Unclassified **NEA/SEN/SIN/SMAP(2005)3**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development **12-Aug-2005**

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/SEN/SIN/SMAP(2005)3
Unclassified

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

SMAP TECHNICAL NOTE
(SMAP Sub-task 1B)

DEFINITION OF GENERALIZED CONCEPTS OF SAFETY MARGINS AND CHARACTERIZATION OF SAFETY MARGIN SOURCES

JT00188205

English text only

FOREWORD

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

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

Task 1 : Definition of Safety Margins and Related Concepts
Task 2 : Assessment Process for Safety Margins
Task 3 : Safety Margin Evaluation Methods
Task 4 : Quantification of Safety Margins
Task 5 : Preparation of a CSNI Guidance Document.

This Technical Note, which represents a SMAP working document, is the result of the SMAP Task 1 - Sub-task 1B:

a) Define generalised concepts of safety margins
b) Characterise sources of safety margins.

Although this paper is an outcome of extensive discussions of the whole SMAP Group, the special appreciation belongs to J. Hortal (CSN Spain) and M. Gavrilas (US NRC) who provided the first outline of this document, as well as to A. Prosek (Institut "Jozef Stefan, Slovenia) and J. Zhang (TRACTEBEL Engineering, Belgium) who provided valuable written comments.

TABLE OF CONTENTS

1. INTRODUCTION 5
2. THE CONCEPT OF SAFETY MARGINS IN DESIGN BASIS SAFETY ANALYSIS 5
3. GENERALIZED CONCEPT OF SAFETY MARGINS IN THE RISK SPACE 8
4. METRICS FOR SAFETY MARGINS. USE AND AGGREGATION OF SAFETY INDICES 11
5. EXISTING REGULATORY LIMITS. FREQUENCY RANGES 15
6. METHODOLOGICAL ASPECTS 18
REFERENCES 19

1. INTRODUCTION

The CSNI Action Plan in the Area of Safety Margins (SMAP) is being developed with the following objectives:

1. To agree on a framework for integrated assessments of the changes to the overall safety of a plant as a result of simultaneous changes in plant operation/condition.
2. To develop a CSNI document, which can be used by member countries to assess the effect of plant changes on the overall safety of the plant.
3. To share information and experience.

A detailed task list has been defined to be developed in a 2.5 year period. This Technical Note is the result of the activities under Sub-task 1B: *Define generalized concepts of safety margins and characterize sources of safety margins*.

2. THE CONCEPT OF SAFETY MARGINS IN DESIGN BASIS SAFETY ANALYSIS

The existing nuclear power plants were designed on the basis of the fundamental safety principles applicable in each country. Defense-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 defense-in-depth principle, the design basis safety analyses are usually performed in a deterministic approach, in which a set of design basis accidents (DBAs)1 are analyzed [2]. An adequate selection of the analysis cases, the use of enveloping and/or conservative codes 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 includes room for insufficient knowledge or uncertainties associated with the design and operation of the plants.

S*afety margin* is a fuzzy term. 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. It is not so clear, however, which particular margin is named with the term *safety margin*. 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 looses 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 the *regulatory acceptance criterion* [2]. The regulatory acceptance criterion is in turn set sufficiently conservative to effectively render negligible the probability of failure. In other cases (see, for example, [7]), 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.

Both types of margins have been found useful for judging the level of safety of a plant. It is clear that, whenever a system or barrier performs a safety function, a margin can be defined to measure the extent to which plant behavior 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

[1] The term Design Basis Accidents (DBAs), as used in this paper, explicitly includes all the analysis cases typically considered in safety analysis reports under the title "Accident Analysis". They range from anticipated operational events (often referred to as "transients") up to postulated accidents like large break LOCA, or rod ejection.

safety barriers or systems, and the existing margin becomes divided in two parts (not necessarily measured in the same units, as discussed below) accounting for the distance from the plant performance to the regulatory limit and from the regulatory limit to the loss of function, respectively. The consequences to the environment or to the workers of the plant operation under normal or abnormal conditions are also subject to regulatory limits, and it is also possible to define margins with respect to those limits.

Although the design basis safety analysis methodologies may vary from country to country or among different technologies, they have common elements that can be described as a set of conceptual steps where different types of safety margins can be identified. These steps are summarized in the following description and illustrated in Figure 1. In this figure, vertical displacements are indicative of safety margins (e.g., Analytical Margin, Licensing Margin, Source Term Margin) while horizontal displacements are indicative of consequential phenomena changing the nature of the significant magnitude used to characterize safety margins. Only those margins represented over the same vertical line are measured in the same units. Note also that a single *safety variable* (SV) with its corresponding acceptance criterion and a single *barrier failure mode* are explicitly represented, but their potential combinations with other similar items are also indicated. The terminology used for margins and limits in this description is not necessarily standard, but it has been found useful for the purposes of this paper.

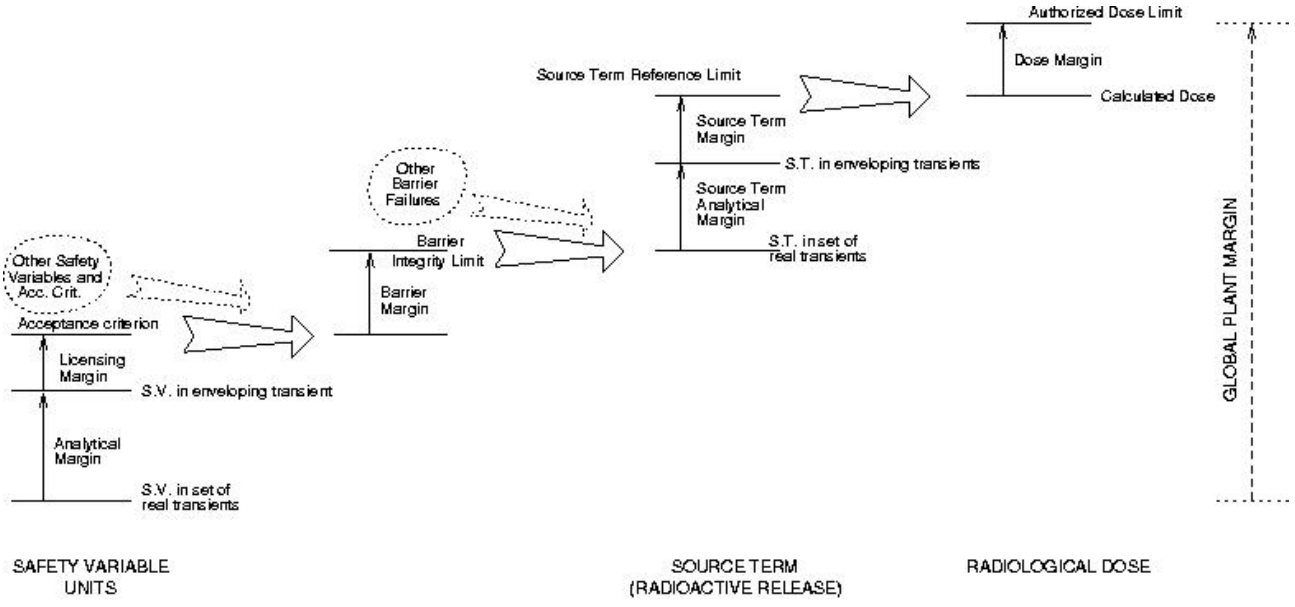

Figure 1: Safety margins in typical design basis safety analyses.

Characterization of barrier performance and related acceptance criteria

Since a key safety element in nuclear power plants is the existence of physical barriers to prevent the dispersion of radioactive material, safety margins should be considered firstly for potential failures of these barriers under adverse conditions. Proximity to barrier failure is characterized by one or more variables (*safety variables* in Figure 1) describing either the barrier performance or the behavior of other systems aimed at preventing the barrier loss. Suitable *acceptance criteria,* often converted into regulatory requirements, are then imposed in terms of those variables. They set the minimum acceptable safety standards that reduce the risk from nuclear plant operation to an acceptably low level. However, violating an acceptance criterion does not necessarily mean that the barrier actually fails. In other words, some margin exists between acceptance criteria and actual barrier failures. This margin has been represented in Figure 1 as *Barrier Margin*. These acceptance

criteria and related safety margins (i.e., the Barrier Margins) are discussed in detail in a separated Technical Note [4].

Selection of DBAs

Plant transients are usually grouped into *frequency classes* according to their probability of occurrence [2, 3] (see section 5). For each frequency class of real plant transients, a set of limiting DBAs (i.e., envelope transients) are selected. For each considered mechanism of barrier degradation there should be at least a protection and for each pair of degradation mechanism/protection, there should be at least a DBA. These transients/accidents are often artificially distorted in order to maximise the protection challenge and some extra conservatisms can be introduced. The differences between the consequences of the DBAs and those of the real plant transients eventually covered by them are called *Analytical Margins (AM)* in Figure 1.

Analysis of DBAs

The DBAs selected as representatives of each frequency class of real plant transients are analyzed to verify compliance with the applicable regulatory acceptance criteria. The analysis should account for uncertainties related to the codes and plant conditions, either by using a *conservative approach* or by adding the uncertainty band if a *best estimate approach* is used [6, 7]. The distance between the licensing calculation results and the acceptance criteria are called *Licensing Margins* (LM) in Figure 1. Generally, there is no restriction on how close to the acceptance criteria the results may go, but the acceptance criterion can not be exceeded in any DBA. When the licensing calculation SV value remains under the regulatory acceptance criterion, ***adequate safety margin*** is often said to exist. However, the correctness of this statement depends on the adequacy of the acceptance criterion which, in turn, depends on the verification of the remaining margins in Figure 1. Note also that there is not a single LM. For each combination of DBA and applicable acceptance criterion, there is a LM and all of them are verified in the safety analysis.

Radiological Consequence Analysis

Depending on the frequency class where a DBA is classified, some combinations of barrier failure modes may be allowed. Even when no barrier fails as a consequence of a transient, some limited barrier degradation is often assumed as initial condition for the analysis. Consequently, some amount of radioactive material can be released to the environment following a DBA. The amount of released radioactivity, usually classified in *radiological groups* according to the nature of the involved radionuclides, is generically called *source term*. For each frequency class, there will be one or more limiting combinations of barrier failures and transient conditions, resulting in maximum values of the source term. Following an enveloping method, similar to the initial selection of DBAs, a new set of radiologically significant DBAs is obtained for each frequency class with the criterion of maximizing the source term. These transients and accidents are analyzed in the *Radiological Consequence Analysis*, traditionally included in safety analysis reports. Again, the selection of DBAs may include unrealistic assumptions aimed at getting a safety envelope of all the possible real transients included in the frequency class. Note that, in general, the radiologically significant DBAs are not the same as the barrier significant ones, although they often appear with the same denomination in safety analysis reports. The source term analysis introduces a new margin in terms of the difference between the calculated source term in radiologically significant DBAs and the possible real source term resulting from transients covered by them. The term *Radiological Analytical Margin (RAM)* is used for this margin in Figure 1.

Dose calculation

In the last step of the safety analysis, source terms are used to calculate the radiological impact (doses) on the public or the plant workers. Several dose estimations which may include whole body or specific organs doses, population averaged or individual, are calculated. These dose calculations are conditioned by site characteristics, and limiting environmental conditions are considered in the analysis. The source term values used in this step are either the ones obtained from the radiological consequence analysis or greater values used as *Source Term Reference Limits*. In the latter case, the source term and dose calculations become decoupled and a new margin is introduced as the difference between the maximum calculated source term (for each frequency class) and the corresponding *Source Term Reference Limit*. This margin is the *Source Term Margin (STM)* in Figure 1. In any case, the resulting doses must be lower than the A*uthorized Dose Limits*, both for annual average doses and for per-event doses. The difference between the calculated doses and the corresponding Authorized Dose Limit is identified as *Dose Margin (DM)* in Figure 1.

All these margins can be considered as contributors to a *global plant margin* with respect to the primary regulatory limits --the radiological limits. In this sense, they can be called *subsidiary plant margins*. It should be pointed out that, although conceptually "consecutive", the different types of subsidiary plant margins contributing to the global plant margin are 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 is not purely additive. Moreover, there are concurrent margins originating from the consideration of different safety variables and different DBAs for a single failure mode, different failure modes for the same barrier, etc. Therefore, the global plant margin, although composed by all the subsidiary margins, cannot be measured on any specific scale, unless subsidiary margins are aggregated in a *safety margin metrics* framework such as the one described in section 4.

The above definitions, based on the whole process of design basis safety analysis methods, cover a wider scope than the previous IAEA definitions, focusing on the barrier integrity analysis in design basis accidents [7, 8]. Other margins related to the plant design (design margin), equipment performance (equipment margin) and plant operation conditions (operational margin) are not explicitly discussed. Some of them refer to safety aspects already covered by the above margins and others result from the verification of some analysis assumptions. For example, the equipment margin verification ensures that the actual equipment performance fulfils the assumed performance in safety analyses. All these margins are considered as embedded in the current licensing basis (safety analysis report and technical specifications) for the existing plants, and need also to be assessed for any plant modification.

3. GENERALIZED CONCEPT OF SAFETY MARGINS IN THE RISK SPACE

At the initial stages of the nuclear industry development, the protection engineering was dominated by system dynamics techniques with a qualitative view of the frequency and probability arguments that inevitably appear as an essential constituent of protection problems. Well defined, enveloping scenarios (DBAs), classified into a few frequency classes, were taken as a design basis. This follows a parallel philosophy to the control system design where the response to step and ramp signals, selected with enveloping criteria, are extensively used as a design basis for system response optimization. This engineering practice was also reflected in licensing requirements since it was considered that the study of the detailed plant response to DBAs provided a satisfactory basis to evaluate the protection adequacy for all situations.

For this limited set of design basis scenarios, that we call the *design basis space*, it is possible to define some class-specific acceptance criteria in terms of extreme values allowed for safety variables. This way, a sufficient safety margin is guaranteed for any scenario covered by the design basis space provided

that uncertainty associated with the predicted safety variable value and with the acceptance criterion is appropriately considered.

Worldwide experience thereafter and especially the occurrence of the TMI accident showed that more complicated scenarios, resulting from out-of-design sequences of events that escaped the design envelopes, needed to be addressed. The question of how to deal with so many possibilities made it inevitable to better evaluate their frequencies in order to weigh their relative importance. This gave rise to the incorporation of system reliability engineering techniques, as it had been advocated by some precursor studies, like WASH-1400 in U.S.A. or the *Deutsche Risikostudie Kernkraftwerke* in Germany. Among other important lessons learned from that experience was that operators and their actions were needed but not necessarily beneficial, so their impact should be taken into account. In parallel, some improvements in the design basis analysis methods were implemented in order to address these problems to the extent possible.

A comprehensive risk assessment requires, therefore, the consideration of all possible scenarios above a credibility threshold, i.e., that have non-negligible frequencies of occurrence. How to determine this threshold will be discussed later. We call this almost complete set of scenarios the *risk space*. An important difference with respect to the design basis space is that no limit in safety variables can be used as acceptance criterion since limit compliance cannot be assured for out-of-design scenarios. The same consideration applies for the loss of function of a safety barrier or system. In other words, no matter what limit is being considered, we can always expect some scenarios that go beyond the limit. Therefore, the concept of safety margin, as applied in the restricted design basis space, is no longer applicable. However, it is possible to extend this concept in such a way that it can be applied in the risk space while being consistent with design basis safety margins.

The underlying philosophy of the design basis safety margin is that the big majority of the possible scenarios in the plant are covered by the design basis accidents and, therefore, they do not challenge the limit if the DBAs do not. Moreover, out of design scenarios going beyond the limit are so unlikely that they do not need to be considered. It is clear that, if exceeding the limit is found to be more likely than expected, we would have a loss of safety margin even if the acceptance criteria of the DBAs are still met.

One of the key elements of the extension of the safety analysis and the safety margin concept to the risk space is, therefore, the evaluation of the *exceedance frequency* of the limit. For this purpose, it is necessary to identify which scenarios in the risk space result in limit exceedance and evaluate their collective frequency. If this frequency is acceptably low, the margin evaluation in the traditional way, i.e., in terms of safety variable values, still makes sense for those scenarios remaining below the limit (*success* scenarios), whether they were expected to be covered in the design basis or not.

Another significant difference between the design basis space and the risk space is that, in the first case, the designer needs to reduce the number of scenarios composing the design basis envelope in order to make the protection design feasible. With continuously increasing computing capability, the verification of the design basis envelope may include the analysis of additional scenarios, although only the most limiting ones (i.e., only a few of them) finally constitute the design envelope. In the risk space, however, although the number of analyzed transients cannot grow to the infinity, there is more flexibility. As a consequence, the DBAs that constitute the design basis space are selected with the criterion of maximizing their enveloping character, even if this results in lack of realism. On the other hand, although the risk space must also envelop all possible situations, this can be done with a larger number of analysed scenarios, resulting in a higher degree of realism for each one of them.

This allows for a better characterization of the existing margin. In the design basis space, only the minimum margin is significant but, in the risk space, once the frequency criterion is met, it is also important to distinguish between situations with many success scenarios close to the limit and those with

most scenarios far away from it. If the margin of each success scenario with respect to a particular limit is adequately characterized, these margins can be combined (for example by frequency-weight averaging all the measured margins) into a single indicator of the plant margin with respect to the limit being analyzed. It should not be forgotten, however, that compliance with the frequency criterion is a prerequisite for margin quantification. If a limit-specific frequency acceptance criterion can be defined, the difference between this criterion and the calculated exceedance frequency for that limit is another component of the safety margin.

This way, we get a generalized concept of safety margin consisting of the joint consideration of two components, namely, the *frequency margin* and the *consequence margin*. Only when the frequency margin exists does the consequence margin need to be evaluated. The consistency between this generalized safety margin concept and the traditional one comes from the fact that the former is an extension of the latter or, in other words, the latter is a particular case of the former. If the frequency margin is taken for granted, rather than evaluated, the set of success scenarios to be analysed is reduced to the DBA and the consequence margin is measured by the minimum distance to the limit along the transient, the resulting safety margin is exactly the same.

A difficulty in the use of the risk space is the potentially unlimited number of scenarios to be considered. The number of scenarios that need to be evaluated grows with the degree of realism required. This number can be reduced in two ways: first, by grouping similar scenarios and analysing a single one from each group, selected with the criterion of maximizing the undesired consequences. The frequency assigned to this enveloping scenario should be that of the whole group. Second, by neglecting the influence of scenarios that are too unlikely. However, one should be careful in the application of this criterion since, if the number of ignored scenarios is very high, their collective influence can be significant and could not be neglected. Only if the collective frequency of **all** the ignored scenarios gives a negligible contribution to the limit exceedance frequency, they can be actually ignored. A screening process based on the individual frequency of each scenario is only advisable if the frequency threshold is several orders of magnitude below the acceptance criterion for the limit exceedance frequency. A third way of reducing the number of scenarios that need to be evaluated is a consequence of the safety margin metric introduced in the next section, and will be described there.

It should be pointed out that the number and nature of the limits being considered do not depend on the concept of safety margin being applied. The particular choice of limits should be such that all the safety aspects of the plant can be addressed. Safety margins are only the measurement instruments of those safety aspects. The same limits can be analysed with both types (traditional or generalized) of safety margins, although the application of the generalized concept needs some criterion to determine whether the exceedance frequency of each limit is acceptable or not.

An additional advantage of the extension of the safety margin concept to the risk space is that it allows for a lower dependency of safety analysis methods on technology details. The determination of the set of DBAs, although subject to some regulatory requirements, is mainly the responsibility of the designer, since it is oriented towards the design of the protection systems. A safety analysis method focusing on the design basis space, apart from its potential weaknesses identified above, is difficult to develop without a deep knowledge of design methodologies. On the other hand, the analysis of scenarios in the risk space requires a good knowledge on how the plant behaves, but depends much less on how it was designed. A consequence of this is that safety analysis methods based on the risk space analysis have a higher ability to address significant plant modifications like increased fuel burnup, power uprates or life extensions.

4. METRICS FOR SAFETY MARGINS. USE AND AGGREGATION OF SAFETY INDICES

4.1 Motivation for safety indices

One additional motivation to generalize the safety margin concept is to recognize the fact that knowledge is imperfect both for the predicted value of a safety variable, as well as for the actual value at which failure occurs. Treating both the predicted value of a variable and the actual value of a variable as randomly distributed, and assuming that they both follow a Gaussian distribution, the concept of safety margin is illustrated in Figure 2.

"Distribution of code predictions" in Figure 2 refers to the values obtained for the most limiting value of the safety variable, e.g., the maximum peak clad temperature during a transient. The distribution is a consequence of uncertainties in initial and boundary conditions, as well as the models that are used to compute the safety variable.

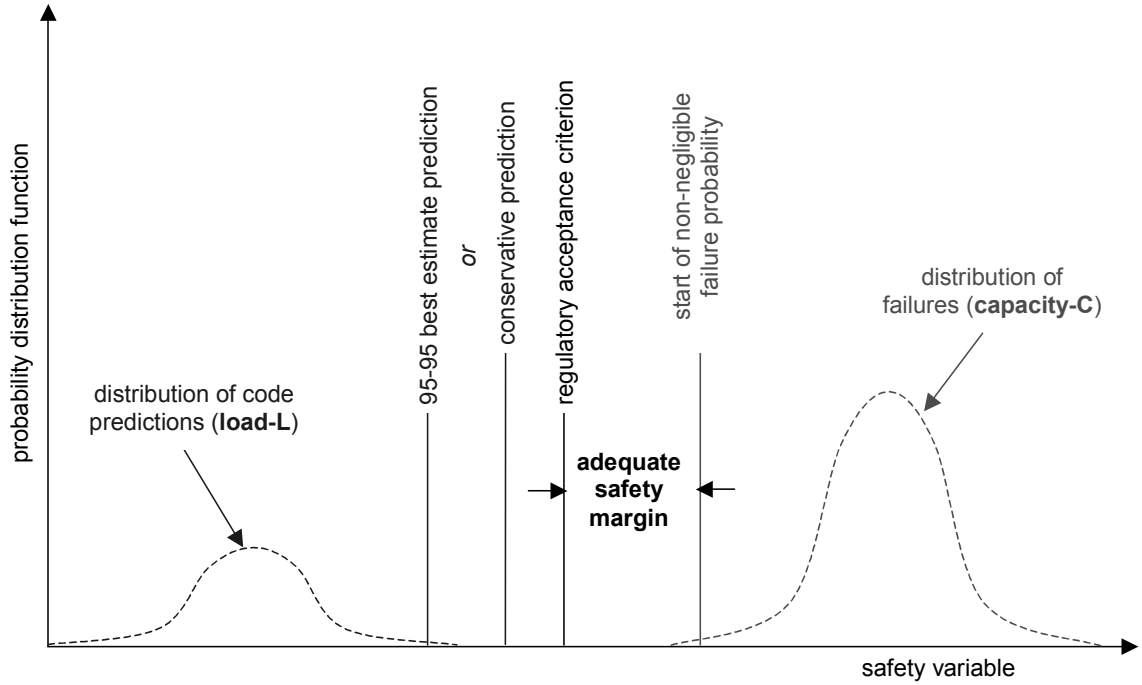

Figure 2. The concept of safety margins illustrated in light of uncertainties in computed value and failure point.

Similarly, "distributions of failures" is a consequence of the fact that failure is a random variable, e.g., if 100 containments are tested to failure, the peak containment pressure values at which each will fail will be randomly distributed along a range. Note that the representation of margins as depicted in Figure 2 is adapted from structural mechanics where the "load-L" and "capacity-C" of a structural component are represented with distributions corresponding to "code predictions" and "failures," respectively.

4.2 Extension into risk space

The safety margin concept can be extended to the risk space by developing a set of metrics that correspond to individual safety variables. Effectively, these metrics are an extension of the existing concept of safety margins. Examples of such metrics are those corresponding to margin to fuel failure, margin to breach to the reactor coolant system boundary and margin to containment failure.

To be able to simultaneously consider all the acceptance criteria impacted by a given plant modification, these safety metrics have to be placed on a common scale. A natural means of devising the common scale is by using the probability of damage associated with the safety variable during a transient. However, such a measure is, in most cases, beyond the current state of the art. This is because the failure probability, C in Figure 2, associated with defence-in-depth barriers (fuel, reactor coolant boundary and containment) is largely unknown. A further complication arises because not only does the failure probability change as a function of safety variable value, but the extent of damage changes simultaneously. For example, as peak clad temperature increases, so does not only the probability of core damage, but also the extent of core damage increase as more and more pins reach the threshold for damage initiation.

The reasons above make it impractical to use actual damage probability. Yet the need to account for consequences when the safety variable escalates into the damage probability range exists for a) plants that seek modifications when they have limited safety margins, and b) advanced reactors that have passive systems that cause code predictions to have very large uncertainties. In other words, if realistic decisions are to be made, the decision-maker must specifically address event scenarios that have non-negligible damage probabilities.

A surrogate approach is to cast safety margins in utility function form by using predefined normalization ranges. The resulting metrics take values between zero and one, and are called safety indices. A proper normalization range is physically significant. For example, accepting the fact that failures do not occur discretely, a range can be defined to span the region from the highest safety variable value at which the barrier or system remains intact to lowest value at which the barrier or system has lost its function. Thinking of safety margins as spanning a range is inherent in the fact that both the failure point and the code prediction are uncertain, and that any realistic analysis of safety has to take into account these sources of uncertainty.

A possible method is to introduce a "safety index" that measures the ascent of a safety variable into the non-negligible damage probability range. An example range, the one associated with the minimum margin, is shown on Figure 3.

For instance, using peak clad temperature as the safety variable, the upper limit would correspond to the point of onset of substantial core disruption 1800°C (3272°F). For a large break LOCA in a PWR, the uncertainty range is about 190°C (300°F). Thus, a suitable range for the margins index would be 1610°C (300°F) to 1800°C (3272°F). The safety index, i_{margin}, is the normalized value of the best estimate predicted safety variable within the normalization range:

$$\begin{aligned} i_{margin} &= 1 \quad for\ f(t)_{\max} < LL \\ i_{\text{margin}} &= \frac{\text{UL} - f(t)_{\max}}{\text{UL} - \text{LL}} \quad for\ LL < f(t)_{\max} < UL \\ i_{margin} &= 0 \quad for\ f(t)_{\max} > UL \end{aligned} \qquad \text{Equation 1}$$

where $f(t)_{max}$ is the maximum peak clad temperature during the event scenario simulation, and LL and UL, are the upper and lower limits of the normalization range depicted on Figure 3.

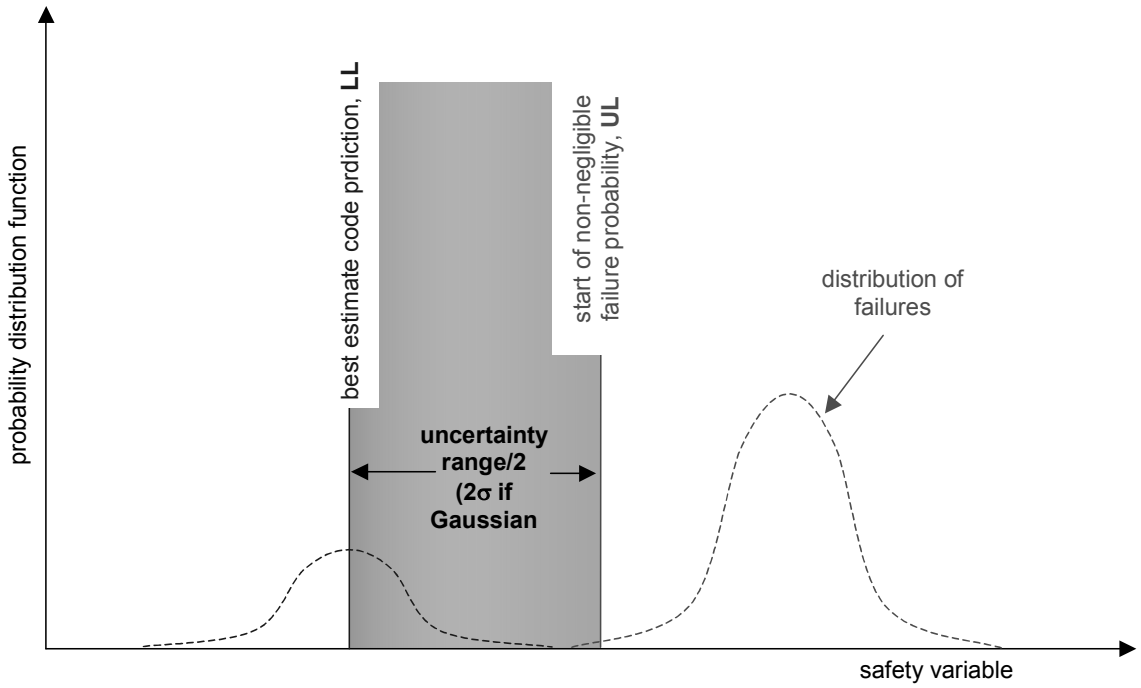

Figure 3. Defining the range for the minimum margin index

Note that the safety index takes a value of one when there is a negligible probability of damage and a value of zero when there is a 100% probability of damage. This reduces the number of necessary code runs, because for transients that are known *a-priori* to have negligible damage probability, a safety index of one can be assigned. Similarly, if an event scenario is known *a-priori* to have a 100% damage probability, the safety index is assigned a value of zero. This is somewhat analogous to the use of success criteria in *probabilistic safety/risk assessment* (PSA/PRA)[2]. This reduction in code runs is in addition to the reductions achieved by grouping of events and discarding events with negligible frequency of occurrence discussed in the previous section.

Safety indices are defined for every safety variable and every barrier or system that is impacted by the design modification and they are computed for every event scenario affected by the proposed plant modification. Safety indices that quantify other safety characteristics, such as time spent near the acceptance criterion or time available for operator intervention can also be defined.

To calculate the overall change in one safety index over the entire event scenario space affected by the plant modification, the indices for each event scenario are frequency-weighted into an aggregate index of the form

$$\overline{i} = \frac{\sum_{\text{all}\,event\,scenarios} (i_{\text{margin,i}} \cdot f_i)}{\sum_{\text{all}\,event\,scenarios} f_i}, \qquad \text{Equation 2}$$

where $i_{margin,i}$ and f_i are the safety index and occurrence frequency of event scenario i.

[2] The terms *"probabilistic safety assessment"* and *"probabilistic risk assessment"* and their respective acronyms *"PSA"* and *"PRA"* are considered equivalent in this document. The former option will be used hereafter.

The aggregate index is a risk metric as it simultaneously considers the probability of occurrence (via the frequencies of each event scenario) and the consequences (via the safety index for the event scenario). The dyad of aggregate safety index and frequency of exceeding the upper limit (UL) of the range provides the comprehensive risk information needed for the decision.

Just like the probability, the safety index is dimensionless and takes values between zero and one. This makes it possible to simultaneously use safety indices associated with different damage mechanisms within the same aggregate index. For example, the consequences of event scenarios in which the containment is damaged by internal pressure can be considered simultaneously with damage induced by external events. Similarly, damage caused to the fuel by loss of coolant accidents can be aggregated with damage caused by reactivity excursion accidents by using either peak clad temperature or enthalpy deposition rates in computing safety indices for each event scenario.

Safety indices also make it possible to consider the safety consequences of non-traditional performance parameters in the decision. For example, the time for operator intervention can be formulated as an index. This quality lends itself to applications to a broad range of technologies.

A final remark needs to be made with respect to the computational effort required to compute aggregate indices. The increased computational expenditure relative to conventional PSA figures of merit is a consequence of the realism required in the decision. With the advances achieved in computer power and numerical methods since success criteria were first introduced in PSAs, the expenditures required to calculate safety indices using best estimate code predictions are quite manageable.

4.3 Global safety indices

If multiple safety indices are used simultaneously, e.g., one for fuel margins and another for containment margin, the decision-maker must attribute importance weights to each aggregate index. This is a challenge of the method and requires further work. However, multi-attribute decisions have clearly established precedence in regulator decision-making, most prominently in using ΔCDF and ΔLERF simultaneously to judge the acceptability of a plant modification. There is a trade-off between accepting the large uncertainty associated with the high level risk metrics, such as person-rem, and assigning weights to the various elements that enter a risk-decision. In limited scope analyses, i.e., analyses that only rely on a limited number of well correlated safety indices, the price of accepting unnecessary conservatism can be eliminated through the use of safety margins indices.

The set of aggregate indices can then be combined into a global safety index by importance weighing each aggregate index. The importance assigned to each aggregate index reflects the priorities of the decision maker.

Computing and aggregating safety indices are described with more detail in [9]. This extension of importance weighing aggregate safety indices is necessary in any decision that involves the simultaneous consideration of multiple factors. The implementation of the safety index methodology would only require the overt ranking of factors, which increases the transparency of the method.

The safety index method provides the regulator with a transparent set of risk metrics. The construct of the method is such that all safety concerns can be included through the definition of an index. At the same time, the safety index risk metrics provide the information at the lowest level possible for each individual decision, as opposed to the traditional risk metric of person-rem, which is at the highest possible level. This has the advantage of limiting uncertainty and effort, as in most cases it becomes unnecessary to propagate consequences from breach of the fuel to radiological dose at the plant boundary, especially if the decoupling techniques typical in safety analyses [4] are applied.

The safety index method can also be used to examine the risk of initiating events that are not part of existing PSAs. Examples are oscillations in BWRs that occur because of recirculation pump trips. The computational expenditures of applying the safety index method are comparable to that required to expand a quality PSA for a new initiator. In general, the computation and aggregation of safety indices is a refined tool for regulatory decision makers that only carries additional computational burden relative to traditional risk computations if the required detail justifies such expenditures.

5. EXISTING REGULATORY LIMITS. FREQUENCY RANGES

Licensing requirements regarding plant protection performance are typically defined as acceptance criteria for transient analysis in the design basis space. According to [2], the IAEA proposes two levels of acceptance criteria to take into consideration:

> *Basic (high level) acceptance criteria are usually defined as limits by a regulatory body. They are aimed at achieving an adequate level of defence in depth. Examples would be doses to the public or the prevention of consequential pressure boundary failure in an accident.*
>
> *Specific acceptance criteria, which may include additional margins, are often developed as well. These acceptance criteria are chosen to be sufficient but not necessarily to meet the basic acceptance criteria. Typically they are used to confirm that there are adequate safety margins beyond the authorized limits to allow for uncertainties and to provide defence in depth. They may be developed by the designer and/or owner and approved by the regulatory body; or they may be set by the regulatory body itself. An example of the latter would be a limit on the cladding temperature in a LOCA in a PWR.*

(...)

> *In some jurisdictions the regulatory body may approve the whole set of acceptance criteria (basic acceptance criteria, specific acceptance criteria and sometimes even analysis targets). In other jurisdictions the regulatory body may not formally approve the more specific criteria or analysis targets but review the choices made by the applicant.*

As stated before, DBAs are classified in qualitative frequency groups. Both basic and specific acceptance criteria are defined for each group. Table 1 below is a particular example of event classification and applicable acceptance criteria taken from [2]. Other frequency classifications have been proposed and used but, most often, they differ only in details.

TABLE 1: POSSIBLE SUBDIVISION OF EVENT OCCURRENCES (IAEA)

Occurrence (1/reactor-year)	Characteristics		Terminology	Acceptance criteria
$10^{-2} – 1$ (Expected in the life of the plant)	Expected	Anticipated Operational Occurrences	Anticipated transients, transients, frequent faults, incidents of moderate frequency, upset conditions, abnormal conditions.	No additional fuel damage
$10^{-4} – 10^{-2}$ (Chance greater than 1% over the life of the plant)	Possible	DBAs	Infrequent incidents, infrequent faults, limiting faults, emergency conditions.	No radiological impact at all or no radiological impact outside the exclusion area.
$10^{-6} – 10^{-4}$ (Chance less that 1% over the life of the plant)	Unlikely	BDBAs	Faulted conditions	Radiological consequences outside the exclusion area within limits.
$<10^{-6}$ (Very unlikely to occur)	Remote	Severe accidents	Faulted conditions	Emergency response needed

Some remarks should be given about the interpretation of tables of this kind. The structure of the tables suggests that, given a design basis event, it should be classified according to its expected frequency and then the applicable acceptance criteria become identified. However, it cannot be forgotten that the ultimate goal of the safety analysis is to verify that the radiological consequences of abnormal events are within acceptable limits. Taking into account that the choice of DBAs is not unique and that a single DBA may cover several or many possible events, it could happen that classifying many events by their individual frequency in the same group could lead to a damage level that, while being within the limits of the group, occurs nevertheless at an unacceptable frequency. The frequency boundaries of each group apply, therefore, to the collective frequency of all the transients/accidents included in the group or covered by them. In some cases (see for example [3]) this precaution is explicitly addressed by defining the frequency groups as *"events **any of which** may occur during..."*

In addition, it should be recalled that DBAs are intended to be very enveloping, even if this results in lack of realism. To estimate the frequency of an unrealistic event is rather difficult and it only makes sense if the frequency assigned to the DBA is that of all the scenarios covered by it.

These difficulties are overcome if tables similar to Table 1 are not interpreted solely as a guide for event classification but also as a condition for acceptability of a given classification of DBAs based on the amount of damage that can be accepted for each range of frequencies. For example, the row corresponding to "Unlikely" events in Table 1 would be interpreted as follows:

a) Events of any kind resulting in radiological consequences outside the exclusion area beyond the established limits should not occur at frequencies higher than 10^{-6} per year.

b) The collective frequency of all the plant transients classified as "Unlikely" should not be greater than 10^{-4}.

If a high quality PSA is available and its success criteria are compatible with the acceptance criteria of design basis frequency groups, the assessment of the frequency classification would be much easier.

Each acceptance criterion applies, therefore, only above a specific frequency value. Exceeding the limit at a frequency lower than this value is acceptable from the safety point of view. Note that this evaluation only makes sense in the risk space. The big value of the analysis in the design basis space is that it allows the translation of safety requirements into protection features but the verification of the plant safety level is better done in the risk space by checking the exceedance frequency of every regulatory limit. Acceptable frequency boundaries for each regulatory limit could be determined from existing legal or technical standards or from very general principles such as established safety goals.

The highest level regulatory limits are the radiological limits since the final objective is to avoid radiological damage. Typically, there are two kinds of radiological limits: annual dose limits to the population or the workers and per-event dose limits at specified locations. The former result in conditions for normal operation of the plant, including the anticipated occurrences that may happen during the plant life. The latter are used as design basis for protection areas around the plant site and apply to event classes with potentially high consequences whose contribution to annual doses is, nevertheless, negligible due to their very low likelihood. For anticipated events, the annual dose limits can also be converted to per-event limits taking into account the expected frequency of each event class.

The generation of radiological damage, i.e., dose, is a consequence of dynamic processes in the plant. It is, thus, necessary to know how these processes relate with damage generation in order to characterize the level of safety of a plant. However, the relationship between plant process variables and generated dose involves several intermediate physical mechanisms of very different nature which make it very difficult to formulate such a relationship in a suitable form. The usual way to solve this problem while maintaining the *defence in depth* philosophy is to obtain a set of surrogate limits, equal or more restrictive than the dose limits, and applicable to variables more directly related with the internal processes in the pant. Compliance with these surrogate limits (equivalent to the *specific acceptance criteria* of [2]) will guarantee compliance with the dose limits.

This process is based on decoupling principles and mechanisms which are discussed in more detail in [4]. Note that each surrogate limit is derived from a particular higher level limit. As a consequence, the frequency range where the surrogate limit applies is related with the frequency range of the basic limit from which it is derived. Although in many cases the frequency range of the surrogate limit will be just the same, it could be different if the relationship between the primary and the surrogate limit is probabilistic or subject to significant uncertainty.

6. METHODOLOGICAL ASPECTS

Sections 3 and 4 above already included some discussions about what kind of methodologies can be used for the assessment of generalized safety margins. The aim of this section is not to discuss in detail a methodology which is still under development, but to address general requirements and concerns with regards to quantifying generalized margins.

One of the results of the discussion in Section 3 is that the assessment of generalized safety margins requires the consideration of the whole risk space rather than the design basis space. For this purpose, a complete set of significant scenarios must be identified and, in order to reduce the analysis effort, the use of grouping and enveloping techniques is inevitable. Also, it was shown that a safety margin assessment can be performed whenever a limit is defined. What limits and associated margins should be considered in each particular case depends on the nature of the safety question being answered.

Every significant scenario constituting the risk space should be classified with respect to each limit being assessed. Those scenarios where the limit is exceeded contribute to the estimation of the frequency margin while the scenarios where the limit is not reached (success scenarios in the PSA terminology) are used to characterize the consequence margin. For this purpose, the safety margin metrics described in Section 4 are particularly adequate.

The tasks of scenario identification and classification and frequency calculation can be developed by extending the event tree / fault tree techniques currently used in PSA. However, some precautions should be taken when extending a technique originally developed for single limit analysis to the case of multi-limit analysis.

In existing PSAs, the sequence classification criteria, also called sequence success criteria are often used at fault tree level in order to determine whether the safety function represented by an event tree header can be considered successful or not. As a consequence, if the sequence classification criteria are changed, the fault trees should be revised. This dependency can be avoided if the fault tree success criteria are defined only at system level (i.e., whether the system works in a given configuration) not at function level (i.e., whether the system is able to reach some objective). The function level success should then be assessed as a part of the sequence verification which is needed in the sequence classification process.

A complete verification of the risk space scenarios should be done with a double objective. First, to adequately classify each scenario, according to its consequences, with respect to each limit. Second, to determine which event tree headers are actually called for intervention in each scenario. Two dynamically identical scenarios, one where a particular safety function has been unsuccessfully demanded and another where that safety function has not been demanded, give very different contributions to the frequency calculation. These difficulties, already present in traditional PSA, are more difficult to solve in the case of multi-limit analysis. In addition, the application of a safety margin metric requires rather detailed knowledge of the evolution of significant variables in each scenario. These considerations lead to the conclusion that the use of powerful simulation resources is almost inevitable. Traditional transient analysis techniques can be adapted for this purpose, taking into account that some typically conservative assumptions made in design basis analysis could be no longer reasonable or necessary for analysis in the risk space.

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 Sub-task 1C), August 2005, NEA/SEN/SIN/SMAP(2005)4*
5. *Quantifying Reactor Safety Margins*; USNRC NUREG/CR-5249; 1989.
6. L. E. Hochreiter, R. D. Ankney, M. Y. Young and S.P. Kalra, *Application of PWR LOCA margin with revised Appendix K rule*; Nuclear Engineering and Design, 132, 1992.
7. *Safety margins of operating reactors. Analysis of uncertainties and implications for decision making*; IAEA TECDOC-1332; Vienna, Jan. 2003.
8. *Implications of power uprates on safety margins of nuclear power plants*; IAEA TECDOC-1418; Vienna, September 2004.
9. 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