Reliability Engineering and System Safety 162 (2017) 122–138

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

# Safety margin sensitivity analysis for model selection in nuclear power plant probabilistic safety assessment

Francesco Di Maio[a,*], Claudia Picoco[a], Enrico Zio[a,b], Valentin Rychkov[c]

[a] Energy Department, Politecnico di Milano, Via La Masa 34, 20156 Milano, Italy
[b] Chair System Science and the Energy Challenge, Fondation Electricite' de France (EDF), CentraleSupélec, Université Paris-Saclay, Grande Voie des Vignes, 92290 Chatenay-Malabry, France
[c] EDF-R & D, Management des Risques Industriels, 7, Bd Gaspard Monge, 91120 Palaiseau, France

ARTICLE INFO

*Keywords:*
Dynamic Probabilistic Safety Margin
Risk-Informed Safety Margin Characterization
Integrated Deterministic Probabilistic Safety Assessment
Dynamic Event Tree
Sensitivity analysis
Seal LOCA
U-Tube Steam Generator

ABSTRACT

The safety assessment of Nuclear Power Plants makes use of Thermal-Hydraulic codes for the quantification of the safety margins with respect to upper/lower safety thresholds, when postulated accidental scenarios occur. To explicitly treat uncertainties in the safety margins estimates within the Risk-Informed Safety Margin Characterization (RISMC) framework, we resort to the concept of Dynamic Probabilistic Safety Margin (DPSM). We propose to add to the framework a sensitivity analysis that calculates how much the Thermal-Hydraulic (TH) code inputs affect the DPSM, in support to the selection of the most proper probabilistic safety assessment method to be used for the problem at hand, between static or dynamic methods (e.g., Event Trees (ETs) or Dynamic ETs (DETs), respectively). Two case studies are considered: firstly a Station Black Out followed by a Seal Loss Of Coolant Accident (LOCA) for a 3-loops Pressurized Water Reactor (PWR), whose dynamics is simulated by a MAAP5 model and, secondly, the accidental scenarios that can occur in a U-Tube Steam Generator, whose dynamics is simulated by a SIMULINK model. The results show that the sensitivity analysis performed on the DPSM points out that an ET-based analysis is sufficient in one case, whereas a DET-based analysis is needed for the other case.

## 1. Introduction

The Safety Assessment (SA) of a Nuclear Power Plant (NPP) is based on the evaluation of the consequences of a number of postulated accidental scenarios and on the quantification of their probabilities of occurrence. This is done to verify that the plant design satisifies prescribed safety margins, i.e., that there is sufficient difference between the values reached by the pre-defined safety parameters during the accidental scenarios and the pre-set thresholds that must not be exceeded in order not to endanger the NPP operability and safety.

Best Estimate (BE) Thermal-Hydraulic (TH) codes are used to simulate the dynamics of the safety parameters during the postulated accidental scenarios. Traditional (static) Probabilistic Safety Assessment (PSA) methods, such as Fault Trees (FTs) and Event Trees (ETs), are used to compute the probability of occurrence of the accidental scenarios.

Recently, Integrated Deterministic Probabilistic Safety Assessment (IDPSA) has been proposed as a way for explicitly embedding the deterministic TH analysis within the probabilistic analysis, by systematically treating both aleatory (stochastic) and epistemic (modelling) uncertainties in the accidental progression [1,36].

IDPSA methods include Discrete Dynamic Event Tree [14], Continuous Dynamic Event Tree [29], Dynamic Event Tree [15,21], Monte Carlo Dynamic Event Tree [12], DYnamic Logical Analytical Methodology [4]. These methods are conceived to dynamically analyze the evolution of accidental scenarios and model the operational risk in complex dynamic systems, explicity accounting for mutual interactions between failures of software and hardware components and their recovery, control and operator actions [1,36].

*Abbreviations:* AC, Alternate Current; **AFW**, Auxiliary Feed Water; **BDBA**, Beyond Design Basis Accident; **BE**, Best Estimate; **DBA**, Design Basis Accident; **DET**, Dynamic Event Tree; **DOE**, Department Of Energy; **DPSM**, Dynamic Probabilistic Safety Margin; **ET**, Event Tree; **FT**, Fault Tree; **IDPSA**, Integrated Deterministic Probabilistic Safety Assessment; **LOCA**, Loss of Coolant Accident; **LWRS**, Light Water Reactor Sustainability; **MAAP5**, Modular Accident Analysis Program version 5; **MCS**, Minimal Cut Set; **MVL**, Multiple Value Logic; **NM**, Near Miss; **NPP**, Nuclear Power Plant; **OS**, Order statistics; **PI**, Prime Implicant; **PID**, Proportional Integrative Derivative; **PSA**, Probabilistic Safety Assessment; **PWR**, Pressurized Water Reactor; **RCP**, Reactor Coolant Pump; **RCS**, Reactor Coolant System; **RISMC**, Risk Informed Safety Margin Characterization; **RPV**, Reactor Pressure Vessel; **SA**, Safety Assessment; **SBO**, Station Black Out; **SG**, Steam Generator; **TH**, Thermal-Hydraulic; **UTSG**, U-Tube Steam Generator

* Corresponding author.
*E-mail address:* francesco.dimaio@polimi.it (F. Di Maio).

http://dx.doi.org/10.1016/j.ress.2017.01.020
Received 7 March 2016; Received in revised form 16 December 2016; Accepted 30 January 2017
Available online 03 February 2017
0951-8320/ 

*Symbols*

| | |
|---|---|
| $a$ | Accidental scenario. |
| $M(y_j, a)$ | Safety margin for the j - th safety parameter during the accidental scenario $a$ |
| $y_j$ | j - th safety parameter. |
| $j$ | Index of the safety parameter, j=1, 2, ..., J. |
| $J$ | Number of safety parameters. |
| $y_j(a)$ | j - th safety parameter for the accidental scenario $a$ |
| $y_{j,ref}$ | Nominal value of the safety parameter $y_j$ during normal operation. |
| $U_j$ | Upper threshold for the j - th safety parameter. |
| $L_j$ | Lower threshold for the j - th safety parameter. |
| $y_{\gamma_1}$ | Real value of the $\gamma_1^{th}$ percentile of the safety parameter. |
| $y_t$ | (Grace) time required to reach $y_j$ |
| $\gamma_1$ | Probability that y is lower than $y_{\gamma_1}$ |
| $y_{t_{\gamma_2}}$ | Real value of the $\gamma_2^{th}$ percentile of the time $y_t$. |
| $\gamma_2$ | Probability that $y_t$ is lower than $y_{t_{\gamma_2}}$ |
| $\hat{y}_{\gamma_1}$ | Estimate of $y_{\gamma_1}$ |
| $\hat{y}_{t_{\gamma_2}}$ | Estimate of $y_{t_{\gamma_2}}$ |
| $\beta$ | Confidence value in the percentile estimation. |
| $\beta_1$ | Confidence in the estimation of $y_{\gamma_1}$ |
| $\beta_2$ | Confidence in the estimation of $y_{t_{\gamma_2}}$ |
| $M(\gamma_1, \beta_1)$ | Probabilistic Safety Margin estimated by the $\gamma_1^{th}$ percentile of y with confidence $\beta_1$ |
| $M(\gamma_1, \beta_1, \gamma_2, \beta_2)$ | Dynamic Probabilistic Safety Margin estimated by the $\gamma_1^{th}$ percentile of y with confidence $\beta_1$ and the $\gamma_2^{th}$ percentile of $y_t$ with confidence $\beta_2$ |
| $\bar{x}$ | Vector of a generic model inputs. |
| $x$ | Model input. |
| $x_k$ | k – th model input, k=1, 2, .... |
| $k$ | Index of the model input. |
| $x_{k,i}$ | i – th value of the k – th model input. |
| $\bar{y}$ | Vector of the calculated safety parameter realizations. |
| $y_n$ | Safety parameter that is calculated during $n$-th calculation, n =1,2,...N. |
| $n$ | Index of the simulations. |
| $\bar{y}_t$ | Output vector of the calculated times at which the values $\bar{y}$ are reached. |
| $y_{t_n}$ | Time at which $y_n$ is reached. |
| $N$ | Number of simulations. |
| $\tilde{x}_{k,i}$ | Normalized input value of $x_{k,i}$ |
| $\Delta y_t$ | Maximum variability range of the normalized output. |
| $\Delta x_k$ | Maximum variability range of the k – th input. |
| $\tilde{y}_t \mid x_k = x_{k,i}$ | Normalized value of $y_t$ computed for the subgroup with $x_k = x_{k,i}$ kept fixed. |
| $I_{x_k}$ | Sensitivity Index for the k – th input. |
| $P_{CD}$ | Core Damage Probability. |
| $t_{rec}$ | Recovery time. |
| $P(x_k = x_{k,i})$ | Probability that $x_k$ assumes the value $x_{k,i}$ |
| $Q_e$ | Feedwater in the UTSG. |
| $P_O$ | Operating Power in the UTSG. |
| $P_n$ | Nominal Power in the UTSG. |
| $Q_v$ | Exiting steam in the UTSG. |
| $W_{rl}$ | Wide Range Level in the UTSG. |
| $N_{rl}$ | Narrow Range Level in the UTSG. |
| $P_F$ | UTSG probability of failure. |

Even though the safety margins quantification required by risk assessment within the Risk Informed Safety Margin Characterization (RISMC) initiated by the US Department Of Energy (DOE) within the Light Water Reactor Sustainability (LWRS) program [17], is expected to be able to effectively catch the system dynamics and the uncertain TH codes assumptions and parameters, this work is the first effective attempt to achieve this goal.

We resort to the quantification of the Dynamic Probabilistic Safety Margin (DPSM), where Order Statistics (OS) is used to compute, with a given confidence, the estimate of a given percentile of the distribution of the safety parameter and a given percentile of the time required for the safety parameter to reach the considered parameter percentile value [10]. This allows giving due account to the dynamics of the system undergoing an accidental scenario.

The DPSM is, then, originally exploited within a novel sensitivity analysis approach to identify which input parameter affects most the safety margin and, in particular, how much dynamic inputs influence the safety margin. This helps understanding whether a dynamic probabilistic safety method (e.g., a Dynamic ET (DET)) or whether a static probabilistic method (e.g., a static ET) is needed for the NPP safety assessment. Indeed, the dynamic approach gives a more detailed description of the process, but at the expense of a large computational burden. In this respect, it would make no sense to waste resources on a dynamic analysis of a system when conventional static methods can provide adequate results. As a matter of fact, the main goal of this paper is just to provide a framework for choosing which approach (whether static or dynamic) better fit to the system under analysis.

In ordert to show how the framework works, two case studies are considered. In the first case, a Station Black Out (SBO) accident followed by a Seal Loss Of Coolant Accident (LOCA) has been modelled and simulated with MAAP5 TH code [22]. Dynamic aspects such as time lag between SBO and LOCA and promptness of operators actions have been simulated. The DPSMs corresponding to the event of core uncovery have been computed and a sensitivity analysis has been performed on these time-dependent results. As we shall see, the results show that the dynamic aspects considered in TH simulations do not affect the calculated DPSMs and, thus, we conclude that the static probabilistic models are sufficient for the analysis and, therefore, no dynamic probabilistic models are developed for the Seal LOCA accident.

The second case study regards a U-Tube Steam Generator (UTSG), modelled with SIMULINK. In the dynamic model, four components (i.e., the outlet steam valve, the safety valve, the Proportional Integral Derivative (PID) controller and the communication between the sensor and the PID) can fail during the accident progression. Dynamic aspects such as the magnitude, the order and timing of the possible failure events have been included in the simulations. The DPSMs have been computed and the sensitivity analysis has been performed, showing the importance of including the dynamic aspects in the probabilistic model. Consequently, for the considered UTSG, a DET analysis is necessary for proper assessment and quantification of the probabilities of occurrence of the accidental scenarios and of the DPSMs.

The rest of the paper is organized as follows. In Section 2, the definition of the DPSM is given and the sensitivity analysis approach is described. In Section 3, the two case studies are presented and worked out. In Section 4, some conclusions are drawn.

## 2. The Dpsm and the Dpsm-based sensitivity analysis

### 2.1. The DPSM

The safety margin is traditionally defined as the minimum distance between the system "loading" and its "capacity" [DOE, 2009]. Mathematically, considering a specific accidental scenario $a$ and a safety parameter $y_j$. ($j$=1...$J$), the safety margin $M(y_j, a)$ with respect to an upper threshold $U_j$ can be written as:

$$M\left(y_j, a\right) = \left\{ \begin{array}{ll} \frac{U_j - y_j(a)}{U_j - y_{j,ref}}, & if y_j(a) \le U_j \\ 0, & if U_j < y_j(a) \\ 1, & if y_j(a) < y_{j,ref} \end{array} \right\} \tag{1}$$