Unclassified **NEA/CSNI/R(2007)9**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(2007)9
Unclassified

Task Group on Safety Margins Action Plan (SMAP)

Safety Margins Action Plan - Final Report

English text only

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

* * *

This work is published on the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full member. NEA membership today consists of 28 OECD member countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Republic of Korea, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has a Co-operation Agreement, as well as with other international organisations in the nuclear field.

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made up of senior scientists and engineers, with broad responsibilities for safety technology and research programmes, and representatives from regulatory authorities. It was set up in 1973 to develop and co-ordinate the activities of the NEA concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations.

The committee's purpose is to foster international co-operation in nuclear safety amongst the OECD member countries. The CSNI's main tasks are to exchange technical information and to promote collaboration between research, development, engineering and regulatory organisations; to review operating experience and the state of knowledge on selected topics of nuclear safety technology and safety assessment; to initiate and conduct programmes to overcome discrepancies, develop improvements and research consensus on technical issues; to promote the coordination of work that serve maintaining competence in the nuclear safety matters, including the establishment of joint undertakings.

The committee shall focus primarily on existing power reactors and other nuclear installations; it shall also consider the safety implications of scientific and technical developments of new reactor designs.

In implementing its programme, the CSNI establishes co-operative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA) responsible for the program of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also co-operates with NEA's Committee on Radiation Protection and Public Health (CRPPH), NEA's Radioactive Waste Management Committee (RWMC) and NEA's Nuclear Science Committee (NSC) on matters of common interest.

FOREWORD

Recent NPPs operating experience shows that in some cases operational and design modifications may lead the plant far away from the original design. Some experts have expressed concerns that 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 the 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 sufficient safety margin exists.

In 1998, the Committee on Nuclear Regulatory Activities issued a report on Future Nuclear Regulatory Challenges. This report discussed the potential erosion of safety margins as an area for further research. 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 consisted 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 Final Report is the result of the SMAP Task Group work as detailed in several Technical Notes issued during the 3-year activity period. Mr Odbjörn Sandervåg (Sweden) skilfully chaired the meetings and the work of the Task Group, which comprised representatives from Belgium, Canada, Czech Republic, Finland, France, Germany, Japan, Korea, Mexico, Slovakia, Slovenia, Spain, Sweden, Switzerland, the USA and the IAEA. The technical secretariat was mainly carried out by Mr. Miroslav Hrehor (OECD Nuclear Energy Agency).

The authors of this final SMAP report are as follows:

Dr. Mirela Gavrilas, NRC, United States, lead Author

Mr. Josef Belac, NRI, Czech Republic
Mr. Risto Sairanen, STUK, Finland
Mr. Giovanni Bruna, IRSN, France
Dr. Michel Réocreux, IRSN, France
Ms. Françoise Touboul, CEA, France
Mr. Krzykacz-Hausmann,GRS, Germany
Dr. Jong Seuk Park, KINS, South Korea
Mr. Andrej Prosek, IJS, Slovenia
Mr. Javier Hortal, CSN, Spain
Mr. Odbjörn Sandervåg, SKI, Sweden, SMAP Chairman
Mr. Martin Zimmerman, PSI, Switzerland

TABLE OF CONTENTS

EXECUTIVE SUMMARY

ES. 1 Background

The decision by the CSNI to develop an Action Plan on Safety Margins (SMAP) arose from the possibility that some changes in existing nuclear power plants could challenge safety margins despite fulfilling all the regulatory requirements. Possible examples are power uprates, plant life extension or increased fuel burnup as well as cumulative effects of simultaneous or subsequent modifications in a plant, which can conceivably be larger than the accumulation of the individual effects of each individual modification. The magnitude of the problem gets bigger as the design modifications push the plant closer (or possibly even beyond) the edge of the original design envelope. In order to monitor the impact of such modifications onto the safety margin, analysis methodologies able to treat the problem in an integrated manner must be developed.

Nowadays, a safety analysis is in most cases performed using either the deterministic or the probabilistic approach. The deterministic approach typically considers a reduced number of limiting transients for which conservative rules for system availability and parameter values are often applied. The accident phenomenology and the related timing are estimated as complete as necessary. In turn, the probabilistic approach emphasizes the completeness of the set of different scenarios and best estimate methods. The approaches have been developed rather independently from each other. This then poses the problem of integrating the two approaches consistently into a single comprehensive methodology necessary to explore safety margins in a general sense. Additional motivation derives from the observation of an increasing trend to use information on risk (where the term “risk” means “results of the PSA/PRA analysis”) to support regulatory decisions that pertain to many countries. Hence, a generalisation of the concept of safety margin is needed in order to make this concept operable in both the probabilistic and deterministic field of application while maintaining the traditional meaning to the maximum extent possible.

To this aim, the CSNI approved the Action Plan on Safety Margins (SMAP) in December 2003 and established an international Working Group aimed at developing a methodological framework for integrated safety assessments of the changes to plant safety as a consequence of simultaneous plant modifications related to the design and the operational envelopes.

ES. 2 Objective of the work

The main objective of the Safety Margin Action Plan (SMAP) Task Group has been to develop guidance on how to assess safety margins in nuclear power plants. The addressees of this guidance include the evaluators in regulatory organisations who must decide on the acceptability of plant changes from the regulatory safety point of view. Nevertheless, other users could also benefit from the results of the SMAP work.

In order to achieve the general objective, three more detailed objectives were defined that have guided the development of the work:

- To agree on a common conceptual framework that, based on both deterministic and probabilistic considerations, could address the safety margins problem.
- To develop guidance on how safety analysis methods and tools can be used to address the safety margins problem.
- To exchange information and experience among the participating organisations.

ES. 3 Description of the work (summary of the Final Report)

In the traditional safety analysis framework, safety margins are introduced in recognition of the fact that uncertainty exists about the proper value(s) of the (set) of safety variable(s) characterizing onset of some type of damage. By setting the regulatory acceptance limits conservatively with respect to the onset of damage, sufficient margin is assured in Design Basis Accidents. Safety margins are introduced at several stages of the analysis where successive acceptance criteria are defined on the basis of decoupling criteria with the ultimate goal of protecting the public and the environment from radiological hazards of potential releases from the plant. Figure 2-1 of this document summarizes the usual types of safety margins used in current safety analyses. The complexity of the analysis and the fact that these margins are defined only at the level of specific scenarios included in the safety analysis makes it difficult to establish a clear relationship between safety margins and overall plant safety, especially when significant concurrent plant modifications are implemented.

At the first stages of the nuclear industry development, protection engineering was dominated by system dynamics techniques with a qualitative view on frequency and probability arguments that inevitably appear as an essential constituent of protection problems. In this mostly deterministic approach, well defined, enveloping scenarios (Design Basis Transients or Accidents, DBT/DBA), classified into a few frequency classes, were taken as the design basis. Class-specific acceptance criteria, set in terms of acceptable extreme safety variable values, were defined for these scenarios as a means to ensure that an adequate level of protection is provided by the plant design, at least for those scenarios covered by the design basis envelope. Due consideration of uncertainty associated with the predicted safety variable value is required in this demonstration. A summary of typical accident classifications, limits and criteria, involved margins and methodological aspects of this approach, mainly taken from French and Finnish regulations, is included in Chapter 2 of this report.

Although the analysis of DBT/DBA is still the most consolidated approach for safety analysis, worldwide experience and especially the occurrence of the TMI-2 accident showed quite soon that more complicated scenarios, resulting from out-of-design sequences of events needed to be addressed. The question of how to deal with so many possibilities made better evaluation of their frequencies inevitable in order to weight their relative importance. This gave rise to the incorporation of system reliability engineering techniques and to the development of the probabilistic approach to safety analysis. Deterministic and probabilistic approaches have existed side by side, contributing with usually complementary insights to the assessment of plant safety, although a consistent use of both approaches is not always easily achieved.

The extension of the reduced set of design basis scenarios (the *design basis space*) to the almost complete set of credible scenarios, including out-of-design situations, leads to the concept of *risk space* where the safety margin assessment framework proposed by the SMAP group should be applied.

As in any other safety approach, including the traditional deterministic one, the “set of triplets” scheme, where each triplet is composed by an identified scenario, its likelihood and its associated consequences, is useful to guide both the description and the application of the proposed analysis approach.

According to this scheme, the first step is the identification of the risk space, i.e., the set of scenarios to be included in the analysis. Event tree techniques, similar to those used in traditional PSA have been found useful for developing a description of the risk space. Both PSA sequences and Design Basis scenarios are taken as initial references for this development, while trying to overcome the limitations of the traditional approaches. On one hand, unlike DBA, risk space scenarios include consideration of non safety-grade equipment as well as failures of qualified safety systems. On the other, the PSA scope is extended to include any type of safety objectives and an explicit consideration of safety margins for each particular sequence. Risk space event trees should have the capability to address, among other possible safety objectives, safety limits and acceptance criteria traditionally applied to DBAs. These extensions make the risk space event trees potentially very different from those of traditional PSA, keeping in mind that traditional PSA focuses only on the safety limits used as acceptance criteria for large break LOCA analysis, which are the sequence success criteria in level 1 PSA.

A consequence of the above is that the determination of the end state of a risk space sequence is more difficult because the success criteria of the safety functions (represented by event tree headers) depend on the respective safety objective being analyzed. Hence, identification of the end states with the aid of dynamic models is highly recommended. At the same time, it provides additional support for sequence delineation since the actual involvement of the event tree headers in each sequence can be confirmed. Extensive dynamic verification also allows for better accounting of dynamic dependencies of probabilities and even opens the possibility of considering stochastic events (such as hydrogen combustion) as particular cases of event tree headers.

In summary, the capability of a risk space model (i.e., a particular set of event trees) to address a given set of safety objectives depends mainly on the following three elements:

- What safety functions and associated systems have been considered?
- How have initiating events and subsequent transient paths been grouped into event tree sequences?
- To which extent are fault trees re-usable for analyses of different safety objectives? A high degree of decoupling between sequence success criteria and fault tree structure is needed for this aim.

Any change in the plant design or in the operation strategies may have an impact on the risk space model. In order to identify whether a detailed analysis is needed, it has been found useful to follow the same philosophy outlined in the U.S. regulations (10 CFR 50.59) for determining the need of a regulatory review for plant changes. Since this regulation is intended only for DBT/DBA analysis, some changes in terminology are needed before applying this scheme to assess changes in the risk space. Whenever 10 CFR 50.59 states "*accidents previously analyzed in FSAR*" it should be replaced by "*sequences previously identified in the risk space*"; and so on.

The figure of merit in probabilistic analyses is the expected frequency at which the sequence success criterion (i.e., the safety objective being analyzed) is exceeded. This is so in traditional level 1 PSA where the safety objective is to avoid severe core damage and the figure of merit is the Core Damage Frequency (CDF) or in level 2 where the figure of merit is the Large Early Release Frequency (LERF). The same type of figure of merit is proposed for analysis in the risk space, referring to a larger set of safety objectives which could include all the safety acceptance criteria used in deterministic safety analyses but allowing also for other types of safety objectives described by capacity probability distributions (e.g.,

containment fragility curves). Other figures of merit such as the "expected damage" over a given period of time can also be addressed within the proposed integrated framework for safety margin assessment.

The frequency of a damage state, i.e., the exceedance frequency of a given safety objective, is an aggregate of the frequencies of all the dynamic paths leading to that damage state. Note that frequency, as a measure of likelihood, is the second element of the "triplets" in the safety description scheme. The methods of quantification for sequence and damage state frequencies are reviewed in the report, starting from those traditionally used in classical PSA, and some limitations and possible improvements have been identified.

One of the usual approximations in classical PSA is to consider that each sequence in an event tree contributes to the appropriate end state as a whole. It is not taken into account that a sequence actually represents a set of different transient paths, all of them composed by the same set of event tree headers, but with possible differences in initial or boundary conditions or in the timing of the events composing the sequence, which could result in different end states for the grouped paths. It is not taken into account either that the determination of the end state, no matter whether it is based on generic header success criteria or on explicit dynamic verification, is subject to some degree of uncertainty. Therefore, the sequence classification as success or damage with respect to a particular safety objective should be replaced by a quantification of the fraction of the sequence frequency that actually contributes to the frequency of the damage state. This fraction is given by the conditional probability of exceedance of the safety objective (given that the sequence has occurred). In the determination of this conditional probability, the quantification of uncertainties in the applied simulation models plays a fundamental role.

The conditional probability of exceedance of the safety objective gives an indication of the existing margin to damage in a particular transient path. The idea of the margin to damage was developed in the context of load-strength interference works in civil engineering applications and it is often referred to as a "safety margin" in the literature. In a general case, both load and strength are described by probability density functions over the axis of a given safety variable. The load function represents the probability that, given a particular scenario, the safety variable takes some maximum value. Similarly, the strength function represents the probability of failure (of a system, structure, etc.) if the safety variable actually takes some value. The margin to damage (acceptance limit), i.e., the probability that the load remains below the strength limit and the failure does not occur, is given by a convolution integral of the two distributions. Its complement, i.e., the conditional failure probability, is the one needed for risk space quantification of damage states as described above.

The higher the exceedance probability, the less the margin. Therefore, the proposed framework is a natural means to aggregate the effects of existing safety margins (or the lack of them) in any possible plant scenario in order to get a quantitative estimation of the level of safety in the plant.

When insufficient information is available for load and strengths functions, they can be replaced by bounding discrete values (so-called δ-functions) ensuring maintenance of enough safety margins. In the nuclear industry, probability distributions for strengths e.g. of fuel pins or containments are normally not easily available and they are replaced by safety limits -limiting values imposed on safety variables. Thus, when operating conditions stay within safety limits, the barrier or system has a negligible probability of loss of function, and an adequate safety margin exists. Given a particular plant scenario, the evolution of the safety variable must be calculated to determine whether it remains below the safety limit or not.

The quantification process in the risk space shows a high degree of coupling between dynamic and probabilistic aspects of the safety evaluation. Extending the scope of the analysis from classical PSA to the risk space appears very difficult due to the mostly decoupled treatment of dynamic and probabilistic

aspects in PSA. The proposed safety margin assessment framework provides a way to treat these aspects in a more integrated manner.

The third element of the safety description "triplets" is the consequences of each identified scenario. Estimation of consequences at any level, from process or safety variable values up to radiological doses outside the plant, is based on dynamic models representing the plant behaviour and the dispersion mechanisms. However, the consequences can be defined to fit the scope of a specific safety analysis and, thus, the effort involved in quantifying the change of margins can be limited.

Other aspects, more related to the simulation tools used for this purpose, have been discussed within the SMAP group. Since these tools are to a large extent the same as those used for analysis of DBT/DBA, much of the work already done worldwide regarding the use of these tools is also applicable in this context. The need for highly qualified models which must include all the relevant phenomena, plant systems and interaction mechanisms has been stressed. Also, a review of different approaches to deal with the uncertainty of calculations has been performed. The approaches were classified as “very conservative” (Appendix K approach), best estimate bounding, realistic conservative, and best estimate plus uncertainty. The "very conservative" approach, typically represented by the 10 CFR 50 Appendix K requirements for analysis of ECCS performance, is intended to allow for lack of knowledge of physical phenomena. The "best estimate bounding" approach is based on the use of best estimate codes with conservatively selected values for code input parameters. The “best estimate bounding” approach is very similar to realistic conservative, except that in the latter besides conservative initial and boundary conditions with respect to licensing parameters some other conservatism is added. Finally, the "Best Estimate Plus Uncertainty" (BEPU) approach represents the biggest effort for a proper use of best estimate models in order to minimize unnecessary conservatism while accounting for uncertainties associated to simulation results. The CSAU methodology was the pioneering approach, and several others have followed its path.

The most recent methodologies in uncertainty analysis discriminate between two fundamental types of uncertainty, namely aleatory and epistemic uncertainty. Aleatory uncertainty, resulting from inherent randomness or stochastic variability, is by its very nature the subject of PSA type of analyses. This type of uncertainty is associated with the occurrence of initiating events, actual value of initial conditions, performance of system components and humans during the accident and others. Epistemic uncertainty, instead, results from imperfect knowledge, e.g. of the physical description of the phenomenology of infrequent (severe accident) scenarios or values of code model parameters. This uncertainty is, at least in principle, reducible, and represents the degree of belief or confidence that a parameter actually takes the given value. The separation of aleatory and epistemic uncertainties is essential to integrating risk and safety margins.

When safety relevant applications of computational models, like traditional PSA or analyses in the risk space, contain both types of uncertainty, they must be distinguished and treated in different ways. A consistent and widely accepted scheme is the so-called "nested two-loop" approach. Epistemic uncertainties are treated on the "outer" loop by propagating the uncertainty of the model parameters used in the "inner" loop, including those associated to the probability values. Aleatory uncertainties are treated in the "inner" loop with appropriate probabilistic computational models (e.g., event tree / fault tree methods). The result will be a sample of aleatory probabilistic results of the "inner" loop (e.g., core damage frequencies) representing the distribution which quantifies the epistemic uncertainty about the probabilistically expressed system safety (probability distribution of probabilities). It should be mentioned that full consensus on the way to include epistemic uncertainties into the analysis methodologies has not yet been reached in the open literature, and hence such approaches need to be developed especially in the perspective of the practical application.

The estimation of the load function is based on the computational simulation tools reviewed above. Among the different approaches for uncertainty in the plant response simulation, BEPU is considered as ideally suited for analysis in the integrated safety margin assessment framework since it directly provides the load probability distribution needed for the calculation of the conditional failure probability. When the safety limit approximation is used for the strength function, the failure probability is approximated by the probability that the load exceeds the safety limit. This is equivalent to the area of the load function which lies above the safety limit. Scenarios where the entire load function is well below the safety limit both before and after the change, do not contribute to the change in safety margins captured with this approach: In these type of scenarios, adequate safety margin exists both before and after the change.

The proposed framework for safety margin assessment, while intended for existing reactors, is also suitable for application in a technology-neutral context. As long as any foreseeable nuclear power plant can be described as a set of volumes defined by successive physical barriers intended to retain fission or activation products, and challenges to barriers can be characterized by adequate safety variables, this framework can be applied. Protective systems or features, intended to preserve the integrity of barriers or to mitigate the effects of barrier failures, should provide the necessary level of safety the assessment of which is the aim of this approach.

The likelihood of incurring some amount of damage in a particular event sequence can be obtained from the conditional probabilities of barrier failure (or bypass) leading to the generation of that damage, given that this particular event sequence has occurred. Multiplying the conditional probability of each event sequence by the frequency at which that sequence is expected to occur, gives the expected frequency at which the public is exposed to that level of damage. This frequency can be compared with existing risk acceptance guidelines. Surrogate risk guidelines stated in terms of acceptable barrier failure frequency can also be defined. A conceptual example of application where the Core Damage Frequency is used as a risk indicator is provided.

Consequences of event sequences are also necessary, even for risk indicators stated in terms of frequency. These indicators always refer to frequencies at which a given limit or level of damage is exceeded. Transport of radioactive material (fission or activation products) through failed or bypassed barriers can be calculated with the aid of simulation codes of the same type of those presently used for severe accident analysis. This provides means to estimate the concentration of radioactive products in any volume between barriers (i.e., inside the plant) or in any point outside the plant.

The expected amount of damage (e.g., the cumulative dose) generated along a unit time (e.g., per year) is sometimes used as the most basic definition of risk and can be used also as an additional risk indicator. The contribution of each event sequence to this indicator is given by the product of its likelihood by its expected consequences. The final value is given by the aggregation of these contributions through the whole risk space.

Two proofs of concept examples are provided. In the first one the effect of debris in containment sumps after a LOCA is analyzed, using CDF as risk indicator subject to existing acceptance criteria. The debris may cause a loss of NPSH in ECCS and containment spray pumps, potentially resulting in the loss of function of these important safeguards. Substantial uncertainties in this type of scenarios make the use of an integrated approach recommendable where uncertainty becomes part of the calculated CDF, thus avoiding both over- pessimistic and over- optimistic results that would be obtained from pure deterministic or probabilistic approaches. A change in the size of debris screens from 125 to 1,100 square feet is analyzed. The loss of NPSH is assimilated to loss of core integrity and, therefore, the calculated probability of NPSH loss is equivalent to the conditional probability of loss of function for the first barrier, and can be used directly to determine the impact on CDF. The second example attempts to quantify the peak clad

temperature (PCT) margin for the design changes due to the power uprates for Kori unit 3 for which the safety and other analyses are being performed regarding power uprate.

ES. 4 Main results and their significance

The developed framework for safety margin evaluation provides a means for estimating the effect of a broad range of plant modifications. It allows for a quantitative response to concerns about erosion of safety margins as a result of multiple plant modifications. The method augments existing deterministic decision-making tools when adequate margin cannot be shown, especially when the possible loss of safety margin involves probabilistic aspects (e.g., reliability issues) not explicitly addressed in this type of analyses.

The proposed framework integrates existing methodologies on safety margins and risk evaluations. As a result, the figures of merit that characterize the overall plant safety are a set of risk indicators which include explicit consideration of safety margins in the calculation process. These risk indicators are given in the form of expected frequencies of specified plant damage states or expected amount of damage for a specified period of time.

This integration allows for a sufficiently accurate and precise evaluation of the overall impact of a modification that has simultaneous positive and negative effects on safety margins. Uncertainties are treated in such a way that they become part of the calculated risk indicators and also the differentiation between epistemic and aleatory uncertainties is suitably addressed throughout the evaluation process.

The proposed approach merges information from all the disciplines that are important in nuclear regulatory decision-making: deterministic safety analysis, probabilistic risk assessments, material science and engineering. The integration is done using existing, tested tools and methods. Yet, the integrated framework has the potential to evolve as new tools and methods will become available.

The two pilot applications show how the framework can be applied to issues of current regulatory interest and they illustrate some of its advantages. (Note: The simplified, abstracted model used to determine the effect of increasing sump debris screen as described in section 6.1 cannot be used to draw any safety conclusions with regard to USNRC’s GSI 191.)

ES. 5 Conclusions and recommendations

To fulfil the objectives of the Action Plan on Safety Margins, the SMAP Group has issued two Technical Notes as working documents and this Final Report; these documents taken together provide guidance on how to address the assessment of changes in safety margins due to significant plant modifications.

The agreed framework results from the integration of existing safety analysis methodologies and allows to implement all current regulatory practices while providing additional capabilities for analysis of plant changes whose implications are difficult to evaluate with traditional analysis techniques applied individually.

A key element of the success of the SMAP activities has been the fruitful exchange of ideas and information among the group members, which was stated as an explicit objective of the Action Plan.

The following features characterize the SMAP framework:

- The standard model from reliability theory (and other engineering sciences) using probabilistic density functions for both the load and the strength (of the barriers) forms one basic element of the SMAP-methodology. However, consistency with current practices is maintained since they can be viewed as particular approximations of the general approach.
- Naturally, the exceedance frequency has been chosen as a scenario-independent indicator for "loss of function". This quantity represents a very general measure of safety margin and quantifies the "distance" between the safety variables (e.g. pressure, temperature, oxidation level) and the respective acceptance limits in the whole set of possible plant scenarios. At the same time, it naturally allows for comparison of the margin available in different physical process parameters (safety variables).
- The methodology proposed by the SMAP group is based on a combination of deterministic and probabilistic approaches and uses the existing analysis technologies (e.g. deterministic safety analysis and PSA). The aggregation of the risk contributions from different event scenarios uses the mathematical concepts of PRA while the evaluation of the consequences is performed using existing transient analysis simulation tools. The two pilot applications propose the application of best-estimate + uncertainty (BEPU) analysis for the consequence evaluation.

Based on the results of the SMAP work, new fields of activity can be identified for further development of the methodology. Some recommendations for CSNI may be as follows:

1. Rather straightforward extensions of the current methodology (as exemplified with the two pilot applications) appear as promising mainly in two directions:

   a) The pilot applications documented in the report are evaluating a rather limited set of scenarios. For a more ambitious, wide scope implementation of the SMAP-methodology, dynamic event tree simulation tools will become necessary in order to support efficient launching of the required large number of transient simulation runs and the related systematic collection of the respective simulation results (risk aggregation). Dynamic event tree methodologies are to some degree still under development. It would be advantageous to explore the performance of the different approaches from the perspective of possible application of such methodologies in the proposed SMAP framework. It is therefore suggested to launch a respective comparison exercise to evaluate existing dynamic event tree methodologies; such an exercise could be organised similar to BEMUSE (CSNI/GAMA) which successfully explored different uncertainty evaluation methodologies.

   b) In order to extend the current methodology to the application of (integral) plant safety margin, the incorporation of severe-accident (SA) analysis tools becomes necessary. It still remains to be determined if the whole analysis should be performed with a modern SA-tool (e.g. MELCOR…) or if the current transient-analysis tools (e.g. TRACE, RELAP5, CATHARE, ATHLET …) should interface to such SA-tools at the proper moment of the respective transients, thereby calling for an interface between the two analysis tools. Requirements on the level of accuracy of the failure prediction are an input needed to answer this question.

2. A more difficult problem will be to properly address the fact that (epistemic) uncertainties tend to be larger in the domain of (low-frequency) severe accidents as compared to the traditional design basis transients. Some studies to explore the influence of this increased uncertainty onto the quantification of plant safety margin are needed and possible simplifications of the present

general framework should be considered in light of such large uncertainties in order to maintain a methodology that remains of practical value. It is very likely that this needs extensive studies based on a suitably chosen and representative pilot case.

3. On a longer-term perspective, the SMAP-methodology could be applied to evaluate plant safety margin in a so-called “technology neutral” setting in terms of frequency-consequence curves that would avoid the usage of (“LWR-specific”) measures such as ΔCDF as a surrogate measure for plant damage. This would, however, require successful completion of the steps outlined before.

1 INTRODUCTION

In the seventies, when the power plants which are now under operation, started to be built and operated, rules and criteria were defined with the objective that the plant could be considered as safe if they were satisfied. During this period, the design basis accidents (DBAs) were defined and the US 10CFR50 Appendix K [1.1] was assembled. Due to several weaknesses in the knowledge base, conservatisms were introduced at almost all levels of the approach. The criteria such as 1204°C peak cladding temperature, 1% mean equivalent cladding oxidation, 17% local maximum cladding oxidation were dictated with varying degrees of conservatisms with regard to the phenomena which they were intended to avoid. Rules were also imposed on boundary conditions, system availabilities and system failures in order to maximize the evaluation of the consequences of DBAs. The physical modeling, which was also largely affected by the lack of knowledge, was treated in a highly conservative way. Some modeling conservatisms were explicitly entered in the prescriptive rules of Appendix K.

When questions were raised whether plants could be considered as safe, the usual answer was first that criteria had been set up to ensure that if they were satisfied, nothing reprehensible could occur, and secondly that plant behavior was evaluated with large conservatisms so that to ensure that the plant was on the right side of the preceding criteria. This, of course, meant that some "distance" existed between the most severe state of the plant and the criteria. This "distance" which was the result of the combination of all kinds of conservatisms (without making any classification) appeared as an additional margin to the criteria, which already was guaranteeing by themselves the safety of the plant. The concept of safety margin was then created. This conceptual two-prong approach - define a safety limit and stay under it - is what is most commonly understood as having “adequate safety margin” in the nuclear industry.

One criticism expressed very soon was that this approach precluded determining how far the plant was from the safety limit, in other words how large were the actual safety margins. In particular, the physical models on which conservatisms were applied, were known to be very crude approximations. As a consequence they were not able to provide any reliable idea of the real plant state, which could effectively allow one to evaluate the safety margins. Moreover nonlinearities in the plant response were already established for some of them. Hence the additivity of the combination of conservatisms could not be demonstrated. Moreover, the combination of conservatisms could not, and cannot, be proven to lead to a conservative prediction [1.2]. In this condition the determination of the real state of the plant appeared to be the only way to get an evaluation of the safety margins. For that, it was necessary to develop more physical models, to start extensive experimental programs on which the models could be validated and to introduce those models in what was called BE (best estimate) codes. This led to the large research program in thermal hydraulics, which was launched in the mid seventies and lasted up to the nineties. The basic reason of this program was the evaluation of the safety margins. Furthermore, this program was explicitly requested in the US Atomic Energy Commission statement of consideration [1.3] that accompanied the 1974 final rule [1.4] with the view to get justifications or substitutes to the prescribed conservatisms.

1.1 The Evolution of the Safety Margins Concept

In the early seventies, the DBA was considered as the major safety case. The safety margin concept was then strongly linked to the DBA and to related conservative approaches, which were defined to get, on one hand, an envelope accident and, on a second hand, to increase knowledge about plant physical behavior.

After the Three Mile Island Unit 2 (TMI-2) accident, the DBA appeared not to be the only safety concern. Transients of several types, operating procedures and severe accidents became integral parts of the safety analysis. In fact the safety margins concept continued to be used in this more general framework. Statements such as "maintain sufficient safety margins" and "increase safety margins" could be found for all types of accidents. **The need to account for all types of accidents in quantifying safety margins has been a strong motivator for the work described in this report.**

The safety margins concept had been extended beyond DBA. It represented, in a very qualitative way, some "distance" of the plant state to either a safety criterion or a feared situation, e.g., core melting. One should note that the extension of this concept did not refer at all to any definition of what the safety margin could be and became then more qualitative than before. Moreover it considered limits other than the ones corresponding to safety criteria. As a result, for some experts, the term safety margin relates strictly to safety criterion. However, for other experts, safety margin is relative to a value above the safety criterion, which accounts for the extra "margins" introduced by setting the safety criterion in a conservative manner. This may generate a lot of confusion, as people using the same word in a discussion could implicitly use it in a different meaning. Chapter 4 of this report discusses further these two definitions.

In the nineties, the use of the "safety margins" concept became more and more frequent. In particular “margin” was often used to justify proposals of safety research programs or proposals of international projects such as the ones of CSNI. The “margin” concept remained nevertheless at a qualitative level, which was considered sufficient by those using it.

After the ten to fifteen years of research programs starting in the mid seventies, best estimate tools for accident analyses started to be issued in the nineties. These tools were expected to provide the real state of the plant. However it was soon realized that this state could only be known within some error band because of remaining uncertainties. A lot of research was performed on this uncertainty evaluation. Significant progress was made but open problems still remained. Currently, best estimate methods and tools have reached a level where they are practicable provided that solutions are used to overcome the remaining open problems with regard to uncertainties.

The mid-seventies goal of evaluating the real state of the plant can be considered as almost reached, and the initial question of the safety margin level could then be answered within the limitations of uncertainty. However, the evaluation of the safety margins as initially envisioned has been rarely performed because analyses to justify plant modifications became the first priority. Meanwhile, some expect these plant modifications to have substantial impact on safety margins.

1.2 The Practices that Modify Safety Margin Levels

In the last decade, largely as a result of general economic pressure and the deregulation of electricity markets, the nuclear industry has tried to maximize the output of operating plants. In some cases this was done through major modifications such as power uprate, increasing the length of the fuel cycle, increasing the maximum fuel burn up, and/or life extension. These modifications required in-depth safety analyses to evaluate the possible safety impact. In other cases, output was increased through several small

design changes. For those small changes that are not individually tested, the effect of accumulation of changes could produce significant differences from the original design. Therefore, any significant grouping of small changes also requires a comprehensive assessment.

Optimizing the output of nuclear power plants can often make plants more reactive to accident initiators. As a consequence, in several cases, it was impossible to meet regulatory criteria with the traditional conservative methods used in the past to design nuclear plants. Those traditional conservative methods were generally the same or of the same type as the ones used to evaluate safety margins in the seventies.

To meet criteria, new methods had to be used. The most common ones predict plant behavior by best estimate methods[1] or at least methods that are less conservative when the uncertainty evaluation cannot be completed. With those methods, the decrease of conservatisms allowed a particular accident case to meet the criteria whereas with the earlier methods it did not. The use of more modern methods has often been claimed to "liberate" extra "margins" which have been simply "used" for the plant optimization. In fact, it appears that the use of the new methods places the optimized plant in a state closer to the criteria than in the plant with no optimization where the conservative methods were able to fulfill the criteria with larger conservatisms.

Another attempt to fulfill the criteria has been to reevaluate a particular safety criterion. In this context, there have been claims that the safety constraints should not introduce excessive burden and that they should be revised for specific cases by decreasing requirements considered unnecessarily high. Given the commonly accepted definition of safety margin in the nuclear industry as the distance between the safety limit and the failure point, raising the safety limit would go, of course, in the direction of reducing safety margins. This reduction would certainly be very complex to evaluate. As of November 2006 there is, to the SMAP task group's knowledge, no example where such an attempt has gone through all the way. However, revising the size of a large break LOCA from the current assumption of double-ended guillotine is one example of trying to alter the criteria.

In the usual traditional safety approach, i.e., the deterministic one, safety criteria and consequently safety margins play an important role. The increased application of risk studies and of probabilistic safety assessments (PSAs) is one practice, which supplants more and more the usual deterministic approach. This impacts the safety margin concept. For example the risk-informed approach is tentatively used to provide justifications for plant optimizations, which could not be easily justified by the deterministic approach. The PSA results, which are used for those demonstrations are generally referring to other criteria than the usual safety criteria defined for design accidents. For example PSA level 1 refers to the criteria of core melting, and PSA level 2 to the amount of fission product released outside the containment. Using these different criteria modifies inevitably the safety margins based on other safety criteria (1204°C, 17%, for example).

1.3 The Objectives of SMAP and Contents of this Report

On occasions, the international nuclear community has expressed concern that some changes in existing plants could challenge safety margins while fulfilling all the regulatory requirements. In 1998, NEA published a report by the Committee on Nuclear Regulatory Activities on Future Nuclear Regulatory Challenges. The report recognized "Safety margins during more exacting operating modes" as a technical issue with potential regulatory impact. Examples of plant changes that can cause such exacting operating modes are the ones mentioned in previous Section 1.2, including power uprates, life extension or increased

[1] Note that, in the current report, any mention of a best estimate method actually means best estimate plus uncertainty.

fuel burnup. In addition, the community recognized that the cumulative effects of simultaneous changes in a plant could be larger than the accumulation of the individual effects of each change. In response to these concerns, CSNI constituted the safety margins action plan (SMAP) task group with the following objectives: "To agree on a framework for integrated assessments of the changes to the overall safety of the plant as a result of simultaneous changes in plant operation/condition; To develop a CSNI document which can be used by member countries to assess the effect of plant change on the overall safety of the plant; To share information and experience."

The two approaches to safety analysis, deterministic and probabilistic, use different methods and have been developed mostly independently of each other. This makes it difficult to assure consistency between them. As the trend to use information on risk (where the term “risk” means “results of the PSA/PRA analysis”) to support regulatory decisions is growing in many countries, it is necessary to develop a method of evaluating safety margin sufficiency that is applicable to both approaches and, whenever possible, integrated in a consistent way.

Chapter 2 elaborates on the traditional view of safety margins and the means by which they are currently treated in deterministic analyses. This chapter also discusses the technical basis for safety limits as they are used today. Chapter 3 looks at techniques for the deterministic calculation of safety margins and discusses the complementary probabilistic risk assessment techniques needed to generalize safety margins beyond design basis accidents.

Chapter 4 examines the definition of safety margin, which is noted to take different meanings in different fields. For example, in civil engineering and applications that deal with the load-strength interference concept, safety margin describes the distance between the means of the load and strength probability density functions with regard to the standard deviation in both. However, in the nuclear industry, the term safety margin evolved to describe the goal of assuring the existence of adequate safety margin in deterministic calculations. Specifically, safety margin refers to keeping the value of a given safety variable under a pre-established safety limit in design basis accidents. Implicitly, safety margin in the nuclear industry is the distance from the safety limit to onset of damage.

The SMAP task group fulfilled its first objective by adopting a methodology for quantifying safety margins that merges the deterministic and probabilistic approaches. The methodology described in Chapter 5 is consistent with the definition of safety margin commonly used in the nuclear industry. The metrics of this methodology quantify the change in safety over a range of accident sequences that extend beyond the design bases. However, the methodology is not described in this report to a level that would meet guidance document requirements. This is in part because methods and techniques needed to quantify safety margins in a global manner are evolving, and thus specific guidance rendered at this time would shortly become obsolete. This report presents the framework in sufficient detail to serve as the basis of an analysis an, thus, this report meets the second objective established for the SMAP group. A proof-of-concept application to further aid potential applicants of the methodology is included in Chapter 6.

As recognized from the beginning, the proposed action plan has been highly multidisciplinary and a wide variety of expertise has been needed for its development. The exchange of information and experience among participating organizations, which was defined as the third objective in the safety margins action plan, has not been only an essential working method, but also a net benefit of the work.

1.4 References for Chapter 1

[1.1] Appendix K, “ECCS Evaluation Models,” to Title 10, Part 50, “Domestic Licensing of Production and Utilization Facilities,” of the Code of Federal Regulations, U.S. Nuclear Regulatory Commission, Washington, DC.

[1.2] “Report to the APS by the Study Group on Light Water Reactor Safety,” Reviews of Modern Physics, Vol. 47 Supplement No, 1, summer 1975

[1.3] Atomic Energy Commission statement of considerations for the final ECCS rules, 10 CFR 50.46 and Appendix K, 1974.

[1.4] Atomic Energy Commission’s decision on the proposed ECCS rulemaking, CLI-73-39, 6 AEC 1085, December 28, 1973.

2 TRADITIONAL DEFINITION OF SAFETY MARGIN

2.1 Margins in Design Basis Analyses

The concept of safety margin was introduced in recognition of the fact that uncertainty exists in the safety variable value at which damage occurs. By setting the regulatory acceptance limit conservatively with respect to the point of damage onset, sufficient margin is assured in DBAs. It should be noted that 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 loss is 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. Therefore, this definition requires to clearly identifying the concept of a safety variable, and how safety variables relate with barrier or system function losses.

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. These consecutive considerations are depicted in Figure 2-1.

Figure 2-1. Contributors to global plant margins

These considerations show that this apparently simple definition of safety margin is not easy to apply even in the traditional field of deterministic analysis where the concept of safety margin has been extensively used. As a consequence, different interpretations, not always consistent, have been used. This difficulty is even greater when significant and concurrent design changes are implemented in the plant and when the requirement about safety margins should be made consistent with conclusions drawn from probabilistic analyses.

At the first 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 (Design Basis Transients or Accidents, DBT/DBA), classified into a few frequency classes, were taken as 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 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 DBT/DBA provided a satisfactory basis to evaluate the protection adequacy for all situations.

For this limited set of design basis scenarios it is possible to define class-specific acceptance criteria in terms of extreme allowed safety variable values, the safety limits. This way, sufficient safety margin is guaranteed for any scenario covered by the design basis space provided that uncertainty associated with the predicted safety variable value 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 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 weight 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 [2.1] or the Deutsche Risikostudie Kernkraftwerke [2.2] 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.

Identification of the most frequently used safety margin definitions can be illustrated by reviewing typical methods and steps applied in design basis analyses. Although the design basis safety analysis methodologies may vary from country to country or among different technologies, the conceptual steps provided in the later paragraphs can describe a typical design basis safety analysis, where the involved safety margins have been identified. The terminology used for margins and limits is not necessarily standard, but it has been found useful for the purposes of clarification. Reference is made to Figure 2-1.

Selection of safety variables and safety limits: Safety variables and safety limits are selected on the bases of preventing barrier failures. However, violating a safety limit does not necessarily mean that the barrier fails. The analysis of the existing margin between safety limits and barrier failure modes is an essential part of the safety analysis. Nevertheless, this is usually done through generic studies, applicable to large groups of plants with common design characteristics or with a particular fuel design. Because of that, they do not usually appear in plant specific safety analyses, although those analyses should address the applicability of generic studies. This margin is called Barrier Margin in Figure 2-1 and it is often evaluated in probabilistic terms of confidence on barrier integrity when the safety limit is reached but not exceeded.

Selection of DBTs: For each frequency class, a set of limiting Design Basis Transients is 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 Design Basis Transient. Selection of limiting envelope transients is a method for reducing the number of accidents to be evaluated. It does not

introduce any margin per se in the accident evaluation but it is one of the basic principles of the deterministic approach, which is to consider only a limited number of accidents. The main question is to be sure that the selected transients are really the limiting cases. Probabilistic methods can be used to complement the selection. Since DBTs are often artificially distorted in order to maximize the protection challenge, there is some margin between the consequences of the DBTs and those of the real plant transients eventually covered by them. This kind of margin is called Analytical Margin (AM) in Figure 2-1. Usually, the AM is not measurable because each possible real transient has a different AM associated and the minimum AM would correspond to a particular transient which, in the general case, cannot be identified. Very sophisticated bounding arguments are the usual way to demonstrate the existence of this margin. Note that each DBT introduces its own particular type of AM and that all of them must be verified.

Analysis of DBTs: The Design Basis Transients selected as representatives of each frequency class are analyzed to verify compliance with the applicable safety limits. The acceptance criterion is that no safety limit can be exceeded in any DBT. In calculating the results of the DBTs it should be taken into account that, if best estimate models are used, the estimated uncertainty band should be added to the results before comparing with the safety limits[2]. There is no restriction on how close to the limit the results may go. The only strict condition is not to go beyond the limit. However, in most cases, there will be some distance between the results of the DBTs and the safety limits. This measurable distance, obtained from the simulation of the DBTs, is called Licensing Margin (LM) in Figure 2-1. Note, however, that there is not a single LM; for each combination of DBT and applicable safety limit, there is a LM and all of them must be verified in the safety analysis.

Source Term Analysis: Depending on the frequency group where a DBT is classified, some combinations of barrier failure modes may be allowed. Even when no barrier gets failed as a consequence of a transient, some limited barrier degradation or barrier bypass e.g. nominal containment leakage rate is often assumed as initial condition for the analysis. Consequently, some amount of radioactive species can be released to the environment as a consequence of a DBT. The release, usually classified in radiological groups according to the nature of the involved radioisotopes, 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 DBTs, a new set of radiologically significant DBTs is obtained for each frequency class with the criterion of maximizing the source term. In general, the radiologically significant DBTs are not the same as the barrier significant ones, although they often appear with the same denomination in safety reports. These DBTs are analyzed in the Analysis of Radiological Consequences, traditionally included in safety reports. Again, the selection of DBTs may include unrealistic assumptions aimed to get a safety envelope of all the possible real transients included in the frequency group. The source term analysis introduces a new contribution to the global safety margin in terms of the difference between the calculated source term in radiologically significant DBTs and the possible real source term resulting from transients covered by those DBTs. As in the case of the AM, the margin must be demonstrated but it cannot be quantified.

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, either population averaged or individual, are calculated. These calculations are strongly conditioned by site characteristics, and limiting environmental conditions should be used in the analysis. The source term values used in this step can be either the ones obtained from the source term analysis, or greater values used as design basis source terms. In the latter case, the

2 Note the difference between the use of bounding techniques for the selection of enveloping DBTs and the use of conservative or best estimate uncertain models for the simulation of the selected DBTs. Although there could be some apparent similarities between both things, they must be conceptually distinguished.

source term and dose calculations become decoupled and a new contribution to safety margin is introduced as the difference between the maximum calculated source term (for each frequency class) and the corresponding design basis source term. The resulting doses must be lower than the legally applicable limits, both for annual average doses and for per-event doses. The difference between the calculated doses and the corresponding legal limit, identified as Dose Margin in Figure 2-1, is the last contribution to the global safety margin.

It should be pointed out that, although conceptually "consecutive", the different types of partial safety margins contributing to the global safety margin are evaluated in a variety of ways that may include different kinds of physical magnitudes or probabilistic characterizations. Therefore, in general, the contributions to the global safety margin are not purely additive. In addition, there are concurrent margins originating from the consideration of different safety variables and different DBTs for a single failure mode, different failure modes for the same barrier, etc.

The traditional definition does not easily allow quantification of the global margin. First, regulations only require that analyses be done in a bounding manner and thus no insight is available in the magnitude of the margins. Second, the contribution of realistic accident sequences is discarded in favor of conservative, enveloping DBAs.

2.2 Deterministic Approach

The safety approaches are generally based on deterministic approach complemented by probabilistic approach in order to improve the prevention and mitigation of accidents. The relative weight of the probabilistic approach in the safety demonstration differs from one country to another, without having ever gone to the point that it has completely substituted the deterministic approach.

The deterministic approach, which is used for system design, is based on the defense in depth concept (three levels) and on the three barriers principle. The three levels of defense in depth are:

- Prevention of departures from normal operation,
- Detection of departure from normal operation and protection systems to cope with this deviation,
- Safety, protective systems and operator actions to mitigate accident consequences.

Concerning the public protection in case of an accident, three successive barriers are considered: fuel cladding, primary system boundary and containment to limit radioactive release to the environment. The defense in depth concept is applied to each barrier in order to maintain the barrier integrity or to mitigate the consequences of a barrier failure.

For the plant system design, potential initiating events are classified in different categories of plant conditions according to their rough expected frequency. One example of those categories is given in [2.3]:

Category 1: transients related to normal operation
Category 2: incidents of moderated frequency ($> 10^{-2}$ / r.y)
Category 3: very low frequency accidents (10^{-2} /r.y to 10^{-4} /r.y)
Category 4: hypothetical accidents (10^{-4} /r.y to 10^{-6} /r.y)

Variations or additions around those categories have been defined depending of the countries. A summary of the French and Finnish categories and acceptance criteria has been presented as a SMAP Technical note [2.4]

Acceptable radiological releases are identified for each accident condition in order to demonstrate that consequences of reactor operation are acceptable for public and environmental protection. The radiological limits have different regulatory status depending on the country. It could be considered either as a reference value for safety demonstration or as a regulatory requirement. Examples of radiological criteria for different reactor operation conditions are presented in [2.4].

Usually, the radiological limits are associated with the frequency of the initiating event. A different approach is given in the UK HSE/NII safety assessment principles for nuclear power plants [2.5]. The rule gives five classes of maximum effective dose to a person outside the site, and limits the total (cumulative) frequency of accidents for each class.

The acceptance criteria are applied to the plant transients by using in the deterministic approach, specific rules and different methods for evaluating them. Those rules and methods are designed in order to introduce conservatisms in the plant evaluations. Those plant evaluations may then differ from the real plant behavior corresponding to the initial initiating event, in particular because they relate to a different and more severe accident than the primitive one. According to the fixed rules it is those plant evaluations, which are compared to the acceptance criteria.

2.3 Decoupling Techniques

The acceptance criteria are directly or indirectly related to the three barriers. Decoupling techniques that cover the range from plant processes to environmental impact are applied to consider the barriers. For the decoupling process to be acceptable, care should be taken to ensure that there is no overlapping between the acceptance criteria of one step and the assumptions of the next one.

First “fuel safety decoupling criteria” associated to the accident condition are defined in order to limit fuel damage in accident condition. The decoupling should ensure that if fuel safety criteria are fulfilled during the accident then radiological releases are limited and acceptable provided that the criteria for the two other barriers (primary circuit and containment) are also fulfilled. The criteria for those two other barriers are based on the mechanical behavior of respectively the primary/secondary circuits and the containment. Those criteria refer to the concept of maximal pressure not leading to a system failure, concept of safety factors varying in function of reactor conditions and concept of design pressure.

To illustrate the general methodology, we will use one example, which is the case of fuel safety criteria for RIA transients. The Reactivity Initiated Accidents (RIA) accident enters in the probability category of the hypothetical accidents for which some reference values for radiological doses are defined. The most severe risk in RIA is that the fuel disintegrates in molten parts and the parts interact energetically with the coolant. In such a case, a very large pressure peak could occur and provoke the failure of the primary circuit. It cannot be excluded that some parts of the primary circuit, like the control rods or the upper head, may be thrown away as missile and may provoke the failure of the containment.

In order to avoid such a situation, several decoupling phenomena are successively defined. In a first step, in order to prevent any catastrophic failure of the containment, it is required that the second barrier (primary circuit) remains intact (first decoupling). To satisfy this new requirement, the fuel coolant interaction should be sufficiently weak. An additional decoupling phenomenon is then defined: it requires that there will be no fuel ejection (second decoupling), which excludes consecutive fuel to coolant interaction. In order to get no fuel ejection, the cladding should not fail or fail in a limited way. This requires that only a small percentage of fuel should melt in order that it will not be ejected (third decoupling). Those requirements differ for fresh or high burn up fuel. With regards to the cladding failure, it depends physically of several parameters. Consequently it is quite difficult to predict this failure with

physical codes. For those reasons a final decoupling phenomena is introduced (fourth decoupling): as the overall consequences of RIA are an increasing function of the enthalpy deposition due to the power excursion, the "no" or "limited" cladding failure requirement is replaced by a requirement on the enthalpy deposition. The final safety criterion is then ultimately defined by setting a sufficiently low value for the enthalpy deposition, which must not be exceeded (decoupling parameter).

This example shows that safety criteria are most often derived from the radiological reference values by applying several decoupling actions: For some of those decoupling actions, a phenomenon is substituted to the primitive one (decoupling phenomena); for some others more restrictive values of parameters are imposed in order that one will be sure that the original requirement is satisfied (decoupling parameter). At each step, conservatisms are introduced that can be considered as margins for safety.

2.4 Safety Limits for Physical Barriers

A detailed discussion on barrier safety criteria based on the French practice is presented in [2.4]. The basic principles without numerical values are listed here.

2.4.1 Fuel safety criteria (First barrier)

An extensive compilation of fuel safety criteria can be found in the NEA summary [2.6]. The summary and conclusions of this compilation emphasizes that despite some differences in the values/levels applied in different countries, the general principles for deriving those criteria are very similar

2.4.1.1 Fuel Safety Criteria for the Events of Lowest Categories Such as Normal Operation and Incidents of Moderate Frequency (Categories 1 and 2)

The probabilities of occurrence of category 1 and 2 initiating events are quite high. For that reason very drastic reference values have been defined for the radiological consequences to be acceptable. For category 2 the limit of activity release for one incident is typically bounded by the integrated annual limit of activity release for normal operation (category 1). The way to fulfill this requirement is that the incidents for category 2 have no effect on the first barrier (fuel cladding).

The phenomena which endanger the fuel rod integrity are thermal and thermo mechanical loads to the cladding and the loss of integrity of fuel pellets by melting. Specific decoupling phenomena and/or criteria are determined to prevent those damages:

- Prevention of critical heat flux (CHF) to avoid large temperature rise in the cladding. Typically it is required that the probability to remain below CHF in the hottest point is 95% with a 95% level of confidence
- Prevention of fuel melting. To guarantee this, acceptance criteria for fuel maximum linear power is usually given.
- Prevention of cladding embrittlement. A decoupled criterion is applied by forcing a maximum value of the cladding temperature not to be exceeded. In addition, limits are given for the cladding oxidation and the hydrogen pick up, characterizing the metallurgical state, which may induce cladding embrittlement.

- Other criteria are defined which are directly related to the mechanical loads to the cladding, limiting:
  - Cladding circumferential deformation
  - Rod internal pressure
  - Cladding stress
  - Cladding fatigue
  - Total strain in a category 1 and 2 transient
  - Fretting wear of cladding
- Cladding thermal loads are limited by fixing the maximum metal oxide interface temperature

As the criteria are applied to transients of normal operation, some of those criteria are not considered in some countries as "safety criteria" but as "operating criteria" or "design criteria" (see reference [2.6]). This is particularly the case for the criteria dealing with long-term phenomena covering 99% of the plant life operation. For the operation conditions of lower frequency (category 3 and 4) long-term phenomena are not any more important for the transient behavior itself due to the brevity of those transients. They may still play an important role, as they will condition the initial state of the fuel before the considered transient.

2.4.1.2 Fuel Safety Criteria for Events of Category 3

In accordance to the lower occurrence probability of category 3, limited fuel damage in some fuel rods is allowed in order to meet the reference values of radiological consequences. However, the fuel damage shall not degrade the reactor core cooling function and the core geometry is required to remain coolable.

The decoupling phenomena used for those conditions are the same as for the conditions of category 1 and 2:

- Prevention of critical heat flux phenomena
- Prevention of fuel melting
- Prevention of cladding embrittlement

However as the occurrence probability is lower, some of the decoupling criteria are set up to less drastic values than for category 1 and 2. This gives:

- The number of fuel rods in CHF condition is limited to some percent
- The fuel melting in the center of the pellets is limited to a small fraction of fuel volume
- The maximum cladding temperature is limited
- Some accidents may be considered with specific rules, for example the small steam line break in the French approach

2.4.1.3 Fuel Safety Criteria for Events of Category 4

Category 4 includes some specific low probability accident types, which require safety criteria not considered in categories 1-3. Most important examples are the LB LOCA and the RIA case for which different decoupling phenomena and decoupling criteria are needed. In some countries, also other accident types are treated in specific manner, for example Main Steam Line Break in France [2.4].

In category 4, significant damage for a few fuel elements is allowed. The core geometry should still be preserved to guarantee the core cooling function in the long term. The requirements for the general case are similar to the requirements in category 3 using the same decoupling principles:

- Prevention of critical heat flux phenomena
- Prevention of fuel melting
- Prevention of cladding embrittlement,

with some relaxed criteria to afford for a less stringent requirement on the fuel damage.

The LOCA decoupling criteria for cladding embrittlement deals with a limitation of the cladding oxidation by specifying a maximum oxide thickness and with limitations in the metallurgical state transformation by specifying a maximum peak clad temperature. Widely used criteria for category 4 LOCAs are:

- Maximum cladding oxidation including corrosion before and during accident shall not exceed 17 % of the clad wall thickness for a Zircalloy cladding material
- Maximum cladding temperature during transient shall not exceed 1204 °C

As CHF may occur largely during LOCA, the decoupling with DNB phenomena is not any more useable for limiting the temperature increase and for limiting the resulting potential rod failure. A "direct" criterion is then sometimes fixed, which determines the maximum acceptable number of rods with failed cladding.

The requirement on core geometry is maintained: core coolant geometry shall be preserved to guarantee reactor core cooling function in the long term. To be complete, a particular criterion is also applied on the global amount of oxidation but actually this is a decoupling criteria related to the containment. In order to avoid unacceptable effect of H_2 combustion on containment, maximum amount of hydrogen production by cladding oxidation shall not exceed 1% of the hydrogen production by total active cladding oxidation.

As shown in chapter 2.3, the reactivity insertion accidents (RIA) criteria are determined by defining several successive decoupling phenomena, which are at each step more and more restrictive. These steps are:

- The second barrier (primary circuit) shall remain intact
- Fuel coolant interaction shall be sufficiently weak
- No fuel ejection shall occur
- Limited cladding damage and limited fuel melting shall occur.
- Enthalpy deposition shall be limited

For high burn-up fuel, the safety limits in case of RIA may change. The limits are being investigated in the experimental programs such as CABRI and other similar research activities. They should result in a proposal of criteria, which will be applicable to high burn up and which will allow easy decoupling.

2.4.1.4 Particular Aspects in Fuel Safety Criteria Application

In category 3 and 4 in which some fuel damages can occur, there is a requirement that the core geometry has to remain coolable. Contrarily to the other fuel safety criteria, which are precisely and

quantitatively defined, this criterion is very qualitative. The objectives of the coolability criterion are several:

- It is to avoid loss of core geometry due to pressure shock waves or abnormal hydraulic loads resulting from overflows.
- It is to avoid loss of geometry of the ruptured rods, which may constitute debris beds difficult to cool.
- It is to avoid flow blockages resulting from the deformation of the fuel rods (ruptured or non ruptured rods) that cannot be cooled.

Several of the events which may lead to difficulties in the cooling of the core during accidents or in the long term are more or less covered by other criteria such as the criteria related to embrittlement. However, as they are not covering all cases of loss of geometry, this qualitative criterion has been retained in order to avoid entering the severe accident category.

In a core containing sometimes more than 60,000 rods, it is statistically probable that a limited number of rods may present defects. This means that they may be subject to leakages at some time during operation (condition of category 1) or with a higher probability during category 2 transients. Those leakages represent failure of the first barrier, which is in contradiction with the no ruptured rod criteria. This fact of not meeting exact of criteria need a special treatment as far as this is unavoidable. For normal operation, requirements are put on the maximum activity of the circuit and on the non-dispersion of fissile material in the circuit.

For the other categories 3 and 4 of accidents for which some rod ruptures are accepted, the case of the defective rods does not raise any problem. The defective rods either initially leaking or experiencing early ruptures due to their defects are added to the rods, which are ruptured due to the accident. This does not affect generally the fulfillment of the criteria, as the number of defective rods is typically small compared to the number of rods failed during the accident.

Defective rods may complicate the category 3 and 4 assessment in cases when no rupture is required. This is particularly the case of RIA where for high burn up there is a tendency to require no cladding rupture. As the defective rods are not satisfying the criteria, special requirements have been defined. One way to handle the problem could be to verify the n-1 decoupling criteria before the no cladding rupture criteria, here the no fuel ejection criteria. In such a case the coolability of the core will be maintained and the effect of defective rods minimized.

2.4.2 Primary Circuit Criteria (Second Barrier)

The primary circuit provides the second barrier between the fission products and the environment. The safety objective for this barrier is to maintain its full integrity. The main risks, which could induce the primary circuit failure, are the thermal loads and the mechanical loads. The criteria used are aiming at limiting those loads to acceptable levels. To limit the loads, the basic methodology in mechanics is the use of safety factors applied to the rupture loads. For example concerning the pressure loads, a design pressure is defined by applying a safety factor to the rupture pressure and it is this design pressure which will become the reference for actual pressure loads.

Comparing the approach with the preceding decoupling approach for the fuel, we could say that replacing the barrier failure itself by the loads is a phenomenon decoupling process whereas applying safety factors is a parameter decoupling process.

Widely used rules and criteria for design and acceptance criteria of the pressure vessel, primary system components and piping are given in the ASME codes [2.7], or RCCM [2.8] or RCC-MR [2.9]. As category 1 events represent normal operation, the design approach applies entirely. A design pressure has been defined by applying a safety factor to the pressure leading to collapse. The risks, which must be avoided in normal operation, are excessive deformation, plastic instability and fatigue damage risk. In that perspective, it is prescribed that the pressure should always remain lower than the design pressure and that the thermal cycling loads are limited. As the probability of category 2 reactor conditions is quite high, the same criterion is applied as for category 1 events.

The transients of category 3 have a lower probability of occurrence. No fatigue analysis is required. Consequently the failure risk that may occur is not any more a fatigue damage risk but a collapse or a fast fracture risk. To take into account the specificity of this risk some relaxing in the safety factor is allowed by fixing limits slightly higher than the design loads for pressure and mechanical loads.

For category 4, the safety criteria are not fully applied to the LOCA case, since the initiating event is the rupture of the circuit per definition. For the other general cases, the risk to be avoided is the same as in category 3 but the occurrence probability is again lower than in category 3. The criteria are then relaxed and consequently defined with a higher percentage of the design loads.

2.4.3 Containment Criteria (Third Barrier)

The phenomena determining the containment safety are:

- Thermal-mechanical loads which could provoke its rupture
- Thermal-mechanical loads and irradiation effects which could increase the leakage rate.

Those two problems are treated separately for the containment. For the first of them (containment rupture) the maximum temperature and pressure load to which the containment may be submitted in the deterministic approach, are either the pressure-temperature reached during a large break LOCA or the pressure and temperature peaks, which could result from burning of hydrogen.

In order to cope with the maximum pressure reached during a LOCA, the maximum pressure evaluated for a LOCA with some fixed conservative rules is chosen as the design pressure for the containment at the temperature reached during the LOCA. As it is usually done in mechanical engineering, this design pressure is derived from the effective rupture pressure by applying a safety factor.

The loads resulting from the burning of hydrogen are coped differently by using a decoupling limiting the total quantity of hydrogen release during a LOCA (see 2.4.1, category 4). The limit is set to a level where the hydrogen detonation is avoided. Consequently, the large loads that could result from such case are also avoided.

The main function of the containment is to confine the eventual fission products released from the primary circuit. To ensure this, containment leak tightness is a major parameter besides the containment rupture which shall be avoided, Maximum values of containment leakage rates are defined that shall not be exceeded. As this function is essential whatever the probability of the considered reactor condition is, it is often decided that the same maximum leakage rate applies as safety criteria to all accident categories. Typically, the containment leakage rate for all reactor conditions is about 0.1%/day of the containment volume.

2.5 References for Chapter 2

[2.1] Reactor Safety Study – An Assessment of Accident Risks in US Commercial Nuclear Power Plants, US NRC, NUREG-75/104, (formerly issued as AEC report WASH-1400), 1975

[2.2] Deutsche Risikostudie Kernkraftwerke, Verlag TÜV Rheinland, Köln, 1979.

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

[2.4] Acceptance Criteria and Related Safety Margins, SMAP Technical note, Sub-task 1C, NEA/SEN/SIN/SMAP(2005)4, September 2005.

[2.5] Safety Assessment Principles for Nuclear Plants, HM Nuclear Installations Inspectorate, www.hse.gov.uk/nuclear/saps.htm, p. 79

[2.6] Fuel Safety Criteria in NEA Member Countries, Compilation of responses received from member countries, March 2003, NEA/CSNI/R (2003)10

[2.7] ASME Boiler and Pressure Vessel Code, Section III, Rules for Construction of Nuclear Power Plant Components, Division 1, the American Society of Mechanical Engineers, New York, 1995.

[2.8] RCCM, "Design and Construction Rules for Mechanical Components of PWR Nuclear Islands", Section I, Subsection B: Class 1 components, 2000 edition.

[2.9] RCC-MR, "Design and Construction Rules for Mechanical Components of FBR Nuclear Islands", Section I, Subsection B: Class 1 components, 2002 edition.

3 ASSESSMENT PROCESS FOR SAFETY MARGINS

Quite generally, decision-making regarding a particular safety issue, for example a change in safety margin, can be approached by characterizing the scenarios associated with that issue, together with their frequencies and their associated consequences, as discussed in section 3 of [3.1]. Many people associate this "set of triplets" idea –a scenario set with its associated consequences and frequencies– with explicitly risk-oriented decision-making [3.2], but it also applies at a high level to the traditional decision-making approach as well, and formally applies to essentially any framework likely to be used in reactor safety decision-making. For example, in today's licensing practice, postulated design basis scenarios are analyzed to show that their consequences are acceptable, including margin; the decision rule qualitatively reflects the relative likelihoods (frequencies) of these postulated events. (refer to [3.3] for examples of postulated scenarios). Within the more generalized framework addressed here, it is important to analyze a more complete set of scenarios, to quantify their frequencies explicitly, and to understand a broader range of margin-related and consequence-related metrics.

Because the "triplets" idea bridges all foreseeable frameworks, including current practice, the discussion of information needs is organized below in terms of this idea. Information needs are discussed for developing the scenarios and quantifying their frequencies and consequences. Structuring the discussion in this way is not meant to imply that these aspects can be discussed independently; they are highly inter-related. For example, both the frequencies and the consequence metrics influence the structure of the scenario set. However, this organizing principle fosters understanding of how the existing approach is generalized for purposes of the integrated margins assessment.

3.1 The Risk Space for Safety Margin Assessment

As explained in [3.4], the assessment of generalized safety margins requires consideration of all possible scenarios having non-negligible likelihood; this almost complete set of scenarios was named the *risk space* and is described through a set of PSA-like event trees which provides capability to analyze multiple safety objectives. The development of the risk space requires building a complete set of representative initiators and associated event trees, using existing analyses of design basis accidents and PSA models as starting points. Such a set of event and fault trees, which provides the risk profile of the plant at its nominal or initial state, before any change is being implemented, can be properly named the base case risk space. The development of a base case risk space is in some aspects similar to the event tree delineation in classical PSA, but the capability to address different safety objectives and to evaluate generalized safety margins introduce additional requirements that result in important methodological differences. Methodological details may depend on the specific plant technology and should be developed on a case specific basis. The evaluation of proposed plant modifications requires representing them on this plant safety description in order to compare the "before" and "after" status of the safety margins.

The following is a summary of the work done as part of the SMAP tasks 2 and 3, on how to build the risk space, the kind of information that will be needed to quantify the effects of the plant modifications on the safety margins and their quantification process. A more detailed discussion can be obtained from Technical Notes SMAP Task 2 [3.1] and 3 [3.5].

3.1.1 The need of the risk space to evaluate safety margins

As discussed in Reference [3.3], licensing is usually based on a conservative analysis of plant physical responses to specific challenges. For example, the licensee in the U.S. is required to demonstrate the plant's capability to achieve "success" despite:

- physically conservative assumptions in the analysis,
- concurrent loss of offsite power,
- concurrent limiting single failure.

Showing this capability for a comprehensive set of demanding challenges of different severity and likelihood (i.e., the design basis transients and accidents) is a deterministic demonstration of plant safety. The acceptance criteria, which define the "success", are dependent on the type of challenge being analyzed. The complement of equipment needed is then subject to many programmatic requirements, including special treatment requirements. The required capability is maintained operationally through compliance with technical specifications that deal for example with functional availability, surveillance and testing.

A key element of the demonstration is the idea of "margin." The physically conservative assumptions mentioned above include such things as conservative values of decay heat, conservative assumptions regarding the timing of events, generally unfavorable assumptions about actuation set points, and safety limits related to design limits that reflect factors of safety. Partly because of this conservatism, licensing demonstrations of plant capability in responding to design-basis events are considered to be robust.

Unfortunately, while significant plant capability is included within the scope of this demonstration, single-failure-proof response to design-basis events would not by itself guarantee a risk profile that would be considered satisfactory. Experience has shown that out-of-design situations are not as unlikely as expected and the deterministic approach was complemented with risk insights based on the PSA technology. PSA takes credit for success paths that are not part of the design basis capability, including interventions of non-safety equipment, or safety-class equipment in situations not necessarily contemplated in the design basis as well as operator actions beyond those (few) contemplated in accident analysis. At the same time, it allows for the possibility that the equipment relied upon in the safety analysis will not perform its intended function. In some cases, the most conservative assumptions used in the design basis accidents are also relaxed. As a consequence, some success paths in risk analyses are not as robust as the design basis success paths, but they give a valuable contribution to the risk profile description.

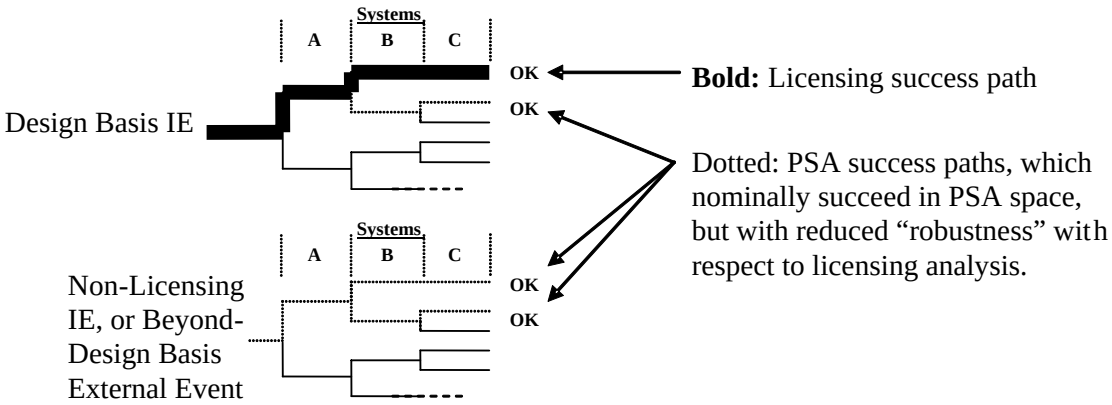

Figure 3-1. Design Basis (Licensing) Approach vs. PSA Approach.

Figure 3-1 shows that typical PSA event trees include some sequences whose success directly derives from the licensing analysis, because a more demanding design basis accident has been shown successful. These sequences are normally located at or near the upper part of the event tree, since they imply a low number of safety equipment failures. The same figure shows that the event tree also includes many other success paths farther down.

Existing PSA approaches, although providing valuable insights to the plant risk profile, have some limitations. On one hand, the idea of "margin" is not used and, consequently, the PSA results and how they are impacted by plant changes should be considered in a mostly qualitative way. On the other hand, among the several safety objectives addressed by licensing analyses, only the potential for severe accidents and their consequences is analyzed in PSA. Less severe barrier failures leading to relatively small but potentially frequent radioactive releases are not included under the scope of PSA. It is then necessary, according to the proposals in SMAP task 1 [3.4], to extend the PSA methods to the risk space in order to get capability to address at least the same safety objectives considered in licensing analyses and to evaluate generalized safety margins.

3.1.2 The risk space attributes

To determine the safety margins for a set of events, it is necessary to have a quantitative measure of the plant response given by deterministic simulation models. The responses will vary over the spectrum of events. To cover the spectrum of events considered in the risk space, all systems in the event trees must be included in the deterministic model. The model must also compute the safety variables relevant to the safety inquiry (i.e., fuel temperature, clad oxidation, containment pressure, etc.). Once the deterministic model is developed, all relevant sequences can be simulated.

While the focus of this step is on the deterministic analysis, it also includes an iterative process with the risk space event tree delineation. The results from the deterministic analysis may trigger new barrier damage mechanisms or safety system failures, which then require iteration back to the event trees and event re-qualification.

Quite generally, the safety objectives to be analyzed with a risk space analysis model determine the level of detail in the definition of end states. In other words, there is a close link between safety objectives and end states since the end state of a sequence is determined by the safety objectives that have been exceeded. Moreover, safety objectives and end states also condition the level of modeling detail both

in dynamic (sequence simulation) and reliability (fault tree) aspects. The selection of initiating events for the event trees is also conditioned by the scope of the analysis. For example, if one is quantifying core damage frequency, then it may suffice to characterize scenarios simply in terms of whether they lead to core damage.

A key point to be discussed is whether or not it is possible to develop a unique base case risk space, i.e., a unique initial set of event trees for a given plant. As above noted, without taking some precautions, a particular choice of initiating events and event tree headers may condition the type of safety objectives that can be analyzed and, therefore, the type of safety inquiries that can be solved. For example, the event trees in a typical level 1 PSA are intended to address the safety objective of maintaining coolable geometry in the reactor core, which is ensured if the sequence success criteria (which are coincident with the LBLOCA design basis acceptance criteria) are not exceeded. However, the same trees cannot be used without extensions, changes or further development to address other safety objectives such as different barrier failures (either failures in other barriers or other types of fuel integrity losses) or their radiological consequences. If one is quantifying the frequency and severity of radiological releases in a severe accident, more detail is necessary even in the core damage model, because the phenomenology of the containment depends on certain characteristics of the scenarios leading to core damage. The application determines the end states, and the end state definitions then determine the success criteria that are the basis for classifying scenarios. As another example, consider the full spectrum of fuel failures from pinhole leaks to catastrophic fuel melt and major core damage. If the application is the assessment of intermediate radionuclide releases, as those allowed for design basis accidents of very low frequency (Condition 3, as described in [3.3]), then the end states will be different and possibly more refined compared to those for severe core damage. An end state could be incipient cladding embrittlement. These newly defined end states then will dictate the appropriate acceptance criteria and the risk space model's success criteria and deterministic attributes. The success criterion could be the decoupling criterion described in Reference [3.3], namely that "the total number of rods affected by DNB must be less than 10%."

Potential restrictions in the type of safety objectives that can be analyzed with a particular set of event trees come from three main sources:

- Selection of safety functions and associated systems,
- Grouping of initiating events and subsequent transient paths,
- Dependency of fault tree structure on sequence success criteria.

A discussion of the influence and importance of these three points can be found in Chapter 2.3 of ref. [3.1]

In the description of the risk space, the use of one or more sets of event trees / fault trees, similar to those of level 1 PSA, has been proposed but, at the same time, the need for a detailed dynamic verification of the sequences has been stressed. Also, as discussed in ref. [3.1], some event tree headers in level 1 PSA contain dynamic dependencies, which are usually modeled as house events in the header fault tree. An advantage of extensive dynamic sequence verification is that it allows for the explicit and detailed accounting of these dependencies. This way, the system states are still modeled through Boolean fault trees while the dynamic dependencies are removed from the fault tree structure. An interesting consequence is that stochastic phenomena can now be modeled as event tree headers where the explicit dependency on system behavior is weak or null but the dependency on sequence dynamics is high. This way, in the risk space description, event tree headers are not restricted to safety functions or systems performing safety functions but they may also include stochastic phenomena, which can significantly alter the course of the accident. The extension of the event tree header concept and the dynamic sequence verification allow to unify the typical methods of level 1 (pure Boolean event/fault trees) and level 2 (Accident Progression Event Tree - APET) PSA, giving rise to the concept of Dynamic Event Tree.

3.1.3 Impact of plant changes on the risk space model

Once the reference risk space is established in accordance with the scope of the safety inquiry, one must determine what modifications must be made to capture the effect of the proposed plant modification. In the U.S., to determine if regulatory review of a proposed plant change is required, licensing success paths are evaluated in terms of a set of conditions spelled out in 10 CFR 50.59. It is helpful to use the approach in 10 CFR 50.59 as a starting point for addressing changes in safety margins. The following excerpt from 10 CFR 50.59 contains a useful conceptual checklist of ideas for the present purpose:

(2) A licensee shall obtain a license amendment pursuant to § 50.90 prior to implementing a proposed change, test, or experiment if the change, test, or experiment would:

(i) Result in more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the final safety analysis report (as updated);
(ii) Result in more than a minimal increase in the likelihood of occurrence of a malfunction of a structure, system, or component (SSC) important to safety previously evaluated in the final safety analysis report (as updated);
(iii) Result in more than a minimal increase in the consequences of an accident previously evaluated in the final safety analysis report (as updated);
(iv) Result in more than a minimal increase in the consequences of a malfunction of an SSC important to safety previously evaluated in the final safety analysis report (as updated);
(v) Create a possibility for an accident of a different type than any previously evaluated in the final safety analysis report (as updated);
(vi) Create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the final safety analysis report (as updated);
(vii) Result in a design basis limit for a fission product barrier as described in the FSAR (as updated) being exceeded or altered; or
(viii) Result in a departure from a method of evaluation described in the FSAR (as updated) used in establishing the design bases or in the safety analyses."

This excerpt is aimed at deciding whether a proposed "change" alters the situation in some way that is not adequately addressed in the current licensing basis. This thought process is generic and comprehensive, and can be applied to power uprates, life extensions, etc. Although one might consider the above to be an essentially deterministic thought process, the essential thoughts are more broadly applicable. It is useful to apply these essential thoughts to a broader class of events than that contemplated in the licensing basis. In the usual application of the above excerpt, the domain of the thought process is the accident analysis in the FSAR. In the present report which is concerned with the risk impact of changes, the domain of the thought process should be the success paths credited in the risk model. Table 3-1 below compares the elements of the deterministic licensing approach with the comparable elements of the risk model. The 10 CFR 50.59 questions raised about each element in the middle column need to be extended to the elements in the right-hand column, and slightly adjusted for context.

Table 3-1. Elements to be considered in revising the risk space

Elements	FSAR Elements Addressed in 10CFR50.59	Risk Model Elements That Need To Be Questioned Regarding Proposed Changes
Initiating Events	Selected IEs including DBAs, AOOs	Comprehensive set of IEs; comprehensiveness determined implicitly by intent to capture "risk-significant" contributors
Success Paths	Complement of success paths, that is, single-failure-proof, assuming a concurrent loss of offsite power; most credited equipment ends up with special treatment requirements. This determines scope of SSC failure mode questions.	All success paths on each event tree. This should determine scope of SSC and operator action failure mode questions.
Evaluation Basis (how "success paths" are shown to be successful)	Conservative phenomenological evaluation compared to the conservative acceptance criteria.	"Success" in the risk space model is no longer an on-off concept. Instead, the conditional probability of exceedance (or conditional loss of function probability) is used to evaluate the "degree of success" of a given path with respect to a particular safety objective
Consequence Evaluation	Barrier challenges as measured by selected safety variables. Radiological consequences of "success paths" and of non-mechanistic source terms are analyzed using prescribed methods and compared with regulatory limits.	Extending from the consequences under the FSAR elements, challenges to any defined safety objective and radiological consequences of all accidents including severe accidents

To be applicable to quantifying changes in global margin, certain terms need to take a more general meaning. For instance, wherever 10 CFR 50.59 refers to "accidents," one needs to apply the thought to "event tree sequences". Thus, based on 10 CFR 50.59, one needs to know whether there are "new" initiating events to be considered (or whether previously-screened-out initiating events need to be considered), or "new" event tree headers to be included in the model which will result in new or different sequences to be analyzed. Similarly, questions about changes in accident frequency should be addressed by accounting for both changes in the initiating event frequency or in event tree header probabilities.

Other terms that assume broader meaning are SCCs, consequences, and design basis limit. Specifically, references to "SSCs evaluated in the FSAR" (essentially, those credited in the accident analysis) need to be broadened to include SSCs (and indeed operator actions) credited in the risk model. The type of consequences to be taken into account include from challenges to barriers potentially resulting in different failure modes up to radiological consequences. All type of failure modes of each barrier are candidates, depending on the nature of the inquiry. The magnitude of the radiological consequences of accident sequences is also of interest. An increase in the magnitude of the consequences could result from an increase in the inventory, release fractions, or physical characteristics (thermal energy) of the release. For safety margin quantification, consequences of each sequence are measured in terms of "conditional probability of exceedance" or "conditional probability of loss of function" as discussed in Chapter 3.1.4 below. Therefore, 10 CFR 50.59 questions about changes in consequences should be interpreted in terms

of changes in exceedance probabilities. A more detailed discussion of the issues raised in Table 3-1 can be found in ref. [3.1].

3.1.4 The quantification process of the risk space

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

The frequency of a damage state is an aggregate of the frequencies of transient paths[3] where the corresponding safety objective is exceeded. Each sequence in an event tree, described by a particular combination of header states, is the set of all the possible transient paths with that combination of header states. Among these paths, some will result in exceedance of the safety objective (they will be called damage paths with respect to that objective) while others will end in a safe state without exceeding the safety objective at any time (success paths with respect to the analyzed safety objective). Event tree headers describe the status of essential safety features like availability of safety functions in terms of safeguard systems configurations, assuming they are demanded during the transients. Damage paths are dependent not only on the state of the set of headers but also on the times in-between events requiring safety functions header activation, once given initial conditions. The set of header states then conditions the damage frequency, but does not entirely determine it.

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

An implicit assumption in classical PSA is that all the safety functions represented by the headers composing a sequence are actually demanded in any transient path included in the sequence. This is reflected in the fact that header probabilities are labeled in “per-demand” terms. This raises the question of the probability of the demand, which is discussed in Chapter 6.4.1 of [3.5] along with other issues regarding the accident-timing problem or the estimation of the fraction of the sequence frequency that actually contributes to the damage state frequency.

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

3 In this context, a transient path can be interpreted as a deterministic transient that can be calculated with the system analysis codes of following sections.

function is then used to calculate the core damage frequency from frequency data for the initiating events and from probabilities of the basic events. There is plenty of literature about event tree / fault tree techniques. See for example [3.6] and [3.7] for fault trees and [3.8] and [3.9] for event trees.

The resulting structure can be reduced by means of the Boolean algebra rules to obtain a canonical form of the Boolean function that represents the system failure. This canonical form is usually the Disjunctive Normal Form (DNF), also called Minimal Cut Set (MCS) representation of the Boolean function, given by a non-reducible set of terms linked by union operators, each term (called a MCS) consisting of the intersection of several basic events and representing a sufficient combination of basic events which results in the loss of the safety function represented by the top event. There are other canonical representations of the Boolean functions, Decision Diagrams [3.10] being the most useful.

In terms of systems failures, an Event Tree can be viewed as a set of sequences of events, starting at the initiator and ending in some (previously defined) damage state[4]. The correct way of reading an event tree is starting from the initiating event and traversing it left to right counting a failed (successful) mitigating action - represented by an event tree header - whenever the line goes downwards (upwards), so that each sequence is a set of failures and successes yielding either success (no damage) or one of several categories of damage. The final state of each sequence is thus indicated to the right of the graphic.

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

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

The process by which the MCS equation of a damage state is obtained and then used to calculate the damage state frequency is called the quantification of the event/fault tree. The MCS equation is obtained by the repeated application of the Boolean absorption and idempotency rules until no further reduction is possible. The difficulty in finding the exact MCS equation of an arbitrary Boolean function is that the number of MCS representing the function may be very large. The reduction of a Boolean formula to a MCS representation is not exclusive to reliability. It is used in testing the correctness of the design of electronic circuits. Several techniques have been devised to perform this reduction (like Karnaugh maps or the Quine-McCluskey procedure), to be found in any reference in computer-aided design of integrated circuits. For reliability uses, though, other algorithms that restrict the search for MCSs in terms of probability are preferred. Other techniques to represent Boolean functions as well as their advantages were presented in [3.5] in more detail.

PSA techniques are by their very nature a way to analyze aleatory uncertainties associated to the behavior of a plant, especially under accident conditions. The outcome of this analysis is the expected likelihood (i.e., expected frequency) of the damage states of interest. However, it was also noted that the parameters involved in the frequency quantification model are also subject to uncertainty (usually modeled

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

as epistemic), leading to a double loop solution scheme. This scheme is usually applied in classical PSA where the input parameter uncertainty is propagated throughout the model in order to characterize the uncertainty of the PSA outputs.

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

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

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

Several issues have been identified (see for instance [3.11]) concerning improvements in the quantification of core damage frequency as performed in current, static PSAs. Furthermore, the evaluation of the frequency of exceedance of a safety objective requires one to identify first the accident paths going beyond that objective, then to group them into sequences. Safety objectives are described in terms of ranges of values of safety variables to be avoided because, if the plant state enters those ranges, there is a non-negligible probability of unacceptable damage. Since safety variables are functions of the plant process variables during transients, the key point to identify situations exceeding safety objectives is the evolution of the process variables along accident paths. Any plant transient state, including damage states, is the result of the plant evolution from a steady state, due to a set of events occurring at different times. This considerably reduces the number of transient states to be considered for evaluation of damage state frequencies. In order to characterize accident paths, the dynamic and reliability models used to represent the plant behavior should describe:

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

For a fixed sequence, items 4 and 5 are fixed, but there will be a lot of paths depending on the other items. Items 1 and 2 depend on the TH model and on the grouping of initiating events, and the final

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

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

Even within the classical PSA scope, analyses supplementing the design basis ones are also performed in order to evaluate additional aspects or new headers beyond those already implicit in the design basis transients. This is usually necessary at least when human actions are required during the sequence. Even when operator actions are considered in design basis analyses, their reliability is not quantified and, in order to calculate the sequence frequency, it is necessary to estimate the available time to perform the action. This refining process is commonly done with the aid of low detail “parametric” models and /or more detailed, best estimate TH codes.

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

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

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

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

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

To properly capture the behavior that leads to change of safety margins, the evolution of plant conditions ought to dictate the accident paths followed. These conditions may persist after the events. A typical example is the occurrence of combustion phenomena only if flammability conditions are met, with delays potentially resulting from stochastic ignition conditions and with potential for multiple combustions if the flammability conditions persist. Those more general conditions (including set points as particular cases) may be considered as stimuli for the events. When accident paths reach those conditions, we speak of the paths “activating stimuli”.

Because stimuli activation conditions the events, the history of activations during the accident paths do matter in calculating the frequencies, and extensions of the Markov process equations accounting for these features are necessary. Those extensions constitute the “so called” Stimulus Driven Theory of Probabilistic Dynamics (SDTPD) [3.12]. It exhibits as a nice feature an explicit relation between the different exceedance frequencies in the terms explained above. SDTPD provides mathematical balances to calculate the probabilities per unit time of entering states with specified activated stimuli and correlate them with each other. In addition, in the calculation of the exceedance frequencies, the probability of the demand and the fraction of damage paths are not factorized but rather embedded in the activation of the stimuli. Exceeding safety objectives is a particular case of stimulus, so SDTPD has the potential for analyzing multiple safety objectives. Work is in progress to better relate the SDTPD theory with the classical probabilistic approach, so as to allow hybrid schemes to be used.

3.2 Deterministic Calculations

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

- Very conservative (Appendix K approach for LOCA),
- Best estimate bounding,
- Realistic conservative,
- Best estimate plus uncertainties (BEPU).

Similar classification was done in the IAEA document [3.13] where the transient analyses for licensing purposes were identified as shown in Table 3-1. The very conservative method agrees well with IAEA no. 1 safety analysis approach, realistic conservative with IAEA no. 2 and BEPU with IAEA no. 3. The IAEA no. 4 safety analysis approach has not yet been used. It is connected with risk-informed regulation.

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

In the following each of the safety analysis approaches will be briefly described. More detailed description of safety analysis approaches can be found in Technical Notes SMAP Task 3 [3.5]. In Section 4 of TN SMAP Task 3 report [3.5] are given examples of applying safety analysis approaches.

Table 3-2: Safety analysis approaches for licensing purposes [3.13]

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

3.2.1 Very conservative approach (Appendix K)

Historically the initial licensing procedures that governed analysis, were established in 1974 when the USNRC published rules for loss-of-coolant accident (LOCA) analysis in 10CFR 50.46 and Appendix K [3.14]. Analysis following these rules is known as the (very) conservative approach. It is the first one used in safety analysis. The basic reason for developing the conservative method has been the need to make allowance for the lack of knowledge of physical phenomena. It is an approach based on the notions of consequences (maximization) and criteria (restrictive).

10CFR 50.46 established the primary safety criteria for peak cladding temperature (PCT), maximum cladding oxidation, maximum hydrogen generation, coolable geometry, and long-term cooling (these remain unchanged today in the US). Emergency core cooling systems (ECCS) cooling performance is evaluated using a computer code model. Appendix K to Part 50 establishes required and acceptable features of the evaluation model. Discussion of the relative importance of the various features of Appendix K is of course found neither in Appendix K nor in the documentation of that time. Since then, several studies have been carried out to provide some information in this regard [3.15]. For LBLOCA the most important features appeared to be use of high peaking factors, lockout of return to nucleate boiling, steam-only cooling during re-flood and bounding decay heat. For small-break (SB) LOCA these were the single failure criterion and bounding decay heat.

Problems raised by the conservative approach are: a) there is no way to prove that the conservatisms that are verified on scaled down experiments are also valid at full scale reactor size; b) due to nonlinearity, the additivity of several conservative measures cannot be verified; and c) the method is inappropriate for emergency operating procedures (EOP) studies (especially obvious after TMI-2 accident). All these limitations have been the motivation for developing best estimate codes.

3.2.2 Best estimate bounding

In the best estimate bounding approach, the best estimate computer code is used while the uncertain input parameter values are selected conservatively to bound the parameter of interest. In this approach the uncertainties are not statistically combined.

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

One of the major limitations of such methods is that they may involve unquantifiable over-conservatism due to the linear combination or bounding of all conservative assumptions. Sometimes, the final licensing results are comparable with or even more conservative than the Appendix K type approach. The bounding best estimate approach using SECY-83-472, as licensed by Westinghouse and General Electric, is no longer allowed in USA.

3.2.3 Realistic conservative

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

The realistic conservative approach is similar to the very conservative approach except for the fact that best estimate computer code is used in lieu of conservative code. An example of realistic conservative approach is German licensing practice where a best estimate code is used with conservative assumptions on availability of plant systems and conservative initial and boundary conditions.

3.2.4 Best estimate plus uncertainties (BEPU)

Original criteria for LOCA were formulated at a time when limitations in knowledge made conservative approaches necessary. Research conducted during 1974-1988 provided a foundation sufficient for the use of realistic and physically based analysis methods [3.16]. A large number of experimental programs were completed internationally. Several advanced best estimate computer codes were developed in parallel with experiments for replacing conservative evaluation models. Based on these research results the USNRC initiated an effort to develop and demonstrate a best estimate (BE) method acceptable for licensing which could bring benefit to nuclear plant operators (less conservative, consideration of uncertainties, economic gains). The Code Scaling, Applicability, and Uncertainty (CSAU) method was developed and demonstrated for LBLOCA in a pressurized water reactor (PWR) [3.17]. After the pioneering CSAU, several new methods were developed which were presented together at a special OECD/NEA/CSNI (Organization for Economic Cooperation and Development/Nuclear Energy Agency/Committee on Safety of Nuclear Installations) workshop on uncertainty analysis methods in 1994 [3.18]. One of the objectives of the workshop was also the preparation of the uncertainty methods study (UMS). In the UMS study (1995-97) five uncertainty methods were compared [3.19]. The OECD/CSNI workshops in Annapolis-1996 [3.20], Ankara-1998 [3.21] and Barcelona-2000 [3.22] also dealt with uncertainty evaluation methods. More recently, the BEMUSE task group (in the framework of CSNI/GAMA) undertook during the first 3 phases a quantitative comparison of different uncertainty evaluation methodologies, based on the LOFT L-2-5 experiment. The reports documenting this effort are

to appear shortly. On the international conferences Best Estimate 2000 and 2004 several applications of BEPU methods were presented, including licensing applications.

The developed methods significantly differ in the way that uncertainties were quantified. Different techniques for the uncertainty propagation in best estimate thermal-hydraulic code calculations were identified, including Monte Carlo analysis, Response Surface (RS) methods, statistical tolerance limits, and internal assessment of uncertainty. For more details the reader is referred to TN SMAP Task 3 [3.5]. Work on incorporating uncertainty estimation into computer code evaluations is ongoing in other disciplines where complex modeling is essential to nuclear regulation. Reference [3.23] provides a picture of how issues related to modeling uncertainty are being addressed in the area of environmental modeling.

In the following each of the techniques mentioned above will be briefly described.

Monte Carlo analysis

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

Response surface methods

Response surface methods (RS) are similar to Monte Carlo analysis except that instead of a thermal-hydraulic computer code a response surface is used. However, for response surface generation code calculations are needed. The number of uncertain input parameters is limited because of the required number of code calculations. The response surface can be defined as a collection of techniques used in the empirical study of relationships between one or more responses, or product characteristics, and a group of input variables. Usually parametric and nonparametric regression analysis is used for response surface generation.

Tolerance limit methods

In the case of relatively many input uncertainty parameters the uncertainty could be determined from the distribution of key code output uncertain parameter. Statistical upper and lower bound of the distribution are then determined as the tolerance limits with a specified probability. There are two ways to calculate the tolerance limit: parametric and nonparametric statistics. Parametric statistics are based on parameters that describe the population from which the sample is taken. In the parametric approach the tolerance limit is calculated from the distribution. Nevertheless, parametric tolerance limits can be determined in very few special cases: normal, exponential distribution type. When the distribution hypothesis is rejected by goodness-of-fit test (it is unknown) it is possible to determine tolerance limits by randomly sampling the character in question. The consideration of nonparametric tolerance limits was presented by Wilks.

Internal Assessment of Uncertainty

An original technique for determining uncertainty bounds is the Code with capability of Internal Assessment of Uncertainty (CIAU) [3.24]. Namely, all of the uncertainty methodologies used in UMS suffered from two main limitations on resources needed for uncertainty methodology development and dependence of results on methodology/user. CIAU has been developed having in mind the objective of removing these limitations. Unfortunately, it suffers from the limited availability of (large-scale) experimental data set necessary to derive the uncertainty information in order to completely cover the full range of the (hypercube) parameters. Any of the available system codes or the uncertainty methodologies can be combined to constitute CIAU. However, for each new code (or code version) the hypercubes needs

to be filled first what currently prevents licensing applications with codes different from RELAP5/MOD3.2.

3.3 Classification and Separation of Uncertainties

3.3.1 Classification of Uncertainties

It is the state of the art not only in safety analyses of nuclear power plants to discriminate between two fundamental types of uncertainty: the **aleatory** and the **epistemic** uncertainty.

Aleatory uncertainty results from the effect of "inherent randomness" or "stochastic variability". It represents the nondeterministic and unpredictable random nature of the performance of the system and its components.

Aleatory uncertainty is quantified by probability. Probability of an event is considered as a quantitative measure of the "chance of occurrence" of that event. The "frequentistic" concept of probability interpretation is appropriate: probability ≈ "relative frequency in a large number of independent random trials".

Variables subject to aleatory uncertainty have intrinsic probability distributions, which represent "random laws". These distributions are usually derived from statistical data.

Roughly speaking, aleatory uncertainty can be associated with the question "what can occur and with which probability".

Aleatory uncertainty as such is the subject of PSA to express probabilistically how safe the system is. In this context aleatory uncertainty is primarily associated with:

- Occurrence of initiating events,
- Initial conditions i.e. the state of the plant at the beginning of an accident,
- Performance of system components and humans during an accident, etc.

Epistemic uncertainty results from the "imperfect knowledge" regarding values of parameters of the underlying computational model. The parameters as such are deterministic in nature, i.e. they have fixed and invariable values which are not precisely known.

Epistemic uncertainty can also be quantified by probability. Probability distributions associated with uncertain parameters represent the "state of knowledge" about the "right" values of the parameters. Here, the "subjectivistic" concept of probability interpretation is appropriate: probability ≈ "degree of belief or confidence that a statement is true". Such probability distributions for uncertain parameters are very often derived from expert judgment.

Epistemic uncertainty can be reduced, at least in principle, and sometimes even eliminated by improving the state of knowledge, e.g., by doing more investigations, experiments and research.

Roughly speaking, epistemic uncertainty can be associated with the question "which value is the right one and how well do we know that".

Epistemic uncertainty is directly addressed in Uncertainty and Sensitivity Analyses of results from deterministic as well as probabilistic computational models. Such analyses quantitatively express how imprecise the results of the computation are and which are the principal sources of this imprecision [3.25].

In deterministic safety analyses epistemic uncertainties are mostly due to approximation, simplification, limitation, incompleteness, etc. of the underlying computational model.

In traditional PSA the epistemic uncertainties considered so far are associated with probabilistic reliability parameters on component level, i.e. failure rates and failure probabilities on demand.

3.3.2 Separation of Uncertainties

In many safety relevant applications of computational models, like in a PSA, both types of uncertainty are present. In such cases it is increasingly recognized that the two types of uncertainty must be distinguished very carefully and treated separately in different ways [3.26, 3.27]. A consistent and widely accepted approach of uncertainty separation is the so-called “two-dimensional nested” or “double loop” probabilistic analysis where:

- Epistemic uncertainties are treated in the “outer” probabilistic analysis loop, directly with Monte-Carlo simulation methods,
- Aleatory uncertainties are treated in the nested “inner” probabilistic analysis loop by the underlying computational/probabilistic model mostly with approximate analytical/numerical methods (e.g. Fault- and Event-Tree or FORM/SORM), sometimes also with Monte-Carlo methods or combinations of both.

A direct result of such two-dimensional epistemic & aleatory probabilistic analysis will be a sample of (aleatory) probabilistic results from the inner analysis loop, e.g. a sample of expected core damage frequencies or other useful probabilistic quantities expressing the effect of the underlying aleatory uncertainties. This sample represents the distribution, which quantifies the epistemic uncertainty about the probabilistically expressed system safety (“probability distribution of probabilities”). It can be statistically analyzed in two ways to show (1) how uncertain (in the epistemic sense) are the computed probabilistic results and (2) which are the principal contributors to that uncertainty.

The “two-dimensional nested” probabilistic analysis approach is for a long time a common practice in traditional PSAs for nuclear power plants [3.28]. In the “inner loop” of a level-1 PSA, e.g., the aleatory uncertainties are quantified with the aid of Fault- and Event-Tree methods leading to probabilistic results like “expected core damage frequency”. The quantification of the epistemic uncertainties (“outer loop”) is conducted by Monte-Carlo simulation of these Fault- and Event-Trees accounting for the epistemic uncertainties in the probabilistic reliability parameters of the system components.

Two-dimensional nested probabilistic analyses are also increasingly performed within the framework of safety analyses of nuclear waste disposals [3.29].

It is immediately clear that the computational effort for a full “two-dimensional nested” probabilistic analysis may be immense and may therefore not be feasible if the underlying models are computationally expensive as in nuclear safety analyses. Nevertheless, it is also clear that it would not be appropriate to ignore the necessity of uncertainty separation and to perform a “one-dimensional” probabilistic analysis with both uncertainty types treated jointly in the same manner. The results of such analysis can be difficult to interpret, misleading or even completely wrong.

Therefore, there is a need for approximate methods, which somehow avoid the full two-dimensional nested probabilistic analysis but, nevertheless, provide interpretable and satisfactory results with a reduced computational/sampling effort.

3.4 Guidelines for Uncertainty Treatment in Deterministic Calculations

Optimizing the output of nuclear power plants makes very often the plants more reactive to accident initiators. As a consequence, in several cases, it was impossible to fulfill the criteria with the traditional conservative methods used in the past to design nuclear plants. Those traditional conservative methods were generally the same or of the same type than the ones on which safety margins evaluation were asked in the seventies. To reach the compliance with the criteria, new methods have to be used. This necessarily leads one toward realistic or best estimate calculations with quantification of the uncertainty in the calculated results. A number of techniques have been developed and are being used to estimate the uncertainty in deterministic predictions of nuclear plant response to transient and accident scenarios. They have been summarized in Section 3.2.Virtually all of the methods have focused on design basis space applications. That is, the intended application is to one or at best a few events.

Some further considerations regarding uncertainty methods in design basis space are provided in this section, but the emphasis is shifted to include applications to deterministic calculations in risk space. Here, the set of design basis accidents (DBA) is named design basis space. On the other hand, the set of all possible scenarios having non-negligible frequencies of occurrence is named the risk space. Whether the analysis is performed for design basis or risk space applications, deterministic code predictions must be made. A number of system codes are available for deterministic analyses including ATHLET, CATHARE, CATHENA, RELAP5, TRAC and TRACE. In addition, more specialized codes such as fuel behavior codes or containment codes are also needed to evaluate safety margins in relation to several fuel-related limits as well as to containment limits. A number of codes are publicly available, e.g., FRAPTRAN, FALCON, TRANSURANUS for fuel behavior analysis, CONTAIN, GOTHIC, MAAP, MELCOR for containment analysis.

3.4.1 Uncertainty issue in risk space

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

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

While the uncertainty issue is also important in the risk space analysis, the higher number of bins results in less demanding enveloping requirements for the representative scenarios. An important consequence is that more realistic scenarios are allowed as representatives in the risk space. This fact, along with the important increase in the number of analyzed cases, makes it unpractical to spend significant resources to obtain results for the representative cases at the 95% confidence level. While

establishing an uncertainty band on the deterministic responses is necessary, it is clear that the technique used should be tailored to the context in which the results will be used. A justifiable band on the key responses that are compared to acceptance criteria and failure limits appears to be the desirable level of rigor for this application.

3.4.2 Uncertainty quantification process for DBA/risk space

There are a number of general considerations that apply to the quantification of uncertainties and to the determination of the approach that is best suited to the application. Figure 3-2 is a schematic that attempts to summarize the process of determining uncertainties. This process involves minimization of uncertainties, identification of significant contributors, and accuracy requirements.

Minimization of uncertainties (upper textbox of Figure 3-2)

Some sources of uncertainty in deterministic analysis results are very difficult to quantify, in particular user effects and intrinsic computer code numerical effects. Therefore, the first manner of dealing with uncertainties is to take appropriate measures to minimize some of them like user effects and intrinsic computer code numerical effects. Use of a well-designed code that is applicable to the analysis at hand by experienced code practitioners is essential to achieving this goal. If there are choices in models, modeling options and correlations, these should be consistent with the assessments and code qualification usage. Convergence of both the nodalization and time step/numerics should be assured by sufficient sensitivity studies. The level of uncertainty can also be reduced by adherence to good user practices [3.30, 3.31, and 3.32].

Identification of significant contributors (middle textbox of Figure 3-2)

There will generally be more sources of uncertainty than can be realistically included in an analysis, so it is important to identify which sources of uncertainties are the most significant and must be included. The intended uses of the results will assist in determining the required level of accuracy. For example, is a probability distribution/density function needed, or are statistical parameters sufficient to obtain confidence intervals required, or will a bounding approach suffice. If a Phenomena Identification and Ranking Table (PIRT) has been developed for the event of interest, it should provide information on which phenomena/models are most important (highly ranked). It is apparent that the PIRT should focus on the same safety variable/acceptance criteria as the current analysis. If a change of the parameter within its range of uncertainty has an insignificant affect on results, further consideration is not warranted. Code assessments are also generally a good resource for identifying the significant contributors to uncertainty in code results. However, when the number of uncertain parameters is not limited like by tolerance limits method and most of uncertainties are treated, sensitivity analysis can be derived directly from the uncertainty analysis (no need to reduce the number of uncertain parameters).

Accuracy requirements (lower textbox of Figure 3-2)

Where a statistical approach is necessary, the choice will depend on availability of the required software, accuracy requirements, and the amount of resources (human and computer hardware). There may be a bias in the results, and if so this needs to be determined regardless of the method applied. Namely, the frozen code version can still consistently overpredict or underpredict certain parameters and the resulting inaccuracy is termed code bias. In most cases it will not be possible to obtain the probability distribution for input parameters; however statistical measures such as the mean value and standard deviation may be available from reference sources. For example, correlations used in the codes may include statistical information.

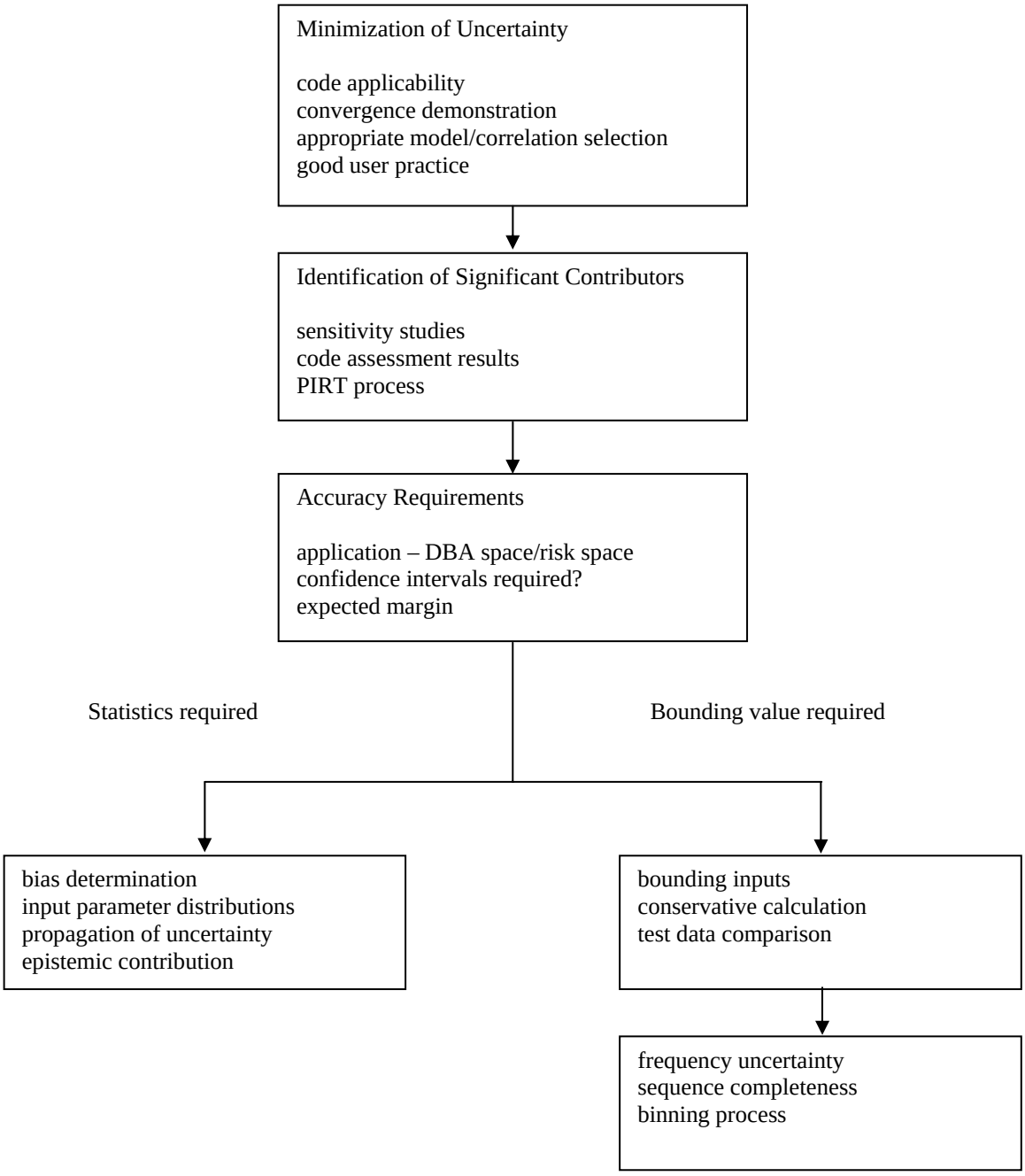

Figure 3-2. Schematic of Uncertainty Quantification Process

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

- Addressing uncertainties must be an integral part of determining safety margins,
- Methods used must be applicable to a wide range of events,

- Required resources for existing methods may require approximations (for example, to reduce the effort, an uncertainty can be established for a particular safety variable for a particular type of transient and then used in all the transients that fit into that category).

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

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

3.5 References for Chapter 3

[3.1] SMAP Group, Task 2: Assessment process for Safety Margin, Nuclear safety, NEA/SEN/SIN/SMAP (2006)2. Issy-les-Moulineaux: OECD Nuclear Energy Agency, Aug 2006

[3.2] Kaplan, S., and B.J. Garrick. 1981. On the Quantitative Definition of Risk. Risk Analysis 1(1): 11–27 (1981).

[3.3] SMAP Group, Sub-task 1C: Technical Note entitled "Acceptance Criteria and Related Safety Margins", NEA/SEN/SIN/SMAP (2005)3. August 2005

[3.4] SMAP Group, Sub-task 1B Technical Note entitled "Definition of generalized Concept of Safety Margins and Characterization of Safety Margin Sources", NEA/SEN/SIN/SMAP (2005), September 2005.

[3.5] SMAP Group, Task 3: Safety Margin Evaluation Methods, Nuclear safety, NEA/SEN/SIN/SMAP (2006)3. Issy-les-Moulineaux: OECD Nuclear Energy Agency, Aug 2006.

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

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

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

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

[3.10] Antoine Rauzy, "A brief introduction to Binary Decision Diagrams", Journal Européen des Systèmes Automatisés, 30(8):1033–1050, 1996.

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

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

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

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

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

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

[3.17] Technical Program Group, "Quantifying Reactor Safety Margins", NUREG/CR-5249, Dec 1989.

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

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

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

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

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

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

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

[3.25] B. Krzykacz, E. Hofer, M. Kloos, “A software system for probabilistic uncertainty and sensitivity analysis of results from computer models”; Proceedings of PSAM-II, San Diego, California, U.S.A., March 20-25, 1994

[3.26] Helton J. C. and Burmaster D.E. 1996, “Guest Editorial: Treatment of Aleatory and Epistemic Uncertainty In Performance Assessment of Complex Systems” *Reliability Engineering and System Safety*, Vol. 54, No. 2-3, 91-94.

[3.27] Perry G. W. 1996, “the characterisation of uncertainty in Probabilistic Risk Assessments of complex systems” *Reliability Engineering and System Safety*, Vol. 54, No. 2-3, 119-126.

[3.28] Gesellschaft für Anlagen und Reaktorsicherheit (GRS). Bewertung des Unfallrisikos fortschrittlicher Druckwasserreaktoren in Deutschland. Methoden und Ergebnisse einer umfassenden Probabilistischen Sicherheitsanalyse (PSA), GRS- 175, Oktober 2001.

[3.29] J. C. Helton, D. R. Anderson, G. Basabilvazo, H.-N. Jow, and M. G. Marietta, "Conceptual Structure of the 1996 Performance Assessment for the Waste Isolation Pilot Plant," *Reliability Engineering and System Safety*, vol. 69, pp. 151-165, 2000.

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

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

[3.32] J.M. Izquierdo, J. Hortal, and L. Vanhoenacker, “Merits and limits of thermalhydraulic plant simulations – towards a unified approach to qualify plant models”, *Nuclear Engineering and Design* 145 (1993) 175-205.

4 SAFETY MARGIN IN THE CONTEXT OF RISK ASSESSMENT

The concept of safety margin is not exclusive to the nuclear industry. As matter of fact, the concept of safety margin was formalized many decades ago through the work on load-strength interference developed in civil engineering applications. It is helpful to discuss the more traditional definition of margin to help distinguish it from the concept of safety margin used in the nuclear industry. To make this discussion possible, the traditional, civil engineering margin will be referred to as "margin to damage", while the nuclear industry concept will be called, safety margin. The distinction is particularly important, because the more traditional definition of margin is connected to the probability of failure, while the nuclear industry definition of safety margin is closer linked to the probability of exceedance, both of which play roles in the determination of risk.

4.1 The Traditional View of Margin to Damage

The general definition of margin to damage often referred to as safety margin in the literature, stems in early load-strength interference work. The load is described by a probability density function that captures all the variabilities expected during the operation of the system. The strength, S, is sometimes called capacity or resistance, and represents the probability density function obtained when the barrier is tested to failure a sufficiently large number of times. Thus, the general definition of margin to damage was cast for structural-mechanics analyses, recognizing the fact that both load, L, and strength, S, are distributed parameters (see, for example [4.1]). Figure 4-1 shows probability densities for load and strength, which form the bases for the general definition of margin to damage.

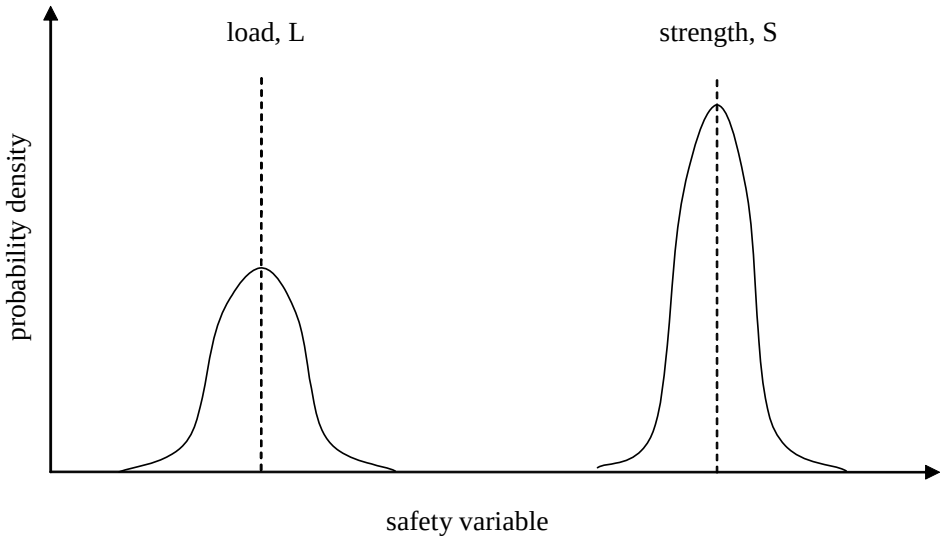

Figure 4-1. Probability densities for load and strength

Two quantities—namely, margin to damage, MD, and loading roughness, LR—describe the reliability of a barrier or system in light of load-strength considerations. These quantities are computed from the following equations:

$$MD = \frac{\overline{S} - \overline{L}}{\sqrt{\sigma_S^2 + \sigma_L^2}}, \text{ and} \qquad \text{Eq. 4-1}$$

$$LR = \frac{\sigma_L}{\sqrt{\sigma_S^2 + \sigma_L^2}}, \text{ respectively,} \qquad \text{Eq. 4-2}$$

where $\overline{S}$ is the mean strength, $\overline{L}$ is the mean load, σ_S is the strength standard deviation, and σ_L is the load standard deviation. Thus, the margin to damage and loading roughness are indirect measures of the overlap in the probability density functions and can be used to estimate the probability that the load does not exceed the strength (i.e., the reliability):

$$p(S > L) = \int_0^\infty f_L(L)\left[\int_L^\infty f_S(S)dS\right]dl, \qquad \text{Eq. 4-3}$$

where $f_S(S)$ and $f_L(L)$ are the probability density functions for strength and load, respectively.

For normally distributed strengths and loads, the probability of failure (i.e., 1-reliability) can be expressed as a function of margin to damage (Equation 4-1) alone. This is one reason why margin emerged as the sole proxy for reliability in many applications. The other reason is that the design goal (in the nuclear industry, as well as other fields such as civil engineering or pressure vessel construction) is to build components and systems that have negligible failure probabilities. Having sufficient margin can attain this (i.e., a large separation between mean strength and load relative to their combined standard deviations). This solidified the generalization that having adequate margin is a sufficient condition for high reliability. Thus, a highly reliable system (i.e., one in which the probability of failure is negligible) looks like Figure 4-1, with practically no overlap between the probability densities of strength and load.

Figure 4-2 is a schematic representation of the probability of failure. Given sufficient information with regard to load, strength, and their standard deviations, reliability can be precisely computed using the concepts of margin to damage and loading roughness discussed above. However, such information is often beyond the current state of the art. In the nuclear industry, for example, probability functions for strengths of fuel or containments are prohibitively expensive to obtain. Furthermore, the two-prong approach to ensuring safety margin adopted in the nuclear industry, lends itself much better to inspection by examining the probability of exceeding the safety limit than calculating the actual probability of failure.

Figure 4.2. The probability of failure in an event sequence

4.2 The Exceedance Probability as a Surrogate for Probability of Loss of Function in Probabilistic Margins Considerations

In nuclear industry DBA discussions, “adequate safety margins” are inextricably linked to safety limits - limiting values imposed on safety variables (e.g., peak clad temperature (PCT) and containment pressure). Thus, when operating conditions stay within safety limits, the barrier or system has a negligible probability of loss of function, and an adequate safety margin exists. Therefore, the first prong of ensuring adequate safety margin is to set safety limits such that the probability of loss of function is negligible, so long as operating conditions stay within those criteria. Figure 4-3 illustrates this concept.

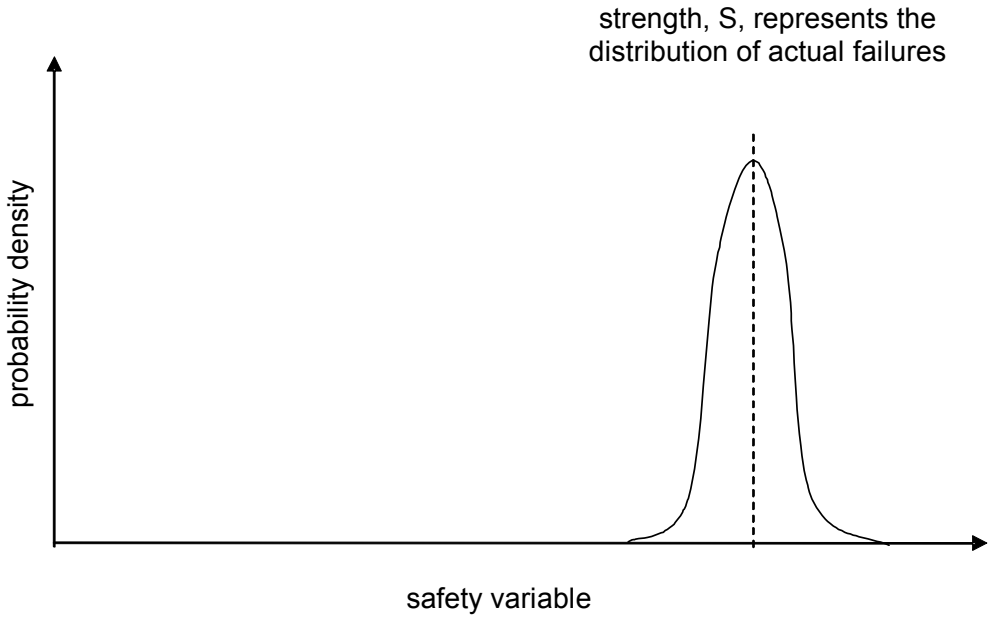

Figure 4-3. Setting the safety limit for a specific safety variable

One or more safety variables characterize operating conditions. For example, for the fuel barrier of a nuclear reactor, PCT and total clad oxidation are safety variables. These safety variables depend on the physical characteristics of the barrier or system being analyzed. In the case of the fuel, both PCT and clad oxidation can be measures of the embrittlement damage mechanism. In setting conservative safety limits for safety variables, the industry builds in margin for lack-of-knowledge uncertainties. The intent is to allow margin for phenomena and processes that are inadequately considered in generating models to simulate the behavior of the given system or physical barrier. Epistemic uncertainty is reflected, for example, in setting the safety limit for maximum PCT in a light-water reactor (LWR). That safety limit, 1204 °C (2200 °F), lies below the onset temperature for autocatalytic oxidation of zirconium, which, in turn, is below the point at which significant radioactive releases are expected from the fuel. Therefore, adequate safety margin exists if operating conditions are such that PCT remains under 1204 °C (2200 °F)[5].

The second prong of ensuring adequate safety margin is to keep operating conditions within safety limits. Figure 4-4 illustrates this concept. The load, L, is the probability density function obtained in a particular scenario for the safety variable by propagating contributing uncertainties. In the computation of PCT in a specific large-break loss-of-coolant accident (LOCA) scenario, for example, uncertainties associated with boundary and initial conditions, heat transfer coefficients, and other modeling assumptions, should all be captured in the load. The 1989 CSAU method of NUREG/CR-5249 has laid the foundation for generating the probability density function associated with the load. [4.2] The fundamental process of identifying key phenomena and variables introduced by CSAU is essential to integrating risk and safety margins as presented in this report. Several advances have been introduced in more recent best estimate plus uncertainty methods, most notable the extension of the Gesellschaft für Anlagen- und Reaktorsicherheit System for Uncertainty and Sensitivity Analysis (SUSA) methodology into SUSA-AB to deal separately with epistemic and aleatory uncertainties, which is discussed in more detail elsewhere in this report. [4.3]

[5] PCT is one of the two safety variables used to ensure that fuel cladding does not become embrittled. The other safety variable is total clad oxidation, which has an acceptance limit of 17 percent.

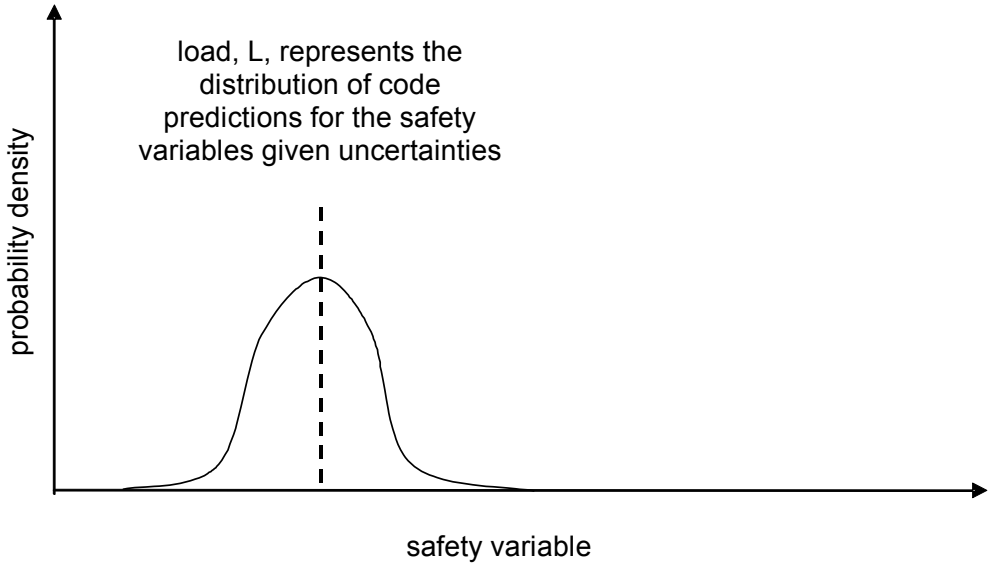

Figure 4-4. Keeping operating values of a specific safety variable under the safety limit

Figure 4-5 shows the approach taken to ensure margin sufficiency in the nuclear industry. The probability density functions in the figure are used for illustrative purposes. The safety limit is conservatively set below the strength probability density function. Simultaneously, the code predicts values used to assess acceptability under conservative assumptions set forth in the emergency core cooling system (ECCS) evaluation models discussed in Appendix K to 10 CFR Part 50 [4.4] or more realistic alternatives. Although it cannot be strictly proven, a conservative calculation of the type imposed by Appendix K is expected to be sufficiently conservative to be more restrictive than one obtained from a more realistic approach (e.g., one that computes the bounding 95th percentile of the safety variable value with 95 percent confidence). Thus, a conservative Appendix K calculation would leave even more room for epistemic uncertainty than simply setting a conservative safety limit.

In general, approaches used to compute the limiting value of a safety variable are classified as very conservative (Appendix K), bounding best estimate, realistic conservative, and best estimate plus uncertainties (see section 3.2). The latter is ideally suited for integrating risk and safety margins. However, where sufficient margin exists, simpler, more conservative approaches can be used, which effectively reduce to current regulatory practice. Best estimate plus uncertainty methods have evolved substantially over the years and include Monte Carlo analyses, response surface methods, tolerance limit methods, internal assessment of uncertainty and other approaches practiced in other technical fields.

The use of safety limits instead of the onset of damage is more suitable for integrating risk and safety margins for two reasons—convenience and consideration of the unexpected. Obtaining the strength probability functions for physical barriers (e.g., fuel, reactor coolant boundary system, and containment) for each damage mechanism will continue to be prohibitively expensive. Therefore, it is convenient to set the safety limit below the onset of damage, by an amount that is commensurate with the lack of data and the importance of the subject safety variables. This gives the requisite confidence that, if operating conditions remain within safety limits, the probability of failure will be negligible and some additional margin will be available for unknown events and phenomena.

Figure 4-5. Ensuring adequate safety margins by setting a conservative safety limit and using bounding code prediction values to assess acceptability

It is important to note that it may be necessary to rethink the appropriate value of a safety limit for risk calculations. For example, the design-basis limit for containment pressure may be justifiably considered overly-conservative in light of the epistemic uncertainty associated with the containment fragility curve. In this case, the value of the limit used to determine the existence of sufficient margin when integrating risk and safety margins may differ from a design-basis safety limit.

As discussed above, adequate margin exists as long as all but a negligible part of the load probability distribution function remains under the safety limit in DBAs. The natural extension of this to all accident sequences, is extracting the probability of exceeding the safety limit for use in building the risk metric. The probability of exceedance is a well-established concept in PSA. When a safety limit exists, the cumulative probability of the load curve that exceeds the safety limit is the probability of exceedance as shown in Figure 4-6. The load probability density function is generated through well-established methodologies such as CSAU or SUSA-AB. [4.2 and 4.3] Simple approximations for exceedance probability can be devised (see, for example, [4.5]). The exceedance probability is conditioned on the occurrence of the event sequence that was simulated to generate the probability density function for strength. Thus, the proper term is conditional probability of exceedance.

Figure 4-6. Calculating the conditional probability of exceedance in an event sequence

To integrate risk and safety margins, the assumption is made that function is lost when the safety limit is exceeded. This is fully consistent with the view taken in judging acceptability in DBAs, and becomes a natural nexus between the deterministic concept of safety margin and the probabilistic quantity needed to evaluate the change in safety margins over the entire risk space. This is, potentially, the most contentious step in integrating risk with safety margins, but it grounds this framework in existing regulatory practice. This assumption is fully justified if one remembers that an important driver in setting the safety limit below the onset of damage is to cope with "unknown unknowns." Because safety limits are set commensurate with the lack of knowledge and the importance of the subject variable, and because both these considerations are equally applicable in risk assessments, it is wise to extend this assumption to PRA analyses.

Once the conditional exceedance probability is defined, the meaning of the term "safety margin" becomes unambiguous. The phrases "sufficient margin" and "loss of margin" also become clear in accidents that are not part of the design basis. Sufficient margin exists if the probability of exceedance is negligible. Margin is lost if and only if a change occurs in the probability of exceedance.

4.3 Caveats in Adopting the Probability of Exceedance in Evaluating Safety Margins for Risk Investigations

There are three caveats with regard to the definition of safety margin as presented above. The first involves setting the safety limit confidently below the onset of damage, which can be achieved for most physical barriers. One can imagine that for certain damage mechanisms and certain barriers, the

uncertainty associated with the onset of damage could be so large as to preclude the ability to set a safety limit such that operations stay below it for certain accidents. This, however, is not the case with barriers of existing LWRs, so discussions on dealing with large uncertainty in the capacity density function will be deferred.

The second, and somewhat related, caveat is that one can make definitive statements with regard to keeping operating conditions below safety limits for design-basis events. However, the same is clearly not true in the risk space. For example, in a classic large-break LOCA event tree, many event sequences end in core damage. That presumes that the safety limit of 1204°C (2200 °F) was exceeded. Thus, there is an additional consideration of frequency of exceedance that should be associated with a given safety limit. The advantage is, however, that the frequency of exceedance can be linked to a high-level risk acceptance guideline (e.g., the Commission's safety goal [4.6]). Thus, for a given plant, the threshold safety limit and its exceedance frequency form a unique point on a frequency-consequence plot. This establishes a link between the integrated risk/safety margin framework and decision-making approaches based on the use of frequency-consequence curves.

The third caveat is that the change in safety margins captured in this report pertains only to cases where a significant fraction of the load probability density function exceeds the safety limit. This is insufficient for those researchers who believe that any change in operating conditions that moves the plant closer to the safety limit is an effective loss of safety margin, whether the safety limit is exceeded or not. In other words, the framework that integrates risk and safety margins is insensitive to changes that move the entire load probability density function through the space below the safety limit. For example, if, following a power uprate, the PCT in a transient changes from 800 °C (1472 °F) to 850 °C (1562 °F), the change is imperceptible to the risk metric calculated by integrating risk and safety margins. To some this change represents an erosion of margin and should be captured. Earlier work on this framework suggested that it is possible to quantify loss of margin that occurs far away from the safety limit, where far is determined by the standard deviation in the load probability density function. One can devise means of capturing such changes (see, for example, [4.5]), but judging the acceptability of such an increase requires setting new acceptance criteria/guidelines, which is beyond the scope of this work. The example provided by KINS for Chapter 6 of this report shows how the concept of safety margin can be used to measure changes of the distance to the safety limit, as opposed to measuring exceedance as is done in the most of this report.

4.4 References for Chapter 4

[4.1] O'Connor, P .D.T., "Practical Reliability Engineering," Third Edition, John Wiley & Sons, Indianapolis, IN, ISBN 0-471-92902, p. 95, 1991.

[4.2] "Quantifying Safety Margins: Application of Code Scaling, Applicability, and Uncertainty Evaluation Methodology to a Large -Break Loss-of-Coolant Accident," NUREG/CR-5249, EGG-2659, 1989 (also Nuclear Engineering and Design, 119, 1990).

[4.3] Krzykacz-Hausmann, B., Hofer, E., and Kloos, M., "A Software System for Uncertainty and Sensitivity Analysis of Results from Computer Models", Proc. Int. Conf. PSAM-II, Vol. 2, Session 063, pp. 20–25, San Diego, CA, 1994 .

[4.4] Appendix K, "ECCS Evaluation Models," to Title 10, Part 50, "Domestic Licensing of Production and Utilization Facilities," of the Code of Federal Regulations, U.S. Nuclear Regulatory Commission, Washington, DC.

[4.5] Gavrilas, M., et al., "A Generalized Framework for Assessment of Safety Margins in Nuclear Power Plants," Proceedings of the International Meeting on Updates in Best Estimate Methods in Nuclear Installation Safety Analysis (BE-2004), Washington DC, November 14–18, 2004.

[4.6] "Safety Goals for the Operations of Nuclear Power Plants: Policy Statement," Federal Register, Vol. 51, p. 30028 (51 FR 30028), U.S. Nuclear Regulatory Commission, Washington, DC, August 4, 1986.

5 QUANTIFICATION OF CHANGES IN SAFETY MARGINS INDUCED BY MODIFICATIONS TO THE PLANT

Recognizing the fact that the integration of risk and safety margins described in this report is suitable to currently operating reactors as well as radically different reactor designs, two fundamental premises cast the framework in a technology-neutral context:

(1) Any foreseeable nuclear power plant can be summarily described as a volume that contains the fuel and fission products surrounded by one or more physical barriers.

(2) For any physical barrier, safety variables can be identified to demarcate the transition from "intact" to "lost function."

The first premise is self-evident. The role of the regulator is, and will continue to be, to protect the public and the environment from inadvertent releases of radionuclides from the barrier(s). The second premise is based on inherent properties of physical barriers. The integrity of physical barriers (i.e., those made of materials, as well as different confinement systems, such as electromagnetic confinements) is subject to operation within acceptable ranges of dominant safety variables. Examples of such variables for the physical barriers of the existing LWR fleet are pressure, temperature, and strain. To determine barrier integrity, these variables must be directly or indirectly measurable, and their values must be predictable for plant conditions during normal and emergency operation.

Furthermore, the ranges over which barrier integrity is maintained must be determined analytically or experimentally. If necessary, the proper function of a physical barrier is ensured by systems and components that maintain safety variables within the range in which the barrier retains its function.

Safety variables that determine barrier integrity are suitable for use in establishing safety limits and quantifying the conditional likelihood of loss of function, as discussed in Chapter 4. The more generic term, "likelihood of loss of function," can encompass failure as well as bypass of a physical barrier.

The process of quantifying the likelihood of loss of function begins with individual event sequences, which can be either design-basis accident sequences or all sequences that comprise the plant's risk space. In this context, the risk space includes all plausible event sequences of non-negligible frequency of occurrence, regardless of the associated consequences. The risk space includes success paths, such as normal operations.

5.1 Likelihood of Incurring Damage in a Particular Event Sequence

The derivations included below assume that both probability and frequency are the proper measures of likelihood. In that case, data availability is the only factor that determines which should be used in computing the risk. Note that frequencies are prevalent in PRA and, more importantly, risk acceptance guidelines are based on frequency, which dictates the use of frequencies in many applications.

The first step in computing the risk metrics is to obtain the unconditional likelihood of loss of function for each event sequence. The probability of loss of function is calculated based on the safety limit

exceedance probability described in Chapter 4. Deterministic calculations that assume a specific progression of events are used to generate the load probability density function. For example, a deterministic calculation is carried out using a thermal-hydraulic code for a specific event sequence in the large-break LOCA tree (LLOCA 07) obtained from a Standardized Plant Analysis Risk (SPAR) model. Thus, the strength curve obtained from these runs will yield the probability that the fuel barrier will lose its function because the 1204 °C (2200 °F) safety limit is exceeded. In other words, the predicted loss of function probability is conditioned upon the occurrence of the sequence of events simulated through the thermal-hydraulic calculation. To obtain the unconditional frequency of loss of function for the event sequence, the conditional probability of loss of function must be multiplied by the frequency of occurrence of the particular event sequence.

More formally, when the strength and load in Chapter 4 pertain to a safety variable that governs the loss of function of barrier n, Bn, then $p(f\_Bn \mid ES_i)$ is the conditional probability of loss of function for barrier n during event sequence i (ES_i):

$$1 - p(S>L) = p(f\_Bn \mid ES_i). \qquad \text{Eq. 5-1}$$

In its most general form—one that ignores the need to afford due consideration to epistemic uncertainty—p(S>L) is the reliability. In the approach taken here, 1 - p(S>L) is approximated by the exceedance probability of the safety limit as defined in Chapter 4.

Two things must happen in order for fission products to be released beyond barrier B1—first, ES_i has to occur, and, second, the barrier B1 must loose its function as shown in Figure 5-1.

Figure 5-1. Computing the likelihood of failure of the first barrier

This is expressed as follows:

$$\lambda_i^{B1} = \lambda(ES_i \cap f\_B1) = \lambda(ES_i) \cdot p(f\_B1 \mid ES_i) \qquad \text{Eq. 5-2}$$

where:

$p(f\_B1 \mid ES_i)$	is the conditional probability that barrier 1 will lose its function given ES_i,
$\lambda(ES_i)$	is the likelihood of event sequence i, and
$\lambda(ES_i \cap f\_B1)$	is the likelihood of occurrence of ES_i and barrier 1 loss of function.

Equation 5-2 can be generalized to any subsequent barrier, Bn. This is a natural conclusion of the fact that deterministic computations to calculate the values of safety variables for barrier n simulate the barrier's response given the initiating event and the breach of previous barriers. The events are illustrated in Figure 5-2.

Figure 5-2. Computing the likelihood of failure of the nth barrier

Thus, the likelihood of loss of function for barrier n is conditioned on the occurrence of event sequence i, as well as the conditional loss of function of preceding barriers and can be expressed as follows:

$$\lambda_i^{Bn} = \lambda(ES_i \cap f\_B1 \cap f\_B2 \cap \ldots) = \lambda(ES_i) \cdot p(f\_B1 \mid ES_i) \cdot p(f\_B2 \mid ES_i \cap f\_B1) \cdot \ldots \quad \text{Eq. 5-3}$$

where:

$\lambda(ES_i)$	is the likelihood of occurrence of ES_i,
$p(f\_B1 \mid ES_i)$	is the conditional probability that barrier 1 will lose function given ES_i, and
$p(f\_B2 \mid ES_i \cap f\_B1)$	is the conditional likelihood that barrier 2 will lose function given ES_i and the loss of function of barrier 1.

If n is the ultimate barrier, the following equation can approximate the likelihood of exposing the public and environment to fission products because of event sequence i:

$$\lambda_i \approx \lambda(ES_i) \cdot p(f\_B1 \mid ES_i) \cdot p(f\_B2 \mid ES_i \cap f\_B1) \cdot \ldots \cdot p(f\_Bn \mid ES_i \cap f\_B1 \cap \ldots \cap f\_Bn-1). \quad \text{Eq. 5-4}$$

5.2 Evaluating Acceptability Given a Core Damage Frequency Guideline

Thus, the relationships derived above can be used to calculate the unconditional occurrence frequencies of any barrier failure. In Equations 5-2 or 5-3, one measures the likelihood of occurrence of ES_i as the frequency of occurrence of ES_i. Note that for severe accident investigations where the likelihood of occurrence of the event sequences is very small, annual probability and frequency assume the same value.

To evaluate the acceptability of a modification, the first step is to identify the parts of the risk space that the modification impacts, either in terms of the distance to the safety limit or the frequency of occurrence of the event sequence. Using the conditional probabilities of loss of function before and after the modification and the associated occurrence frequency of each event sequence, one can generate the expected frequencies of occurrence before and after the modifications. As outlined in the CSNI/SMAP technical note for Task 2 [5.1], the questions of 10 CFR 50.59, “Changes, Tests and Experiments,” [5.2] can be adapted into a rigorous process for determining the changes that are needed to the risk space model to capture a given modification.

The framework to integrate risk and safety margins makes it possible to evaluate the available margin for a specific function that comes into question at any given time. The approach is best demonstrated using a highly abstracted example. Consider a reactor that has the risk space depicted in Figure 5-3. For the first barrier (i.e., the core), two known initiating events (IEs) can lead to damage—IE1 and IE2 (e.g., a LOCA and a reactivity insertion accident). There are two mitigation systems (MSs)—MS1 mitigates IE1, and MS2 mitigates IE2. For example, MS1 is a makeup system for the LOCA, and MS2 is a neutron-poison injection system for the reactivity insertion accident.

Figure 5-3. Risk space of a representative reactor

To better illustrate the applicability of integrating risk and safety margins, the end states are identified for all possible damage mechanisms. Core damage can occur through one of two damage mechanisms (DMs), DM1 (e.g., embrittlement of the first barrier) or DM2 (e.g., cracking), which can lead to the release of fission products from the core.

The embrittlement damage mechanism occurs as a consequence of an increase in the safety variable (SV), SV1 (e.g., PCT). Similarly, SV2 (e.g., enthalpy deposition rate) governs the initiation of cracking, DM2. It is important to refine the event trees to sufficient detail, such that only one possible independent damage mechanism is present at the end of an event sequence.[6] This ensures the integrity of the conditional probability of loss of function in the computation of the risk metric.

Table 5-1 specifies the frequencies of occurrence of event sequences and the conditional loss of function probability for each event sequence in Figure 5-3. For example, IE1 triggers ES2; MS1 does not work. The frequency of occurrence of this event sequence, given the expected frequency of occurrence of IE1 and reliability of MS1, is 5x10-5. The conditional probability of loss of function is calculated from the distribution of deterministic code predictions for SV1 given the known input/model variabilities and the safety limit, as discussed in Chapter 4.2. For ES2, the conditional probability of loss of function is 50 percent; multiplying this by the frequency of occurrence, the unconditional frequency of loss of function for ES2 is 2.5x10-5.

[6] However, it is acceptable to have several safety variables related to a single damage mechanism (e.g., both PCT and total clad oxidation can be tracked if the subject damage mechanism is embrittlement).

By computing the unconditional frequency of loss of function for each event sequence, and then adding them for all sequences that comprise the risk space the expected value for CDF is determined.

Table 5-1 Frequencies of Loss of Function for the Representative Reactor

Event Sequence	Frequency of Occurrence of the Event Sequence	Conditional Probability of Loss of Function	Unconditional Frequency of Loss of Function
1	1.00E-04	0.00	0.00E+00
2	5.00E-05	0.50	2.50E-05
3	3.00E-03	0.20	6.00E-04
4	2.00E-07	0.90	1.80E-07
Expectation value for core damage due to DM1 and DM2			6.25E-04

For economic reasons, the licensee operating the representative reactor proposes two modifications, including a reduced testing schedule and a reduced injection capacity for MS1. Both modifications impact only the embrittlement damage mechanism, DM1, and have no bearing on core cracking, DM2. Assume that guidelines exist (similar to those of Regulatory Guide 1.174 [5.3]) with regard to the maximum increase in CDF allowable for the representative reactor.

Given the proposed modifications, the reduced injection capacity challenges the PCT safety limit, SL1, but not the cracking safety limit, SL2. Thus, the risk space for the inquiry can be reduced as shown in Figure 5-4. Because the modification does not impact the core damage triggered by cracking, the change in the expectation value for CDF is given by the change in the expectation value for DM1 frequency.

Figure 5-4. Reduced risk space for the example safety inquiry

For the representative reactor, the unconditional frequency of core damage via embrittlement, DM1, is calculated from the values shown in Table 5-2. The reduced testing schedule lowers the reliability of MS1 by 5x10-5. The reduced injection capacity increases the best-estimate maximum value and alters the probability density function of PCT, SV1, such that the conditional probability of loss of function after the modification increases in ES2 from 50 percent to 75 percent. The change in CDF due to DM1 is 2.00E-05. This value can be compared to the permissible change in CDF to determine the acceptability of the proposed modifications.

Table 5-2 Data Used to Calculate the Change in Expected Unconditional Frequency of Core Damage Before and After the Modifications Proposed for the Representative Reactor

Frequency of Occurrence of the Event Sequence	Conditional Probability of Loss of Function of the Safety Limit	Unconditional Frequency of Loss of Function
	Before Modifications	
1.00E-04	0.00	0.00E+00
5.00E-05	0.50	2.50E-05
Expectation value for core damage due to DM1 before modification		2.50E-05
	After Modifications	
9.00E-05	0.00	0.00E+00
6.00E-05	0.75	4.50E-05
Expectation value for core damage due to DM1 after modification		4.50E-05

This abstraction shows how the probability of loss of function can be integrated within PRA results and used directly when subsidiary risk acceptance guidelines (e.g., for ΔCDF or ΔLERF) exist. Applying the ΔLERF limit is largely similar, but it involves the introduction of another conditional probability—the probability that the time between the loss of the core and loss of containment function is shorter than a pre-specified interval.

5.3 Consequences

When a modification impacts the consequences of accidents, not just the frequencies of their occurrence, then it is necessary to include a measure of consequence in the risk metric. For example, consider the case of a power uprate achieved by flattening the axial profile. In a reactor with a flat power profile, a perturbation that leads to exceeding the safety limit affects more fuel bundles than in a reactor with a higher peaking factor. Another example is a modification that affects both CDF and consequences, such as the proposal to remove trisodium phosphate from the containment of certain PWRs in response to GSI-191. This modification lowers the probability of chemical effects and thus the CDF. Simultaneously, offsite and personnel doses are expected to increase for all accidents that involve the release of iodine. A proper evaluation of the risk implications of such a modification can only be done if consequences are considered. Most often risk will be evaluated using radiological consequences but alternative risk metrics build on, for example, financial consequences could be developed using the proposed methodology.

Consequences can be considered in a generic form that is suitable to existing as well as future reactor concepts. The reminder of the discussion uses radiological consequences for exemplification. Figure 5-5 depicts the premise that any power-generating reactor consists of fuel and fission products contained within concentric physical barriers. As in current practice, an initial source term must be computed or assumed. If a concentration of fission products, CFP, is contained within the first barrier at the time the event sequence occurs, the decrease in the concentration of fission products as they pass through successive barriers is a function of many factors, including the following:

- volume confined by each barrier
- extent of damage to the barrier
- scrubbing by sprays and water pools
- time between the breaches of successive barriers

Deterministic calculations using severe accident type codes can calculate a transmission factor through a barrier, t, which reflects dependencies on dilution, extent of damage, and other factors. This practice is common in current severe accident analyses.

Figure 5-5. Schematic representation of multiple barriers containing the fuel and fission products

The consequence of an event sequence within a barrier is quantified by the sum of radioisotope concentrations confined by the barrier prior to the initiation of the event and transferred from preceding barriers that have been breached during the event sequence. Thus, for barrier n, the concentration, Cn, can be represented by the concentration of fission products within the confines of that barrier and calculated as follows:

$$C_n \approx C_{0,n} + C_{FP} \cdot t_1 \cdot t_2 \ldots t_{n-1}, \qquad \text{Eq. 5-5}$$

where:

C_{FP} is the concentration of fission products within the primary barrier, and
$C_{0,n}$ is the concentration of fission products within barrier n at the initiation of the event sequence.

Note that Equation 5-5 includes contributions from isotopes that are present in areas outside of the first barrier. This is particularly important if a barrier bypass event sequence is being considered. The formulation of consequences within the confines of barrier n is also useful in calculating risk to personnel. It is not necessary to compute transmission factors for each event sequence; they can be grouped according to barrier, damage mechanism, extent of damage, time lapsed since the breach of the previous barrier, and other factors. Also, conservative transmission factors (e.g., an extreme value of 1) can be used to assess the risk posed by individual event sequences, provided that the plant has sufficient margins to radiological damage limits.

The consequences to the public and the environment are calculated from a generalization of Equation 5-5 to transport beyond the ultimate barrier. In sequence i, the consequences, $C_{P\&E}$, can be computed from the following equation:

$$C_{P\&E} \approx C_{FP}\, t_1\, t_2 \ldots t_n. \qquad \text{Eq. 5-6}$$

A consequence measure related to the one computed above may be better suited for application within existing regulations (e.g., person-rem), but the form above is sufficiently descriptive for the current discussion. The approach described in the preceding paragraphs has already been developed and refined, and is employed in Level 3 PRA calculations.

5.4 Risk from a Single Event Sequence and the Aggregate over the Entire Risk Space

In its simplest form, risk is the product between the likelihood of occurrence of an event and its consequences. The risk to the public and the environment because of event sequence i, r_i, is the product between the likelihood described in Section 5.1 and the consequences discussed in Section 5.3 can be illustrated as seen on Figure 5-6.

Figure 5-6. Risk from a single event sequence

The risk is thus calculated from:

$$r_i=\lambda_i \cdot C_{P\&E,i}, \qquad \text{Eq. 5-7}$$

where the likelihood of release to the public, λ_i, is computed from Equation 5-4, and the consequences of event sequence i, $C_{P\&E,i}$, are computed from Equation 5-6.

The expected risk for the plant can be calculated assuming that only one event sequence can occur at any given time. In other words, it is fair to assume that at any given time the plant is in one distinct end state. The aggregate risk is the arithmetic sum over all event sequences:

$$\text{aggregate risk} = \Sigma_{\text{over all i}}\, r_i. \qquad \text{Eq. 5-8}$$

From equations 5-7 and 5-8, it can be seen that this simple concept of risk is mathematically equivalent to the expected value of damage resulting from plant operation during a specified period of time, usually, per year. When consequences are expressed in terms of doses, the calculated risk given by Equation 5-8 is suitable for comparison with existing radiological criteria and the Commission's safety goals. [5.4].

5.5 References for Chapter 5

[5.1] Regulatory Guide 1.174 - An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, Revision 1, November 2002

[5.2] SMAP Group, Task 2: Assessment process for Safety Margin, Nuclear safety, NEA/SEN/SIN/SMAP (2006)2. Issy-les-Moulineaux: OECD Nuclear Energy Agency, Aug 2006

[5.3] Title 10, Section 50.59, "Changes, tests and experiments," of the Code of Federal Regulations, U.S. Nuclear Regulatory Commission, Washington, DC.

[5.4] "Safety Goals for the Operations of Nuclear Power Plants: Policy Statement," *Federal Register*, Vol. 51, p. 30028 (51 FR 30028), U.S. Nuclear Regulatory Commission, Washington, DC, August 4, 1986.

6 PROOF OF CONCEPT EXAMPLES

As discussed in the introductory chapters, the term safety margin is often used to mean different things. Although it is generally accepted that the concept of safety margin is linked to uncertainty, let us assume for the moment that both the operating point and the failure point are discrete and void of uncertainty. In such a case, the following figure 6-1 would summarize the role of safety limit in ensuring adequate margin for regulatory purposes.

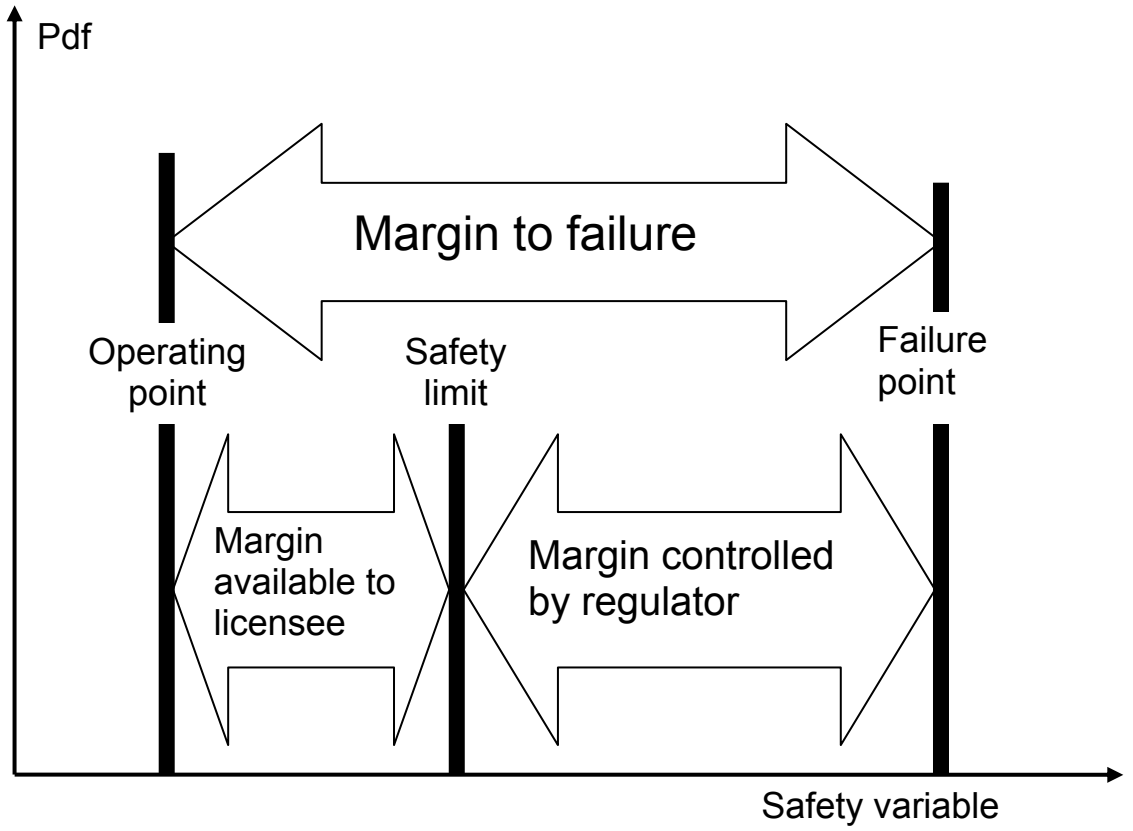

Figure 6-1. Distinguishing between margin available to the licensee and the margin controlled by the regulator

The bulk of this report deals with the margin controlled by the regulator. From a probabilistic perspective the change in that portion of is measured by exceedance frequency as shown in Chapter 5. The example of section 6.1 illustrates the computation of a change in margin controlled by the regulator. In section 6.2, an example is given in which a plant modification has negligible impact on the margin controlled by the regulator. However, the example shows how the modification affects the margin that is available to the licensee, in a manner that is fully consistent with measuring changes in margin controlled by the regulator.

6.1 NPSH Using CDF as Acceptance Criteria (USNRC)

Several potential candidates for the proof-of-concept demonstration were identified. They include cases of limited margin, which are typically of interest to multiple stakeholders. Because of this, it is especially important to note that the example included in this report has no intrinsic value in drawing safety conclusions. It is strictly a highly simplified, abstracted application to a generic increase in the sump debris screen of a PWR.

The phenomena considered do not constitute a comprehensive list. For example, the increase in screen size only affects the change in minor losses in the suction part of the recirculation pump piping. No consideration is given to changes in downstream-effects that could be induced by increasing the screen size. Furthermore, the values used to illustrate the framework are generic and do not represent any particular plant or grouping of plants. Data used to compute minor form losses due to accumulation of debris on the screen is excerpted from an industry survey [6.1]. For these reasons, no conclusions can be drawn regarding risk reduction achieved by increasing sump debris screens from the current example.

The case involves the following issues. After a LOCA, debris can travel to the sump screen and potentially cause a loss of NPSH for ECCS and containment spray system pumps as suction headers become blocked. The postulated amount of blockage exceeds that for which the system was designed and, thus, emergency core cooling and containment spray functions are lost. In the absence of emergency core cooling, the core becomes damaged and fission products escape from the first barrier. The consequences of the event can be significant because the loss of containment spray function increases the probability of releases beyond the ultimate barrier.

To evaluate the effect of increasing the debris screen size, one can examine the impact on CDF before and after the modification. This can be done with traditional probabilistic analyses. However, in the case of NPSH margin, substantial uncertainties are associated with parameters that determine whether core damage occurs. Thus, a realistic calculation without regard to uncertainties can be misleadingly optimistic. If the uncertain parameters are treated conservatively, the picture will be overly pessimistic. By integrating risk and safety margins, the uncertainty becomes part of the calculated core damage probability. Furthermore, conservatism is only required when lack of data demands it. Thus, one obtains a realistic picture that is informed by participating uncertainties and in which conservatism is used only where necessary.

The example considers a PWR that has debris screens of 125 square feet (ft2); this value is representative of current PWR debris screens. The PWR will increase the screen to 1,100 ft2; this value is close the median proposed new screen size for the 69 PWRs operating in the United States. The proof-of concept example examines the effect of this plant modification on CDF.

Assuming that the proposed modification has no impact other than changing the pressure drop through the debris bed formed on the screen, one can link the change in NPSH margin to CDF. Specifically, the probability of losing emergency cooling because of lost NPSH margin can be calculated before and after a modification. One can reasonably assume that loss of NPSH leads to failure of ECCS recirculation, which in turn leads to the loss of function of the first barrier. Therefore, the probability of loss of NPSH margin is equivalent to the conditional probability of loss of function for the first barrier, and can be used directly to determine the impact on CDF. Specifically, the product of the probability of losing NPSH margin in an event sequence and the frequency of occurrence of that event sequence is the unconditional probability of core damage due to loss of NPSH for the particular event. Because the computed metric is the unconditional CDF, only event sequences in which the margin is inadequate need to be considered before and after the modification.

6.1.1 Identifying the Risk-space

Integrating risk and safety margins starts with generating (1) the risk space (i.e., all the event sequences that the modification affects) and (2) a phenomena/variables identification table used to compute the conditional probability of loss of function for each event sequence. To generate the risk space, one must consider all initiating events that challenge NPSH margin. In general, the questions in 10 CFR 50.59 [6.2] can be modified to systematically determine how event trees change as a result of a plant modification; the SMAP Task Group technical note for Task 2 [6.3] addresses tailoring the questions in 10 CFR 50.59 to examine changes in event trees. Event sequences must be refined to capture important input variabilities. For NPSH margin, the variabilities would include actuation of containment spray, choosing to start only one makeup injection/core spray train at a time, and others. The process of identifying refinements to event sequences requires knowledge of the phenomena that impact NPSH, as mentioned above. This intrinsic link between PRA and deterministic analyses makes the process of generating the risk space iterative with the process of identifying key safety variables. Refinements to event trees exceed the proof-of-concept scope of this example.

Several practical simplifications can be made that are consistent with current practice in PRAs. For example, one could limit the risk space to medium LOCAs when it can be shown that they dominate the risk. For some plants, it may be reasonable to assume that for small LOCAs, alternative means of making up water can be found to preclude the need for recirculation from the sump[7]. Large LOCAs have relatively low initiating event frequencies so they can be ignored in rough calculations of risk. However, to fully illustrate the framework, this example considers event sequences for small, medium, and large LOCAs. Figure 6-2 depicts the event tree for the large-break LOCA initiating event.

Another simplification to the risk space is that core damage paths do not need to be considered because paths that lead to core damage prior to NPSH considerations do so by different mechanisms of damage. This proof-of-concept example assumes that increasing the size of the sump screen does not impact these mechanisms of damage, and thus the CDFs along those paths do not change before and after the modification. This type of simplification is possible because of the use of probabilities in developing the integrated risk/safety margins framework, which assures consistency in decision-making metrics. Specifically, it is possible if one ensures that the end states of all event sequences of interest result from distinct damage mechanisms. Given this simplification, for the large-break LOCA event sequences of Figure 6-2, NPSH margin needs to be determined only for path one, because all other paths lose function due to other mechanisms.

Furthermore, it is common practice to truncate below a certain frequency threshold. One should ensure that the sum of all truncated event sequences is not of a magnitude that would change the decision. This exercise treats event sequences with frequencies of less than 10E-6 as failed. These will not show up in the ΔCDF, but the baseline CDF includes their sum before and after the modification; thus, their total contribution can be assessed by inspection. A close examination of the scope of each safety inquiry can lead to additional simplifications. For example, in a given plant, one may be able to eliminate an entire range of break sizes that could not generate enough debris to pose blockage problems regardless of break location. No such additional simplifications have been attempted for the proof-of-concept NPSH example.

[7] In PWRs, this may be limited by the reactivity insertion that results if deborated water is used.

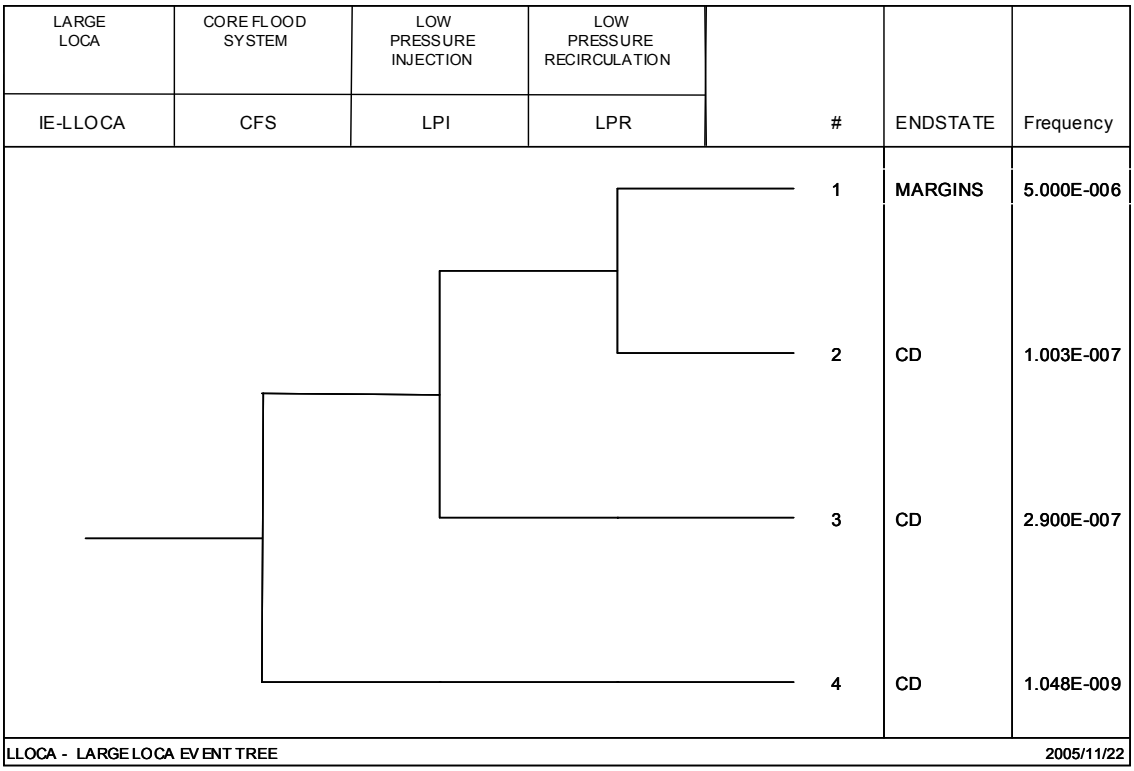

Figure 6-2. Large LOCA event tree for NPSH margin calculation

6.1.2 Calculating Margin in Each Sequence

The next step is to identify the variables that determine the amount of NPSH margin available in each event sequence. The definition of NPSH is a good starting point for the development of the phenomena/variable list. In most applications, a phenomena identification and ranking table (PIRT) developed by a panel of experts would be available as a starting point. Los Alamos National Laboratories generated some earlier PIRTs for GSI-191, but they are not directly relevant to the development of this proof-of-concept example. Instead, a list of phenomena and variables was developed from first-principle considerations.

A pump-specific amount of NPSH is necessary to ensure that the pump functions without cavitations in the impeller region. Both the injection capacity and the reliability of a pump are predictable only as long as the required NPSH ($NPSH_r$) is less than the available NPSH ($NPSH_a$). The factors that increase the available NPSH are the containment pressure and the height of the water in the sump. $NPSH_a$ deteriorates with increased pressure drops in suction piping and with increased sump water temperature and can be expressed as follows:

$$NPSH_r \leq NPSH_a = p_{atm} + p_{stat} - p_{vap} - p_{loss} \qquad \text{Eq. 6-1}$$

where: p_{atm} is the pressure head (containment pressure), p_{stat} is the static suction head (sump level), p_{vap} is the vapor pressure (at maximum pumping temperature), and p_{loss} is the friction and K-loss head in the suction side, including losses at the screen.

Keeping with the notion that having margins requires room for “unknown-unknowns” epistemic uncertainties, it is reasonable to assume that loss of safety function occurs when the $NPSH_a$ is less than the $NPSH_r$ required for the specific pump. No other attempt was made to separate aleatory and epistemic

uncertainty in the example calculation. Examining the terms of Equation 4-1, one can generate the table of phenomena that govern the availability of NPSH margin; see Table 6-1. The same table lists some of the variables and considerations that are necessary to determine the probability density function of NPSH margin. The table is not intended to be exhaustive but to illustrate the type of information that must be collated to integrate risk and safety margins.

For individual plant cases, the analysis would proceed by running each event sequence with a deterministic code (e.g., RELAP5 or TRACE) to obtain the ranges of values necessary to compute the NPSH margin distribution. Specifically, given variabilities in code models and input/boundary conditions, one would obtain distributions for sump water temperature, sump level, and containment pressure. This was not done for the current example; instead, generic ranges were obtained from industry and NRC documents (e.g., [6.1 and 6.4] as shown in Table 6-2).

Table 6-1. Variables that Determine the Available NPSH

Pressure Head	
Containment pressure	operator depressurization, evolution of the event sequence
Containment leakage	ranges from negligible to that allowed by the technical specifications
Containment spray duration/capacity	affected by measures taken to decrease the need for going to recirculation
Containment temperature	accident sequence, spray action, initial and boundary conditions
Static Suction Head	
sump level	break size
makeup injection	affected by measures taken to decrease the need for going to recirculation
water hideout	compartment geometry
water density	sump water temperature
impurities (solutes and particulates)	debris dissolved or suspended in the sump water
Vapor Pressure	
thermodynamic properties	sump water temperature
impurities	debris dissolved or suspended in the sump water
Friction Head	
suction piping	piping configuration
impurities (solutes and particulates)	debris dissolved or suspended in the sump water
viscosity	temperature and impurities
losses due to debris	amount and composition of debris (accident sequence)
screen configuration	Vendor
debris distribution	debris source, initiating event, and accident sequence
dispersed obstructions (gloves, reflecting metal)	debris source
presence of sludge	chemical effects

The type of information contained in Table 6-1 is similar to that in the PIRTs and is consistent with information developed to identify uncertainty in deterministic calculations. In addition to being a requisite for the integration of risk and safety margins, Table 6-1 has another important attribute—it lends transparency to the process. The analyst or the regulatory decision-maker can focus on elements such as the completeness of information in the table, the ranges of values, and the adequacy of the source material. For example, uncertainties associated with pool level can be substantial depending on the potential for water-hideout in a particular containment. Similarly, a complicated suction-piping configuration will have a substantial uncertainty associated with minor and major pressure losses. All these sources of uncertainty become important if the licensee is only able to calculate a margin that is less that a foot. Conversely, a licensee who has indeed treated all sources of uncertainty in a conservative manner can easily indicate so in Table 6-1. Thus, this table is also useful in deciding when it is cost-beneficial to use accurate ranges as opposed to a conservative value.

Table 6-2. Variables and Values Used to Generate the NPSH Margin Distributions for the Large-Break LOCA Event Sequence in the Proof-of-Concept Example

Variable	Units	Nominal Value	Minimum (% of nominal)	Maximum (% of nominal)	Source Reference and Comment
Mineral wool volume	ft^3	126	40	100	NUREG/CR-6808 [6.1]: 10 to 25% range of total (5 to 10% if no CS)
Dirt-dust mass	lbm	170	40	100	NUREG/CR-6808: 10 to 25% range of total (5 to 10% if no CS)
Qualified epoxy mass	lbm	260	40	100	NUREG/CR-6808: 10 to 25% range of total (5 to 10% if no CS)
Paint chips mass	lbm	95	40	100	NUREG/CR-6808: 10 to 25% range of total (5 to 10% if no CS)
Flow rate through strainers	gpm	8700	95	105	representative of 10% controller range
Screen area	ft^2	125/1100	80	100	allow for up to 20% obstruction
Water temperature	°F	187	100	130	NUREG/CR-6224 [6.4]: ranges from 187 °F to 243 °F
Screen losses (nominal)	ft	-32/-0.35			calculated according to NUREG/CR-6224
Containment pressure ($p_{st-part}$)	psi	14.7–21.7	80	100	NUREG/CR-6224: ranges from 0 to 7 psig; conservative
Pool level above suction	ft	25	90	110	representative pool level
Friction and K losses	ft	-3.00	80	100	account for impurities
Cavitation pressure	ft	20–21.7	100	100	corresponding to sump temperature
$NPSH_r$	ft	-13	90	110	deterioration due to viscosity
$NPSH_a$	ft	20/51			calculated according to Equation 6-1
Mean NPSH margin	ft	-6.7/12.8			$NPSH_a$-$NPSH_r$

The variables listed in Table 6-2 were sampled to generate the probability density of NPSH margin. Simple Monte Carlo sampling was used. The probability density functions were generated using 500 samples. The variables were assumed to range uniformly between the maximum and minimum values of Table 6-1. Figures 6-3 and 6-4 show the probability density functions and the integral loss of function probabilities for NPSH margin given a 125-ft2 and 1100-ft2 screen, respectively. The probability of losing function because of inadequate NPSH is more than 80 percent in LLOCA1 if a small debris screen is used. The probability drops to less than 20 percent if the screen is enlarged to 1100 ft2.

It is important to note that the spread of the distributions in Figures 6-3 and 6-4 is highly relevant. The generic variable values and ranges used to generate the plots are representative of actual plant conditions. Therefore, the ±15-foot band that captures most of the trials is not unreasonable, in light of the uncertainties associated with NPSH margin. A sensitivity study showed the impact of sump temperature to be a dominant factor in determining the spread of the NPSH distribution even if different temperature distribution shapes are used. This means that the only acceptable conservative calculation of NPSH is one in which the temperature takes its most limiting value for the time of the computation. This conclusion is important because, if an analyst computes an NPSH margin of 0.4 feet that was calculated with the mean of the temperature range, he/she is effectively reporting a 50 percent probability of failure due to NPSH margin loss if the breadth of the uncertainty range is taken into consideration.

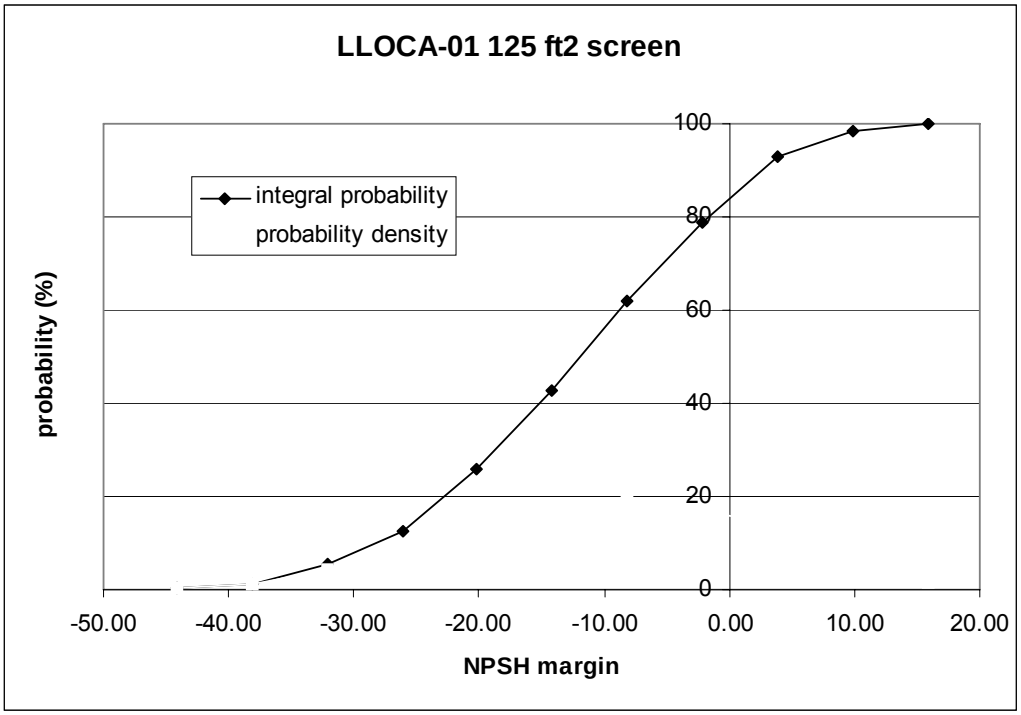

Figure 6-3. Distributed and cumulative probability of loss of NPSH with a 125-ft2 debris screen

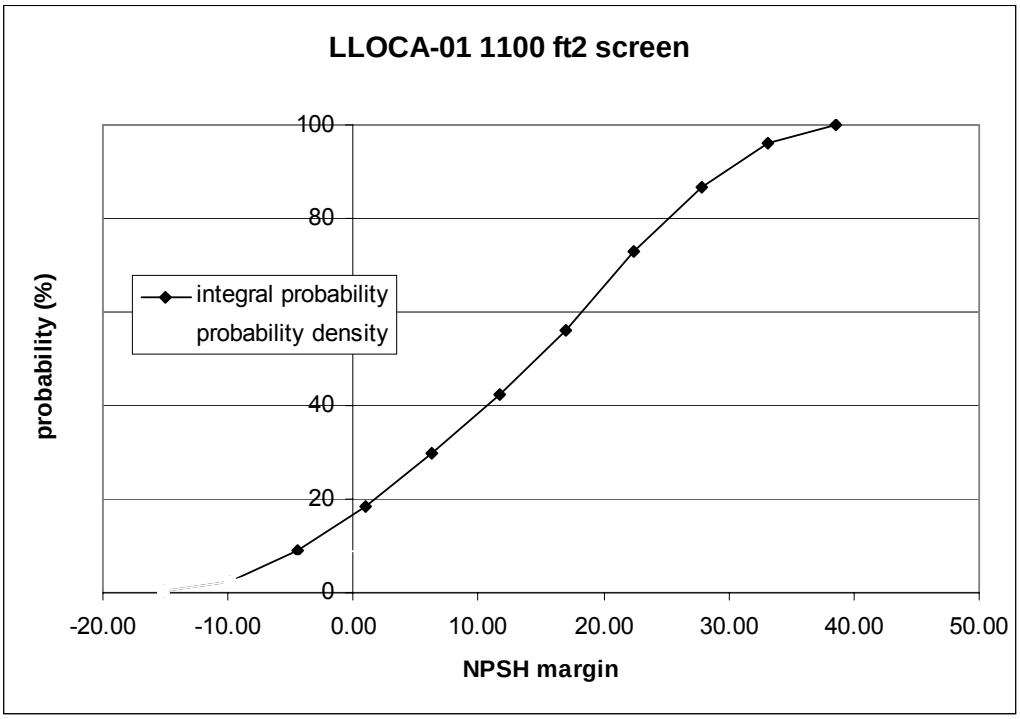

Figure 6-4. Distributed and cumulative probability of loss of NPSH with a 1100-ft2 debris screen

6.1.3 Computing the Risk Metric

The probability density functions for NPSH margin are calculated for all the LOCA event sequences that do not lead to core damage by other mechanisms. Table 6-3 lists all the LOCA event sequences, as obtained from a SPAR model, and their frequencies of occurrence. For every event sequence that was identified as acceptable before considering NPSH margin, the conditional probability of loss of function was calculated as demonstrated for LLOCA-01 first for a small debris screen and then for a large screen (see Figures 6-3 and 6-4). Blank entries under conditional probability of failure in Table 6-3 indicate that the particular event sequence leads to core damage by other mechanisms.

The unconditional frequency of loss of function due to loss of NPSH margin was computed for each event sequence and each screen size. For every event sequence, the increase in screen size reduced the conditional probability of loss of NPSH margin and, thus, the unconditional probability of core damage.[8] The last column of Table 6-3 lists the change in unconditional frequency of core damage due to loss of NPSH margin for every affected event sequence.

In the last row, the total change in CDF is computed by adding up the changes in frequencies calculated for all the LOCA event sequences. For the simplified model and generic numbers used in the proof-of-concept example, the expected CDF is calculated to decrease by 4E-5 if the debris screen is increased from 125 ft2 to 1100 ft2. Again, this value has no significance in the context of GSI-191. The uncertainty bands of NPSH margin in Figures 6-3 and 6-4 are, however, remarkable.

[8] Note again that this is a highly simplified proof-of concept example and that the conclusion of reduced CDF with increased debris screen size is by no means general.

Table 6-3. Calculation of ΔCDF from Conditional Probability of Loss of NPSH and Event Sequence Frequency

Event Sequence Designator from SPAR Model, (ES)	Frequency of Occurrence of the Event Sequence, f(ES)	Small Screen		Large Screen		Change
		Probability of Loss of NPSH Margin in the Event Sequence, p(loss|ES)	Unconditional Frequency of NPSH Loss in the Event Sequence, f(ES)	Probability of Loss of NPSH Margin in the Event Sequence, p(loss|ES)	Unconditional Frequency of NPSH Loss in the Event Sequence, f(ES)	
ROT	1.00E+00					
LLOCA-01	5.00E-06	70%	3.50E-06	18%	9.00E-07	2.60E-06
LLOCA-02	1.00E-07					
LLOCA-03	2.90E-07					
LLOCA-04	1.05E-09					
MLOCA-01	4.00E-05	17%	6.80E-06	0%	0.00E+00	6.80E-06
MLOCA-02	1.90E-07	100%	1.90E-07	100%	1.90E-07	
MLOCA-03	4.60E-10					
MLOCA-04 to 09	2.53E-10					
SLOCA-01	4.00E-04	8%	3.20E-05	0%	0.00E+00	3.20E-05
SLOCA-02	3.31E-06	20%	6.62E-07	0%	0.00E+00	6.62E-07
SLOCA-03	1.03E-06					
SLOCA-04	4.00E-07	100%	4.00E-07	100%	4.00E-07	
SLOCA-05	2.19E-08					
SLOCA-06	4.83E-09					
SLOCA-07	1.48E-09	100%	1.48E-09	100%	1.48E-09	
SLOCA-08	1.20E-11	100%	1.20E-11	100%	1.20E-11	
SLOCA-09	3.24E-12					
SLOCA-10	1.45E-12	100%	1.45E-12	100%	1.45E-12	
SLOCA-11	5.74E-14					
SLOCA-12	1.91E.13					
SLOCA-13	8.00E-07	100%	8.00E-07	100%	8.00E-07	
SLOCA-14	6.64E-09	100%	6.64E-09	100%	6.64E-09	
SLOCA-15	2.05E-09					
SLOCA-16	8.00E-10	100%	8.00E-10	100%	8.00E-10	
SLOCA-17	4.36E-11					
SLOCA-18	1.60E-07	100%	1.60E-07	100%	1.60E-07	
SLOCA-19	7.63E-10					
SLOCA-20	1.60E-08					
SLOCA-21	8.18E-10					
TOTAL			4.43E-05		2.27E-06	4.21E-05

6.2 PCT Margin for Power Uprate Case (KINS)

The objective of this proof-of-concept demonstration is to quantify the peak clad temperature (PCT) margin for the design changes due to the power uprates using the framework to integrate risk and safety margins. The framework to integrate risk and safety margins described in Chapters 4 and 5 makes it possible to evaluate the available margin for a specific function that comes into question at any given time.

Note that in this example, the portion of the margin that is quantified is that available to the licensee; see Figure 6.1.

The application of proof-of concept was performed for Kori unit 3 for which the safety and other analysis are being performed regarding power uprate. The insights from the application are presented in this report.

Integrating risk and safety margins starts with generating (1) the risk space (i.e., all the event sequences that the modification affects), and (2) a phenomena/variables identification table used to compute the conditional probability of loss of function for each event sequence. To generate the risk space, one must consider all initiating events that challenge PCT margin. This example could limit the risk space to large-break LOCA and small-break LOCA when it can be shown that they dominate the risk. Several practical simplifications can be made that are consistent with current practice in PRAs.

6.2.1 Event identification

The framework to integrate risk and safety margins is applied to Kori unit 3 4.5% power uprate case. The initiating event chosen is large-break LOCA and small-break LOCA. The event scenarios of large-break LOCA and small-break LOCA are presented in event tree shown in Figure 6-5 and Figure 6-6, respectively [6.5].

Figure 6-5. Large-Break LOCA Event Tree of Kori unit 3

Figure 6-6. Small-Break LOCA Event Tree of Kori unit 3

6.2.2 Calculating Margin in Each Sequence

The next step is to identify the variables that determine the amount of PCT margin available in each event sequence. Five variables are selected to generate the distribution of PCT from the information of UMS (Uncertainty Methods Study) group report [6.6] and KINS report [6.7]. Table 6-4 shows the variables selected. Latin hypercube sampling method is used to generate 59 input decks for each event sequence.

Table 6-4. Sensitivity Variables and Values Used to Generate the PCT Distributions

Variables	Distribution	Nominal Value	St. Dev.	Min.	Max.	Source Reference and Comment
Discharge Coefficient	Bounded Normal	0.947	0.109	0.729	1.156	KINS/RR-279, Henry Fauske Model and Experimental Results of Marviken Critical Flow
Decay Heat	Bounded Normal	1	0.03	0.97	1.03	KINS/RR-279, RELAP5/Mod 3 Decay Heat Model
HPSI Injection Setpoint	Normal	1.35E+07	3.65E+05			Uncertainty of PZR Pressure Instrument
HPSI Flow Rate Multiplier	Normal	1	0.02			Uncertainty of Kori unit 3 Flow Measurement
HPSI Water Temperature [K]	Uniform	310.9		298	312	KINS/RR-279

Sensitivity variables are selected based on engineering and expert judgment in terms of the impact on the accident phenomena propagation. Discharge flow through break point is one of the most important factors which affect the core cooling during LOCA. Three sensitivity variables related to the operation of high pressure safety injection system are chosen because the HPSI is the most required safety feature during large break and small break LOCA for Kori nuclear unit 3 and 4. For power uprates, decay heat shall be changed due to the power modification.

Class "OK" event sequences shown in Figure 6-5 and 6-6 are selected to generate the distribution of PCT. The analysis would proceed by 59 times running for each event sequence with a RELAP5/Mod3.3 computer code to obtain the ranges of values necessary to compute the PCT distribution. Initial conditions are shown in Table 6-5 and the nodalization of RELAP5/Mod3.3 is shown in Figure 6-7. Peak cladding temperatures for base case (100% power) and uprated case (104.5% power) of Kori unit 3 are calculated for small-break LOCA and large-break LOCA. The probability density functions are generated using 59 times computation results for each event sequence.

Table 6-5. Initial Conditions for Small-break LOCA and Large-break LOCA

	100% Power	104.5% Power
Reactor Power [MWt]	**2775**	**2900**
Operating Pressure [MPa]	**15.5**	
Operating Temperature [^{O}K]		
- Cold Leg	**564**	**562**
- Hot Leg	**600**	
Break Size at Cold Leg [cm]		
- Small Break LOCA	**5**	
- Large Break LOCA	**Guillotine**	

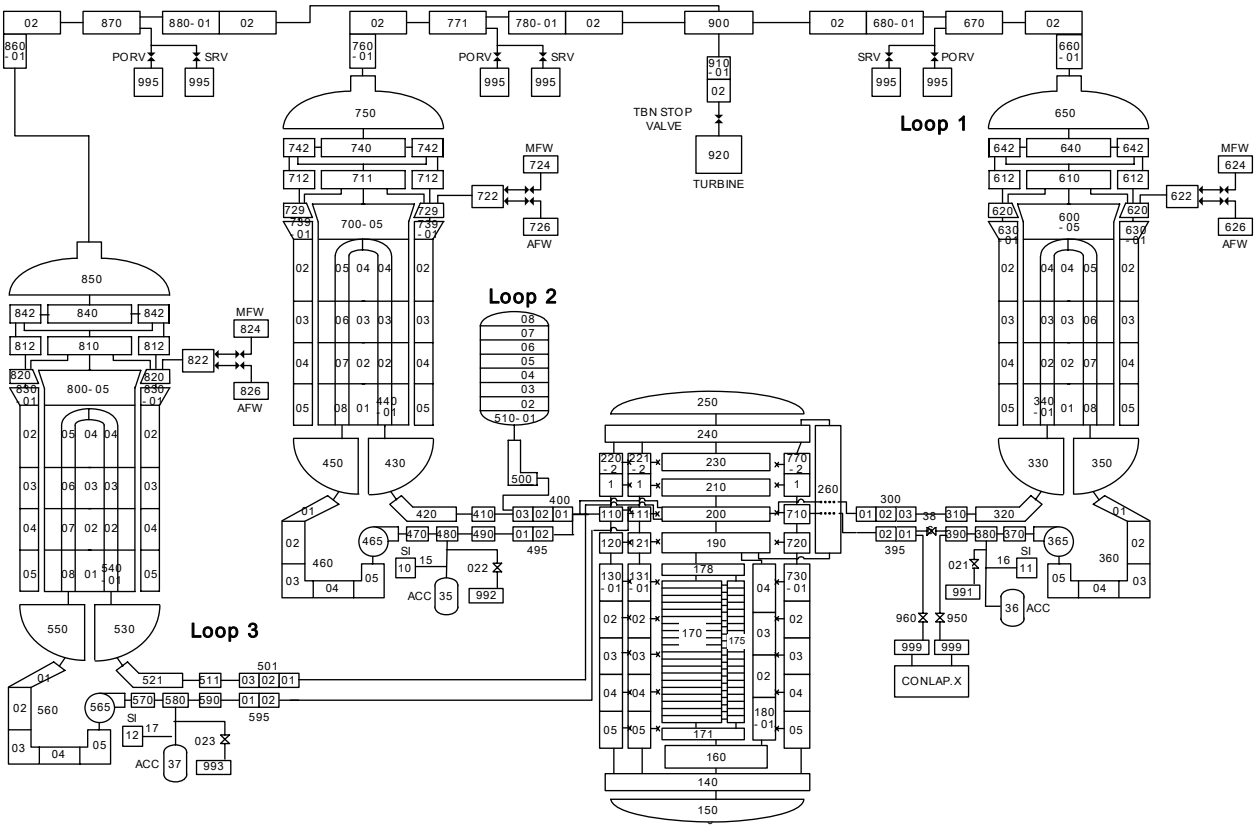

Figure 6-7. RELAP5/Mod3.3 Nodalization

Figure 6-8 shows the histogram for PCT of large-break LOCA at 100% power and Figure 6-9 shows the histogram at 104.5% power. The PCT distribution of large-break LOCA is anticipated as normal distribution on the basis of the histogram.

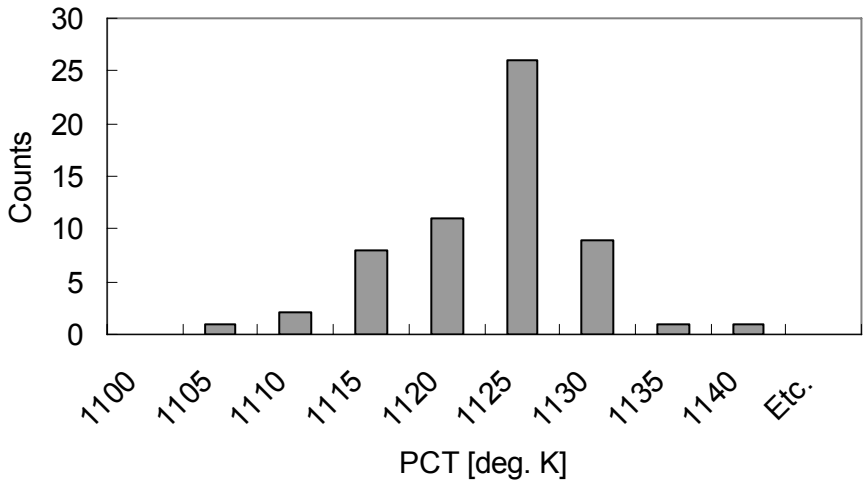

Figure 6-8. Histogram for large-break LOCA PCT at 100% power

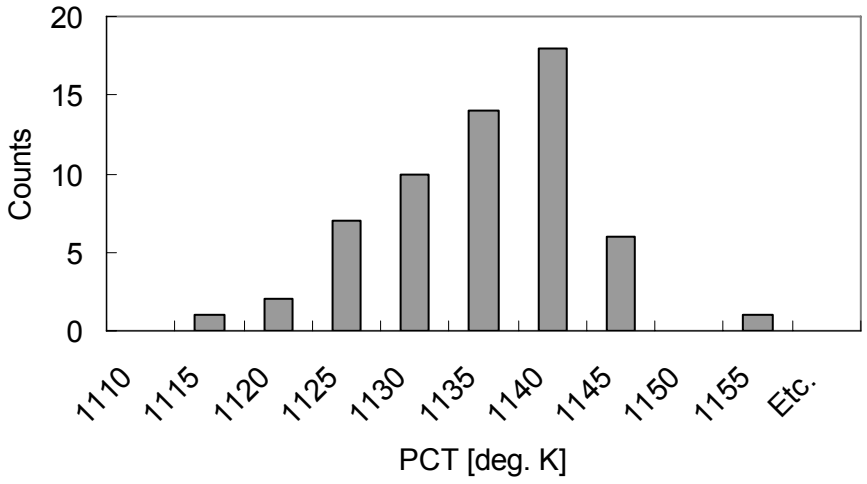

Figure 6-9. Histogram for large-break LOCA PCT at 104.5% power

Figure 6-10 shows the histogram for PCT of small-break LOCA SB07 sequence at 100% power and Figure 6-11 shows the histogram at 104.5% power. The PCT distribution of large-break LOCA is anticipated as normal distribution on the basis of the histogram also.

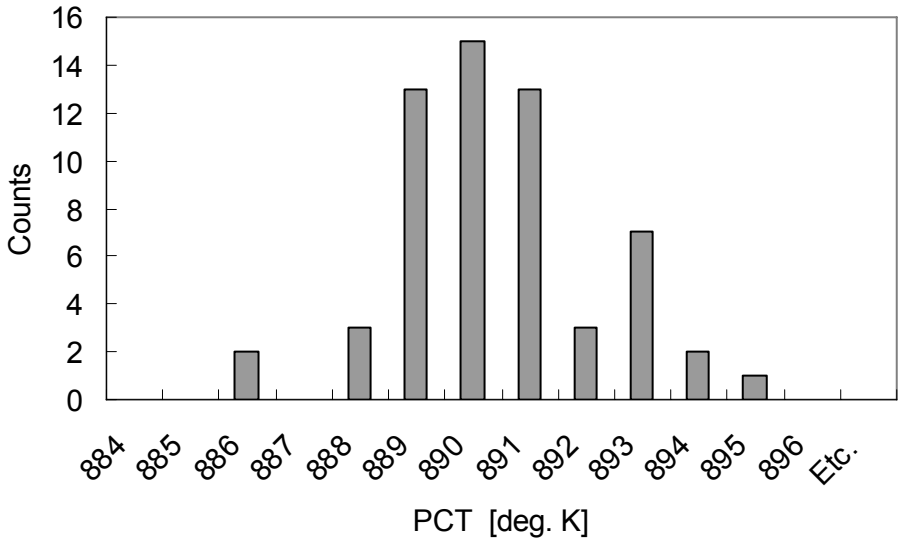

Figure 6-10. Histogram for small-break LOCA PCT at 100% power

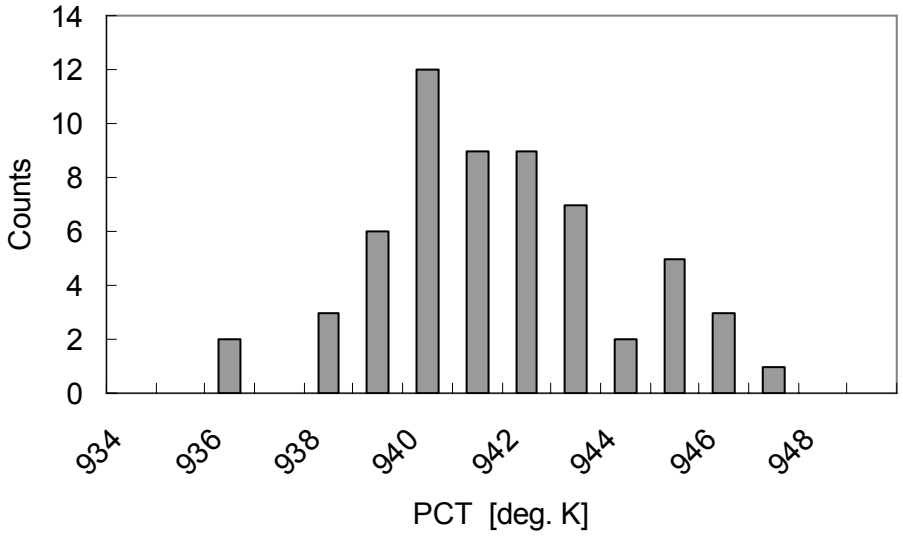

Figure 6-11. Histogram for small-break LOCA PCT at 104.5% power

Figure 6-12 shows the distribution of PCT at large-break LOCA. Figure 6-13 to 6-16 shows the distribution for the small-break LOCA cases. All PCTs are well below the safety limit value (1477 K). PCTs at 104.5% power are increased compared to that of 100% rated power cases. PCT distribution shapes well followed normal distribution shape.

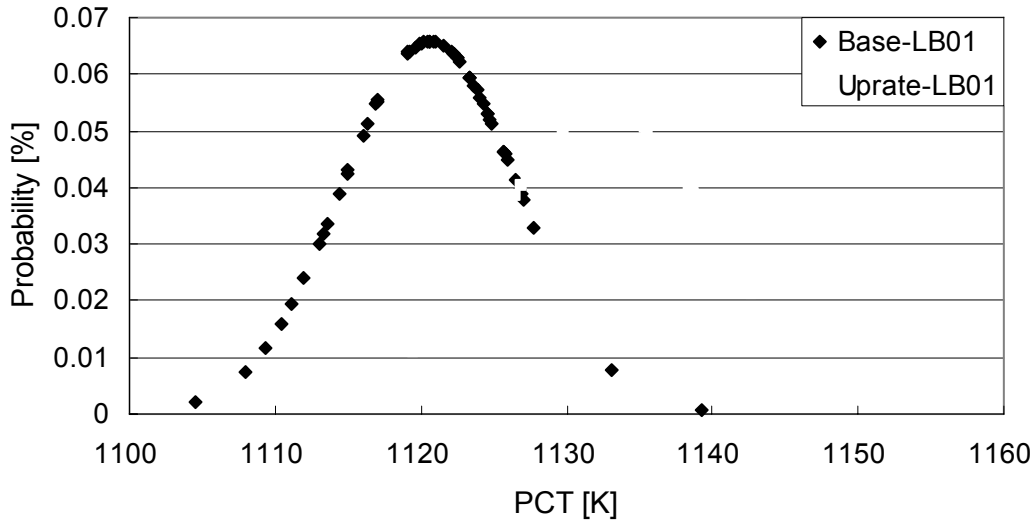

Figure 6-12. Distributed Probability of PCT at Large-break LOCA

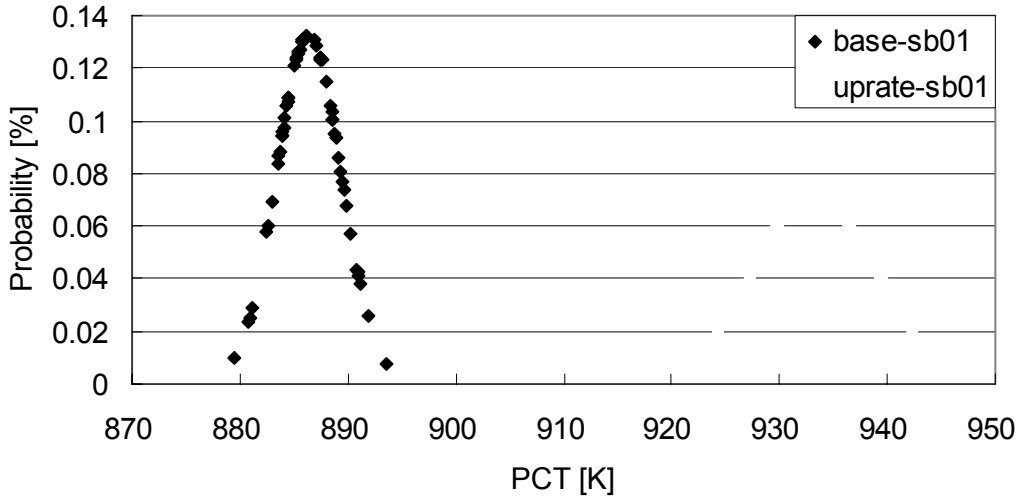

Figure 6-13. Distributed Probability of PCT at Small-break LOCA SB01 Sequence

In Figure 6-13 and 6-14, distributed probabilities of PCT in small break LOCA sequence no. 1 and no. 4 are calculated same. This is mainly due to the event sequence characteristics that major difference of event sequence no. 1 and no. 4 is success of cooldown and depressurization operation while PCTs in event sequence no. 1 and no. 4 appeared much earlier in event sequence propagation. Therefore, PCTs estimated by RELAP code were same.

Calculated PCT distributions for base and uprate case in Figure 6-16 are much overlapped compared with PCT distributions for other event sequences. In small break LOCA sequence no. 11, high pressure safety injection in early phase of event is failed. Therefore the 3 sensitivity variables related with high pressure safety injection, or high pressure injection set point, high pressure injection flow rate and high pressure injection water temperature (RWST water temperature) do not affect the PCTs appeared during event sequence no. 11.

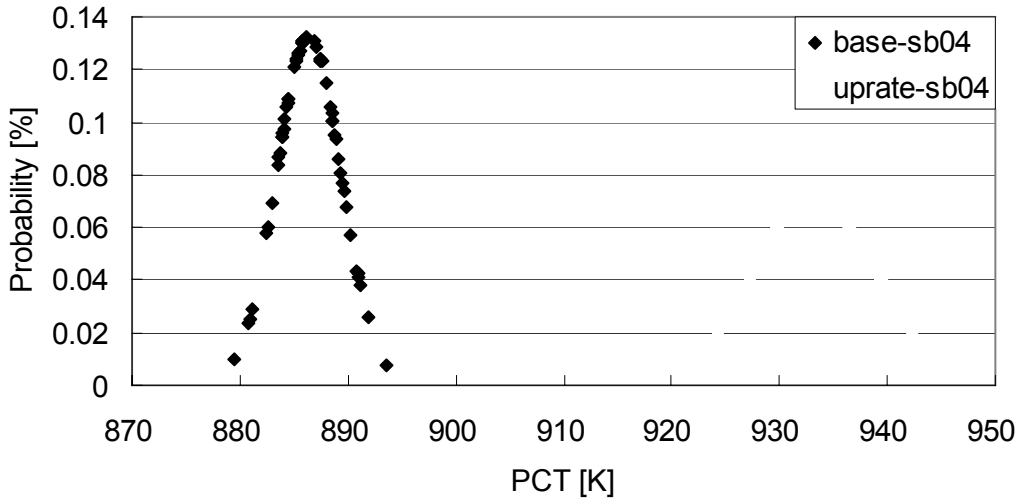

Figure 6-14. Distributed Probability of PCT at Small-break LOCA SB04 Sequence

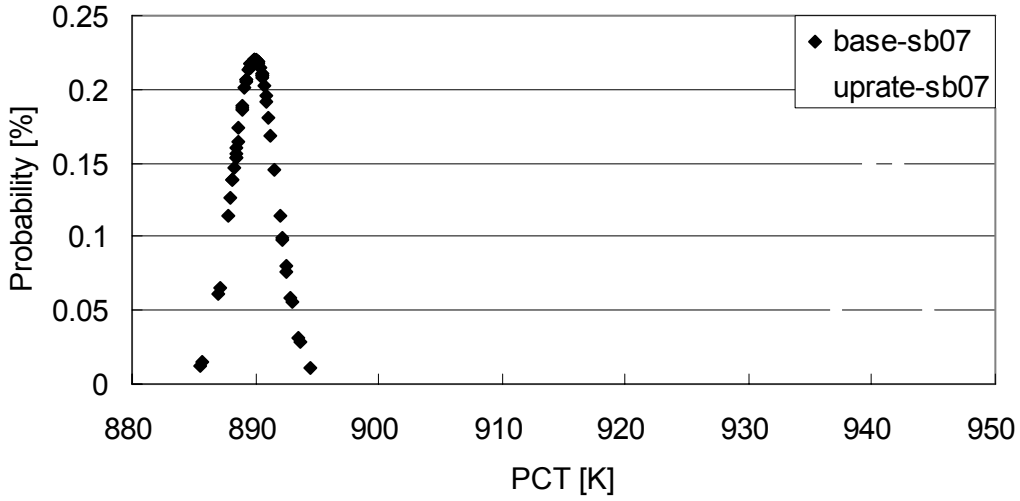

Figure 6-15. Distributed Probability of PCT at Small-break LOCA SB07 Sequence

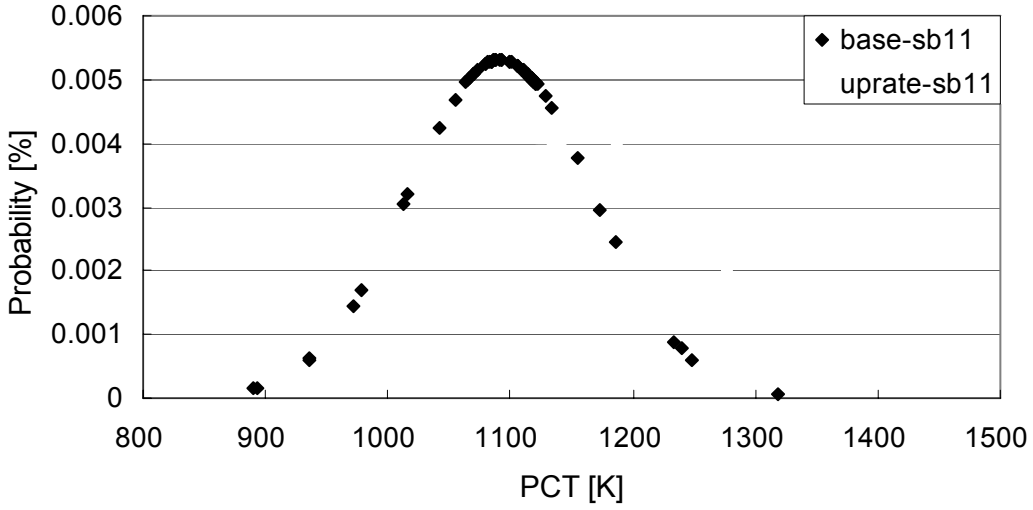

Figure 6-16. Distributed Probability of PCT at Small-break LOCA SB11 Sequence

6.2.3 Computing the Risk Metric

As shown in Figures 6-12 to 6-16, all PCTs are well below the safety limit value. This means that the adequate safety margin is ensured after power uprate. In this case, the change in margin available to the licensee can be estimated using the concept of equation 4-1. Thus, the safety is indirect measure of the overlap in the probability density functions and can be used to estimate the probability that the PCT does not exceed the safety limit.

Figure 6-17 illustrates the concept of safety margin quantification for the adequate safety margin ensured. Frequency of each sequence presented in Table 6-6 was estimated from Kori unit 3 PSA report [6.5].

Figure 6-17. Safety Margins by setting safety limit and code prediction values

Table 6-6. Event Frequencies of LOCA

Large-brake LOCA

Seq. No.	Frequency	Class
LB01	4.98E-06	OK

Small-break LOCA

Seq. No.	Frequency	Class
SB01	4.98E-04	OK
SB04	1.72E-08	OK
SB07	7.92E-08	OK
SB11	1.52E-07	OK

Table 6-7. Safety Margin Variation in large-break LOCA

Event Sequence	LB01	
	Before	After
Average PCT [K]	1120.62	1132.65
Standard Deviation [K]	6.0591	7.3142
ΔPCT [K]	356.38	344.35
Margin available to the licensee	58.82	47.08

Table 6-8. Safety Margin Variation in small-break LOCA

Event Sequence	SB01		SB04		SB07		SB11	
	Before	After	Before	After	Before	After	Before	After
Average PCT [K]	886.38	933.37	886.38	933.37	889.93	940.95	1091.87	1160.20
Standard Deviation [K]	3.0064	5.5030	3.0064	5.5030	1.8115	2.4173	75.0659	96.9582
ΔPCT [K]	590.62	543.63	590.62	543.63	587.07	536.05	385.13	316.80
Margin available to the licensee	196.46	98.79	196.46	98.79	324.07	221.75	5.13	3.27

The probability density functions for PCT margin are calculated for event sequences of large-break LOCA and small-break LOCA using the concept of safety margin quantification illustrated in Figure 6-17.

As shown in Table 6-7, PCT margins of large-break LOCA before and after power uprate are 58.82 and 47.08 respectively.

For small-break LOCA, 4 event sequences are considered to generate PCT margin. In this case, frequency of each event sequence is used to calculated total PCT margin of small-break LOCA. Total PCT margin of small-break LOCA is computed from the following equation:

$$SM_{SBLOCA} = \sum_{i=1}^{n} \frac{freq_{Es\_i}}{freq_{SBLOCA}} SM_{Es\_i} \qquad \text{Eq. 6-2}$$

Where $freq_{Es\_i}$ is frequency of event sequence i, $freq_{SBLOCA}$ is initiating event frequency of small-break LOCA, SM_{Es_i} is the margin to the safety limit of event sequence i as calculated in Eq. 6-3. The frequency of each event sequence is described in Table 6-6 and the initiation event frequency of small-break LOCA is 5.0E-4. [6.7]

$$SM_{Es\_i} = \frac{\text{safety limit} - \text{best estimate value}}{\sqrt{\sigma_{\text{best estimate}}{}^2 + 0^2}} \qquad \text{Eq. 6-3}$$

As shown in Eq. 4-1 and Eq. 6-3, the margin available to the licensee for each event sequence or SM_{Es_i} can be obtained by dividing ΔPCT by standard deviation of PCT distribution calculated. This definition of safety margin can imply the distance from the safety limit and the uncertainty of distribution of safety variable estimated.

Using above equation and the frequency, PCT margin of small-break LOCA before power uprate is 195.73 and PCT margin after power uprate is 98.43. PCT margin of small-break LOCA is much more reduced than that of the large-break LOCA.

6.3 References for Chapter 6

[6.1] Rao, D.V., et al., “Knowledge Base for the Effect of Debris on Pressurized- Water Reactor Emergency Core Cooling Sump Performance,” NUREG/CR-6808, LA-UR-03-880, Los Alamos National Laboratory, February 2003.

[6.2] Title 10, Section 50.59, “ Changes, tests and experiments,” of the *Code of Federal Regulations*, U.S. Nuclear Regulatory Commission, Washington, DC.

[6.3] SMAP Group, Task 2: Assessment process for Safety Margin, Nuclear safety, NEA/SEN/SIN/SMAP (2006)2. Issy-les-Moulineaux: OECD Nuclear Energy Agency, Aug 2006

[6.4] “Parametric Study of the Potential for BWR ECCS Strainer Blockage Due to LOCA Generated Debris,” NUREG/CR-6224, Los Alamos National Laboratory, October 1995.

[6.5] Jae-hun Yang, “Kori unit 3,4 PSA final report – internal event quantification analysis”, K34-PSA-INT-07, Korea Power Engineering Company, Inc., June 2003

[6.6] Tony Wickett, et al., “Report of the Uncertainty Methods Study”, NEA/CSNI/R(97)35, OECD/NEA CSNI, June 1998.

[6.7] In-goo Kim, et al., “Improvement of the ECCS Best Estimate Methodology and Assessment of LOFT L2-5 Experiment”, KINS/RR-279, Korea Institute of Nuclear Safety, January 2005.

7 CONCLUSIONS

7.1 Summary of the Results Achieved

The SMAP group has described a framework for the quantification of plant safety margins:

- A discussion of existing related concepts and the needs of the stakeholders is found in Chapter 1.
- The different contributors to the global plant safety margin and the definition of proper terminology are described and in Chapter 2 that also includes a short description of existing systems of safety- and acceptance limits.
- Chapter 3 discusses the assessment process of the safety margin quantification: It first develops the conceptual model in the risk space and then proceeds to characterize transient analysis tools and the possible modes of application to safety analysis. In a next step, uncertainties are classified and the separate treatment of the two categories is discussed, including guidelines for its implementation in the quantification process.
- The link between the physical damage limits and the risk space via the load-strength concept is established in Chapter 4.
- Chapter 5 describes the general concept to quantify plant safety margin and ways of aggregating the risk contributions for different event sequences.
- Finally, pilot applications of the methodology are documented in Chapter 6.

The following features characterize the SMAP framework:

1. The standard model from reliability theory (and other engineering sciences) using probabilistic density functions for both the load and the strength (of the barriers) forms one basic element of the SMAP-methodology.

2. Naturally, the exceedance frequency has been chosen as indicator for “loss of function”. This quantity represents a very general measure of safety margin and quantifies the “distance” between the safety variables (e.g. pressure, temperature, oxidation level) and the respective acceptance limits. At the same time, it naturally allows for comparison of the margin available in different physical process parameters (safety variables).

3. The methodology proposed by the SMAP group is based on a combination of deterministic and probabilistic approaches and optimally uses the existing analysis technologies (e.g. deterministic analysis and PSA). The aggregation of the risk contributions from different event scenarios uses the mathematical concepts of PRA while the evaluation of the consequences is performed using existing transient analysis simulation tools. The current pilot application proposes the consequence evaluation the application of best-estimate + uncertainty (BEPU) analysis.

Given the limited resources of the SMAP group, an application to address plant safety margin was not feasible. However, the pilot applications presented in the report document the basic concepts of the SMAP-methodology even though the scope of evaluation is limited to a rather restricted set of scenarios necessary to evaluate the effect of a simple plant modification. This means that the step of risk aggregation (as outlined in Chapter 5) to evaluate plant risk does not form part of the pilot applications.

7.2 Recommendations

1. Rather straight-forward extensions of the currently implemented methodology (as demonstrated with the pilot applications) are called for mainly in two directions:

   a) The pilot applications documented in the report are evaluating a rather limited set of scenarios. For a more ambitious wide scope implementation of the SMAP-methodology, dynamic event tree simulation tools will become necessary in order to support efficient launching of the required large number of transient simulation runs and the related systematic collection of the respective simulation results (risk aggregation). Dynamic event tree methodologies are to some degree still under development. It would be advantageous to explore the performance of the different approaches from the perspective of possible application of such methodologies in the proposed SMAP framework. It is therefore suggested to launch a respective comparison exercise to evaluate existing dynamic event tree methodologies; such exercise could be organised similar to BEMUSE (CSNI/GAMA) that successfully explored different uncertainty evaluation methodologies.

   b) In order to extend the current methodology to the application of (integral) plant safety margin, the incorporation of severe-accident (SA) analysis tools becomes necessary. It still remains to be determined if the whole analysis should be performed with a modern SA-tool (e.g. MELCOR…) or if the current transient-analysis tools (e.g. TRACE, RELAP5, CATHARE, ATHLET …) should interface to such SA-tools at the proper moment of the respective transients, thereby calling for an interface between the two analysis tools. Requirements on the level of accuracy of the failure prediction are an input needed to answer this question.

2. A more difficult problem will be to properly address the fact that (epistemic) uncertainties tend to be larger in the domain of (low-frequency) severe accidents as compared to the traditional design basis transients. Some studies to explore the influence of this increased uncertainty onto the quantification of plant safety margin are needed and possible simplifications of the present general framework should be considered in light of such large uncertainties in order to maintain a methodology that remains of practical value. It is very likely that this needs extensive studies based on a suitably chosen and representative pilot case.

3. On a longer-term perspective, the SMAP-methodology could be applied to evaluate plant safety margin in a so-called “technology neutral” setting in terms of frequency-consequence curves that would avoid the usage of (“LWR-specific”) measures such as ΔCDF as a surrogate measure for plant damage. This would, however, require successful completion of the steps outlined before.

GLOSSARY

AM	Analytical Margin
APET	Accident Progression Event Tree -
BEPU	Best Estimate plus Uncertainty
CDF	Core Damage Frequency
CFP	Concentration of Fission Product
CFR	(US) Code of Federal Regulations
CHF	Critical Heat Flux
CIAU	Code with capability of Internal Assessment of Uncertainty
CSAU	Code Scaling Applicability and Uncertainty
CSNI	NEA Committee on Safety of Nuclear Installations
DBA	Design Basis Accident
DBT	Design Basis Transient
DM	Damage Mechanism
DNB	Departure from Nucleate Boiling
ECCS	Emergency Core Cooling System
ES	Event Sequence
FSAR	Final Safety Analysis Report
GSI	Generic Safety Issue (US NRC)
IE	Initiating Events
LB	Large Break
LWR	Light Water Reactor
KINS	Korean Institute for Nuclear Safety
LERF	Large Early Release Frequency
LM	Licensing Margin
LOCA	Loss of Coolant Accident
MCS	Minimal Cut Set
MD	Margin to Damage
MS	Mitigation System
NRC	US Nuclear Regulatory Commission

NPSH	Net Pressure Suction Head
PCT	Peak Clad Temperature
PIRT	Phenomena Identification and Ranking Table
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
RIA	Reactivity Insertion Accident
RS	Response Surface
SDTPD	Stimulus Driven Theory of Probabilistic Dynamics
SMAP	Safety Margins Action Plan
SSC	Structure, System or Component
ST	Source Term
SV	Safety Variable
SUSA	System for Uncertainty and Sensitivity Analysis
TH	Thermal Hydraulic
TN	Technical Note
UMS	Uncertainty Methods Study