accumulation. Tables 2 summarizes the uncertainty quantification.

Table 2: Uncertainty quantification.

Parameter	Probabilistic modeling (Aleatory uncertainty)	RaFU modeling (Epistemic uncertainty)
PHBO (n°20) Nom. Val.: 1, Range : [0.15 ;6.5]	Histogram probability distribution	Triangular possibility distribution
PHCFV (n°18) Nom. Val.: 1,Range: [0.5 ;2]	Histogram probability distribution	Triangular possibility distribution
P1CLx (n°12) Nom. Val.: 1, Range: [0.8 ;1.9]	Histogram probability distribution	Triangular possibility distribution

Uncertainty propagation and statistical treatment

The propagation is performed by Monte-Carlo simulations from probability distributions (probabilistic modeling) and also from possibility ones (RaFU). The statistical quantity of interest is the 95%-percentile which is the most relevant quantity to estimate in safety studies. Table 3 summarizes the 3 parameters required for the RaFU propagation.

Table 3: The three parameters of the decision step within the RaFU modeling.

γ_S	0.95	0.95
γ_E	random α-cut for each badly-known parameter within each sample (Uncertainty compensation)	α-cut identical for all badly-known parameters within each sample (Uncertainty accumulation)
γ_A	95%-accuracy #samples=200	95%-accuracy #samples=200

The numerical tests allow to derive an estimation of the 95% percentile within the probabilistic modelling and a couple of type [95%min,95%max] when choosing the RaFU approach (Figure 7). The lower (resp.upper) 95%-percentile corresponds to the "most optimistic" (resp. the "most pessimistic") choice of pdf according to the real state of knowledge.

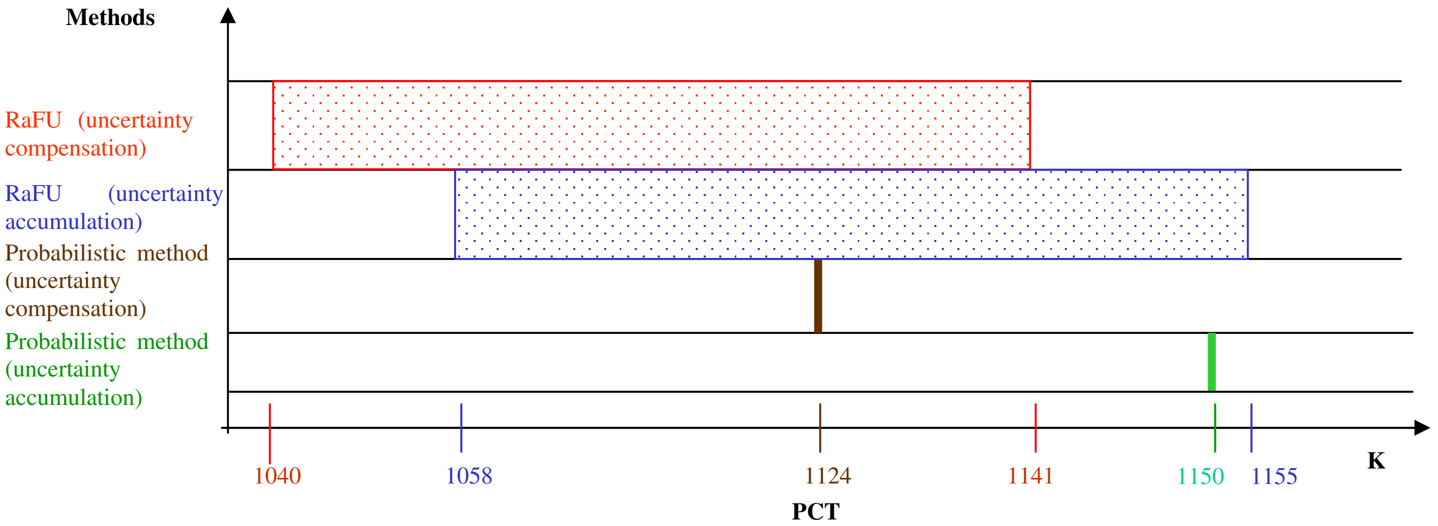


Figure 7: Estimation of the 95%-percentile with the probabilistic and the RaFU modellings.

As expected, the 95% percentile obtained with the probabilistic method is lying between the lower and upper percentiles derived from our approach as for the same assumptions about uncertainty compensation or accumulation.
This figure illustrates two main effects that need to be taken into account if a decision-making process follows the uncertainty analysis:

- Effect of the choice of pdfs: a difference of 100K on the 95%-percentile is noticeable between all pdfs with same mode and support.
- Effect of the assumptions related to compensation or accumulation of uncertainties: assuming uncertainty accumulation (which is similar to ignoring dependencies) instead of uncertainty compensation (i.e independence between parameters) leads to a difference of 30K in the estimation of the 95%-percentile.

4.3.2 Second series of tests

Contrarily to the previous section, the number of sample within the RaFU modeling is not fixed here by the user but automatically derived to reach a given accuracy (95%-accuracy on the estimation of the 95%-percentile in our case).
Table 4 provides a comparison between our methodology and the classical approaches of [7] and [8] in term of sample size. We recall that [7] and [8] assume that the whole random fuzzy variable has been built before deriving the statistical quantity of interest. This construction requires Monte-Carlo simulations for each α-cut of the possibility distributions (the number of α-cuts is set to 21 in this test, i.e α=(0,0.05,…,1)).

Table 4 : Comparison between classical methods and RaFU modeling.

Methods	Classical methods	RaFU
Baudrit et al	#sample=1239	#samples=59
Ferson and Ginzburg	#sample=1239	#samples=118

Clearly, the RaFU method, knowing the desired final quantity before propagation and exploiting relevant results from order statistics, reduces drastically the number of calculations to perform: a factor ~20 in the case of Baudrit *et al* and ~10 in the case of Ferson and Ginzburg.

5 CONCLUSION

A new approach, called the RaFU method, has been constructed and applied in this paper to uncertainty analysis in presence of incomplete knowledge. Its contruction is based on the theory of evidence framework that allows to handle both aleatory and epistemic uncertainties in order to respect the real state of knowledge. It is coupled with an optimal numerical treatment (based on an extension of Monte-Carlo simulations to the theory of evidence framework and on the introdution of a decision step before the propagation) that minimizes the required computation and allows the analyst to possibly revise her/his desires. Morever, this method offers a way to control the numerical accuracy of the result. The RaFU method has successfully been applied to the uncertainty analysis of a LBLOCA transient (LOFT-L2-5). It came out that this new approach provides robust uncertainty margins related to the assumptions about pdfs that are required within the classically probabilistic modeling. These results are less precise (i.e an interval instead of a value) but are more reliable for safety studies. The effect of pdf choices can be evaluated. Moreover, thanks to its numerical strategy, it is well fitted to uncertainty analysis of complex computer codes such as CATHARE where computer cost has to be taken into account. In the frame of the BEMUSE OECD program, it is currently tested to derive uncertainty margins for a real nuclear power plant in case of LBLOCA.

REFERENCES

[1] J.E. Gentle, Monte-Carlo Methods, volume 5, pages 612-617, in S. Kotz and N.L. Johnson editors, Encyclopedia of Statistics, John Wiley and Sons, New-York (1985).

[2] W.J. Conover, Practical Nonparametric Statistics, Wiley Series in Probability and Statistics, New-York (1999).

[3] J. Baccou, E. Chojnacki and S. Destercke, “Numerical accuracy and efficiency in the treatment of epistemical and aleatory uncertainty”, submitted to Reliability Engineering and System Safety (2008).

[4] D. Dubois, H.T. Nguyen and H. Prade, Possibility Theory, Probability and Fuzzy Sets: Misunderstandings, Bridges and Gaps, pages 343-438, Fundamentals of Fuzzy Sets, Kluwer Academic Publishers, Boston (2000).

[5] G. Shafer, A Mathematical Theory of Evidence, University Press, Princeton (1976).

[6] S. Ferson, L. Ginzburg, V. Kreinovitch, D.M. Myers and K. Sentz, “Constructing probability boxes and Dempster-Shafer structures”, Technical report, Sandia National Lab. (2003).

[7] S. Ferson and L. Ginzburg, “Different methods are needed to propagate ignorance and variability”, Reliability Engineering and System Safety, volume 54, pages 133-144 (1996).

[8] C. Baudrit, D. Guyonnet and D. Dubois, “Joint propagation and exploitation of probabilistic and possibilistic information in risk assessment”, IEEE Trans. Fuzzy Syst., volume 14, page 593-608 (2006).

[9] A. Petruzzi, F. D’Auria, J-C. Micaeli, A. De Crecy and J. Royen, “The BEMUSE programme (Best-Estimate Methods – Uncertainty and Sensitivity Evaluation ”, Proc. of the Int. Meet. On Best-Estimate Methods in Nuclear Installation Safety Analysis (BE-2004), IX, volume 1, page 225-235 (2004).

[10] B. Brun, “Current implementation and future plans on new code architecture, programming language and user interface”, Proc. of OECD/CSNI workshop on transient thermal-hydraulics and neutronic requirements, Anapolis (1996).

[11] E. Chojnacki and A. Ounsy, “Description of the IPSN method for the uncertainty and sensitivity analysis and the associated software: SUNSET”, Proc. of ASME/JSME ICONE, volume 3, page 545-550, Louisiana (1996).

TOPSAFE
Dubrovnik, Croatia, 30.09 - 3.10.2008

NUCLEAR SAFETY RISK-INFORMED DECISION MAKING

F. Mark Reinhart
International Atomic Energy Agency
Wagramer Strasse 5, P.O. Box 100, A-1400 Vienna, Austria
f.reinhart@iaea.org

ABSTRACT

The Discipline:

Nuclear Safety Risk-Informed Decision Making (RIDM) is a discipline. It involves considering, weighing, and integrating often complex inputs and insights from traditional nuclear safety engineering (deterministic) analyses, nuclear safety probabilistic analyses, operational experience, compensating or mitigating measures, or other pertinent considerations. It considers each aspect in context with each other aspect and in context with the whole. It assesses conformance to guidance or criteria. It involves assessing safety or risk. It involves a way of thinking to integrate such inputs, insights, and assessments to result in safe, sound, and optimum management or operational actions or decisions.

The international nuclear community increasingly recognizes and emphasizes that probabilistic safety assessment (PSA) and other nuclear safety risk evaluations provide extremely valuable complementary insight, perspective, comprehension, and balance to deterministic safety assessment (DSA) of nuclear installations.

The Guidance:

Accordingly, there is a need to establish international standards for RIDM. The International Atomic Energy Agency is working to fulfill such need through its international Safety Standards. One of such standards, the developing high level RIDM Safety Guide and its implementation program will provide guidance to Member States on how to adequately and responsibly establish an infrastructure to perform, document, report, track the results of, and to follow-up on RIDM.

There is good consensus for the RIDM Safety Guide among the 35 delegates from the 18 Member States, the OECD/NEA, and the IAEA who have contributed to it. The delegates represent nuclear regulators, nuclear power plants (NPP), and nuclear safety support organizations. RIDM continues to be a critical aspect for nuclear safety in mature and maturing Member States. In parallel, there is a need to transfer that discipline to Member States which are emerging into the nuclear energy technology arena.

The Implementation:

A number of Member States, their regulators and NPPs, have expressed interest in being pilots for the RIDM Safety Guide and its implementation program. Similarly, it will be important to assist other Member States. Accordingly, the IAEA, in the implementation program, is pursuing a service to assess organizational culture, to implement RIDM, and to implement specific RIDM applications. This service will include progressive training as well as independent audits and coaching of Member States' progress and success.

1 INTRODUCTION

While many individuals, organizations, and nations appreciate, support, and use RIDM, there appears to be a genuine need for continued safety culture enrichment with respect to RIDM and its benefits within the international nuclear community. This enrichment would especially benefit that part of the community not routinely involved in RIDM. As with any cultural development, safety culture enrichment involves change. Culture change requires first a recognition of a need and then time and effort to satisfy the need. A critical aspect for culture enrichment is vision. A nation, national organization, or private organization needs to see and appreciate the end point of such enrichment in order to build consensus in the correct direction.

During an organizational culture survey of a nuclear engineering staff at an internationally respected organization, one engineer offered a very significant comment. He said that while he appreciated that RIDM key elements were to be integrated, he did not know how his deterministic work could really contribute, and he did not know how to accomplish integrating it with risk assessment. Another individual expressed that he felt that when risk considerations entered the picture, they took precedence over deterministic considerations. It appears as if such perspectives are not isolated, and some national regulators, NPPs, or support organizations remain cautious about the value of RIDM. However, such perspectives appear to be in the minority, and they become more favourable toward RIDM following a genuine and mutual interchange of information.

Because of this awareness, the IAEA is working to provide informative guidance and appropriate support through programs, assessment missions, and information access.

2 DISCIPLINE

RIDM is a discipline. It starts with a need, an issue or situation for which a decision is required. It involves considering, weighing, and integrating often complex inputs and insights from deterministic analyses, probabilistic analyses, operational experience, compensating or mitigating measures, or other pertinent considerations. It considers each aspect in context with each other aspect and in context with the whole. It assesses conformance to guidance or criteria. It involves assessing safety or risk. It involvs a way of thinking to integrate such inputs, insights, and assessments to result in safe, sound, and optimum management or operational actions or decisions. The discipline, while having static aspects, is fundamentally dynamic or fluid and is sensitive to responsible long term and near term feedback; it is ongoing. Responsible feedback can and should influence management or operational decisions or actions, previous decisions or actions, or the implementation of the discipline itself. Key elements of RIDM and their interrelationships are depicted in Figure 1 below.

Figure 1 shows broadly the considerations to be integrated and evaluated given a need (the yellow box) for which a decision is needed. The figure shows each of the RIDM Key Elements—Defenes-in-Depth, Safety Margins, Risk Assessment, Performance Monitoring, and Regulatory Compliance—to be considered (the blue boxes), and it shows that each Key Element has an impact on and is impacted by each of the other Key Elements (the green and orange lines). Next the Figure shows that the integrated output from the Key Elements is evaluated with respect to its impact on deterministic and probabilstic insights, considerations, guidance, or criteria. Finally the Figure indicates that the insights from such disciplined thinking are focused to reach a decision.

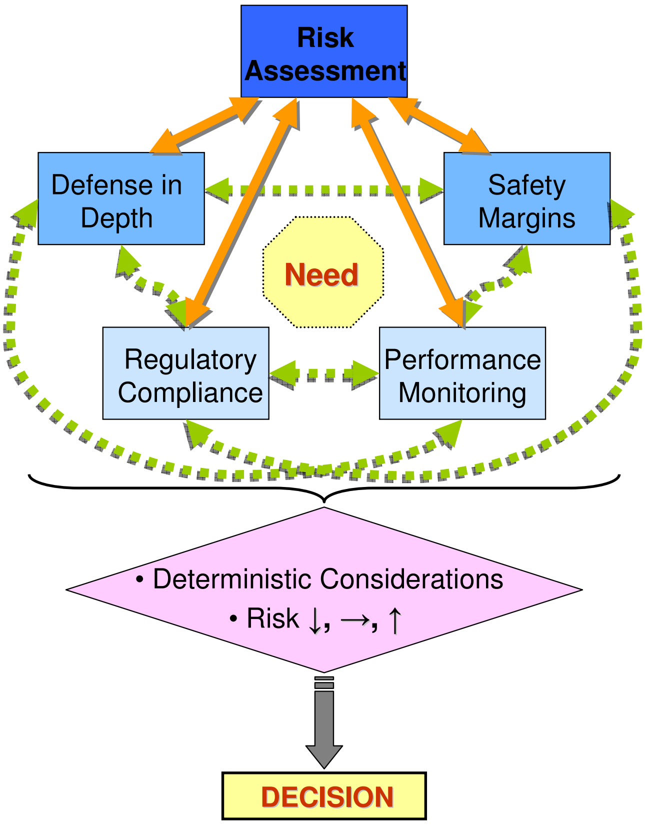


Figure 1: Key Elements of Risk-Informed Decision Making

RIDM is a progressively developing discipline. Experience indicates that it is effective in refining and improving safe operations of nuclear installations. It has also proved to be effective in providing an appropriate balance among operational, maintenance, and design strategies and decisions.

3 GUIDANCE

The IAEA provides high level guidance through its three tier Safety Standards Series documents. The three tiers are fundamentals, requirements, and guides. In support of RIDM, the IAEA is working on four documents: One is a draft requirements document, *Safety Assessment for Facilities and Activities* [1]. Three are draft Safety Guides: Risk *Informed Decision Making* [2], *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants* [3], and *Development and Application of Level 2, Probabilistic Safety Assessment for Nuclear Power Plants* [4].

Associated with the IAEA Safety Standards Series documents, an overall assessment mission document, the RIDM-International Review (RIDM-IR), is in preparation.

Recently, the WWER Regulators Forum PSA Working Group, representing nine nations, emphasized that the international nuclear community increasingly wants to and needs to look to IAEA guidance. Accordingly it encouraged the IAEA management to continue to support the issuance of the RIDM Safety Guide and its associated implementation program. Similarly it encouraged the management to support the issuance of the Safety Guides on PSA, Level 1 and Level 2. These documents and program are viewed as very important.

In addition to IAEA guidance, each nation or organization implementing RIDM should have its own high level guidance. Such guidance may be based on IAEA guidance;

however, it should include and conform to national or organizational vision, principles, policies, and regulations.

4 PROGRAM

As mentioned above, each nation or organization implementing RIDM needs programmatic controls. The highest level in the hierarchy of programmatic controls should be a detailed upper tier description of RIDM, principles involved, and national policies and requirements. Under this upper tier document, there should be more detailed guidance. The IAEA Requirements document and Safety Guides mentioned above could provide a solid foundation for this program.

Lower level program elements should provide for development, review, approval, control, maintenance, revision, and security of RIDM tools. Included among such tools is software. The software includes probabilistic safety assessment (PSA) programs, installation-specific PSA models, Configuration Risk Analyzers (CRA) [also knows as a Risk Monitors, Safety Monitors, etc.], and deterministic safety assessment codes. Also included among such tools is the associated computer hardware. The program should provide controls to assure that the various models and codes analyze the actual installation configuration (real time) or the actual configuration under consideration. The program should also control access to the tools, their inputs, and their outputs.

The program should provide for personnel training and qualification in several categories as follows:

- Personnel who work directly with the tools, their inputs, and their outputs.
- Personnel who access and directly use the analytical outputs and results.
- Personnel who are not directly involved in the analytical outputs and results but who receive such outputs and insights to make recommendations or decisions.
- Management.

The program should provide for the development, review, approval, distribution, control, and use of procedures for specific program aspects.

A very important set of procedures would be for specific RIDM applications. Each application should be implemented through a specific procedure or set of related procedures. Current applications are shown in Table 1 below, and additional applications continue to emerge. While almost all RIDM applications are currently at nuclear power plants (NPP), a number of non-NPP applications appear to be under consideration.

Table 1: RIDM Applications

Nuclear Power Plants	**Configuration Management**
Plant Vulnerability Assessment	Configuration Risk Analyzer (CRA)
Design & Design Review	Technical Specifications
Plant Improvement	Maintenance & Outage Planning, Assessment, and Management
Program Improvement	**Regulatory**
In-Service Inspection	Regulation Development
In-Service Testing	Licensing
Quality Assurance	Inspection Planning
Special Treatment	Significance Determination
Security	Events Assessment
Training	Emerging Issues

A very significant part of the RIDM program should be an ongoing enrichment of the organizational culture. While some uses of the concept of culture address, for example, "safety culture," an organizational culture has actually many aspects. Accordingly, in this context, organizational culture includes operational culture, safety culture, risk culture, security culture, management culture, etc.

With respect to merging RIDM into an existing culture, the organization should develop a perspective of what the desired "target culture" should be. Then the organization should have an evaluation of the existing culture. The evaluation should identify gaps between the existing culture and the target culture. Next the organization should develop and implement a plan to achieve the target culture. Such assessment and refinement should be performed or at least considered periodically. The goal, the target culture, of such efforts should be to help all levels of personnel—management and staff—to appreciate and respect the relative benefits, strengths, weaknesses, limitations, boundary conditions, and cautions of RIDM.

This cultural enrichment is critical for RIDM to succeed. RIDM has proved to be very beneficial to organizations in which the organizational culture fully understands the discipline, approach, and implementation.

5 SUPPORT & IMPLEMENTATION

Deterministic safety analyses as well as probabilistic safety analyses use calculations. Such calculations require the best available information: inputs, assumptions, boundary conditions, etc. One significant input is statistical data; e.g., initiating event frequencies; structure, system, and component failure probabilities; common cause failure probabilities; human error probabilities; etc.

The more applicable data that is available for statistical analyses, the more uncertainties can be understood and reduced. Accordingly, the IAEA is pursuing an approach to make international PSA and RIDM data, insights, references, and related information available through the secure IAEA Centre for Advanced Safety Assessment Tools (CASAT). Such information may be accumulated directly in data bases or it may be linked through the internet.

As mentioned above, a significant tool to independently assess an organization's culture, program, and procedures to use RIDM is the RIDM-IR mission to be offered to Member States by the IAEA. In an RIDM-IR mission, a team of international experts would review a nation's policies and regulations and the organization's culture, programs, and procedures with respect to the guidance mentioned above and with respect to experience with other similar organizations' use of RIDM. Accordingly, the team would provide valuable constrictive comments for additional development and enrichment.

Based on the guidance mentioned above and accumulated experience, the IAEA intends to offer national, regional, and international workshops and other forums to build RIDM capacity. A key feature of such events would be an exercise to get the participants involved and to facilitate disciplined thinking.

Finally, a number of IAEA Member States have initiated or formally requested to be pilots to implement the RIDM program and further build their related capacity. A number of other Member States have orally expressed interest in being pilots or in having assistance to implement and enhance RIDM.

The IAEA intends to support this interest, to analyze experience from the above activities, to distil lessons learned and insights, and to make the lessons learned and insights available on the CASAT.

6 SELECTED INSIGHTS

To provide a flavour of RIDM good practices and insights discussed through various RIDM discussions at meetings, seminars, or actual RIDM applications, the following selected insights are provided.

Some nations strive to achieve risk “As Low As Reasonably Achievable” (ALARA) through cost effective measures. They focus more on insights than numerical results. Numerical results provide ranking insights, but absolute numerical results are not the primary focus.

One nation offered that it realizes improvements by implementing RIDM applications as a whole rather than implementing them item by item in a stand alone fashion. Such holistic application provides enhancements to procedures, overall infrastructure, and safety and risk culture.

The consensus of a significant discussion on “safety” and “risk follows: For RIDM to optimize decisions does not require that a decision maker be able, in an absolute sense, to maximize safety and minimize risk. In an absolute sense, to minimize the risk of using nuclear engineering technology — as would be true for most technology — would be to not use the technology at all. In a realistic sense, RIDM balances a spectrum of insights and inputs integrated with risk information to strive for an optimum and safe decision. Such inputs and insights would be from deterministic safety assessment, compensatory measures, mitigating measures, operational experience, probabilistic safety assessment, etc. While RIDM has the potential to offer cost effective options, economic considerations would not take precedence over safety considerations.

Definitions used in PSA can vary among PSAs and can be ambiguous. Terms for hardware, for dependencies, and terms used in the PSAs, per se, differ; e.g., initiating event, safe state, core damage. There are some definite differences in the initiating event frequencies used among similar NPPs. A goal is to have harmonious definitions internationally.

7 CONCLUSION

As discussed, the value of RIDM has been increasingly recognized in the international nuclear community for a number of years. Additionally, nations developing nuclear engineering technology programs and nations emerging into that arena are recognizing the value and potential of RIDM. At the same time, nations, organizations, and individuals express genuine concerns and cautions that need to be satisfied. Establishing a solid RIDM infrastructure and developing a conforming and supportive organizational culture are keys to allowing all members of the international nuclear community to increasingly benefit from this valuable discipline.

REFERENCES

[1] Draft Safety Requirement DS 348, Safety Assessment for Facilities and Activities, IAEA, Vienna

[2] Draft Safety Guide DS 365, Risk Informed Decision Making, IAEA, Vienna

[3] Draft Safety Guide DS 394, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA, Vienna

[4] Draft Safety Guide DS 393, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA, Vienna

TOPSAFE
Dubrovnik, Croatia, 1 - 3 October 2008
International Topical Meeting on Safety of Nuclear Installations

Current Trend in Nuclear Safety in Belgium

Ray Ashley
AVN
Rue Walcourt, 148 B-1070 Brussels, Belgium
ray.ashley@avn.be

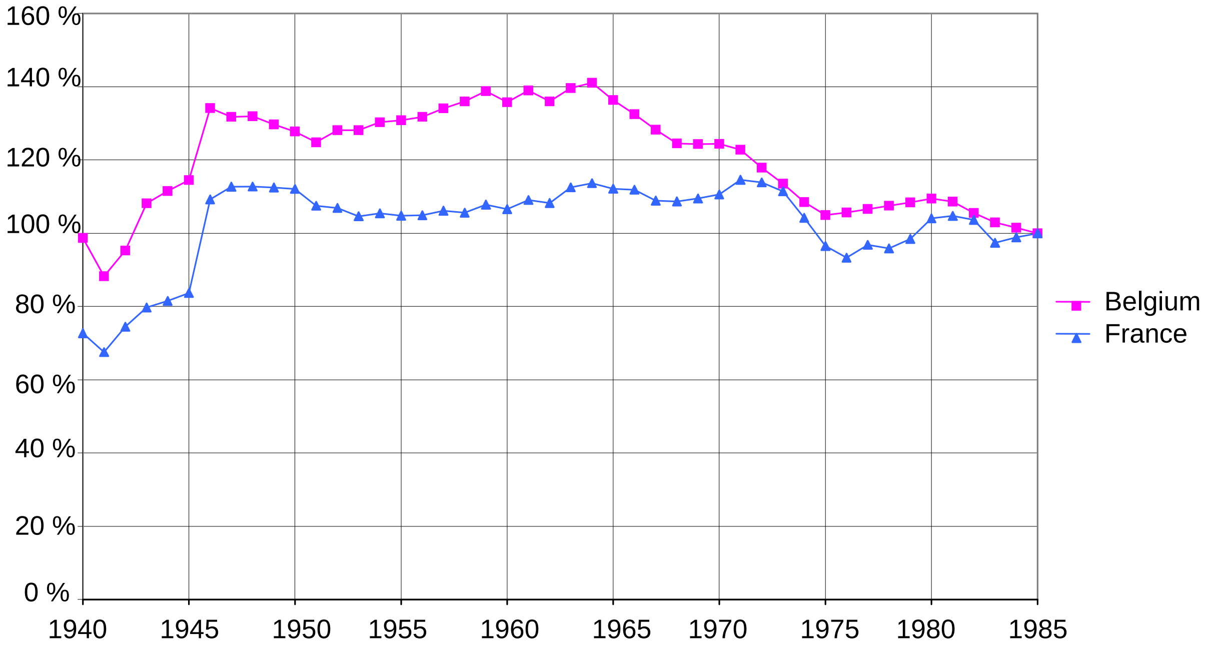
ABSTRACT

Nuclear phase out is legally in force in Belgium for the time being. The electricity demand kept however increasing and alternative power sources alone will not be able to match the difference between the offer and the demand. As a consequence, most of the Belgian nuclear power plants (NPPs) underwent a power uprating process these last years. In Belgium, the NPPs must be re-assessed each ten years to demonstrate that the level of safety is at least maintained throughout the years and that the plant can safely operate for the ten years to come. Amongst other decennial activities, this led us to set up and run a complete aging management program adapted to each NPP. The power uprates by themselves gave rise to extra concerns in terms of system solicitations and capacities and safety analyses. Extra concerns require extra resources but Belgium, alike other nuclearized countries, is facing a shortage of experimented human resources. Hence, there is a need for improving the efficiency of the nuclear safety activities and for enhancing the implementation of the safety culture in the operation of the nuclear sites, be it power reactors or other facilities. This paper presents the high-level top-down approach that has been proposed in order to streamline the training in safety culture and the operational safety efforts, pinpointing particular benefits of the method.

1 INTRODUCTION

The global decline of manpower resources is inescapable in Western Europe as a consequence of the post-World War II baby-boom leading to the current pappy-boom effect. To illustrate this, let's have a look at Figure 1 showing the birthrate curves in Belgium and in France for the period ranging from 1940 to 1985 (source: ref.[1]). People born after 1985 are not likely to be of help as nuclear safety expert this year; this is the rationale for the end of the graphic at the one hand. At the other hand, 100 % has been chosen as reference for the birthrate that year in order for the numbers to be comparable for the two countries.

Figure 1: Evolution of the birthrates (1940-1985)

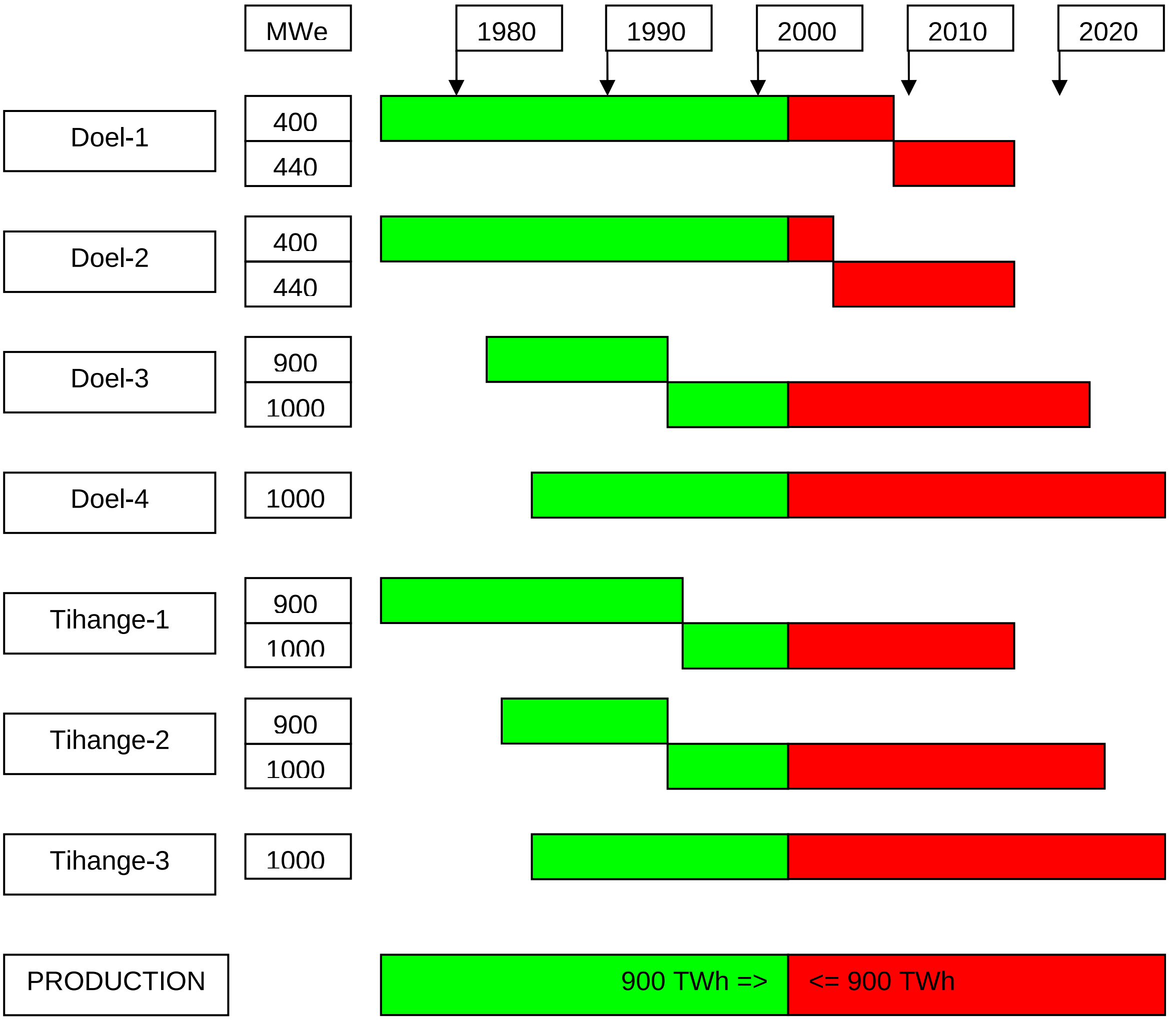


As you may see, the baby-boom clearly appears in 1946 with an echo 18 years later coupled with a golden-sixties effect. After that there is a decrease by 40% in Belgium to reach the situation in 1985. This means that all the jobs created by the baby-boomers since 1965 will hardly find successors after those will retire. This is not specific to the nuclear safety sector but it shows that any shortage in human resources for a particular sector will hardly benefit from resources released by another sector.

In Belgium the situation worsened when the Government stated in 2002 the close-down of the nuclear power plants after 40 years operation. Figure 2 shows the status of the nuclear electricity production at that time. Based on a 40-year lifetime for each plant, this decision intervened roughly when 50% of the installed capacity had been used. The last plants were connected to the grid in 1985 so they had still about 60% of their capacity to be produced over the next 23 years, which is about one generation time. To cope with this situation, fresh human resources are needed.

Now, imagine the dilemma for the students in the engineering schools who were decided to go for nuclear engineering when they hear about the limited future of the nuclear power plants in Belgium! Most of them reoriented their options for other sectors, thereby increasing further the gap between needed and available resources for the specific sector of nuclear safety. This explains why there is an urgent need for enhancing the working methods in the field of nuclear safety in Belgium.

Figure 2: Electricity production before and after the phasing-out decision



2 KEEPING SAFE WITH LESS RESOURCES

Considering the usual steps of a project development one could classify the successive activities in a standard format where following phases appear:

- information to be gathered
- objectives to be set
- tasks definition
- project development
- implementation of the outcomes
- verification & validation
- start-up & operation

Let’s examine each of those phases in the context of a nuclear safety project.

2.1 Information

This phase is very crucial. It requires gathering information both about the status of the plant and about the applicable regulations and reference documents. Any shortcoming or wrong ranking of this kind of information might lead to improper orientation of the project. It is therefore a good candidate for improvement action in the light of previous experiences.

2.2 Objectives

Based on the current plant and safety cases documentation status on the one hand and the goals to be reached at the other hand, clear objectives should be set. Any ambiguity, lack of precision or shortcoming might have a disastrous effect on the process. A thorough review of this phase is therefore greatly advised.

2.3 Tasks

The next step concerns the translation of the objectives into a specific set of tasks. Once more one must ensured that the process is complete and well documented. A good documentation will allow the right introduction of holding points and/or monitoring actions that will have to be conclusive when applied during the next phases

2.4 Development

By far the most resources-demanding phase, it will be the largest beneficiary of the efforts invested in the previous phases through a precise definition of the required objectives to be achieved and an optimized fit of the tasks associated to each objective.

2.5 Implementation

This phase will benefit of the holding points and monitoring actions set forth during the task definition phase. Any deviation against the foreseen progress will be identified in due time so that appropriate corrective actions may be initiated to redirect a correct implementation.

2.6 Verification

The verification phase will include a check of the fulfillment of the objectives as they have been defined in the “Objectives” phase. In case of failure, the good documentation of the process should help to identify the root cause of the discrepancy – be it at the task definition level or in the course of the project development – allowing efficient corrections to be easily designed.

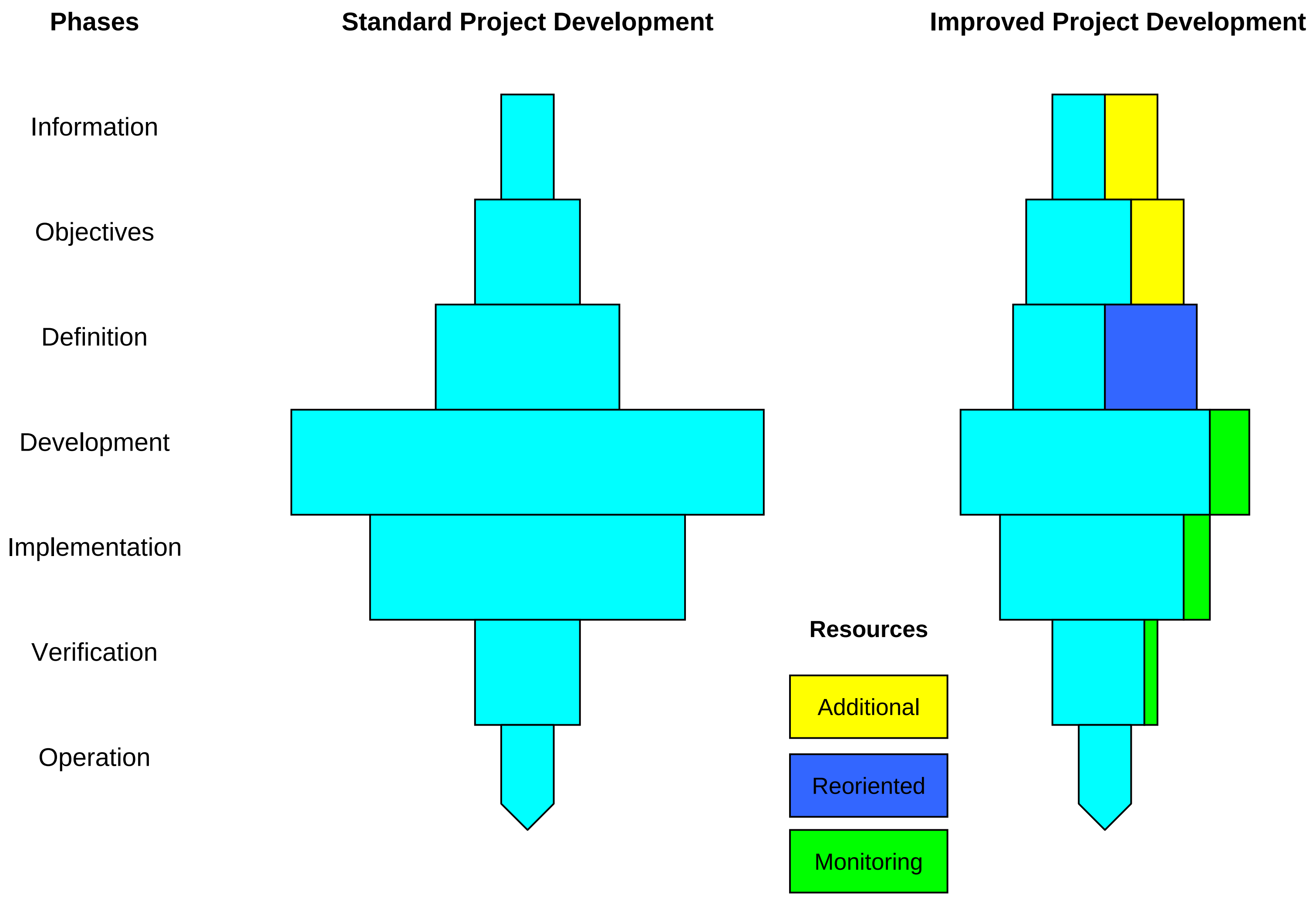
2.7 Operation

This last phase should not be impacted by the improved project development process as the aim of the improvement was to reach the same final goal but with a global reduced amount of manpower involved in the project.

2.8 Global evaluation of the needed resources

Enhancing the care for project definition through its precise positioning in the overall safety management process, and close monitoring of its development will lead to an improved efficiency of the whole process as illustrated by Figure 3.

Figure 3 : Resources involved in the projects



3 APPLICATION TO DECENNIAL SAFETY REVIEW

Decennial safety reviews are imposed by the Royal Decree for Authorization issued for each nuclear power plant (NPP) in Belgium. The purpose is to reassess the safety of the plant taking into account the evolution of the international regulatory context as well as the evolution of the knowledge databases including the experience feedback with the aim of ensuring the safety of the NPP for at least ten more years. Because of this provision, the lifetime of the Belgian NPPs has never been technically fixed and hence the concept of life extension does not apply.

The outcomes of the decennial safety reviews may nevertheless lead to the necessity of replacing equipments, even large ones such as a vessel head for instance or the need for setting up monitoring programs as for the follow-up of the ageing related degradation mechanisms.

3.1 Information

Since the last decennial safety review, new applicable reference documents have been issued: the IAEA issued the Safety Guide NS-G-2.10 “Periodic Safety Review of Nuclear Power Plants” and WENRA published its reference levels for NPPs. The ranking came in favour of the IAEA document because it was the better adapted to existing plants but the WENRA reference levels were kept in mind for the quantification of some proposals for modifications. This was an improvement versus the subject list of the previous decennial safety reviews where both the Utilities and the Authorized Body set up separate lists that were finally assembled in a common list of concerns that was approved by the Federal Agency for Nuclear Control.

3.2 Objectives

Although the objectives were clearly to ensure an acceptable treatment of all the issues listed in the Safety Guide, it was agreed that the scope of the safety review itself would be, when applicable, limited to the validation of the processes that were to be put in place and to the verification of the outcomes of the existing processes, for instance the ageing management program initiated during the previous decennial safety review.

This will allow the safety review project to be completed in a reasonable time schedule, say two or three years. The previous decennial safety reviews included the evaluation of the outcomes of such processes what imposed to keep the project teams alive a long period of time and delayed the official closure of the safety review.

3.3 Tasks

A special attention is to be paid to the final issue raised by the Safety Guide: the global assessment. This task aims at verifying the completeness and the consistency of the outcomes of the whole set of the tasks. To avoid findings about incompleteness or inconsistency late in the course of the project, holding points are included in the schedules of the tasks. They are designed to allow pinpointing any indication that the global assessment could reveal incompleteness or inconsistency when performed at the end of the project. Early corrections will minimize time losses should such indication appear.

3.4 Development

The development phase is presently on-going and proceeds in line with the monitoring actions have been programmed.

3.5 Implementation, verification and operation

These phases are not yet activated at the time this paper is being written. Updated information will be given during the topical meeting.

3.6 Global assessment

As this exercise has been anticipated along the tasks of the project, it is expected that the outcome will be satisfying without demanding any extra resource.

4 CONCLUSION

Keeping the nuclear safety level as high as reasonably achievable is no more a question of the amount of money one could spend but a question of the amount of experimented manpower available to optimize the safety management.

In line with the development of quality system, efficient use of the available expertise requires enhanced efforts for the definition of nuclear safety projects with a view of its final global assessment in order to streamline and monitor the subsequent development phases.

The most important benefits of the method described above are twofold. First, the enhanced efforts, devoted to enlarge the scope of the contextual information to be gathered, allow adjusting the definition of a project to what it should really produce in terms of safety. Second, the verification process and its hold points are designed with a special attention paid to the final impact of the outcomes of the project upon the global safety of the unit. This makes sure that the project will be effective and that it will be performed in accordance with an appropriate efficient method.

To present it shortly, one could summarize the spirit of the approach as being THE "Think High Early".

ACKNOWLEDGMENTS

The author gratefully acknowledges the support received from Mr. Pierre BRIEGLEB (with Bel V), project leader of the current decennial safety review, in sharing his experience of the application of the method described in this paper.

REFERENCES

[1] Demographic Yearbooks, United Nations Statistics Division

[2] "Periodic Safety Review of Nuclear Power Plants", Nuclear Safety Guide NS-G-2.10, IAEA Safety Standards Series, Vienna - 2003

European Nuclear Society

Rue Belliard 65
1040 Brussels
Belgium
Telephone +32 2 505 30 54
Fax + 32 2 502 39 02

topsafe2008@euronuclear.org

www.euronuclear.org

HND

AEN
NEA

IAEA
International Atomic Energy Agency
Atoms For Peace