32nd Annual CNS Conference
Niagara Falls, Ontario, Canada, June 5-8, 2011

On the Functional Failure and Quantification of Margins

Dumitru Serghiuta
Canadian Nuclear Safety Commission
Dumitru.Serghiuta@cnsc-ccsn.gc.ca

Abstract

Recent NPPs operating experience shows that in some cases operational and design modifications may lead the plant far away from the original design. Aging and operating life extension, power uprates, new fuel designs with increased performance, such as increased burnup, and R&D discovery issues, as well as cumulative effects of simultaneous or subsequent design changes in a plant, which can be larger than the accumulation of the individual effects of each change, can challenge original safety margins while fulfilling all the regulatory requirements. The aspects related to margin quantification have received a considerable amount of attention from utilities, designers, methodology practitioners, and regulators, due to the significant impact on operation and the need to better evaluate and understand the overall level of safety of operating plants. At the root of the debate are two questions: (1) what is an appropriate framework of criteria and limits, and methods and methodologies for quantification of margins and (2) what are the main areas for new research directions and efforts to reduce the current uncertainties for better economics and improved safety of the current reactors and requirements of the new reactors designs.
This paper reviews some of the modern approaches in treatment and quantification of uncertainties in the context of quantification of margins and potential benefits offered by the use of "functional failure" concept and application of order-statistics modern techniques in safety assessments, as well as some of main areas for R&D. It presents some observations and suggestions aimed at contributing to the debate related to quantification and qualification of margin for CANDU reactors. The views expressed in this paper are those of the author and do not necessarily reflect those of CNSC, or any part thereof.

1. Introduction

The existing nuclear power plants were designed on the basis of fundamental safety principles. Defence-in-depth is one of such fundamental safety principles, which strongly influences safety philosophies, licensing requirements, plant design and operation [1]. As a key element of the defence-in-depth principle, the design basis safety analyses are usually performed in a deterministic approach, in which a set of design basis accidents (DBAs) are analyzed [2]. An adequate selection of the analysis cases, the use of enveloping and/or conservative methods and assumptions and the selection of suitable acceptance criteria provide confidence that the plant operation will not result in unacceptable damage, even in the eventuality of abnormal occurrences in the plant. In other words, the probability of damage should be negligible even under the worst considered plant conditions, which are kept away from damage generation with

sufficient margin. This margin should cover for insufficient knowledge or uncertainties associated with the design and operation of the plants.

Recent NPPs operating experience shows that in some cases operational and design modifications may lead the plant far away from the original design. Aging and operating life extension, power uprates, new fuel designs with increased performance, such as increased burnup, and R&D discovery issues, as well as cumulative effects of simultaneous or subsequent design changes in a plant, which can be larger than the accumulation of the individual effects of each change, can challenge original safety margins, i.e., in some instances the traditional framework of safety assessment predicts erosion of margins, while fulfilling all the regulatory requirements.

One key driver of the discussion about margins, especially in the context of predictions of their erosion, as a result of aging or R&D findings, is the coverage of uncertainties. The defence-in-depth has provided the traditional ways to handle unquantified uncertainties. Employment of multiple barriers, redundancy and large design margins have been the main ways to deal with uncertainties within the defence-in-depth framework. The judgment of level of safety has been rather qualitative within the traditional defence-in-depth framework. In the traditional framework, the evaluation of safety is typically bottom-up, i.e., it starts with postulated failures and proceeds to identify their consequences. If a design basis event is judged to lead to unacceptable consequences, measures are taken either to make it less likely (without knowing quantitatively by how much) or to mitigate its potential consequences. Typically, these actions include the introduction of redundant elements and additional design margins, at the design stage, and adjustments to operating limits and conditions, including the settings of safety systems, and design modifications (retrofit) for plants in operation. These actions are based on engineering judgment informed by analyses, tests, and operating experience. The development and use of PRA has improved the safety evaluation by quantifying accident frequencies, but while the effect of redundancy and multiple barriers is quantified, that of margins is not.

A guiding principle of industry practices, as based on the defence-in-depth principle, has been the maintenance of margin between the predicted conditions to which a barrier is exposed in a bounding postulated design basis event and the acceptance criterion limit set for that barrier. In case of erosion of this margin, due to adverse impact of aging or R&D findings, preservation of this margin has typically been done at the expense of safety systems performance margins and operational flexibility.

The aspects related to margin quantification have received a considerable amount of attention from utilities, designers, methodology practitioners, regulators, and academia, due to the significant impact on operation and the need to better evaluate and understand the overall level of safety of operating plants. It has been recognised that currently used methods for safety assessments within the framework defined by traditional defence-in-depth and complemented by current PRA methodologies may not be sufficient to guarantee that enough safety margin exists. At the root of the debate are two questions: (1) what is an appropriate framework of criteria and their limits, and methods and methodologies for quantification of margins and (2) what are the

main areas for research and efforts to reduce the current uncertainties for better economics and improved safety of the current reactors and requirements of the new reactors designs.

This paper reviews the attributes of current deterministic and probabilistic approaches, some of the modern approaches in treatment and quantification of uncertainties in the context of quantification of margins and potential benefits offered by the use of "functional failure" concept and application of order-statistics modern techniques in safety assessments, as well as some main areas of R&D. It presents some observations and suggestions aimed at contributing to the debate related to quantification and qualification of margin for CANDU reactors.

2. The Need to Quantify Margins

The safety assessments are generally based on deterministic approaches complemented by probabilistic approach in order to demonstrate adequate prevention and mitigation of accidents. A conceptual two-prong approach, namely the definition of acceptance criteria limits and assurance that these are not exceeded, is what is most commonly understood as having "adequate safety margin" in the nuclear industry. Regulatory requirements provide high level guidance, but in some cases mandatory low level quantitative limits might be prescribed by regulatory requirements.

The result of safety assessments is frequently a complex set of requirements for the design and operation of the system. A facility that meets the requirements is judged "acceptable" in the sense that there is no "undue risk". What "undue risk" is remains unquantified in deterministic safety assessments. The presumption is that meeting the requirements guarantees adequate protection, i.e., the (unquantified) risk is acceptably low. The PRA complements the deterministic assessment by quantifying the risk and determining its main contributors. But, while the impact of redundancy has been explicitly modeled and quantified, safety margins are not taken into account explicitly. This makes it difficult to judge the quantitative impact of erosion in margins on plant risk.

As an example, let consider an increase in the calculated fuel enthalpy in a CANDU postulated large LOCA simulation due to more accurate representation of core neutronic response to voiding conditions. This leads to a decrease in the margin. As long as the calculated value is below the limit in Safety Analysis Report, the change seems acceptable. The judgement of the actual impact on plant risk is difficult, however, because the current PRA models are not able to predict the increase in probability of failure due to a reduction in margins.

Many other similar examples can be given for relatively higher frequency events, such as slow loss of regulation, loss of flow, and small LOCA, for which the adverse impact of aging on Critical Channel Power leads to calculated reduced margins to dryout or even exceedance of dryout criterion.

To make risk-informed, technically sound, decisions and avoid imposing unnecessary conservatism on plant operation it is important to be able to quantify the margins and to evaluate their impact on the plant risk.

3. Attributes of Current Deterministic and Probabilistic Assessments

In the so-called *deterministic* methodology whose results (in the internationally recommended practices, [2, 3]) are summarized in the chapter 15 of the Final Safety Analysis Report, a set of design basis events (DBE) which trigger challenging transients are selected and grouped in different frequency classes (called *Conditions*). In the classification of ANSI- 51.1/ANSI-N18.2, normal operation manoeuvres are classified as *Condition I*. The *Condition II* groups events such that any of them may occur during a calendar year. *Condition III* includes events any of which may occur during the plant life. Finally, *Condition IV* events are very unlikely events that, due to the potential severity of their consequences, give rise to specifically designed automatic protections. This classification shows that even in the chapter 15 analysis (very often considered as the paradigm of the *deterministic* analyses) there are some *probabilistic* elements.

The design basis events (DBE) (and the subsequent design basis transients (DBT)) take their name from the fact that they are used to **design** the automatic protections. A **necessary** condition for a plant to be safe is that, for any anticipated or postulated event, there is at least a protective function able to prevent unacceptable damage.

The design of automatic protections is a very practical problem with very complex solutions. Because of that, the automatic protections cannot be designed to cope with any possible situation since this would lead to an endless design process. Real life, therefore, does not always fit into design assumptions and some plant transients may go beyond the design basis envelope, i.e. they cannot be represented by any design basis transient. There are a number of reasons that could lead to this situation, among possibly others, [9, 18]:

- The initiating event occurs from initial conditions not considered in the selection of the design basis events.
- There are concurrent “initiating” events, either simultaneous or subsequent.
- There is more than one failure additional to the initiating event, and the protective function does not work or fails to arrest the transient.
- Human intervention takes the evolution of the transient away from the design conditions.

The *probabilistic* analysis was developed to deal with these situations. While in deterministic analysis the actuation of the protective functions is assumed, in the probabilistic analysis the protections are assumed to fail with some probability.

A summary comparison of objectives and characteristics of the two approaches is presented in the Table 1, based on the discussion in [8, 9].

Table 1. Main Attributes of Deterministic and Probabilistic Approaches (based on Reference 9)

Deterministic Assessment		**Probabilistic Assessment**	
Objective: To Answer	Main Characteristics	Objective: To Answer	Main Characteristics
What is unacceptable damage?	Any (initiating) event can be classified in a *Condition* or frequency class, or in a residual group of "beyond design basis events".	What are the possible evolutions of the situation?	Any sequence included in the analysis is classified from the damage point of view as "success" or "core damage".
How can it be assured that the unacceptable damage is prevented?	The *probabilistic* elements of the analysis are addressed by implicit or explicit assumptions but no probability calculation is performed.	How often could they occur?	In general, damage is not calculated. Instead, its estimation is derived from the header combination in the sequence. Supporting or confirmatory calculations are sometimes performed but in most cases they are not a cornerstone of the method.
Is there a protective function for every transient?	From the point of view of the subsequent evolution, any event in the design basis region can be classified in a class whose representative is a design basis event.	How much damage can be expected from each evolution?	Any possible plant transient should be covered by the set of sequences of the *probabilistic* analysis. However, the identification of a transient with a single sequence will, in general, be difficult to do. A frequent case is that different parts of the transient are represented by different parts of sequences in the analysis.
	A design basis transient usually consists of an initiating event (design basis event) that triggers a single protective function able to terminate the transient while preventing unacceptable damage.		An event tree consists of an initiating event, defined from given initial conditions, and all the realistically possible combinations of success/failure of the involved protective functions.
	The damage associated to a design basis transient must be a bound of the damage of any transient included in its class. This bounding damage (or its corresponding bounding value of the safety variable) is calculated with more or less detailed simulation models.		The frequency of each sequence in the tree is calculated from the frequency of the initiator, detailed logical models of protection failures and basic probability data. Since each sequence is actually a representative of a group, its frequency should be at least equal to the collective frequency of the transients included in the group.
	The concept of unacceptable damage can be precisely defined for each frequency class.		It would be possible to define an "acceptable core damage frequency limit". However, the lack of homogeneity among the *probabilistic* models used by different analysts in different plants does not allow implementing this concept. Instead, the core damage frequency (CDF) obtained for each plant by the PSA analysis is taken as a reference value for later re-evaluations.

There are many analogies and some differences between the *deterministic* and the *probabilistic* approaches; however, both aim at describing the level of safety.

The analogies can be derived from the similarity between event trees and design basis transients. Both are representations of the evolution that follows an initiating event, and in both cases a frequency is assigned to the initiating event. Moreover, both of them are enveloping representatives of groups of evolutions with common characteristics. A design basis transient is essentially a particular case of event tree with a single header whose corresponding failure branch has been truncated by low frequency. As a result, the frequency of the only sequence resulting from a design basis event (i.e. the frequency of the design basis transient) is equal to the frequency of that event, while in the general case the frequency of a sequence is the product of the initiating event frequency and the probability of the header combination. Also, the design basis transients can be viewed as particular sequences in a complete set of event trees.

The differences are mainly related with the assumptions of the protection actuation and with the primary objective of the analysis:

- In a design basis transient the actuation of the protection is assumed because the focus is on the higher frequency ranges. Protection failures are expected to be of low probability and they are considered only in the *probabilistic* analysis that focuses on low frequencies.
- The evaluation of a design basis transient is the determination of an amount of damage while the evaluation of an event tree consists of the determination of a frequency, namely, its contribution to the core damage frequency.

A common argument used when comparing *probabilistic* and *deterministic* analysis methods is that the former are more realistic while the latter are too conservative. As argued in [9], this is a false controversy because of the following reasons:

- Both methods are based on the use of envelopes, and this is an intrinsic characteristic of any safety analysis. The degree of conservatism contained in the models and assumptions of the analyses results in a different “distance” between *reality* and *envelope*, i.e. different size of the safety margins. Both methods try to reduce unneeded conservatism but in any case the enveloping character of the analysis must be guaranteed.
- Concerning frequency calculations, the *probabilistic* analyses are much more detailed, but the methods to obtain input data are, still, plenty of bounding assumptions. They are, perhaps, more realistic than the estimation of frequencies made in the *deterministic* case, but it is because the objective is to find an envelope rather than to describe the reality.

With respect to damage calculations, the *deterministic* analyses have been more detailed and, despite the use of more or less conservative models and assumptions, a calculated result appears likely more realistic than an estimation based on the pure combination of event tree headers. However, the objective, again, is not realism but safety.

Usually, a frequency boundary between "design basis" and "beyond design basis" domains is defined. The "design basis" domain would correspond to the high frequency region, while the "beyond design basis" would correspond to the low frequency region. The region of high frequency has been the application field of the *deterministic* analysis.

Analogously, there is a damage boundary between "success" and "damage" regions in probabilistic analysis. The application field of the *probabilistic* analysis has been the "damage" region.

One condition to avoid contradictions between *deterministic* and *probabilistic* methods would be that both application areas must not overlap, [9]. In other words, the frequency limit for "Core damage" must be lower than or equal to the "design basis" boundary and the damage limit for the higher *Condition or Class* category must be lower than or equal to the "PSA-damage" boundary. The case of equality in these conditions would guarantee the completeness of the safety analysis.

The separation of the respective scopes of the methods does not imply either that there is no interaction between them. The separation is only possible because each method implements assumptions based on the existence and particular characteristics of the other.

Any change in the models or inputs associated to a safety analysis method, may alter the validity of some models or assumptions of the other method. For example, a change in the setpoint of some protective function primarily affects the *deterministic* analysis; however, that change might also have the effect of changing the protective function to be requested in a particular situation, which affects the delineation of some event trees in the *probabilistic* analysis. Similarly, any change that affects the failure probability of a protective function in the *probabilistic* analysis (such as a change in a surveillance test interval) could invalidate the assumption that any failure sequence in the *deterministic* analysis can be ignored because of its negligible contribution to the safety envelope.

From a different perspective, both deterministic and probabilistic approaches try to answer the Kaplan and Garrick's basic "risk analysis" questions, [12], but in different ways. These are summarized in the following Table 2. It is, therefore, reasonable to assume that eventually the two approaches would converge into an integrated deterministic-probabilistic framework, as argued again recently in [6] and [7].

3.1 Uncertainties and Margins

In spite of the wide spread use of Modeling and Simulation (M&S) tools it remains difficult to provide objective confidence levels in the quantitative information obtained from numerical predictions. The complexity arises from the uncertainties related to the inputs of any computation attempting to represent a real physical system. Use of M&S predictions in high-impact decisions requires a rigorous evaluation of the confidence.

The concept of defence-in-depth has provided a practical recipe to ensure confidence without explicit quantification of level of confidence. The concept of defence-in-depth in nuclear engineering originated in 1940s, [13, 16], and dominated by the lack of precise knowledge of design margins evolved into a set of design and safety principles namely:

1. Use of multiple active/or passive engineered barriers to rule out any single failures leading to release of radioactive materials.

2. Incorporation of large design margins to overcome any lack of the precise knowledge (epistemic uncertainty) about capacity of barriers and magnitude of challenges imposed by normal or accident conditions.
3. Application of quality assurance in design and manufacture.
4. Operation within predetermined safe design limits.
5. Continuous testing, inspections, and maintenance to preserve original design margins.

The main intent of these design and safety principles is to address unquantified uncertainties. Key elements of these principles are: (1) incorporation of large design margins and (2) preservation of original design margins. Here, the use of term "design" margin is based on the definition of "design basis" in 10CFR50.2: "*Design bases means that information which identifies the specific functions to be performed by a structure, system, or component of a facility, and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be (1) restraints derived from generally accepted "state of the art" practices for achieving functional goals, or (2) requirements derived from analysis (based on calculation and/or experiments) of the effects of a postulated accident for which a structure, system, or component must meet its functional goals*.", and represent the distance between "design centered" or "operating centered" value and the "design reference bound" value, as it related to the protective system performance or operating parameters, such as channel and bundle maximum powers, etc, for example.

Table 2. Deterministic and Probabilistic Approaches and Kaplan & Garrick's Questions

Kaplan & Garrick's Questions	Deterministic Approach	Probabilistic Approach
What can happen?	Postulated DBA and bounding DBT	Formal fault and event tree procedure
How likely is it to happen?	Not quantified; multiple barriers, redundancy, postulated frequency classes with specific damage limits, and single failure criterion aimed at ensuring that protection failures are of very low probability	Detailed frequency calculations
What are the consequences if it happens?	Detailed damage calculations using conservative methods and criteria limits for DBE. Low probability protection failures and "unreasonable" events not covered.	Damage in low probability events estimated.
How much confidence exists in the answers to the above questions?	Not explicitly estimated; multiple barriers, redundancy and large design margins aimed at ensuring a high level of confidence	In general, level of confidence is estimated based on a tolerance limit and explicit account and quantification of aleatory and epistemic uncertainties.

With the evolution of safety assessment methods and methodology, the widely used term has become "safety margins". There is however a significant difference between the traditional

engineering concept of "safety" margin, which can be referred to as "margin to damage", and the nuclear industry concept of safety margin. This is because the more traditional definition of "safety" margin is connected to the probability of failure, while the nuclear industry definition of "safety" margin is more closely linked to the probability of exceedance, both of which play roles in the determination of risk, [4, 5].

The safety margin concept applies explicitly to either barrier or system losses. Therefore, in a complex facility, like a nuclear power plant, there will be as many safety margins as barriers or systems whose losses are considered to be a safety problem. Furthermore, for each barrier or system safety margins will exist for each damage mechanism that can lead to the loss of the barrier or system.

Whether the loss of a particular system or barrier is a safety problem or not, depends on its expected consequences. Since the ultimate goal of nuclear safety is to prevent unacceptable radiological releases to the public or to the environment, safety limits and margins should be considered at least for those systems and barriers whose failure could potentially contribute to unacceptable radiological releases.

The lack of explicit quantification of margins has always raised questions related to "how large is large enough?" and "what is the safety margin which should be preserved?"

A comprehensive examination of generalized concepts of safety margins and sources of safety margins, based on the whole process of design basis safety analysis methods, covering a wider scope than the previous IAEA definitions, [8, 10], and focusing on the barrier integrity analysis in design basis accidents, has been the topic of the recent NEA CSNI Action Plan in the Area of Safety margins (SMAP), [4, 5]. As discussed in [4], s*afety margin* is still a fuzzy term in the context of safety assessment of a nuclear power plant. It is generally accepted that the term *margin* refers to a "distance" between two values of a variable, or between two states defined in some way, or between some other two comparable things. Several types of margins with clear safety significance are defined for various practical purposes, such as "design margin", "equipment margin", "operational margin", etc, and all together are used for judging the level of safety of a plant and support the confidence that the plant operation within its design basis will not result in unacceptable damage. All these margins are considered as embedded in the current licensing basis (safety analysis report and safe operation envelope) for the existing plants, and need also to be assessed for any plant modification.

It remains still unclear, however, which particular margin should be named with the term *safety margin*, [4], or even if the term "*safety margin*" should be used to identify one particular margin, since all these margins are safety significant contributors to a *global plant margin* with respect to the primary regulatory limits - the radiological limits. There are examples in which the term *safety margin* is used as "the distance between the regulatory acceptance criterion and the safety variable value at which the system or barrier loses its function". This definition is inferred from the most common use of the term "safety margin" in DBA analyses. In DBA analyses, "adequate safety margin" exists if a conservative or bounding best estimate prediction of a variable remains under a selected acceptance criterion limit or the *regulatory acceptance criterion* [2], when the acceptance criterion and its limit is set by the regulator. The acceptance criterion limit is typically set sufficiently conservative to effectively render negligible the probability of failure. In other cases (see, for example, [8]), the term is used in a broader

sense which includes, in addition to the previous meaning, the comparison between some indication of the plant performance and a limit or acceptance criterion not to be exceeded.

The different types of margins contributing to the global plant margin have been evaluated in a variety of ways that may include different kinds of physical magnitudes or probabilistic characterizations so that, in general, their contribution to the global margin would not necessarily be additive, [4, 5]. Moreover, there are concurrent margins originating from the consideration of different safety variables and different DBEs for a single failure mode, different failure modes for the same barrier, etc. It has been, therefore, concluded that quantification of the global plant margin requires aggregation of all margin contributors in a *safety margin metrics* framework, [4, 5].

4. A Case of Margins Erosion

Conceptually, whenever a system or barrier performs a safety function, a margin can be defined to measure the extent to which plant behaviour under specified circumstances may challenge the system or barrier capability to perform its function. In some cases, regulatory acceptance criteria are imposed to prevent the loss of those safety barriers or systems, and the existing margin becomes divided in two parts (not necessarily measured in the same units) accounting for the distance from the plant performance to the regulatory limit and from the regulatory limit to the loss of function, respectively.

A generic graphic representation of margins in a deterministic approach with no explicit account of uncertainties is illustrated in Figure 1.

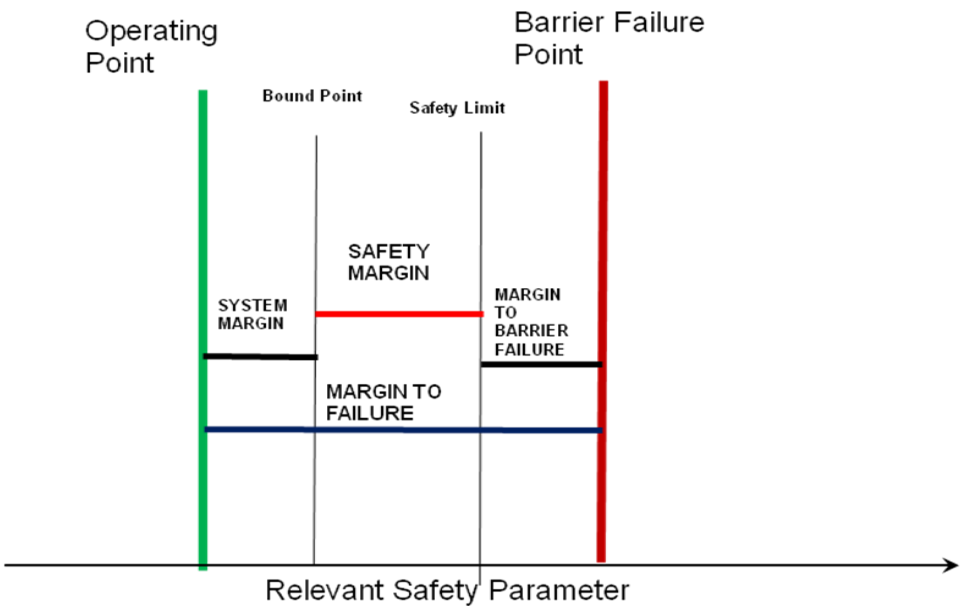

Figure 1. Graphic representation of margins in deterministic approach: no explicit account of uncertainties

Let's consider, for exemplification, the case of a postulated large LOCA accident in a CANDU reactor and the fuel channel, as the physical barrier of interest, and the fuel enthalpy, as the relevant safety parameter. In this case, the interpretation of Figure 1 would be:

- The vertical red line ("barrier failure point") correspond to fuel enthalpy value at which failure of fuel and fuel channel occurs

- The vertical "safety limit" is the value of fuel enthalpy conservatively selected to minimize the likelihood of fuel and fuel channel failure (the selected limit is assumed to implicitly cover the uncertainty related to the more limiting mechanism and path which would lead to fuel and fuel channel failure)
- The vertical green line ("operating point") correspond to the calculated fuel enthalpy in a postulated large LOCA assuming the most likely initial conditions and protective system performance and using best estimate simulation methods
- The vertical "bound point" line is the calculated fuel enthalpy in a postulated large LOCA assuming very unlikely, but credible, initial conditions, minimum allowable performance of protective system, and best estimate simulation methods (similar to the so called Limit of Operating Envelope (LOE) methodology)

Typically, the distance between the "bound" calculated fuel enthalpy and the fuel enthalpy "safety limit" values would be called "safety margin" in licensing safety analysis. The distance between "operating point" and "barrier failure point" would be the best estimate "margin to failure".

Now let's assume the case where the impact of a R&D finding, such as an increase in the calculated best estimate value of core positive void reactivity worth, or a change in plant conditions, due to aging, for example, is assessed. These types of conditions would affect the "operating point" and "bound point" calculated values, which will move closer to "safety limit" value, resulting in a decrease in "safety margin" and best estimate "margin to failure". Typically, the licensing practices would require restoration of "safety margin" value to get back within the safety case documented in Safety Analysis Report. One immediate option to do this has been to identify and implement measures to compensate for the increase in the calculated value of "bound point" by modifying the protective system minimum allowable performance and trip settings (decrease in system "design" margin) and/or changes in operating limits and conditions (again, decrease in plant "design" margins). Here, the use of term "design" margin is based on the definition of "design basis" in 10CFR50.2, ("*Design bases means that information which identifies the specific functions to be performed by a structure, system, or component of a facility, and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be (1) restraints derived from generally accepted "state of the art" practices for achieving functional goals, or (2) requirements derived from analysis (based on calculation and/or experiments) of the effects of a postulated accident for which a structure, system, or component must meet its functional goals*."), and represent the distance between "design centered" or "operating centered" value and the "design reference bound" value, as it relates to the protective system performance or operating parameters, such as channel and bundle maximum powers, etc.

Similarly, any situation which would adversely impact the "safety limit" value would lead to reduction of "design" margins, should the "safety margins" is to be preserved.

The following observations can be made, based on the discussed example:

- In the deterministic approach preservation of "safety margin" leads to erosion of "design" margins of protective systems, both in terms of systems "design" margin, defined by the distance between best estimate performance and minimum allowable performance, and overall best estimate margin to barrier failure – note that "operating" margins are also maintained, as required by compliance practices, the only change being related to compliance limits

- The safety benefit of preserving the "safety margin" cannot be quantified, while the erosion of "design" margin and its impact on plant operation and risk are quantifiable

There is, therefore, a need to better clarify the meaning of different margins and if the term "*safety margin*" should be used to identify one particular margin or, rather, a *safety margin metrics* framework should be used.

5. Reliability Approaches and the "Functional Failure" Concept

5.1 The Functional Failure Probability

As discussed in [4, 5, 11, and 17 to 22], the more traditional definition of safety margin is connected to the probability of failure, while the nuclear industry definition of safety margin is more closely linked to the probability of exceedance, both of which play roles in the determination of risk. From this perspective, it has been found useful to look at the existing reliability practices, [18 - 22]. From the classification of reliability methods discussed in [14] and used in support of approaches proposed in [18 – 22], the reliability approaches, based on the concepts of "load" and "capacity", can be grouped in four levels of complexity, with lower level methods containing less information than higher level methods. These are summarized in Table 3.

Table 3. Safety Margin in Reliability Approaches

Level #	Description	Observations
1	The "load" and "capacity" are described by point estimates (the characteristic values) and the safety of the system is evaluated through a safety margin or coefficient describing the relationship between these two point estimates.	Safety margins are identified as a Level 1 reliability approach. Similar to traditional deterministic approach, as discussed in previous section. This type of approach is the one most commonly implemented in the regulations.
2	Normal distributions are assumed to describe the "load" and "capacity" uncertainty. Values as the mean, variance and covariance are sufficient to describe the system uncertainty. It introduces the notion of "reliability index" to measure the safety of the system. It provides a first quantification of uncertainty through the variance.	The approach can provide erroneous results for applications where normal distributions are not a good approximation (for example in case the tail effect is important)
3	Generalized probability distributions are derived to describe the uncertainties. The safety of the system is measured by the probability of failure using a convolution formula with the "load" and "capacity" probability distribution functions, assumed to be independent. The calculation employs order statistics methods.	It needs quantification of the uncertainty distributions and significant computational effort.
4	Comprehensive approach that includes not only safety information, but also the economic aspects of the design. It uses the concept of "utility function" which could take into account risk, economics, and stakeholder interest objectives.	It needs using an optimization process based on the maximization of a utility function, accurate information and significant computational effort.

The concept of "load" and "capacity" and margins are illustrated in Figures 2 and 3. For the stylized LOCA case discussed in section 4, the "load" would correspond to the calculated fuel enthalpy and

the "capacity" would correspond to the fuel enthalpy dependent fuel and fuel channel failure, and the schematic representations in these Figures are their probability distribution functions.

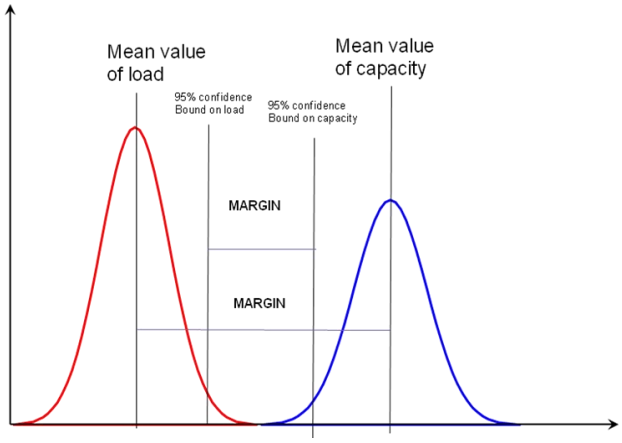

Figure 2. Generic representation of "load and "capacity"

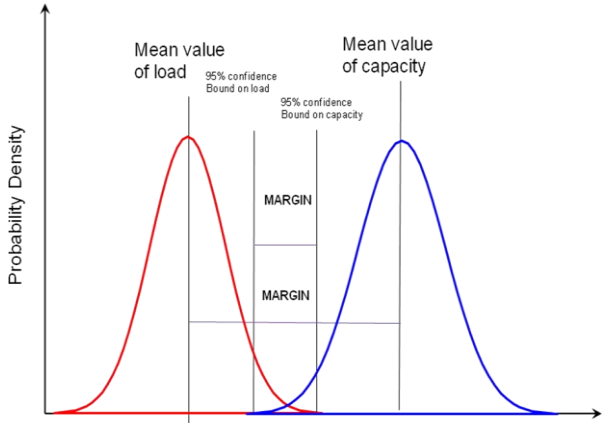

Figure 3. Generic representation of "load and "capacity" and "margins

Figure 2 illustrates the case where there is no overlap between the "load" and "capacity" distributions. This would correspond to the "ideal" objective of deterministic approach (probability of exceedance negligible). Figure 3 illustrates the case where there is overlap between the "load" and "capacity". This might be the case of originally optimized design or the result of incorporation of R&D discovery issues, as in the example discussed in section 4. The "safety" margin can be defined as the distance between a characteristic value of the capacity (median or low percentile value (5%) or a conservatively set value) and a characteristic value of the load (median or high percentile (95%) or a conservatively set value). The objective of a negligible probability of exceedance can be achieved either by imposing large "safety" margins or by reducing the uncertainties, both leading to moving the two distributions far one from the other. Selection of the best approach requires understanding the shape of "tails" of probability density function in the "overlap" region.

The graphical illustration is, however, somehow misleading, in the sense that the common area below the two distributions is not a measure of the probability of failure. The probability of failure is given by the probability that "load" will exceed the "capacity", i.e., by the convolution formula:

$$P(L > C) = \int_{c=-\infty}^{c=+\infty} \int_{l=c}^{l=+\infty} f_C(c) f_L(l) dl dc = \int_{c=-\infty}^{c=+\infty} f_C(c)[1 - F_L(c)] dc$$

where f_C and f_L represent the distribution of "capacity" and "load" respectively. The f_C and f_L are conditional on the scenario.

Burgazzi, Pagani, and Apostolakis have proposed the use of qualifier "functional failure" for this probability, [17 – 22], to indicate that it characterizes the case where the systems works, but the desired outcome of its action might not be achieved.

With this concept, the effect of "safety" margin on the level of safety, or conversely on risk, can be quantified by introduction of functional failures in PRA. To include functional failures into PRA, it is necessary to take into account the possibility of a failure even when the acceptance criteria are met

and the possibility of success even when the acceptance criteria are violated. An example of application for the passive cooling system and a large LOCA scenario for a 600 MW Gas-cooled Fast Reactor is discussed in [18, 19, 21]. A schematic illustration of corresponding event tree is presented in Figure 4 (reproduced from [18])

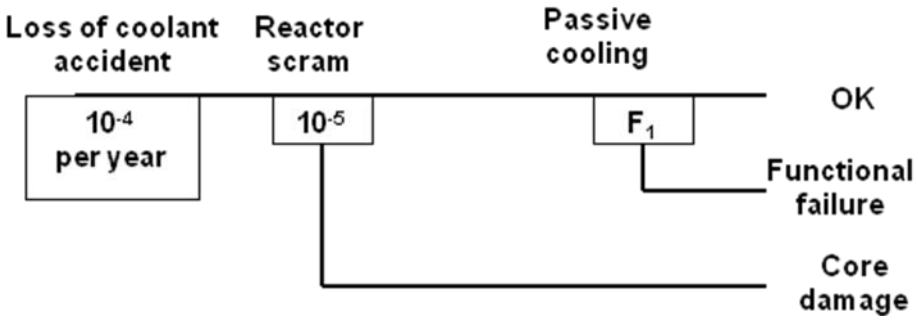

Figure 4. Schematic illustration of event tree including "functional failure" (reproduced from [18])

The numerical examples, [18, 19, 21], show that the correction to calculated CDF could be significant: a correction by a factor of 1000 for the calculated CDF value, when "functional failure" is considered. At the same time, the few cases discussed in literature, show little, negligible, impact for active ECCS: on the order of a small percentage of the calculated CDF.

Another application of interest for the concept of "functional failure" is in determination of failure limit for the fuel cladding for high-burnup fuels, [18, 20, 21]. The results, illustrated in Figure 5 (reproduced from [18]), indicate the importance of accurate quantification of shape and tail of the probability distribution on quantifying the "safety" margin in fuel failure limit.

The examples discussed in literature show that "safety" margins affect PRA at the level of success criteria and the impact of "safety" margins can be significant for scenarios characterized by large epistemic uncertainty.

In the case of the stylized example of the LOCA case discussed in section 4, it should be noted that application of functional failure probability may indicate that redundancy in protective function, two independent and fast acting shutdown systems, would reduce the potential effect of large uncertainties in predictions of "load".

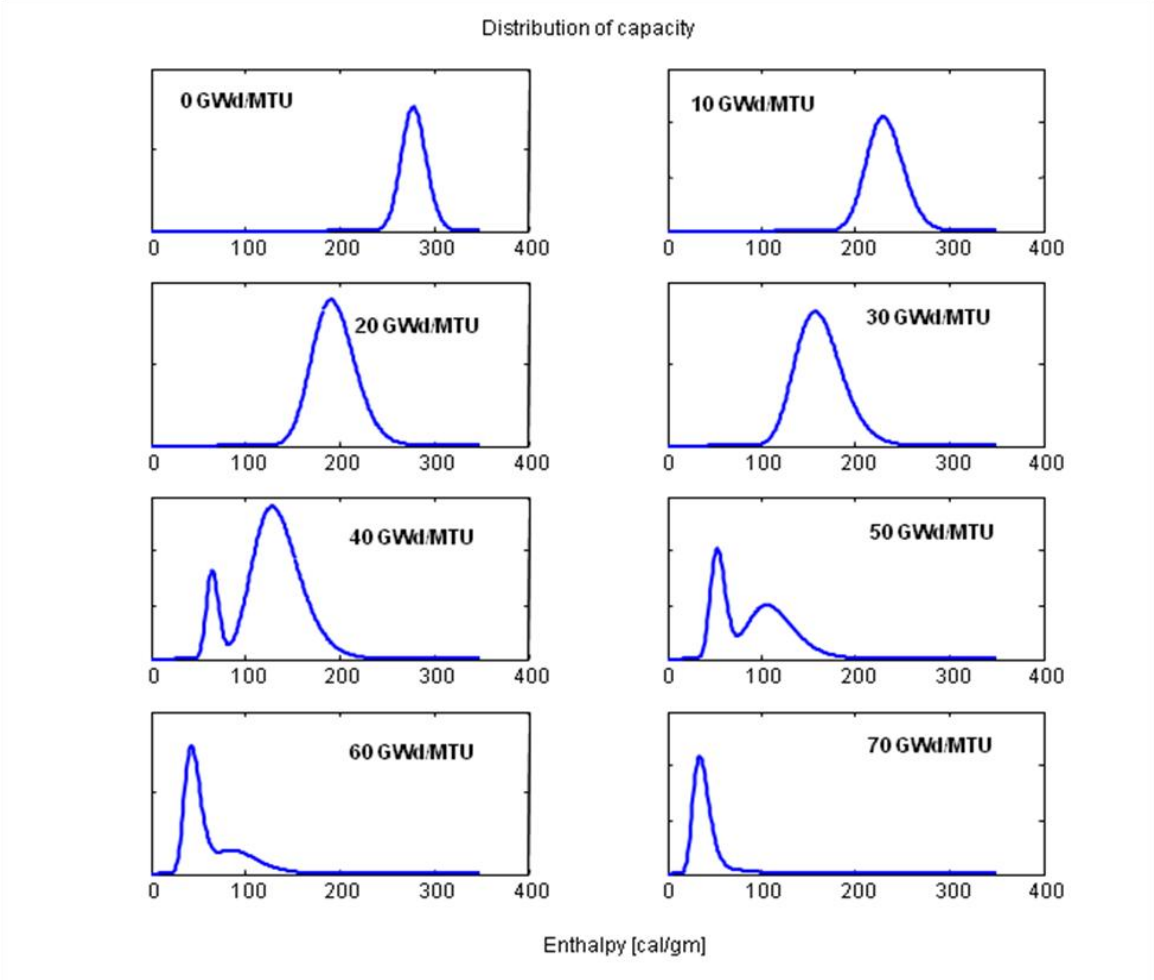

Figure 5. High-burnup fuel: Distribution of capacity (reproduced from [18])

The use of level 3 reliability approach and the concept of functional failure probability could provide the basis for defining a safety margin metrics which would include a limit for the probability of functional failure, in line with the definition of a reliability-based design, which is one where the probability of failure is less than some acceptable value, [24]. It can also allow a quantification of level of confidence, by explicit modeling and quantification of uncertainties, and provide a better framework for representation of actual design and optimization of design margins within an integrated probabilistic-deterministic model under the frequency-consequence constraints and the deterministic defense-in-depth requirements. A potential approach has recently been proposed in [45] in the context of the risk-informed technology neutral framework (TNF) for licensing new reactors that has been proposed by the U.S. Nuclear Regulatory Commission staff, [46]. In lieu of design-basis accidents (DBAs), the TNF imposes limits on the frequency and consequences of accident sequences called licensing-basis events (LBEs). The proposed approach is based on a method to define LBEs using functional event trees and a new importance measure, the Limit Exceedance Factor (LEF). It is the factor by which the failure probability of structures, systems, and components (SSCs) may be multiplied such that the frequency of a risk metric reaches a limit. LEF could allow a designer to know how much margin exists to the safety limit for each SSC. Alternatively, in the case where a design does not meet the frequency limit (very large consequence

events are considered beyond the licensing basis in the TNF as long as their mean frequencies are less than 1×10^{-7} per reactor year), LEF can reveal which systems are candidates for improvement to satisfy the limit.

5.2 Application of Functional Failure Concept: Treatment of Uncertainties and Order Statistics Approaches

Application of level 3 reliability approaches and the concept of functional failure probability require accurate inference of generalized probability distributions to describe the uncertainties in the "load" and "capacity" and the calculation need to employ order statistics methods. In particular, the need to make the distinction between the aleatory and epistemic uncertainties has been emphasized, [15]. Several procedures have been proposed, [5, 11, 18 - 22, 23, 25-27, 29 – 33], and specialized software is now available, [28, 32, 47]. A common aspect of all procedures proposed to date is the need to use realistic (best estimate) system models for calculation of "load" and "capacity" with quantification of uncertainties.

5.2.1 Predictive Capability and Validation Needs

In spite of the wide spread use of Modeling and Simulation (M&S) tools it remains difficult to provide objective confidence levels in the quantitative information obtained from numerical predictions at the system level. The complexity arises from the uncertainties related to the inputs of any computation attempting to represent a real physical system. Use of M&S predictions in high-impact decisions requires a rigorous evaluation of the confidence. The accepted process of evaluating M&S tools and solutions is based on the general concept of Verification and Validation (V&V). The last step of the process is invariably based on comparisons between numerical predictions and physical observations. Precise quantification of the errors and uncertainties is required to establish predictive capabilities and, therefore, uncertainty quantification is a key ingredient of validation.

System simulation requires the use of multi-physics code systems. However, as discussed in [34], the current qualification procedures of coupled multi-physics code systems are still based on the verification and validation of separate physics models/codes. Although some V&V of the coupling methodologies of the different physics models is possible, it may be too limited, because of availability of experimental data (integral-effect test data).

While there is general agreement on the need to use realistic, best estimate models, there are still divergent opinions about what an adequate methodology to qualify the uncertainties in predictions should be. It is noted in a recent review and comparison of various methodologies carried out at Argonne National Laboratories, [35]: "*While there is general agreement as to the distinction between conservative and best estimate models, there is no universally accepted approach to bounding and quantifying the effect of uncertainties on analysis results. The term "uncertainty analysis" is not always defined consistently by authors in the field. In particular, there is sometimes confusion as to the distinctions between uncertainty analysis and the related area of sensitivity analysis. Most authors classify uncertainty analysis of a modeling evaluation as the determination of the amount of imprecision present in the predicted output parameters of interest, while sensitivity analysis is the means of identifying the contribution to this imprecision made by the uncertainty in each input parameter to the model.*"

The current approaches to V&V in the nuclear energy field are diverse and depend not only on the discipline but also on the origin of the code being validated, [36, 37]. In general, industrial codes have relied on comparisons of predictions with representative mockup measurements to establish calculation to uncertainty biases and uncertainties (often estimated by expert judgment); these biases and uncertainties are then applied to project calculations. R&D codes often rely on a more formal V&V process, where the individual sources of V&V are identified and quantified and then propagated to the final solution by using statistical techniques. Neutronics has probably the most well established formal V&V process, where the uncertainties on the basic nuclear data can be formally propagated through the constitutive equations and treated statistically along with information available from integral experiments.

Model V&V is an enabling methodology for the development of computational models that can be used to make engineering predictions with quantified confidence, [36, 37]. Model V&V procedures can help to reduce the time, cost, and risk associated with full-scale testing of products and materials. Quantifying the confidence and predictive accuracy of model calculations provides the decision-maker with the information necessary for making high-consequence decisions.

Model verification and validation are the primary processes for quantifying and building credibility in numerical models. Verification is the process of determining that a model implementation accurately represents the developer's conceptual description of the model and its solution. Validation is the process of determining the degree to which a model is an accurate representation of the real world from the perspective of the intended uses of the model. Both verification and validation are processes that accumulate evidence of a model's correctness or accuracy for a specific scenario; thus, V&V cannot prove that a model is correct and accurate for all possible scenarios, but, rather, it can provide evidence that the model is sufficiently accurate for its intended use.

Model V&V is fundamentally different from software V&V, [36, 37]. Code developers developing computer programs perform software V&V to ensure code correctness, reliability, and robustness. In model V&V, the end product is a predictive model based on fundamental physics of the problem being solved. *The expected outcome of the model V&V process is the quantified level of agreement between experimental data and model prediction, as well as the predictive accuracy of the model.* Guidelines, standards and procedures for performing model V&V for complex numerical models are just now being developed.

The use of complex, computational intensive, predictive models may be prohibitive in application of level 3 reliability approaches and functional failure probability concept. This difficulty can be overcome by the use of „emulators", based on Bayesian inference and Gaussian processing of outputs, and a formal elicitation procedure, as proposed in [47].

While a computer model, typically referred as *simulator*, aims to simulate some real-world phenomenon, a *meta-model*, sometime referred as *reduced order model* or *surrogate*, is a simplified representation or approximation of a *simulator*, which should run much more quickly than the *simulator*. Various kinds of meta-models have been proposed by modellers and model users, notably regression models and neural networks. The main shortcomings of these approaches are: potential misrepresentation of provided data, indicated by inexact reproduction of and non-zero variance for the provided points.

An *emulator* is a particular kind of meta-model: it is more than just an approximation, because it makes fully probabilistic predictions of what the simulator would produce, and the probability statements correctly reflect the provided information. The main properties of an adequate emulator are, [47]:

- ✓ If asked to predict the simulator output at one of the provided data points, it returns the observed output with zero variance, assuming the simulator output does not have random noise;
- ✓ It must be sufficiently flexible to pass through all the provided data points, rather than being restricted to some regression form
- ✓ If asked to predict output at another point its predictions will have non-zero variance, reflecting realistic uncertainty
- ✓ Given enough simulator data points are provided, it should be able to predict simulator output to any desired accuracy

An emulator also allows for comprehensive sensitivity and uncertainties analyses, [47].

5.2.2 Aleatory and Epistemic Uncertainties

There is increased interest from regulatory agencies, design teams and operators to specifically characterize and quantify epistemic uncertainty and separate its effect from that of aleatory uncertainty. A significant driver for this interest is the fact that the treatment of uncertainty in the analysis of computer models is essential for understanding possible ranges of outputs or scenario implications. Most computer models for engineering applications are developed to help assess a design or regulatory requirement. As part of this task, the capability to quantify the impact of variability and uncertainty in the decision context is required, because, typically, the design or regulatory requirement is often stated as: the probability that some system response quantity exceeds a threshold value is less than some required probability, [29]. Therefore, the capability to quantify the impact of uncertainty in the decision context is critical, [15, 29, 41, 43, 44].

However, guidelines and standards to help deciding on what an adequate methodology should be for a given application are just now being developed.

The terms “aleatory” and “epistemic” are used since quite a while in risk analysis with, so far, limited applications for regulatory purposes. To date the application of probabilistic methodologies with separation of aleatory and epistemic uncertainties for safety and regulatory purposes has been limited to the area of severe accident risks, [38, 39, 40].

The aleatory uncertainties have thus far been treated as epistemic in the traditional methods and typically added in rms. This might be a poorer way of handling these uncertainties than a higher order approximation, but the effect on the results has been deemed acceptable in the overall framework of deterministic analysis.

In the context of analysis of uncertainty in system response given uncertain input parameters, incertitude (commonly referred to as “uncertainty”) can be formally classified as aleatory uncertainty and epistemic uncertainty. Guidance from a US Department of Energy document related to

quantification of margins and uncertainties using modeling and simulation states: "Where it is practical, calculation input characterizations should separate aleatory and epistemic uncertainties", [41].

According to technical literature, aleatory uncertainty characterizes the inherent randomness in the behaviour of the system under study. Alternative terminologies include: variability, stochastic uncertainty, irreducible uncertainty, and Type A uncertainty. Aleatory uncertainty is irreducible except through design modifications. Examples of aleatory uncertainty are component failures or material properties derived from statistically significant testing under conditions relevant to the application. Aleatory uncertainties are characterized by frequency distributions; and aleatory uncertainties propagated through a model will result in distributions for key system response quantities that should also carry a frequensic interpretation. Epistemic uncertainty characterizes the lack of knowledge about the appropriate value to use for a quantity that is assumed to have a fixed value in the context of a specific application. Alternative terminologies include: state of knowledge uncertainty, subjective uncertainty, reducible uncertainty, and Type B uncertainty. Epistemic uncertainties are reducible through increased understanding (research), or increased data, or through more relevant data. Epistemic uncertainties are characterized by degrees of "belief" and many developers argue that it should not be given a frequensic or probabilistic interpretation, [29, 41].

Epistemic distributions for the models themselves are not developed routinely. The most used methods currently employed for quantifying model uncertainties are sensitivity studies and expert elicitation. Common procedure is not to separate aleatory and epistemic uncertainties, but rather:

- ✓ Represent epistemic uncertainty with a uniform probability distribution
- ✓ For a quantity that is a mixture of aleatory and epistemic uncertainty, use second-order probability theory

Second-order probability approaches have a regulatory precedent and have been used extensively in the performance assessment for nuclear waste repositories and in nuclear reactor safety assessments, [39, 40].

The second-order probability approaches were developed to deal with the common situations where one may know the form of the probability distribution for an uncertain variable (for example, that it is distributed normally), but one is not sure of the parameters governing the distribution. In this case, the analysis is done with an outer loop and an inner loop.

In the outer loop, the epistemic variables are specified. The epistemic variables could be specified as intervals on parameter values such as means or standard deviations of uncertain variables. A particular value is selected from within the specified intervals. Then, this value is sent to the inner loop.

In the inner loop, the values of the distribution parameters are set by particular realizations of the epistemic variables, and the inner loop performs sampling on the aleatory variables in the usual way (e.g., a Monte Carlo or Latin Hypercube Sampling sample is taken). Figure 6 shows the sampling structure of second-order probability approach – reproduced from [42].

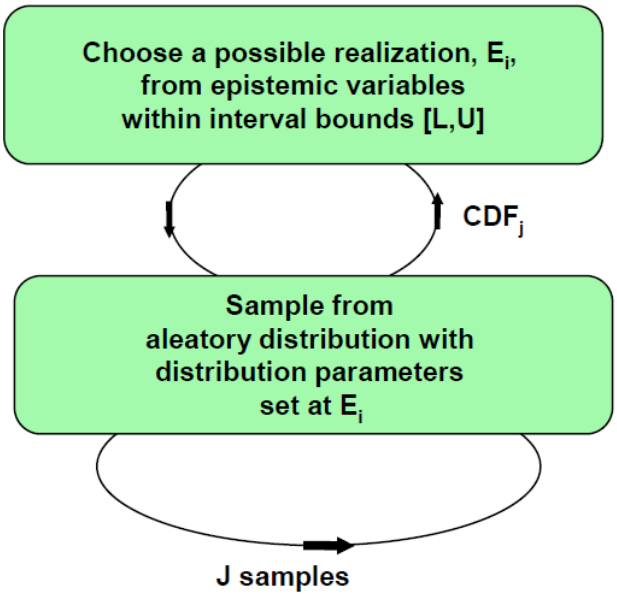

Figure 6. Schematic representation of second-order probability method (reproduced from [42])

Many experts support the use of traditional probability theory with strict separation of aleatory and epistemic uncertainty and treatment of epistemic uncertainty as possible realizations with no probability associated with those realizations obtained from sampling. However, there is considerable diversity of opinion within the community of experts engaged in quantitative analysis and simulation of complex engineered systems about both methods and fundamental issues. An Epistemic Uncertainty Project at Sandia National Laboratories has focused on the question of how epistemic and aleatory uncertainty should be handled within probabilistic modeling and quantitative risk analyses. The project investigated the use of both probabilistic and non-traditional forms of uncertainty quantification for modeling the performance of complex engineering systems. An „Epistemic Uncertainty Workshop' sponsored by Sandia National Laboratories was held in Albuquerque, New Mexico, on 6–7 August 2002. The workshop was organized around a set of Challenge Problems involving both epistemic and aleatory uncertainty that the workshop participants were invited to solve and discuss. A special issue of *Reliability Engineering and System Safety* (No. 85, 2004) was dedicated to the workshop discussions and presented papers and included a technical comparison among different approaches, based on results for the set of challenge problems proposed by Sandia National Laboratories. The Challenge Problems were computationally simple models that were intended as vehicles for the illustration and comparison of conceptual and numerical techniques for use in analyses that involve: (i) epistemic uncertainty, (ii) aggregation of multiple characterizations of epistemic uncertainty, (iii) combination of epistemic and aleatory uncertainty, and (iv) models with repeated parameters, [44].

It has been noted that there is a number of technical questions about which there is little or no consensus across the disparate communities of risk analysts, modellers and information theorists engaged in the quantitative analysis and simulation of complex engineered systems. In order of importance, these questions are, [43]:

a. How should epistemic uncertainty about a quantity be represented?
b. How can epistemic and aleatory uncertainty about a quantity be combined and propagated in calculations?

c. How should multiple estimates of uncertain quantities be aggregated before calculation?
d. How should the technical issue of repeated uncertain parameters be handled in practical calculations?
e. How might various approaches be adapted for use in practical calculations based on sampling strategies?

A significant outcome of that work has been the identification of a number of key topics that must be successfully addressed in order to produce a meaningful and useful representation of the uncertainty in analysis outcomes, regardless of whether probability theory or some other mathematical structure is used to represent epistemic uncertainty. These are:

(1) *Conversion of available information into the mathematical structure used to represent epistemic uncertainty*. For many analyses, this is likely to involve some type of expert review or elicitation procedure.

(2) *Aggregation of information from multiple sources into a single representation of uncertainty*. Multiple sources of information are common in large analyses and the manner in which this information is aggregated (i.e. coalesced into the mathematical structure being used to represent uncertainty) can have a substantial effect on the final analysis result.

(3) *Propagation of the uncertainty structure imposed on analysis inputs through the model or models underlying the analysis to obtain the corresponding uncertainty structure on analysis results*. Specifically, the uncertainty structure on analysis results depends on both the uncertainty structure on the analysis inputs and the model (i.e. function) that transforms this input. In real analyses, this propagation is likely to be a major computational challenge. Mathematical structures for uncertainty representation that are too demanding computationally are not practicable.

(4) *Presentation and interpretation of uncertainty results*. Typically, analysis results must be presented to, and understood by, many individuals in addition to those actually carrying out an analysis. Such individuals could include other analysts, managers with supervisory responsibility for the analysis, outside reviewers, interested members of the public and formal decision makers who must make decisions on the basis of the analysis. Uncertainty results that are not understood or, even worse, are misunderstood are of no value. Thus, the mathematical structure used to represent uncertainty must be understandable by individuals in addition to those carrying out the analysis and care must be taken to assure (or, at least, facilitate) the communication of this understanding to those who will use the results of the analysis.

(5) *Performance of sensitivity analyses*. Although sensitivity analysis does not enter directly into the propagation and presentation of epistemic uncertainty, sensitivity analysis should be a fundamental part of any analysis that involves the assessment and propagation of uncertainty. In particular, appropriately designed sensitivity analyses provide insights with respect to the

correctness of the analysis (i.e. analysis verification), which input uncertainties dominate the output uncertainties, and how to appropriately invest resources to reduce uncertainty in analysis results.

Sandia has also made available dedicated software for uncertainty quantification and propagation in engineering simulations and quantitative risk analyses developed under the DAKOTA project (http://dakota.sandia.gov/index.html). The DAKOTA (Design Analysis Kit for Optimization and Terascale Applications) toolkit provides an interface between simulation codes and iterative analysis methods, [28]. DAKOTA contains algorithms for optimization with gradient and non gradient based methods; uncertainty quantification with sampling, reliability, and stochastic finite element methods; parameter estimation with nonlinear least squares methods; and sensitivity/ variance analysis with design of experiments and parameter study methods. The DAKOTA software framework can also be configured for pure interval analysis, Dempster-Shafer evidence theory, and second-order probability analysis.

The most recent development in this area is the MUCM (Managing Uncertainty in Complex Models) project, funded by Research Councils UK, involving collaboration between five universities: Sheffield, Aston, Southampton, Durham, and the London School of Economics and advisors from across UK and Europe as well as the USA, [47].

The project is concerned with quantifying and reducing uncertainty in the predictions of complex models across a wide range of application areas, including basic science, environmental science, engineering, technology, biosciences, and economics. The project is multi-disciplinary, and the unifying theme is a Bayesian statistical approach to inference. A web-based toolkit which provides a framework of techniques and procedures allowing developing an application-specific procedure and software has been produced in the first phase of the project, completed in 2010.

6. Summary Remarks

A review of current status and trends indicates that level 3 reliability approaches and application of "functional failure" concept in the area of quantification of margins are gaining popularity and interest for application by the industry and the regulators. Although, the practical processes and procedures have not reached yet a level of maturity needed for application in safety assessment of design basis events for nuclear power plant, it is a promising approach which should be considered for development for CANDU reactors applications, due to the significant benefits it could provide. The following remarks highlight main benefits and areas of further development related to this approach.

6.1.1 Benefits of Functional Failure Concept

The main benefits of application of level 3 reliability approaches and the concept of functional failure probability are:

- It simplifies and adds clarity to the discussion about "safety" margins and could provide the basis for defining a *safety margin metrics* which would include a limit for the probability of functional failure, in line with the definition of a reliability-based design, which is one where the probability of failure is less than some acceptable value – note that this would be a natural development of CANDU practices where limits on protective systems (availability)/reliability have traditionally been set in design and regulatory requirements.

- It provides a better framework for risk-informed critical decisions, because it allows a better quantification of effectiveness of defence-in-depth in design and the impact of erosion of margins on risk, by taking into account the possibility of a failure even when the acceptance criteria are met and the possibility of success even when the acceptance criteria are violated.

- It could provide a better representation and quantification of the impact on risk of the redundancy in active protective systems in CANDU design.

- It can allow quantification of level of confidence, by explicit modeling and quantification of uncertainties, and provide a better framework for representation of actual design and optimization of design margins within an integrated probabilistic-deterministic model under the frequency-consequence constraints and the deterministic defence-in-depth requirements.

6.1.2 Main R&D Areas for Application of Functional Failure Concept

Main R&D areas for application of level 3 reliability approaches and the functional failure concept include:

- It would need complex integrated multi-physics models and a new framework and standard for verification and validation. The current coupling methodologies and the framework of individual codes verification and validation would not be sufficient.

- It would need development of a data base of integral-effects test data or surrogates (plant data) and fuel and fuel channel experimental data for adequate characterization of "load" and "capacity" distributions and setting of more accurate acceptance limits.

- It would need a physics and mathematical framework for forward propagation of uncertainties thru the integrated multi-physics model which distinguish between aleatory and epistemic uncertainties where practical.

- It would need development of PRA models to include functional failure sequences.

- It would need high computational capability, because it is computationally resource intensive. However, the recent developments in computing capabilities combined with the use of emulators could alleviate this aspect.

7. References

[1] *Basic Safety Principles for Nuclear Power Plants*; IAEA INSAG-3, Vienna, 1999.

[2] *Accident Analysis for Nuclear Power Plants;* IAEA Safety Report Series No. 23; Vienna, 2002.

[3] ANSI *N18*.2-1973, *Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants*.

[4] *SMAP Technical Note on Acceptance (Licensing) Criteria and Related Safety Margins (SMAP Subtask 1C), August 2005, NEA/SEN/SIN/SMAP(2005)4*

[5] Task Group on Safety Margins Action Plan (SMAP) Safety Margins Action Plan - Final Report, NEA/CSNI/R(2007)9

[6] G. Apostolakis, "Managing Uncertainties in the Regulation of Nuclear Facilities: The Issue of Unknown Unknowns", *ESREL 2010*, *Rhodes, Greece, September 6, 2010*

[7] Y. Orechwa, "Formal Considerations in Establishing Risk-Consistent Acceptance Criteria for Reactor Safety", Nuclear Technology / Volume 170 / Number 3 / June 2010 / Pages 383-396

[8] *Safety margins of operating reactors: Analysis of uncertainties and implications for decision making*, IAEA TECDOC-1332; Vienna, Jan. 2003

[9] J. Hortal, "Safety Margins: Deterministic and probabilistic Views", Paper in IAEA TECDOC 1332, Vienna, Jan. 2003

[10] *Implications of power uprates on safety margins of nuclear power plants*; IAEA TECDOC-1418; Vienna, September 2004.

[11] Gavrilas et al. *A Generalized Framework for Assessment of Safety Margins in Nuclear Power Plants,* Proceedings to BE 2004: International Meeting on Updates in Best Estimate Methods in Nuclear Installations Safety Analysis, Washington, DC, November 14-18, 2004, CD-ROM, ANS Lagrange Park, IL

[12] Kaplan S, Garrick BJ, "On the Quantitative Definition of Risk." *Risk Analysis* 1981; 1(1):11-27

[13] W. Keller, M. Modarres, "A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late Professor Norman carl Rasmussen" *Reliability Engineering & System Safety* 2005; 89:271-285

[14] H.O. Madsen, K. Krenk, N.C. Lind, "Methods of Structural Safety", 1986, Prentice-Hall Inc, Englewood Cliffs, New Jersey, USA

[15] G. Apostolakis, "The distinction between aleatory and epistemic uncertainties is important: an example from the inclusion of aging effects into PSA", In Proceedings of the PSA '99 International Topical Meeting on Probabilistic Safety Assessment, Washington, DC, 22-26 August, 1999

[16] J. H. Bickel, "The Precaution Principle Applied to Nuclear Power Regulation in the USA", A Transatlantic Dialogue on "The Reality of Precaution: Comparing Approaches to Risk and Regulation" 13-15 June 2002

[17] L. Burgazzi, "Reliability evaluation of passive systems through functional reliability assessment", Nuclear Technology, 2003, 144, 145-150

[18] G. Apostolakis, "On the Inclusion of Safety Margins in Probabilistic Risk Assessment", Presented at the University of California, Berkeley, November 2, 2004

[19] L. P. Pagani, G. Apostolakis, P. Hejzlar, "The impact of uncertainties on the performance of passive systems", Nuclear Technology, Volume 149, February 2005, Number 2, Pages 129-140

[20] L. P. Pagani, G. Apostolakis, "A Methodology for Developing a Probability Distribution for the Failure Enthalpy of High-Burnup Fuels via Simulation", Nuclear Technology, Volume 153, January 2006, Number 1, Pages 9-17

[21] L.P. Pagani, "On the Quantification of Safety Margins", PhD Dissertation, Massachusetts Institute of Technology, September 2004

[22] G. Patalano, G. Apostolakis, P. Hejzlar, "Risk-Informed Design Changes in a Passive Decay Heat Removal System", Nuclear Technology, Volume 163, Number 2, August 2008, Pages 191-208

[23] J.C. Helton, "Conceptual and Computational Basis for the Quantification of Margins and Uncertainty", SANDIA Report SAND2009-3055, June 2009

[24] G. Iaccarino, "Introduction to Uncertainty Quantification", CSE09 Mini-tutorial, SIAM CSE Conference, Miami, 2009

[25] M.S. Eldred, L.P. Swiler, "Efficient Algorithms for Mixed Aleatory-Epistemic Uncertainty Quantification with Application to Radiation-Hardened Electronics", SANDIA Report, SAND2009-5805, September 2009

[26] M. Pilch, "The Method of Belief Scales as a Means for Dealing with Uncertainty in Tough Regulatory Decisions", SANDIA Report SAND2005-4777, October 2005

[27] J.C. Helton, J.D. Johnson, W.L. Oberkampf, C.B. Storlie, "A Sampling-Based Computational Strategy for the Representation of Epistemic Uncertainty in Model Predictions with Evidence Theory", SANDIA Report SAND2006-5557, October 2006

[28] Brian M. Adams, Keith R. Dalbey, Michael S. Eldred, David M. Gay, Laura P. Swiler, "DAKOTA, A Multilevel Parallel Object-Oriented Framework for Design Optimization, Parameter Estimation, Uncertainty Quantification, and Sensitivity Analysis", Version 5.0 User's Manual, SANDIA Report SAND2010-2183, December 2009, Updated May 7, 2010

[29] M. Pilch, T. G.Trucano, J. C. Helton, "Ideas Underlying Quantification of Margins and Uncertainties (QMU): A White Paper", SANDIA Report SAND2006-5001, September 2006

[30] J. C. Helton, J. D. Johnson, W. L. Oberkampf, C.J. Sallaberry, "Representation of Analysis Results Involving Aleatory and Epistemic Uncertainty", SANDIA Report SAND2008-4379, August 2008

[31] L. P. Swiler, A. A. Giunta, "Aleatory and Epistemic Uncertainty Quantification for Engineering Applications", SANDIA Technical Report, SAND2007-2670C, Joint Statistical Meetings, July29-Aug.2, 2007

[32] D. L. Kelly, C. L. Atwood, "Bayesian Modeling of Population Variability – Practical Guidance and Pitfalls", PSAM – 9, INL/CON-08-14208, May 2008

[33] M. Eaton, M.M.R. Williams, "A probabilistic study of the influence of parameter uncertainty on solutions of the neutron transport equation", Progress in Nuclear Energy 52 (2010) 580–588

[34] M.N. Avramova, K.N. Ivanov, "Verification, validation and uncertainty quantification in multi-physics modeling for nuclear reactor design and safety analysis", Progress in Nuclear Energy 52 (2010) 601–614

[35] L.L. Briggs "Status of Uncertainty Quantification Approaches for Advanced Reactor Analyses", ANL-GenIV-110, September 2008

[36] W. L. Oberkampf, T. G. Trucano, C. Hirsch, "Verification, Validation, and Predictive Capability in Computational Engineering and Physics", SANDIA Report SAND2003-3769, February 2003

[37] Workshop on Simulation and Modeling for Advanced Nuclear Energy Systems, *Co-sponsored by* Office of Nuclear Energy, Office of Advanced Scientific Computing Research, U.S. Department of Energy, *Co-chairs* Phillip Finck, David Keyes, and Rick Stevens, Washington, D.C., August 15–17, 2006

[38] Nuclear Regulatory Commission, "Severe Accident Risks: an Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, 1990

[39] J.C. Helton, D.R. Anderson, H. Jow, M.G. Marietta, G. Basabilvazo, "Performance Assessment in Support of the 1996 Compliance Certification Application for the Waste Isolation Pilot Plant" *Risk Analysis*, Vol. 19, No. 5, 1999

[40] J.C. Helton, R. J. Breeding. "Calculation of reactor accident safety goals" *Reliability Engineering and System Safety* Vol. 39, pp. 129-158, 1993.

[41] K. Diegert, S. Klenke, G. Novotny, R. Paulsen, M. Pilch, T. Trucano. "Toward a More Rigorous Application of Margins and Uncertainties within the Nuclear Weapons Life Cycle – A Sandia Perspective", Sandia Technical Report SAND2007- 6219, October 2007

[42] Laura P. Swiler, Thomas L. Paez, Randall L. Mayes, "Epistemic Uncertainty Quantification Tutorial", Proceedings of the IMAC-XXVII February 9-12, 2009 Orlando, Florida USA

[43] Scott Ferson, Cliff A. Joslyn, Jon C. Helton, William L. Oberkampf, Kari Sentz, "Summary from the epistemic uncertainty workshop: consensus amid diversity", *Reliability Engineering and Systems Safety*, 85, 2004

[44] Oberkampf WL, Helton JC, Joslyn CA, Wojtkiewicz SF, Ferson S., "Challenge Problems: uncertainty in system response given uncertain parameters" *Reliability Engineering and Systems Safety*, 85, 2004

[45] B.C. Johnson, G.E. Apostolakis, R. Denning, "Application of a Limit Exceedance Importance Measure to Risk-Informed Design", Nuclear Technology / Volume 172 / Number 2 / Pages 108-119, November 2010

[46] Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing, Volumes 1 and 2 (NUREG-1860), 2007, US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC

[47] Management of Uncertainties in Complex Models (MUCM) Toolkit, http://mucm.aston.ac.uk/MUCM/MUCMToolkit/index.php?page=MetaHomePage.html