Safety margins estimation method considering uncertainties within the risk-informed decision-making framework

S. Martorell*[1], Y. Nebot[1], J.F. Vilanueva[1], S. Carlos[1], V. Serradell[1],
F. Pelayo[2] and R. Mendizabal[2]
[1] *Department of Chemical and Nuclear Engineering, Polytechnic University of Valencia,*
Camí de Vera, s/n. 46022 Valencia, Spain
[2] *Spanish Nuclear Safety Council, C/ Justo Dorado, 11 28040 Madrid, Spain*

Abstract

The adoption by regulators of the risk-informed decision-making philosophy has opened the debate on the role of the deterministic and probabilistic approaches to support regulatory matters of concern to NPP safety (e.g. safety margins, core damage frequency, etc.). However, the typical separation of the application fields does not imply that both methods cannot benefit from each other. On the contrary, there is a growing interest nowadays aimed at developing methods for using probabilistic safety analysis results into requirements and assumptions in deterministic analysis and vice versa. Thus, it appears an interesting challenge for the technical community aimed at combining best estimate thermal-hydraulic codes with probabilistic techniques to produce an effective and feasible technology, which should provide more realistic, complete and logical measure of reactor safety. This paper proposes a new unified framework to estimate safety margins using a best estimate thermal-hydraulic code with help of data and models from a level 1 LPSA (low power and shutdown probabilistic safety assessment - PSA) and considering simultaneously the uncertainty associated to both probabilistic and thermal-hydraulic codes. It is also presented an application example that demonstrates the performance and significance of the method and the relevance of the results achieved to the safety of nuclear power plants.

KEYWORDS: Safety margins, probabilistic method, uncertainties, risk, thermal-hydraulics, probabilistic and deterministic safety analysis

1. Introduction

The adoption by regulators of the risk-informed decision-making philosophy (e.g. US NRC RG 1.174) [1] has opened the debate on the role of the deterministic and probabilistic approaches to support regulatory matters of concern to NPP safety. The traditional deterministic safety assessment focuses normally on a small set of enveloping accidental scenarios, named design bases accidents (DBAs), while probabilistic safety assessment focuses on a widest set of less conservative scenarios in the framework of the so called Beyond Design Basis Accidents (BDBAs).

---

* Corresponding author, Tel. +34-963877098, Fax. +34-933877099, E-mail: smartore@iqn.upv.es

The deterministic approach focuses on verifying acceptance criteria for such DBAs normally in terms of maintaining sufficient safety margins for defense-in-depth barriers. Thus, the calculated safety margin has been traditionally defined as the absolute difference between a calculated safety parameter and its limiting (threshold) value with regard to the state of a given barrier for the corresponding DBA. An example is the comparison between the calculated peak cladding temperature during a loss-of-coolant accident (LOCA) and the corresponding safety limit (e.g. 2200 ºF), which is related to the fuel integrity.

The probabilistic approach focuses mainly on deriving the frequency of those of such BDBA that end with damage for the NPP (e.g. Core Damage Frequency for a level 1 PSA). The development of a PSA also requires the verification of acceptance criteria for such BDBA in terms of success criteria of the safety-related systems (i.e. availability of redundant safety-related equipment) designed to mitigate BDBA and their role in leading the plant to a safe state. For both types of consequences, damage to the plant or plant OK, one could derive the frequency of each particular accident scenario, which depends on the frequency of the involved initiating event and the probability of failure of safety functions (i.e. due to equipment failures or other physical limitations) and the safety margin available.

Both deterministic and probabilistic methods apply its main power in the aspect they focus: damage in the deterministic case and frequency in the probabilistic one. In its respective field, each method is more detailed and likely more realistic, but in the other's field both of them use rough approximations [2]. Based on it, the main application areas of both methods have been divided traditionally into the analysis of deterministic safety criteria (e.g. safety margins) in the former case and on the analysis of the frequency of the sequences leading to severe damage (e.g. core damage frequency) in the latter case.

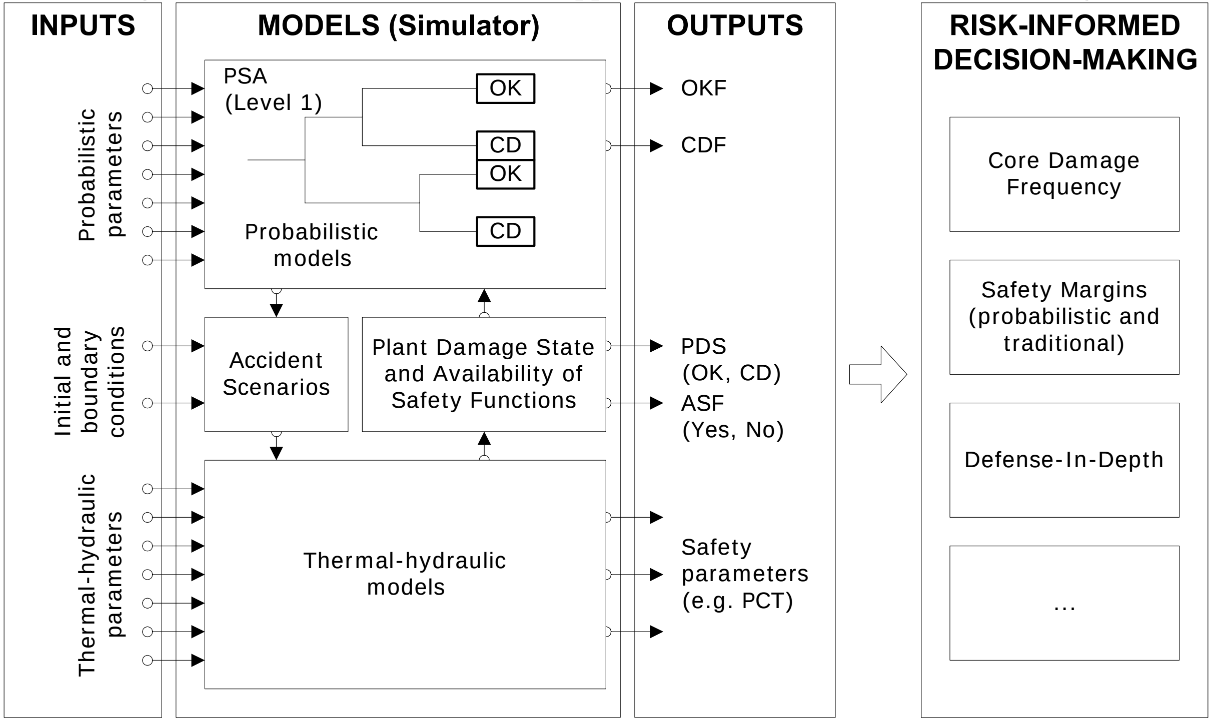
However, the typical separation of the application fields does not imply that both methods cannot benefit from each other. On the contrary, as suggested in Ref. [2], introducing probabilistic results into requirements and assumptions in deterministic analysis (i.e. DBA) and, vice versa, analyzing BDBA (i.e. of concern to the probabilistic analysis) with a deterministic approach are the main issues of risk informed regulation. Thus, Ref. [3] discusses the complementary use of the deterministic and probabilistic analyses in the context of risk informed decision-making linked to the analysis of BDBA. Also, Ref. [4] suggests the possibility of performing an improved reactor safety analysis process based on the combination of the information of thermal-hydraulic outputs taken from "Best-Estimate" codes supporting the deterministic analysis and the measures of core damage or some other suitable measure of risk. In addition, both references introduce the need of a process that considers the uncertainties modeled in the thermal-hydraulic codes combined with uncertainties and probabilities that are now represented in the probabilistic safety assessment (PSA). The task of combining thermal-hydraulic codes with PSA techniques to produce an effective and feasible technology, which would provide more realistic, complete, logical and honest measure of reactor safety, seems an interesting challenge for the technical community as discussed in [4].

The objective of this paper is to show the interest of a new unified framework to estimate safety margins using a best estimate thermal-hydraulic code with help of data and models from a level 1 LPSA (low power and shutdown PSA) and considering simultaneously the uncertainty associated to both probabilistic and thermal-hydraulic codes. It is also presented an application example that demonstrates the performance and significance of the method and the relevance of the results achieved to the safety of nuclear power plants.

2. The risk-informed decision-making framework

Three of the five principles that support the risk-informed philosophy of RG 1.174 [1] issued by the USNRC (US Nuclear Regulatory Commission) in 1998 are: 1) when the proposed change to the licensing bases result in an increase in core damage frequency (CDF) and/or risk, the increases should be small, 2) the proposed change maintains sufficient safety margins and 3) the proposed change is consistent with the defense-in-depth philosophy. Each of these principles should be considered in an integrated decision-making process. Thus, any evaluation of licensing issues supported by a safety analysis should consider both deterministic and probabilistic aspects of the problem. In our particular application area, even if the problem seems to be located in the probabilistic area (i.e. BDBAs in the PSA), there must be a check of the validity of the assumptions of the deterministic analysis. The same would be true in the opposite way. The particular risk-informed decision-making context under consideration here is shown in Figure 1.

Figure 1: Mathematical model to support the risk-informed decision-making.



As indicated in Figure 1, both the PSA and the analysis of the physical system (e.g. thermal-hydraulic analysis) are required for the purpose of making or aiding in the decision-making process as both probabilistic and thermal-hydraulic analysis interact to each other.

In this context, PSA models and data are used to estimate not only the expected frequency of occurrence of individual BDBAs leading the plant to a damage state (CDF) but also the frequency of those BDBAs leading the plant to a safe state (OKF), which depends on the frequency of the involved initiating event and the probability of failure of safety functions, i.e. due to hardware failures or other physical limitations.

In addition, best estimate thermal-hydraulic codes are used to support the verification of acceptance criteria in the context of the PSA, for example, in terms of availability of the safety functions with regard to physical limitations (e.g. success criteria and available margins to keep redundancy), verification of the plant damage state (e.g. OK or CD) and safety margins with regard to defense-in-depth barriers (e.g. PCT for fuel).

This unified framework should accomplish to perform a quantification that is inclusive of defense-in-depth barrier integrity, safety margins and CDF, making it possible to integrate deterministic and probabilistic analysis uncertainties and in this way enabling the overall treatment of uncertainty in risk-informed decision-making [5].

However, the unified framework can be understood as being comprised of two fundamental and relatively independent parts: 1) development of safety measures (i.e. safety margins) for individual BDBAs, and 2) integrating the safety measures into risk-based metrics (i.e. probabilistic safety margins) for individuals BDBAs, initiating event groups, or all the accident scenarios as a whole.

The presence of uncertainties associated with the simulation codes (i.e. thermal-hydraulic and PSA codes) adds difficulty in calculating the safety margins and corresponding frequencies or risk-metrics. The appropriate incorporation, propagation and presentation of the implications of uncertainty is widely recognized as a fundamental component of analyses of complex systems whatever the quantification model being adopted [6].

Here, the probability theory is used to represent uncertainty and the Monte Carlo Method and one embedded Simple Random Sampling procedure (i.e. Crude Monte Carlo procedure) is adopted for propagating uncertainties. However, management of uncertainty in output results will be conducted in a way different from the typical estimation of the distribution function of the output results and the corresponding upper and lower bound. The alternative method is presented later on after the formulation of safety margins.

3. Formulation of safety margins accounting for probabilities

Plant safety margins can be described in the general context of performance-based decision-making. Thus, in the present context, safety barriers performance is closely related to fundamental safety objectives and characterizes the plant state. The proposed set of safety margins accounting for probabilities should constitute a comprehensive statement of plant performance, reflecting in some detail not only the barrier states but also the frequencies of getting into, or near, those barrier states.

Following the main idea introduced in Ref. [5], a performance-based evaluation in the present context begins with the specification of functional requirements of each barrier (i.e. barrier damage mechanisms) and performance indicators (i.e. safety parameters) are identified that assess the extent to which a required function of the barrier is fulfilled. The performance standard (i.e. threshold limit) is associated to the level required to consider the function met. Comparing the real value of safety parameters against the performance standard using appropriate performance metrics (i.e. safety margins) must allow characterizing the barrier state. Thus, for example, the fuel barrier is associated to the peak cladding temperature (PCT) as safety parameter which is limited by the PCT regulatory acceptance limit [2]. Other examples can be found in Ref. [5].

In general, following the schematic view shown in figure 1, one can associate traditional safety margins as continuous variables with regard to safety parameters connected with the integrity of plant barriers (e.g. fuel, reactor coolant system boundary, containment, etc.) and in addition with regard to safety parameters connected with the availability of safety related functions (ASF) which support the integrity of these barriers (e.g. safety features, operator intervention in response to an initiating event, etc.) as well. Moreover, one can also associate safety margins as binary variables connected with plant damage states (PDS) (e.g. plant OK or CD).

Let us suppose that V represents a calculated safety parameter with an upper safety threshold limit L(V). For example, V and L(V) are continuous variables for the case of the PCT safety parameter, while they are binary variables for the case of PDS (e.g. L(V)=1, and V=1 if PDS=CD and V=0 otherwise). The corresponding traditional safety margin with regard to the safety parameter V and threshold limit L(V) can be quantified for each BDBA, named k, as follows:

$$M(V,k)=\begin{cases}\dfrac{L(V)-V(k)}{L(V)-V_{ref}} & \text{if} \quad L(V)\geq V(k)\geq V_{ref}\\ 0 & \text{if} \quad V(k)>L(V)\\ 1 & \text{if} \quad V(k)<V_{ref}\end{cases} \tag{1}$$

where Vref is a reference value for V(k), supplying a normalization factor. Note that V(k) is a random variable because it comes from calculations. Therefore M(V,k) is a random variable too, and ranges in the interval [0,1].

The traditional safety margins are not probabilities, and therefore cannot de combined by the probabilistic rules. However, the interest herein is on proposing (traditional) safety margins conditioned to the probability of occurrence of the accident scenario k following the corresponding initiating event i. The most meaningful way of describing the conditional margin is just the couple

$$\{M(V,k)\,,\,PR(k/i)\} \tag{2}$$

or alternatively

$$\{M(V,k)\,,\,\nu(k)\} \tag{3}$$

where ν(k) is the frequency of such accident scenario k, and PR(k/i) is the conditional probability of occurrence of the accident sequence k provided that the initiating event i has occurred. Note that ν(k) and PR(k/i) are random variables too.

4. Estimation of safety margins and frequencies

Estimation of couples safety margin and frequency uses the formulation introduced in the previous section. However, hundreds or thousands of executions of the codes may be required to address uncertainties depending on the particular uncertainty analysis method adopted. Being aware of the computational cost of each execution, sometimes taking hours or even days, it seems necessary to adopt an alternative method of analyzing uncertainty of output results from those codes in order to reduce the computational effort of estimating safety margins. As stated, in this work we suppose a 'crude' Monte Carlo method, with simple random sampling of the uncertain input parameters.

As defined in section 3, the safety margin is a random variable, defined as the normalized difference between the calculated value of a safety variable and the corresponding limit. Each accident sequence has associated a safety margin (or one for each safety variable), and a frequency of occurrence too (or a conditional probability with respect to the initiator). In a safety study, the safety margin must be conservatively calculated, i.e. a lower quantile of its probability distribution must be estimated. In this work we will use for such calculation the order statistics methodology, which is becoming popular with the name of Wilks' method [7]. It is a nonparametric methodology (independent of the type of probability distribution under study). In thermal-hydraulic safety calculations it was used for the first time by the German 'Gesellschaft fur Anlagen und Reaktorsicherheit' (GRS) [8]. It has also been used in AREVA's realistic LOCA analysis methodology based [9]. Several authors propose additional formulation for this purpose based on the use of order statistics method [10, 11].

Wilks' method is based in a Monte Carlo calculation with simple random sampling, but with much less calculations than usual, so that it does not allow estimating the probability distribution of the output but only tolerance intervals. In addition, this nonparametric approach decouples the number of uncertainty parameters and the number of required calculations.

The method proposed exploits the advantages of order statistics to provide distribution free tolerance intervals for an output variable based on the number of runs (N) necessary to guaranty a probability content or coverage (γ) with confidence level (β). The 0.95/0.95 confidence/coverage has been recognized by the USNRC has having sufficient conservatism for LBLOCA analyses adopting V(k)=PCT as safety parameter [9]. The minimum number of sampled cases is given by Wilks' formula for the case of one output variable and one-sided tolerance limits. However, one is interested herein in deriving the one-sided tolerance limits for the case of two variables represented by the couple $\{M(V,k)\ ,PR(k/i)\}$ or $\{M(V,k)\ ,\nu(k)\}$. For example, Ref. [11] proposes the performance of N=93 runs of the codes (i.e. thermal-hydraulic and probabilistic codes) to achieve the couple coverage/confidence of 0.95/0.95 for the one-sided tolerance limits.

5 .Application example

Experience from current PSA studies has shown the importance of some risky scenarios with the plant at low power and shutdown conditions as compared to the accident scenarios with the plant operating at full power. In particular, current low power and shutdown PSA (LPSA) studies shows that the loss of the Residual Heat Removal System (RHRS) transient is one of the most risk-significant events under low power conditions [12]. The application example is performed for a loss of coolant accident (LOCA) in the RHRS during plant operational state POS 3, corresponding to Mode 4, for a PWR NPP, in which the RHRS is pressurized (27 Kg/cm2). This transient can be initiated for example by a break in the RHR pipes. Figure 2 shows the corresponding event tree for the S4A initiating event group included in the LPSA for this PWR NPP [13]. Table 1 shows a brief description of the initiating event and headers.

Figure 2: Accident scenarios after a LOCA in one RHR train (Mode 4).

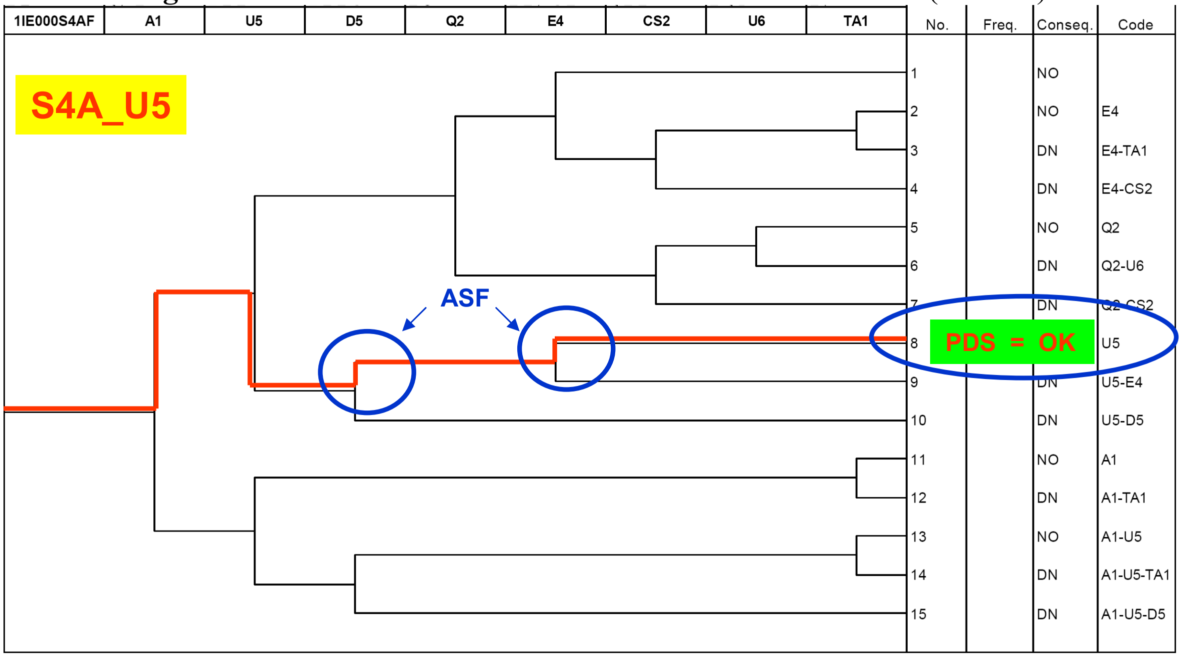


Table 1: Event tree description.

Initiating Event	**Description**
1IE000S4AF	LOCA in one RHR train (POS 3, Mode 4)
Event tree headers	**Description**
A1	Isolation of RHR train with breaks
U5	High pressure safety injection by one of two pumps (1/2 IHI)
D5	Low pressure safety injection by a pump (1/1 ILI)
Q2	Safety injection flow reduction
E4	Cooling through PORV's from one Steam Generator and reposition or through the RHR train available
CS2	Pressurizer PORV's opening
U6	Recirculation with high pressure pump
TA1	RWST Reposition

In particular, this study focuses on sequence number 8 (sequence U5) of the S4A initiating event, named sequence S4A_U5, which, in principle, should lead the plant to a safe state (PDS=OK). According to this accidental sequence, after the LOCA in the RHR, the RHR train with the break is isolated (A1), and then the available train of the low pressure injection system (D5) is started and aligned following a failure of the high pressure injection system train (U5). Finally, heat removal is initiated by means of one of the SG's and its relief valves or through the RHR train available when possible, keeping in this way the plant in a stable condition.

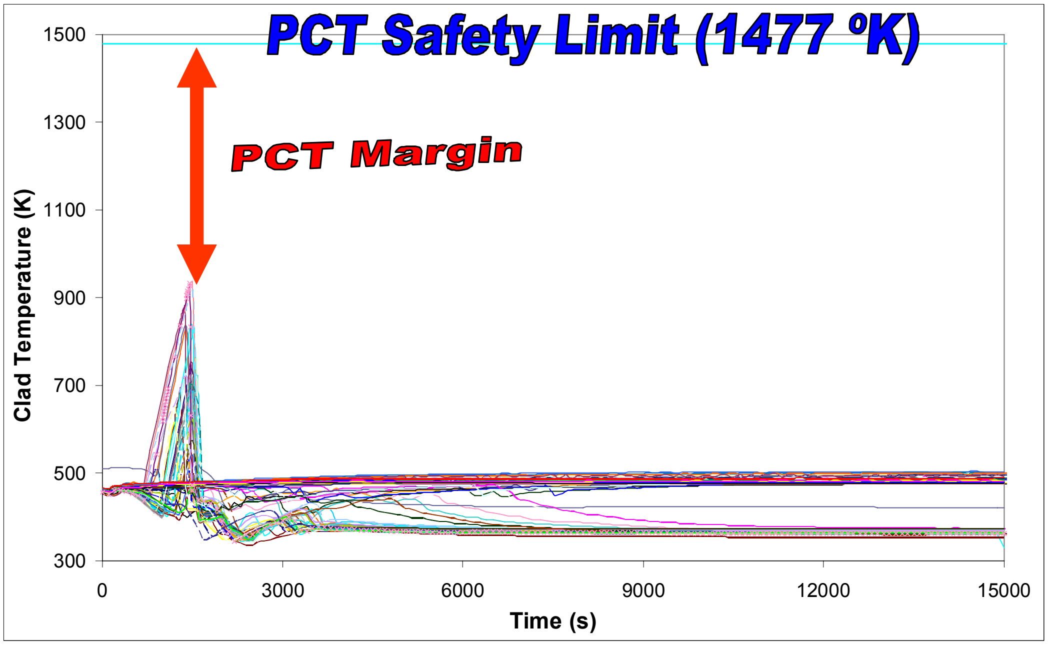
The study of safety margins accounting for probabilities and considering uncertainties consists of the following steps: 1) Identify important uncertainty contributors and define their density functions, 2) Sampling those contributors for N times over their application range (e.g. N=93 as discussed above), 3) Perform N calculations of the desired safety parameters and the corresponding probabilistic safety margins for the accidental sequence S4A_U5 using the thermal-hydraulic/probabilistic codes. RELAP 5 Mod 3.3 is used as the best estimate thermal-hydraulic code to derive the safety parameters and Risk Spectrum is used to perform the quantification of frequencies and conditional probabilities.

Three sets of uncertainty contributors have been considered in this work: thermal-hydraulic parameters (core power, fuel radius, fuel conductivity, etc.), boundary conditions (break size, isolation time, water injection time, etc.) and probabilistic parameters (initiating event frequency, equipment failure rate, probability of failure per demand, etc.).

In this example of application we performed 93 runs of both the thermal-hydraulic and probabilistic codes. Two basic prerequisites necessary to perform the 93 calculations are the availability of the thermal-hydraulic model, i.e. "input deck" for RELAP 5 Mod 3.3 in this case, and the availability of the LPSA, i.e. "input deck" for Risk Spectrum in this case, of the PWR NPP. Both models need to be modified according to the plant conditions with regard to the random sampling of the significant uncertainty contributors. Thus, the previous step was to develop one input deck for the RELAP 5 Mod 3.3 and the Risk Spectrum codes for each one of the 93 samples of the uncertainty contributors.

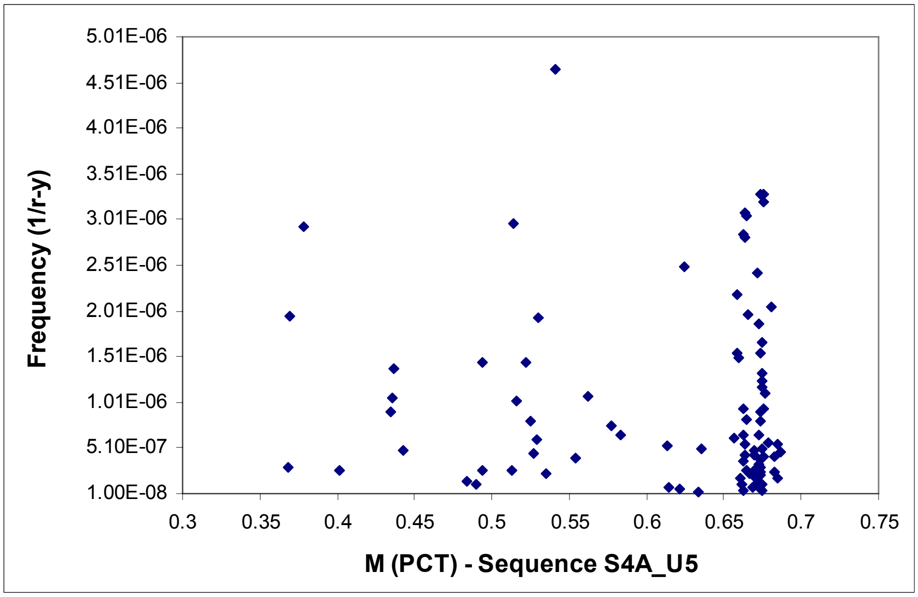
Finally, 93 simulations have been implemented in the thermal-hydraulic/probabilistic codes to obtain the evolution of the fuel clad temperature as safety parameter of interest for the accidental sequence S4A_U5 (see figure 3). Figure 3 shows how according to the evolution of the fuel clad temperature the PDS=OK for all the cases, which is coherent with the logical result (plant OK) identified in the LPSA (see figure 2). However, this temperature rises during the first 2000s for some samples were the PCT safety margin is reduced significantly.

Figure 3: Fuel clad temperature evolution and PCT margin in accidental sequence S4A_U5.



In addition, the PCT safety margin has been computed jointly with the frequency of its occurrence and its conditional probability for each of the 93 simulations of sequence S4A_U5 shown in Figure 3 for the fuel clad temperature. Figure 4 shows a 2D plot with the 93 couples $\{M(PCT, S4A\_U5), \nu(S4A\_U5)\}$. Based on these results, it has been estimated a one-sided 0.95/0.95 tolerance interval for this couple being $\{0.369, 4.66E\text{-}6\}$, which represents minimum PCT margin with maximum occurrence frequency.

Figure 4: PCT margin versus occurrence frequency for accidental sequence S4A_U5.



6. Conclusion

There is an interesting challenge in the field of risk-informed decision-making on reactor safety on how to combine the probabilistic and deterministic information to provide more complete and realistic measures to support the decision-making.

This paper presents a new method developed in this framework, which is aimed at estimating safety margins using a best estimate thermal-hydraulic code with help of data and models from a level 1 LPSA (low power and shutdown probabilistic safety assessment - PSA) and considering simultaneously the uncertainty associated to both probabilistic and thermal-hydraulic codes.

The application example shows the viability of the methodology and the significance of the results achieve that encourage continuing this research. There are several ways of improving the methodology proposed herein, which however bring new challenges, for example:

1. Consider all the accident sequences associated with the initiating event instead of performing the analysis of an individual sequence. The drawback is that as some sequences are more unlikely they may not appear with a limited number of code runs.
2. Obtain real probabilistic safety margins instead of the traditional safety margins with probabilistic information being considered herein. This imposes a need for the formulation of the problem in an alternative way, i.e. aimed at obtaining directly the probability of excedence of a safety margin or criteria.

References

1) RG 1.174: An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis. Final draft, February 1998.
2) IAEA-TECDOC-1332, Safety margins of operating reactors: Analysis of uncertainties and implications for decision-making, IAEA, Vienna, 2003.
3) S. Martorell, Y. Nebot, J. F. Villanueva, S. Carlos, V. Serradell, F. Pelayo, R. Mendizábal. Estimating safety margins considering probabilistic and thermal-hydraulic uncertainties. IAEA Technical Meeting on the Use of Best Estimate Approach in Licensing with Evaluation of Uncertainties, Pisa, Italy, 12-16 September 2005.
4) Graham B. Wallis, "Uncertainties and probabilities in nuclear reactor regulation". 11th International Topical Meeting on Nuclear Reactor Thermal-Hydraulics (NURETH-11). Popes' Palace Conference Center, Avignon, France, October 2-6, 2005.
5) Gavrilas, M., Meyer, J., Youngblood, B., Prelewicz, D., Beaton, R., A Generalized Framework for Assessment of Safety Margins in Nuclear Power Plants, Proceedings to BE 2004: International Meeting on Updates in Best Estimate Methods in Nuclear Installations Safety Analysis, Washington, DC, November 14-18, 2004, CD-ROM, ANS Lagrange Park, IL.
6) Oberkampf WL, Helton JC, Joslyn CA, Wojtkiewicz SF, Ferson S. Challenge problems: uncertainty in system response given uncertain parameters. Reliability Engineering & System Safety 2004; 85(1-3):11-19.
7) Wilks S.S. "Collected papers: Contributions to mathematical statistics". Ed: John Wiley, 1967.
8) Glaeser, Horst G., Uncertainty evaluation of thermal-hydraulic code results, Int. Meeting on "Best-Estimates" Methods in Nuclear Installation Safety Analysis (BE-2000).
9) Martin, R.P., O'Dell, L.D., "AREVA's realistic large break LOCA analysis methodology", Nuclear Engineering and Design, 235, pp 1713-1725, 2005.
10) Nutt W.T., Wallis G.B., "Evaluation of nuclear safety from the outputs of computer codes in the presence of uncertainties", Reliability Engineering and System Safety, 83, pp 57-77, 2004.
11) Guba A., Makai M., Pál L., "Statistical aspects of best estimate method-I", Reliability Engineering and System Safety, 80, pp 217-232, 2003.
12) NUREG/CR-5820, "Consequences of the loss of the residual heat removal systems in pressurized water reactors". NUREG/CR-5820. USNRC. May 1992
13) C.N.Ascó, APS de Sucesos Internos en Otros Modos de Operación de C.N.Ascó, Rev 1 ANAV, Junio 2002.