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

Francesco Di Maio, Claudia Picoco, Enrico Zio, Valentin Rychkov

CrossMark

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

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 satisfies 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].

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_{γ_1}	Real value of the γ_1^{th} percentile of the safety parameter.
y_t	(Grace) time required to reach y_j
γ_1	Probability that y is lower than y_{γ_1}
$y_{t_{\gamma_2}}$	Real value of the γ_2^{th} percentile of the time y_t.
γ_2	Probability that y_t is lower than $y_{t_{\gamma_2}}$
$\hat{y}_{\gamma_1}$	Estimate of y_{γ_1}
$\hat{y}_{t_{\gamma_2}}$	Estimate of $y_{t_{\gamma_2}}$
β	Confidence value in the percentile estimation.
β_1	Confidence in the estimation of y_{γ_1}
β_2	Confidence in the estimation of $y_{t_{\gamma_2}}$
$M(\gamma_1, \beta_1)$	Probabilistic Safety Margin estimated by the γ_1^{th} percentile of y with confidence β_1
$M(\gamma_1, \beta_1, \gamma_2, \beta_2)$	Dynamic Probabilistic Safety Margin estimated by the γ_1^{th} percentile of y with confidence β_1 and the γ_2^{th} percentile of y_t with confidence β_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 $x_{k,i}$
Δy_t	Maximum variability range of the normalized output.
Δx_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 order 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:

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

(1)

and with respect to a lower threshold L_j as:

$$M\left(y_j, a\right) = \begin{cases} \frac{y_j(a) - L_j}{y_{j,ref} - L_j}, & if L_j \le y_j(a) \\ 0, & if y_j(a) < L_j \\ 1, & if y_j(a) > y_{j,ref} \end{cases} \quad (2)$$

where $y_{j,ref}$ is the nominal value of the safety parameter y_j during normal operation.

The safety margins are, traditionally, computed by TH codes for a set of postulated scenarios, called Design Basis Accidents (DBAs). Conservatism in assumptions and parameters values is adopted in order to take into account uncertainties in models and parameters [5].

Recently, safety margins are being evaluated also for Beyond Design Basis Accidents (BDBAs), thus, considering a larger set of scenarios. Moreover, Best Estimate (BE) TH codes are employed to evaluate the safety parameters with less conservatism and more realistic assumptions [2,32,34]. To account and propagate all the aleatory and epistemic uncertainties affecting the BE TH codes, a Dynamic Probabilistic Safety Margin (DPSM) has been proposed in [10]. The DPSM extends the definitions of safety margin in Eqs. (1) and (2), by replacing y_j with y_{γ_1}, and also by considering in the safety margin quantification $y_{t_{\gamma_2}}$. In particular, y_{γ_1} is the γ_1th percentile of the distribution of the safety parameter y_j (usually the 95th, according to regulatory guidance), whereas $y_{t_{\gamma_2}}$ is the γ_2th percentile (usually the 5th) of the distribution of the earliest (grace) time y_t required to reach y_{γ_1} (i.e., the available time for recovering from the occurrence of accidental scenario a).

Order Statistics (OS) is a non parametric approach that can be used for the estimation of y_{γ_1} and $y_{t_{\gamma_2}}$, as it allows evaluating the values of the required percentiles with confidences β_1 and β_2, respectively, as explained in Appendix A, on the basis of a limited set of BE TH dynamic simulations of the system evolution.

In this work, two different approaches will be used for the computation of the estimates of y and y_t, namely the Bracketing and the Coverage approaches (see Appendix A). The former assumes the outputs y and y_t to be uncorrelated. Their corresponding percentile estimates ($\hat{y}_{\gamma_1}$ and $\hat{y}_{t_{\gamma_2}}$, respectively) are, therefore, computed separately and independently ranked. On the other hand, since the coverage approach assumes correlation between the outputs, and, consequently, y is sorted corresponding to y_t, and they are required to simultaneously lie in the estimated percentile γ_1 and γ_2 [10].

We can, thus, define a DPSM with respect to an upper threshold U_j as in [10]:

$$M(\gamma_1, \beta_1, \gamma_2, \beta_2) = \begin{cases} \frac{U_j - \hat{y}_{\gamma_1}}{U_j - y_{j,ref}}, & if \hat{y}_{\gamma_1} \le U_j \\ 0, & if U_j < \hat{y}_{\gamma_1} \\ 1, & if \hat{y}_{\gamma_1} < y_{j,ref} \end{cases} \text{with grace time} \hat{y}_{t_{\gamma_2}} \quad (3)$$

where

$$\gamma_1 = Pr\left\{y < y_{\gamma_1}\right\} \quad (4)$$

$$\beta_1 = Pr\left\{y_{\gamma_1} < \hat{y}_{\gamma_1}\right\} \quad (5)$$

and

$$\gamma_2 = Pr\left\{y_t < y_{t_{\gamma_2}}\right\} \quad (6)$$

$$\beta_2 = Pr\left\{y_{t_{\gamma_2}} > \hat{y}_{t_{\gamma_2}}\right\} \quad (7)$$

where $\hat{y}_\gamma$ is the estimate of the γth percentile.

As we shall see in what follows, it is worth mentioning that in those cases in which the number N of BE TH available simulations is low, the analyst should decide whether it is better to fix β or γ for providing the proper estimate of the DPSM that, in principle, should be given with $\gamma_1 = \beta_1 = \beta_2 = 0.95$ and $\gamma_2 = 0.05$, as prescribed by regulation guidances [5].

2.2. Sensitivity analysis on the DPSM

Sensitivity analysis can help finding insights on the behaviour of a model, on its structure and on the way it responds to changes in the model input [3,27,35]. It also allows ranking the model parameters according to the different contributions they give to the variability of the output [8].

In this work, the model output of interest is the DPSM as defined in Section 2.1 and the aim is to determine whether the inputs of a dynamic simulation code influence (or not) the DPSM quantification. A sensitivity index must be defined and, based on this, one can decide the appropriate probabilistic approach (static/dynamic) for the quantification of the probabilities of occurrence of the accidental scenarios to be analysed.

Sensitivity indexes can be classified into local and global [27,35]. However, since local sensitivity indexes provide information that is only valid locally, for the purpose of our work a global index seems to be more suitable. Global sensitivity indexes, indeed, aim to measuring the contribution of an input to the variability of the output over the entire range of both the input and the output, also accounting for the input interaction through dependences [8,27,35]. Among popular global indexes are the Pearson and the Sobol indexes [30], the latter being an extension of the Variance Decomposition method [3,13,19,30]. However, Pearson and Sobol indexes are limited by the assumptions on the linearity and monotonicity of the model (Pearson) and by demanding computational costs (Sobol).

We therefore define a novel sensitivity index I_x (where x is a generic model input) that, even if approximate, is simple to calculate and does not require any hypothesis on the model. Without loss of generality, let assume that $\bar{x} = \{x_1, x_2, x_3\}$ where x_1, x_2 and x_3 are three input variables, with instances $\bar{x}_1 = \{x_{1,1}, x_{1,2}, x_{1,3}\}$, $\bar{x}_2 = \{x_{2,1}, x_{2,2}\}$ and $\bar{x}_3 = \{x_{3,1}, x_{3,2}, x_{3,3}, x_{3,4}\}$. We also assume that one simulation is available for each combination of these values. Consequently a total of $N = 24$ different simulations is available resulting in vectors of N possible values of y and y_t, $\bar{y} = \{y_1, y_2, ..., y_N\}$, and $\bar{y}_t = \left\{y_{t_1}, y_{t_2}, ..., y_{t_N}\right\}$, respectively. By resorting to OS (see Appendix A), the DPSM for each input parameter and the corresponding time can be computed, as shown in Section 2.1, by using all the available simulations (that would account for the input variable interdependences) but also by considering the partitioning of the N available simulations in subgroups (that would account for the contribution of single inputs, independently). In other words, considering each input parameter separately, a DPSM is computed for each fixed value that the parameter can assume and using only the simulations in which the variable assumes the considered value. Thus, for example, when referring to x_1, we compute the DPSM considering only results of y_t collected for the subgroups of simulations done with $x_1 = x_{1,1}$, $x_1 = x_{1,2}$ and $x_1 = x_{1,3}$, (i.e., $y_t \mid x_1 = x_{1,1}$, $y_t \mid x_1 = x_{1,2}$ and $y_t \mid x_1 = x_{1,3}$, respectively).

For the computation of the sensitivity index, both the input (e.g., x_1) and the output (e.g., $y_t \mid x_1 = x_{1,i}$ with $i=1,2,3$ when $x=x_1$) are first normalized with respect to their maxima:

$$\tilde{x}_{1,i} = \frac{x_{1,i}}{max\,(x_{1,1}; x_{1,2}; x_{1,3})}, with\ i=1,2,3 \quad (8)$$

$$\tilde{y}_t \mid x_1 = x_{1,1} = \frac{y_t \mid x_1 = x_{1,1}}{max\,(y_t \mid x_1 = x_{1,1}; y_t \mid x_1 = x_{1,2}; y_t \mid x_1 = x_{1,3})} \quad (9)$$

Similarly, $\tilde{y}_t \mid x_1 = x_{1,2}$ and $\tilde{y}_t \mid x_1 = x_{1,3}$ can be obtained. The sensitivity index I_{x_1} can be, therefore, defined as:

$$I_{x_1} = \frac{\Delta y_t}{\Delta x_1} \tag{10}$$

where Δy_t is the range of variability of the normalized output, i.e, the difference between the maximum normalized output $max \; (\widetilde{y}_t \mid x_1 = x_{1,1}; \widetilde{y}_t \mid x_1 = x_{1,2}; \widetilde{y}_t \mid x_1 = x_{1,3})$, that is equal to 1 (according to the normalization), and the minimum normalized output $min \; (\widetilde{y}_t \mid x_1 = x_{1,1}; \widetilde{y}_t \mid x_1 = x_{1,2}; \widetilde{y}_t \mid x_1 = x_{1,3})$; similarly, Δx_1 is the range of variability of the normalized input x_1. Also, I_x can be computed for the other input variables x_2 and x_3.

Notice that the index I_x is not constrained by any linearity and/or monotonic assumption on the input/output relationship (opposed to Pearson coefficient) with limited computational costs (opposed to Sobol indexes), and gives an indication on the variability of the output depending on the variability of the input: the larger I_x, the more the considered input x influences the output y.

As we shall see, the proposed strategy for deciding which probabilistic method should be used for the analysis is based on the ranking provided by I_x: when a dynamic input is ranked below others that are not time-dependent, a static probabilistic analysis of accident progression by ET is sufficient to compute the probabilities of occurrence of the considered accidental scenarios; when a dynamic input is among the top ranked, a dynamic probabilistic analysis, e.g., with a DET, is needed.

3. The case studies

In this Section, we present two applications of the proposed method for the selection of the probabilistic model to be used in a safety assessment. In the first case study, a Station BlackOut accident followed by a Seal Loss Of Coolant Accident is considered. The outcomes of the sensitivity analysis will suggest that a static probabilistic model for representing the accident progression to be enough for the purpose of the safety analysis. For this, ETs are built. In the second case study, a U-Tube Stam Generator is considered in which some components fail at different times and magnitudes. In this case, the calculated sensitivity indexes are larger for the dynamic inputs and, consequently, a framework for the DET is developed for the purpose of performing a safety analysis.

3.1. Sbo Seal Loca

3.1.1. The accidental scenario

The accidental scenario considered is a station blackout accident followed by a Seal LOCA in a 3-loops Pressurized Water Reactor (PWR). During a SBO, a Loss Of Offsite Power (LOOP) is worsened by the failure of all the emergency diesel engines. Under these circumstances, the reactor trip is activated and the Reactor Coolant Pumps (RCPs) are shut off.

In this sequence of events, we focus on the behaviour of the Reactor Coolant Pumps (shown in Fig. 1), and in particular on its seal package. The RCPs are installed on the cold leg of each loop of the NPP between the Steam Generators (SGs) and the Reactor Pressure Vessel (RPV). They contain a seals package consisting in three different seals (i.e., seal stages), each made up by a primary and a secondary seal. These seals must continuously be cooled in normal operation as well as during the SBO [26,28]. During normal operation, a seal injection system (that consists in a seal water inlet and a cooling water outlet) and a thermal barrier heat exchanger are the systems devoted to cool the seals. However, when a SBO occurs, seals cooling systems are lost and the seals overheat. Consequently, a Seal LOCA occurs at different leakage rates, that depend on the seal that fails. We consider leakage rates equal to 76, 182 and 480 gpm/RCP [31], corresponding to the failure of the first seal alone, both the second and third seals and all the three seals, respectively. Seals failure can occur according to three possible failure modes [31]: popping-open (i.e., opening of the seal
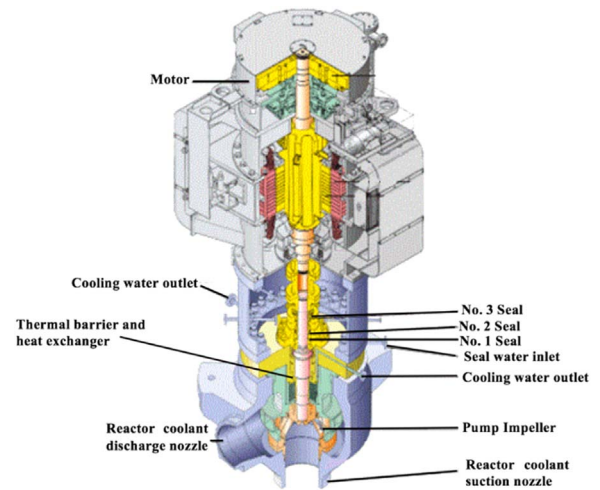
Fig. 1. Typical design of a Reactor Coolant Pump [20].

faces due to hydraulic instability caused by fluid flashing), binding (i.e., binding failure of the seal ring against the housing inserts due to secondary seal extrusion), O-ring extrusion (i.e., overheating of the secondary sealing elastomers, allowing excessive leakage).

3.1.2. Dynamic MAAP5 simulations

The Seal LOCAs scenarios have been simulated for all the considered leakage rates with a BE TH MAAP5 code [22], whose nodalization scheme is shown in Fig. 2. This code reproduces, when fed with the set of initiating events and operators actions listed in Table 1, the responses of the reactor to the postulated accidental scenario. Although the code is able to provide the simulation results also beyond core damage, the analysis will focus on the core uncover. Then, the values of the safety parameter y_j, the threshold L and the value of y_t required to evaluate the DPSM can be retrieved from the simulations. In fact, we can simulate the evolution in time of the boiled-up water level of the primary coolant y_j (with $j = 1$, since this the only safety parameter considered) and the core uncovery time y_t. In MAAP5 the core uncover corresponds to the condition when the boiled-up water level falls below the top of active fuel $L = 6.6$ m. The corresponding core uncover time is therefore a result provided by the code. It is worth mentioning that, during normal operation, the reference level is equal to $y_{ref} = 7$ m.

The scenario modelled is the following. The simulation starts with the SBO occurrence. All the seals cooling systems are, therefore, assumed to be lost, leading to the seals overheating. Seals can fail (due to popping-open) at

Fig. 2. Water nodalization for 3-Loops PWR [13].

Table 1

MAAP5 simulation inputs.

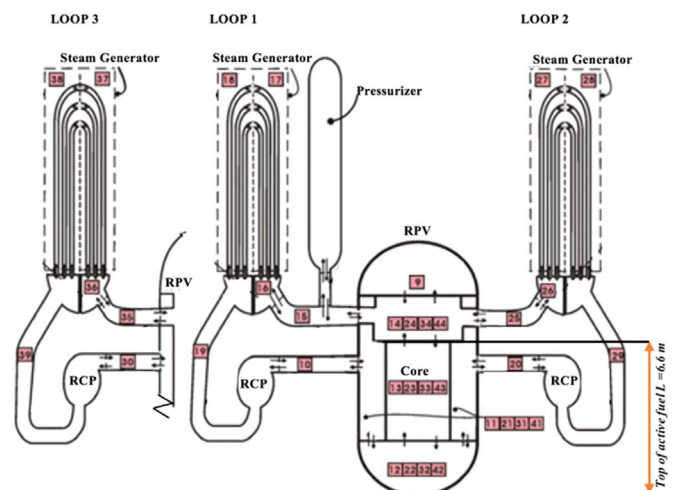|	
x_1[min]	0
Time of the leakage rate increase after SBO	13
	30
x_2[gpm/RCP]	76
Leakage rate	182
	480
x_3[min]	20
Time of activation of secondary cooling	30
	40
	50
	60
x_4 Strategy	A: t (AFW operation) = t (relief valve opening)
	B: t (AFW operation) = 3 h after the leakage rate increase

Table 2

DPSM (N=90 and with fixed γ_2) for the Seal LOCA.

γ_2	β_2 "Bracketing"	β_2 "Coverage"	$\hat{y}_{\gamma_1}$[m]	$\hat{y}_t$ [s]	DPSM
0.05	0.98	0.94	6.6 = L	7406	0 within a grace time of 7406 s

Table 3

DPSM (N=90 and with fixed β_2) for the Seal LOCA.

β_2	γ_2 "Bracketing"	γ_2 "Coverage"	$\hat{y}_{\gamma_1}$[m]	$\hat{y}_t$ [s]	DPSM
0.95	0.04	0.03	6.6 = L	7406	0 within a grace time of 7406 s

different times (x_1) from the onset of the SBO: immediately ($x_{1,1}$ = 0 min), after 13 min ($x_{1,2}$ = 13 min) or after 30 min ($x_{1,3}$ = 30 min). With the seal failure, the leakage rate increases from 21 gpm/RCP to a value that depends on the number of seals that have failed ($x_{2,1}$ = 76, $x_{2,2}$ = 182 and $x_{2,3}$ = 480 $\frac{gpm}{RCP}$). Operators are, thus, called to undertake counteracting measures to mitigate the possible consequences of this accident. They, first, activate a secondary cooling by opening a relief valve at different times ($x_{3,1}$ = 20, $x_{3,2}$ = 30, $x_{3,3}$ = 40, $x_{3,4}$ = 50, $x_{3,5}$ = 60 min from the seal failure) and, then, regulate the Auxiliary Feed Water (AFW) system (by decreasing the target of the SG level) by following either strategy "A" ($x_{4,1}$ = "A"), that is the AFW regulation occurs at the same time of the relief valve opening, or strategy "B" ($x_{4,2}$ = "B"), that is the regulation of AFW occurs 3 h later than the leakage rate increase. Moreover, when the primary pressure falls below 4 MPa, the accumulators automatically inject water in the cold leg of each loop. The values of the input variables for the dynamic simulations are shown in Table 1.

Assuming x_1, x_2, x_3 and x_4 to be independent and described by discrete uniform distributions in the ranges of the simulation inputs of Table 1 (i.e., joint distributions are neglected), all the possible combinations of these inputs leads to N = 90 alternative dynamic simulations for the case under analysis.

3.1.3. The DPSM-based sensitivity analysis results

3.1.3.1. The DPSMs. The collected values of $\bar{y}$ and $\bar{y}_t$ (i.e., the boiled-up water level and the uncovery time, respectively) have been employed for the calculation of the DPSM. Since the core uncovery occurs when the boiled-up water level falls below the top of the active fuel length L, we assume the safety margins to be calculated with respect to L as lower threshold. Resorting to OS and using all the N = 90 available simulations as well as all the possible subgroups of simulation (that is, considering the simulations when each input variable is kept fixed), we have estimated the values of the γ_1^{th} and γ_2^{th} percentiles of the boiled-up water level and of the time at which such level is reached, with confidences β_1 and β_2, respectively.

The DPSMs with "Bracketing" and "Coverage" approaches, N = 90 (i.e., all the possible values of x_1, x_2, x_3 and x_4 have been considered simultaneously) and γ_2 = 0.05 are shown in Table 2, whereas in Table 3 the DPSMs with N = 90 and β_2 = 0.95 are shown, again, for the both approaches.

It is worth mentioning that, even though the regulatory guidances prescribe the DPSM to be given with $\gamma_1 = \beta_1 = \beta_2$ = 0.95 and γ_2 = 0.05, the limited number N of available simulations:

– limits the analysis on the estimation of the grace time available before core uncovering with the desired γ_2 and β_2;

– is not large enough to allow for an estimate of $\hat{y}_t$ with γ_2 = 0.05 and β_2 = 0.95.

Therefore, in Table 2, we provide the result of the γ_2^{th} percentile of y_t, with as large as possible β_2, according to the two different approaches of "Bracketing" and "Coverage", as explained in Appendix A. Instead, in Table 3, we provide the results when the confidence in the estimation, i.e., β_2, is fixed to at least equal to 0.95 whereas the value of the estimated percentile γ_2 varies according to theory (Appendix A).

In general terms, all these simulations of y are "up to core uncovery", i.e., y reaches the lower threshold L in all the available simulations and, thus, the margin is estimated to be equal to 0. The DPSM of Eq. (3), however, provides the analyst with the additional information the grace time $\hat{y}_t$ (before the core uncovery), which is a main benefit of the DPSM with respect to a traditional safety margin. When the $\hat{y}_{\gamma_1}$ is equal to L, the value of the grace time $\hat{y}_t$ is the time available for taking counteracting/mitigation actions before core uncover.

Results of the computation of the DPSM for the case of subgroups are shown hereafter. It is worth mentioning that: (i) being only "up to core uncover" transients available for the DPSM quantification; (ii) being the $\hat{y}_{\gamma_1}$ equal to L (as shown before in Tables 2 and 3); (iii) being the number N of available simulations lower than 90 for each considered subgroup, we focus only on the estimation of the value $\hat{y}_t$ that, incidentally, as already said, cannot be estimated with both β_2 and γ_2 values, as required by regulatory guidances (as shown in Tables 2, 3). We first present in Table 4 the results when γ_2 = 0.05, even though with a reduced confidence β_2 in its estimation. As we can see, for each case considered, we rely on a different number N of available simulations. This is due to the fact that when we consider a variable fixed at a given value, the number of simulations reduces to only those that have as inputs the selected fixed value of that input variable and the combination of all the other possible values of the other input variables. We show that:

● the "Bracketing" approach generally provides a larger confidence β_2 for the estimation of the γ_2^{th} percentile of y_t than the "Coverage" approach;

● when we consider results obtained with fixed values of the inputs, the confidence β_2 generally unfavorably increases, being the number N of available simulations lower than when all possible values of x_1, x_2, x_3 and x_4 are simultaneously considered; the values of β_2, indeed, go from 0.98 and 0.94 ("Bracketing" and "Coverage", respectively), to 0.36 and 0.24 (when x_3 is kept fixed and N = 18);

● the worst case (i.e., the shortest grace time available for counteracting the developing accident $\hat{y}_t$ = 7406 s) corresponds to the scenario in which a leakage rate x_2 = 480 gpm/RCP occurs at the beginning of the scenario (x_1 = 0 s) and operators act after twenty minutes (x_3 = 20 min) with strategy x_4 = "A".

Table 4
DPSM results for Seal LOCA simulations (fixed N and γ).

		N	γ_2	β_2"Bracketing"	β_2"Coverage"	$\hat{y}_t$ [s]
	All possible values of x_1, x_2, x_3 and x_4 are considered simultaneously	90	0.05	0.98	0.94	7406
$\mathbf{x_1[min]}$	0	30	0.05	0.62	0.45	7406
is kept fixed	13	30	0.05	0.62	0.45	8516
	30	30	0.05	0.62	0.45	9555
$\mathbf{x_2}$[gpm/RCP]	76	30	0.05	0.62	0.45	30713
is kept fixed	182	30	0.05	0.62	0.45	15118
	480	30	0.05	0.62	0.45	7406
$\mathbf{x_3}$[min]	20	18	0.05	0.36	0.24	7406
is kept fixed	30	18	0.05	0.36	0.24	8298
	40	18	0.05	0.36	0.24	7608
	50	18	0.05	0.36	0.24	7544
	60	18	0.05	0.36	0.24	7599
$\mathbf{x_4}$	A	45	0.05	0.81	0.67	7406
is kept fixed	B	45	0.05	0.81	0.67	7544

Table 5
DPSM results for Seal LOCA simulations (fixed N and β).

		N	β_2	γ_2 "Bracketing"	γ_2 "Coverage"	$\hat{y}_t$ [s]
	All possible values of x_1, x_2, x_3 and x_4 are considered simultaneously	90	0.95	0.04	0.03	7406
$x_1[\mathbf{min}]$	0	30	0.95	0.12	0.1	7406
is kept fixed	13	30	0.95	0.12	0.1	8516
	30	30	0.95	0.12	0.1	9555
x_2 [gpm/RCP]	76	30	0.95	0.12	0.1	30713
is kept fixed	182	30	0.95	0.12	0.1	15118
	480	30	0.95	0.12	0.1	7406
x_3[min]	20	18	0.95	0.19	0.16	7406
is kept fixed	30	18	0.95	0.19	0.16	8298
	40	18	0.95	0.19	0.16	7608
	50	18	0.95	0.19	0.16	7544
	60	18	0.95	0.19	0.16	7599
x_4	A	45	0.95	0.08	0.07	7406
is kept fixed	B	45	0.95	0.08	0.07	7544

In a similar way, Table 5 presents the results of estimating the value of γ_2 with β_2 =0.95, and both "Bracketing" and "Coverage" approaches. The goal is to provide the γ_2 estimates with the desired confidence, even though it cannot be the 95th. We show that:

- when β_2 is fixed, the "Bracketing" approach provides an unfavorable estimate of the γ_2^{th} percentile with fixed β_2 with respect to the "Coverage" approach.;
- when we consider results obtained with fixed values of the inputs, the value of the percentile that can be estimated unfavorably increases, being the number N of available simulations lower than when all possible values of x_1, x_2, x_3 and x_4 are simultaneously considered; the values of γ_2, indeed, go from 0.04 and 0.03 ("Bracketing" and "Coverage", respectively), to 0.19 and 0.16 (when x_3 is kept fixed and N =18).
- the worst case (i.e., the shortest grace time available for counteracting the developing accident $\hat{y}_t$ = 7406 s) corresponds to the scenario in which a leakage rate x_2 = 480 gpm/RCP occurs at the beginning of the scenario (x_1 = 0 s) and operators act after twenty minutes (x_3 = 20 in) with strategy x_4 ="A".

3.1.3.2. Sensitivity analysis. On the basis of the results shown in Tables 4, 5, the proposed sensitivity index of Eq. (10) has been computed for each input variable x_k, k=1, 2, 3, 4 (see Section 2.2). Results are shown in Table 6, where in column 2 the possible values $x_{k,i}$ of x_k are listed, in column 3 the estimated values of the grace time $\hat{y}_t$ are listed, in columns 4 and 5 the variability range of the normalized input Δx_k (as explained in Section 2.2) and the variability range $\Delta \hat{y}_t$ of the

Table 6
Results of the sensitivity analysis for the Seal LOCA case study.

x_k	$x_{k,i}$	$\hat{y}_t$	Δx_k	$\Delta \hat{y}_t$	I_{x_k}
$\mathbf{x_1[min]}$	0	7406	1.00	0.23	0.23
	13	8516			
	30	9555			
$\mathbf{x_2}$[gpm/RCP]	76	30713	0.84	0.76	**0.90**
	182	15118			
	480	7406			
$\mathbf{x_3}$[min]	20	7406	0.67	0.11	0.16
	30	8298			
	40	7608			
	50	7544			
	60	7599			
x_4	A	7406	0.89	0.02	0.02
	B	7544			

normalized $\hat{y}_t$, are listed respectively, for the simulations where each input variable is kept fixed. Finally, in the last column, the value of the sensitivity index I_{x_k} computed for each input variable is shown.

Based on the results of the sensitivity index I_x shown in Table 6, we can conclude that x_2 (the leakage rate) is the input variable that most affects the grace time, followed by x_1 (time of the leakage rate increase after the SBO). On the other hand, x_3 (the time of the activation of the

secondary cooling by operators) and x_4 (the strategy they adopt for this) have little influence on the grace time and, thus, on the safety margin.

Since the dynamic variables x_3 and x_4 are not the most influencing the output, a static probabilistic safety assessment is considered sufficient for the analysis of a Seal LOCA following an SBO accident in a 3-loops PWR. The related following probabilistic analysis will focus only on the role of the leakage rate, and, eventually, of the time of the leakage rate increase. For this, we will resort to the models proposed by the Westinghouse Owners Group and named the WOG2000 and the WOG2000 (revised), the model revised by the US Nuclear Regulatory Commission (NRC), to build the static ETs for the computation of the probabilities of occurrence of the accident scenarios considered.

3.1.4. The Seal LOCA ETs models

For the safety assessment of the Seal LOCA accidental scenario considered, we calculate its probability of occurrence with static ETs, defined as WOG2000 and WOG2000 (revised) [31] that essentially differ in:

- the assumption on the time of the leakage rate increase after the SBO (30 min for the WOG2000, 0 and 13 min for the WOG2000 (revised));
- the value of the popping-open/binding failure probability of the third seal stage (this is explicitly accounted for the WOG2000, whereas it is not for the WOG2000 (revised) that assumes the failure can occur only when the second seal stage fails);
- the assumption on the seal failure probability due to O-ring extrusion (a value of 0.5 is assigned to the probability of occurrence of this failure mode in the WOG2000 (revised), whereas it is set equal to zero in the WOG2000, since this latter assumes the Reactor Coolant System (RCS) pressure is kept lower than 118 bar within two hours, avoiding O-ring extrusion).

These models define the first, second and third failure probabilities, for each seal failure mode (i.e., popping-open, binding, O-ring extrusion). However, a single probability is defined for the popping-open and binding failure mode as for the high-temperature O-ring failure mode (to which both the probabilistic models refer), and the binding failure mode is negligible. Each ET branch is characterized by a leakage rate probability that depends on the number of failed seals and by the probability of the different failure modes (i.e., popping-open, binding, O-ring extrusion), as listes in Table 7.

Fig. 3 shows the static ET for the WOG2000 model, whereas Fig. 4 the static ET for the WOG2000 (revised). Figs. 3 and 4 show the branches that arise from an initiating event of SBO (with the consequent loss of the seal cooling), evolving according to the failure of the different seals. In the ETs, we can notice that O-ring extrusion is not considered for any of the models, since it has been demonstrated that the condition provided by the WOG2000 (revised) (depressurization resulting in a RCS pressure lower than 118 bar within two hours) leads to a probability of failure equal to zero.

The different number of possible sequences is due to the fact that the WOG2000 model considers five possible leakage rates (21, 57, 76,

182, 480 gpm/RCP), whereas four leakages (21, 76, 182, 480 gpm/RCP) are considered for the WOG2000 (revised) model because in this latter model, as already said, third seal fails with the second seal, otherwise it does not fail.

The static ETs can be used for the quantification of the different probabilistic models for the Seal LOCA. For this purpose, a probability has been assigned arbitrarily to each discrete possible value of the input variables of the dynamic simulations (in particular, for x_3 and x_4). Referring for example to x_3, we have arbitrarily assigned a value to the probability that x_3 assumes the value $x_{3,1}$ (i.e., $P(x_3 = x_{3,1})$), $x_{3,2}$ (i.e., $P(x_3 = x_{3,2})$), $x_{3,3}$ (i.e., $P(x_3 = x_{3,3})$), $x_{3,4}$ (i.e., $P(x_3 = x_{3,4})$) and $x_{3,5}$ (i.e., $P(x_3 = x_{3,5})$), where $P(x_3 = x_{3,1}) + P(x_3 = x_{3,2}) + P(x_3 = x_{3,3}) + P(x_3 = x_{3,4}) + P(x_3 = x_{3,5}) = 1$. Analogously, we have assumed $P(x_4 = "A")$, $P(x_4 = "B")$. Whereas, for x_2, probabilities that x_2 assumes its possible values (i.e., 21, 57, 76, 182 and 480 gpm/RCP) are defined by the different branches probabilities of the static ET (defined by the probabilistic model).

The probabilities assigned for each possible value of the inputs x_3 and x_4 are listed in Table 8.

Since each simulation, fed by a given input vector $\bar{x} = \{x_1, x_2, x_3, x_4\}$, leads to a core uncovery at time y_t, we can define the probability to have core uncovery at time y_t as the conditional probability that $\bar{x}$ assumes the corresponding input values (considering fixed both the value of x_1 by the probabilistic model and of x_2, as the different leakage rates have been considered separately). Correspondingly, for each scenario (and, thus, for each simulation), we can calculate the Core Damage Probability (P_{CD}), defined, in general, as the probability of the occurrence of core uncovery at y_t, conditioned to the probability that the recovery of AC power (with the consequent restoration of safety systems to mitigate the consequences of the Seal LOCA) occurs at t_{rec} after the uncovery at y_t and, thus, the AC power recovery does not contribute to preventing the core damage. We assume the recovery time t_{rec} to follow a lognormal distribution with a mean value of 10800 s.

Tables 9–11 show the values of the P_{CD} and the accident sequence risk (computed by multiplying by the leakage initiating event probabilities) for the different probabilistic models, WOG2000, WOG2000 (revised) with $x_1 = 13$ min, and the WOG2000 (revised) with $x_1 = 0$ min, respectively.

For each probabilistic model, the P_{CD} for each leakage rate x_2 is listed in the second column of the tables: this is defined as the sum of the P_{CD} calculated with fixed x_2 and x_1 (that is fixed by the probabilistic model) and all the possible combinations P_{CD} of x_3 and x_4. For instance, for the WOG2000 model (corresponding to $x_1 = 0$ min), the P_{CD} of $x_2 = 480$ gpm/RCP has been computed as the sum of all the P_{CD} computed for sequences of vectors $\bar{x} = \{0min, 480\frac{gpm}{RCP}, x_3, x_4\}$, with $x_3 = 20$ min, 30 min, 40 min, 50 min, 60 min and $x_4 = "A","B"$. It is worth mentioning that, even though no sequences were available for 21 gpm/RCP and 57 gpm/RCP we have assumed for the former negligible consequences, whereas for the latter the same core uncovery time of the case $x_2 = 76$ gpm/RCP, conservatively. The probability of occurrence of x_2, listed in the third column (as presented in Figs. 3 and 4), is multiplied by the computed P_{CD} to obtain the accident sequence probability related to each leakage rate listed in the fourth column. Finally, the total CD probability is the sum of the accident sequence probability related to all the leakage rates (i.e., 21, 57, 76, 182, 480 gpm/RCP for the WOG2000 and 21, 76, 182, 480 gpm/RCP for the WOG2000 (revised)) as reported in the fifth column.

We can conclude that WOG2000 (revised) with $x_1 = 0$ min provides the largest estimation of the CD probability that is contributed mostly by $x_2 = 480$ gpm/RCP and $x_2 = 182$ gpm/RCP. For the other models, only $x_2 = 480$ gpm/RCP really contributes to the CD probability, confirming the results of the DPSM-based sensitivity analysis of Section 3.1.3.2, that had identified x_2 as the input variable that most affects the available grace time. Moreover, this probabilistic analysis also confirms that the worst case (i.e., the shortest grace time available for counter-

Table 7
Probabilities of the branches of the RCP Seal LOCA ET models.

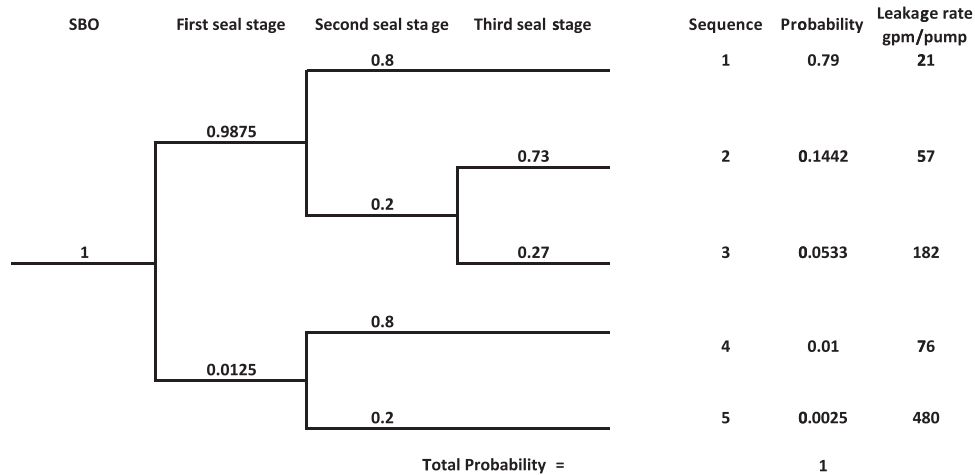| Failure mode		WOG2000 (x_1=30 min)	WOG2000 (revised) (x_1=13 min, x_1=0 min)
Popping-open Binding	1st Seal Stage	0.0125	0.0125
	2nd Seal Stage	0.2	0.2
	3rd Seal Stage	0.27	1 (only if the second seal stage fails)
O-ring extrusion		0	0.5

Fig. 3. WOG2000 static ET [21].

acting the developing accident $\hat{y}_t$ = 7406 s) corresponds to the scenario in which a leakage rate x_2 = 480 gpm/RCP occurs at the beginning of the scenario (x_1 = 0 s) and operators act after twenty minutes (x_3 =20 min) with strategy x_4 ="A".

As a last remark, it is worth mentioning that an increase of x_1 =13 min of the time of the leakage rate increase for the WOG2000 (revised) implies the total CD probability to be reduced of approximately 55% with respect to the same probabilistic model but with x_1=0 min. Whereas, a further increase of the time of the leakage rate increase up to x_1 = 30 min (WOG2000) implies a reduction of approximately 31% with respect to the WOG2000 (revised) model with x_1 =13 min. Therefore, the reduction is not significant for a relevant increase of x_1, that, again, confirms the results of the DPSM-based sensitivity analysis that ranks x_1 lower than x_2 with respect to its effects on the accident progression.

3.2. U-Tube Steam Generator

3.2.1. The system

A schematic of a U–Tube Steam Generator (UTSG) of a NPP is shown in Fig. 5. This system has been chosen because several studies have shown that its malfunction can be considered as one of the major causes of NPP unavailability [11,16,18].

The reactor coolant enters the UTSG at the bottom, moves upward and then downward in the inverted U-tubes, transferring heat to the secondary fluid before exiting at the bottom. The secondary fluid, the feed water (Q_e), enters the UTSG at the top of the downcomer, through the space between the tube bundle wrapper and the SG shell. The value

Table 8
Probabilities arbitrarily assigned for x_3 and x_4.

x_i	$x_{k,i}$	$P(x_i = x_{k,i})$
x_3 [min]	20	0.42
	30	0.17
	40	0.15
	50	0.14
	60	0.12
x_4	"A"	0.6
	"B"	0.4

Table 9
WOG2000.

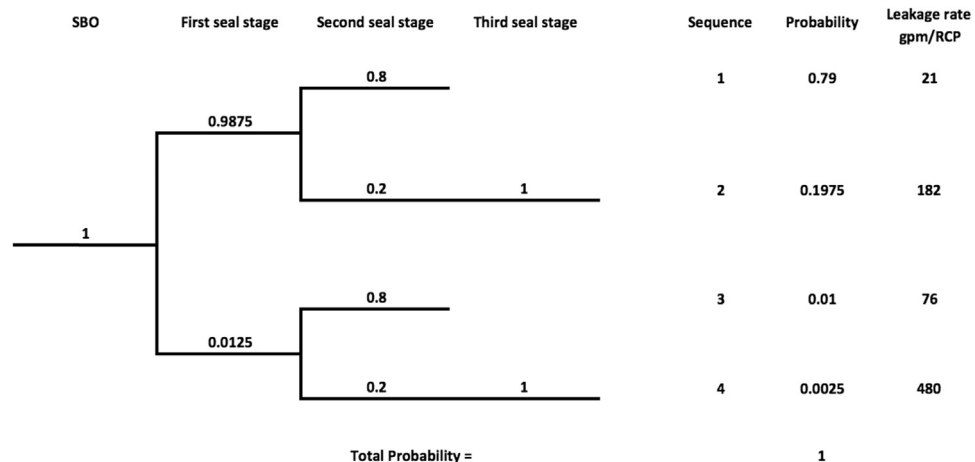| Leakage rate x_2	P_{CD}	Probability of occurrence	Accident sequence	CD probability
21 gpm/ RCP	0	0.79	0	1.35E-003
57 gpm/ RCP	0	0.1442	0	
76 gpm/ RCP	0	0.01	0	
182 gpm/ RCP	1.15E-004	0.0533	6.14E-006	
480 gpm/ RCP	5.36E-001	0.025	1.34E-003	

Fig. 4. WOG2000 (revised) static ET [21].

Table 10
WOG2000 (revised) with x_1 = 13min.

Leakage rate x_2	P_{CD}	Probability of occurrence	Accident sequence	CD probability
21 gpm/ RCP	0	0.79	0	1.93E-003
57 gpm/ RCP	–	–	–	–
76 gpm/ RCP	0	0.01	0	
182 gpm/ RCP	2.65E-004	0.1975	5.23E-005	
480 gpm/ RCP	7.15E-001	0.025	1.88E-003	

Table 11
WOG2000 (revised) with x_1 = 0min.

Leakage rate x_2	P_{CD}	Probability of occurrence	Accident sequence	CD probability
21 gpm/ RCP	0	0.79	0	4.26E-003
57 gpm/ RCP	–	–	–	–
76 gpm/ RCP	1.37E-008	0.01	1.37E-010	
182 gpm/ RCP	9.86E-003	0.1975	1.95E-003	
480 gpm/ RCP	9.26E-001	0.025	2.31E-003	

Fig. 5. Schematic of the UTSG [IAEA-TECDOC-981, 1997].

of Q_e is regulated by a system of valves: a low flow rate valve, used when the operating power (P_o) is smaller than 15% of nominal power (P_n), and a high flow rate valve when $P_o > 0.15 P_n$ [Aubry et al., 2012]. In the secondary side of the tube bundle, water heats up, reaches saturation, starts boiling and turns into a two-phase mixture. The two-phase fluid moves up through the separator/riser section, where steam is separated from liquid water, and through the dryers, which ensure that the

exiting steam (Q_v) is essentially dry [6]. The separated water is recirculated back to the downcomer. The balance between the exiting Q_v and the incoming Q_e governs the change in the water level in the SG. Because of the two-phase nature, two types of water level measurements are considered, as shown in Fig. 5, each reflecting a different level concept: the Narrow Range Level (N_{rl}) is calculated by pressure difference between two points close to the water level and indicates the mixture level, whereas the Wide Range Level (W_{rl}) is calculated by pressure difference between the two extremities of the SG (steam dome and bottom of the downcomer) and indicates the collapsed liquid level that is related with the mass of water in the SG [6].

The goal of the system is to maintain the N_{rl} (y) at a reference position y_{ref}=151.67 cm. The SG fails if y rises (falls) above (below) the threshold U =177.417 cm (L =106.2 cm), that triggers an automatic turbine trip. Indeed, if the y exceeds U, the steam separator and dryer lose their functionality and excessive moisture is carried in Q_v, degrading the turbine blades profile and the turbine efficiency; if y decreases below L, insufficient cooling capability of the primary fluid occurs. Similarly, the W_{rl} is relevant for the cooling capability of the primary circuit [16].

A dedicated model of the system has been implemented in SIMULINK to simulate the dynamic response of the UTSG at different P_o values [6]. In this model, both feedforward and feedback digital control schemes have been adopted. The feedback controller is a PID that provides a flow rate Q_{pid} resulting from the residuals between y and y_{ref}, whereas the feedforward controller operates a safety relief valve that is opened if and only if y exceeds the N_{hl} (which is an upper pre-alarm), and removes a constant flow rate (Q_{sf}).

Multiple component failures considered can occur during system operation continuously at random time between [0,4000] (s). This mission time (T_{miss}=4000s) has been chosen in order to account for the complete development also of slow dynamic accident scenarios [6].

Components can fail according to different magnitudes of the failure. In particular:

1. The outlet steam valve can fail in three different positions: i) closed; ii) stuck open at 50% of the nominal Q_v that should be provided at P_o; iii) stuck open at 150% of the nominal Q_v that should be provided at P_o.
2. The communication between the sensor that monitors y and the PID controller can fail, returning the same input value of the previous time step.
3. The safety relief valve can fail at a uniform random value Q_{sf} in the range [0.5, 50.5] (kg/s).
4. The PID controller can fail providing a uniform random flow rate Q_{pid} belonging to [−18, 18] % of the nominal Q_e that should be provided at P_o.

Although in a real accident progression, timing, order and magnitude of failure events should assume continuous values, this would make the problem intractable within a classical PSA framework. To deal with this (and at the same time leveraging the computational demand) we have approximated the problem with discretized timing and magnitude values of the failure events in order to generate the dynamic scenarios. In particular, a Multiple Value Logic (MVL) for an approximated description of the continuous time of occurrence of component failures and their magnitudes has been adopted [6]. The MVL allows describing a situation in which the components can fail at any (discrete) time along the scenario ($x_{1,comp}$, referring to a generic component $comp$) with different (discrete) magnitudes ($x_{2,comp}$) [6]. In the MVL vector, an additional variable ($x_{3,comp}$) indicates the order of occurrence of the different failure events in the sequence.

The discretization of the time and magnitudes values is as follows:

• time discretization: we refer to $x_{1,comp}$=1, $x_{1,comp}$=2, $x_{1,comp}$=3 and $x_{1,comp}$=4, for failures occurring in the intervals [0,1000] (s),
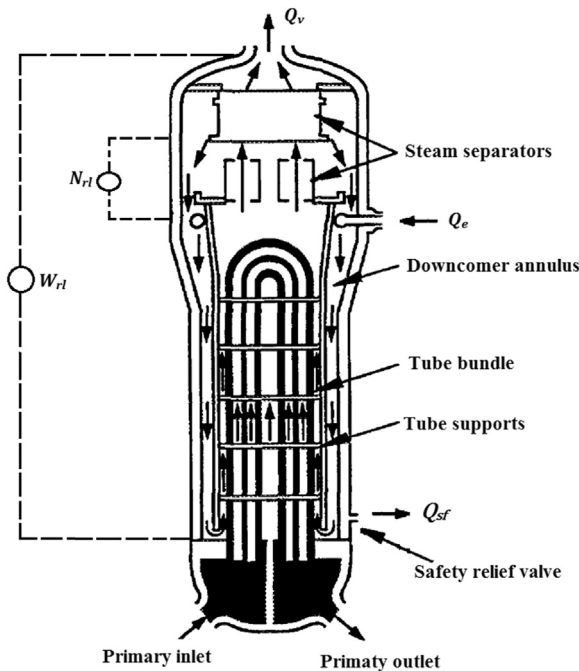
[1001,2000] (s), [2001,3000] (s), [3001,4000] (s), respectively; if the label $x_{1,comp}$=0, the component does not fail within the time of the whole scenario, T_{miss}.

- Magnitude discretization:

– the steam valve magnitude ($x_{2,steam}$) is indicated as 1, 2 or 3 for failure states corresponding to stuck at 0%, stuck at 50% and stuck at 150% of the Q_e value that should be provided at P_o, respectively; if $x_{2,steam}$ =0, the component does not fail in T_{miss};

– the communication between the sensor measuring y and the PID controller $x_{2,comm}$=0 if the communication works, $x_{2,comm}$=1 otherwise;

– the safety relief valve fails with magnitude $x_{2,safety}$ that can assume the values 1, 2, 3 and 4, if it is stuck between [0.5, 12.6) (kg/s), (12.6, 25.27) (kg/s), (25.27, 37.91) (kg/s) and (37.91, 50.5) (kg/s), respectively; $x_{2,safety}$=0, indicates that the component does not fail in T_{miss};

– the PID controller failure magnitude range is discretized into 8 equally spaced magnitude intervals, $x_{2,PID}$ labeled from 1 to 8, representative of failure states corresponding to discrete intervals of output value belonging to [−18,18]% of the Q_e value that should be provided at P_o; if $x_{2,PID}$=0, the component does not fail in T_{miss}.

The possible failure events combinations give rise to 100509 possible sequences, each described by a MVL vector. Among these sequences, in order to reproduce the same conditions of the previous case study for the comparison of the results, an arbitrary number N =90 of simulations have been randomly selected to challenge the DPSM sensitivity analysis method presented in Section 2 (i.e., we assume independent inputs and, therefore, as in Section 3.1.2, no joint distributions). For each dynamic simulation, the value y of the level that is reached along the scenario progression and the corresponding grace time y_t have been collected, $\bar{y}$ and $\bar{y}_t$ respectively. In particular, when $y = U$ = 177.417 cm is reached (and, thus, the corresponding safety margin is 0), we record the grace time y_t for reaching the threshold; otherwise, for the scenarios in which $y < U$, during the entire accidental progression, the maximum value reached by y and the corresponding grace time y_t at which it is reached are recorded.

3.2.2. DPSMs and sensitivity analysis results

3.2.2.1. The DPSMs.
The collected values of $\bar{y}$ and $\bar{y}_t$(i.e., the Narrow Range Level N_{r-l} and the corresponding time, respectively) have been employed for the calculation of the DPSMs (see Section 2.2). Since the alarm triggers either when N_{r-l} falls below the lower threshold L or rises above the upper threshold U, we focus, without loss of generality, on the upper threshold U. Resorting to OS, we have estimated the values of the γ_1^{th} and γ_2^{th} percentiles, with confidences β_1 and β_2, of the Narrow Range Level y and of the time at which this level is reached. This has been determined using all the N =90 simulations, as well as all the subgroups, that is, considering the simulations when each input variable is kept fixed, and components are analyzed independently.

In Tables 12, 13, we report $\hat{y}_{\gamma_1}$, the value of $\hat{y}_t$ and the values of the DPSM for two different cases (γ_2 and β_2 is fixed, respectively), when all the N =90 simulations results are considered.

Results of the computation of DPSM for the case in which all the N

Table 12
DPSM (N=90 and with fixed γ₂) for the UTSG.

γ_2	β_2 "Bracketing"	β_2 "Coverage"	$\hat{y}_{\gamma_1}$[cm]	$\hat{y}_t$ [s]	DPSM
0.05	0.98	0.94	177.417 = U	213	0 within a grace time of 213 s

Table 13
DPSM (N=90 and with fixed β₂) for the UTSG.

β_2	γ_2 "Bracketing"	γ_2 "Coverage"	$\hat{y}_{\gamma_1}$[cm]	$\hat{y}_t$ [s]	DPSM
0.95	0.04	0.03	177.417 = U	213	0 within a grace time of 213 s

=90 available simulations are used simultaneously is shown in Tables 12, 13. The estimation of the value of the Narrow Range Level $\hat{y}$ results equal to U. The DPSM of Eq. (3) provides the additional information of the grace time $\hat{y}_t$ = 213 s (to reach the alarm triggering).

DPSM provides the analyst with the additional information of the grace time $\hat{y}_t$ (before the alarm triggering), which is a main benefit of the DPSM with respect to the traditional safety margin. This means that, when $\hat{y}_{\gamma_1}$is equal to U, the value of the grace time $\hat{y}_t$ is the time available for taking counteracting/mitigation actions before alarm triggering. It is worth mentioning that, even though the regulation guidances prescribe the DPSM to be given with $\gamma_1 = \beta_1 = \beta_2$ =0.95 and γ_2 =0.05, the limited number N of available simulations:

– limits the analysis on the estimation of the grace time available before core uncover with the desired γ_2 and β_2;
– is not large enough to allow for an estimate of $\hat{y}$ with γ_2 =0.05 and β_2=0.95).

Therefore, in Table 12, we provide the results when we aim at estimating exactly the γ_2^{th} percentile of y_t, with the as large as possible β_2 according to the two different approaches ("Bracketing" and "Coverage" as explained in Appendix A). On the contrary, in Table 13, we provide the result when the confidence in the estimation, i.e., β_2, is fixed to at least equal to 0.95 whereas the value of the estimated percentile γ_2 varies as theory.

Results of the computation of DPSM for the case of subgroups are shown hereafter. It is worth mentioning that: (i) being the computed $\hat{y}_{\gamma_1}$ equal to U (as shown before in Tables 12, 13); (ii) being the number N of available simulations lower than 90 for each considered subgroup, and each component separately, we focus only on the estimation of the value $\hat{y}_t$ that, incidentally, cannot be estimated with both $\beta_2$and $\gamma_2$with the values, as required by regulation guidances. The reduced number N of simulations results is due to the fact that, when we consider a variable to be kept fixed at a given value of its possible instances, the number of available simulations reduces to only those that have as inputs the selected fixed value of that input variable and the combination of all the other possible values of the other input variables.

Results of the computation of DPSM for the case of subgroups (and focusing on the single component) are shown hereafter. Tables 14–17 show the DPSM quantification when the steam valve, the communication, the safety valve and the PID fail independently, respectively.

In particular, in Table 14, the results of the estimated grace time $\hat{y}_t$, when the steam valve fails, are shown, when a different number N of simulations are available due to the input $x_{1,steam}$, $x_{2,steam}$, $x_{3,steam}$ being kept fixed at given values. As already said, both the case when γ_2 is fixed and $\beta_2$is fixed are presented.

Similarly to the first case study, we find that:

- the "Bracketing" approach generally provides a larger confidence β_2 for the estimate of the γ_2^{th} percentile of y_t than the "Coverage" approach. Contrarily, when β_2 is fixed, the "Bracketing" approach provides unfavorable estimated value of the γ_2^{th} percentile with fixed β_2 with respect to the "Coverage" approach.
- When we consider results obtained with fixed values of the inputs, the value of the percentile that can be estimated unfavorably increases, being the number N of available simulations lower than when all simulations are simultaneously considered; the values of γ_2,

Table 14
DPSM for the steam valve.

		N	β_2 "Bracketing" γ_2 =0.05	β_2 "Coverage"	γ_2 "Bracketing" β_2 =0.95	γ_2 "Coverage"	$\hat{y}_t$
	All simulations values of $x_{1,\ steam}$, $x_{2,\ steam}$ and $x_{3,\ steam}$ accounted	90	0.98	0.94	0.04	0.03	213
$x_{1,\ steam}$ Time is kept fixed	1	17	0.34	0.22	0.19	0.17	213
	2	26	0.54	0.38	0.13	0.11	544
	3	24	0.5	0.35	0.14	0.12	266
	4	11	0.19	0.11	0.28	0.25	544
$x_{2,steam}$ Magnitude is kept fixed	0	12	0.21	0.13	0.26	0.23	312
	1	19	0.39	0.25	0.18	0.15	318
	2	32	0.65	0.49	0.11	0.09	213
	3	27	0.56	0.40	0.13	0.11	253
$x_{3,steam}$ Order is kept fixed	1	19	0.39	0.25	0.18	0.15	253
	2	29	0.6	0.44	0.12	0.1	213
	3	18	0.36	0.24	0.18	0.16	307
	4	12	0.21	0.13	0.26	0.23	266

indeed, go from 0.04 and 0.03 ("Bracketing" and "Coverage", respectively), to 0.28 and 0.25 (when $x_{1,steam}$=4 is kept fixed and N =11). Similarly, we can see that the confidence β_2 unfavorably decreases, when the value of γ_2 is fixed to 0.05. The values of β_2, indeed, go from 0.98 and 0.94 ("Bracketing" and "Coverage", respectively) for the best case with N =90, to 0.19 and 0.11 (when $x_{1,steam}$=4 is kept fixed and N =11);

- The worst case (i.e., the shortest grace time available for counteracting the developing accident $\hat{y}_t$ =213 s) corresponds to the scenario in which the failure of the steam valve occurs at time $x_{1,steam}$=1, with magnitude $x_{2,steam}$=2 when the failure is the second event of the progression, $x_{3,steam}$=2.

In Table 15, the results of the estimated grace time $\hat{y}_t$ when the communication between the sensor and the PID fails, are shown, for a different number N of simulations with the input $x_{1,comm}$, $x_{2,comm}$, $x_{3,comm}$ kept fixed at given values. As already said, both the case when γ_2 is fixed and β_2 is fixed are presented. The insight from the results obtained are similar to the ones obtained before.

In Table 16, the results of the estimated grace time $\hat{y}_t$ when the safety valve fails, are shown, for a different number N of simulations, with the input $x_{1,safety}$, $x_{2,safety}$, $x_{3,safety}$ kept fixed at given values. As already said, both the case when γ_2 is fixed and β_2 is fixed are presented.

Also in this case, the insight from the results obtained are similar to the ones obtained before.

In Table 17, the results of the estimated grace time $\hat{y}_t$, when the PID controller fails, are shown, for a different number N of simulations, with the input $x_{1,PID}$, $x_{2,PID}$, $x_{3,PID}$ kept fixed at given values. As already said, both the case when γ_2 is fixed and secondly, the β_2 is fixed are presented. Results obtained are similar to the previous ones.

3.2.2.2. Sensitivity analysis. On the basis of the results shown from Table 14 to Table 17, the proposed sensitivity index of Eq. (10) has been computed for each input variable x_k, k=1, 2, 3 (see Section 2.2), considering the components independently. Results, referred to each component, are shown in Tables 18–21, where in column 2 the possible values $x_{k,i}$ of x_k are listed, in column 3 the estimated values of the grace time $\hat{y}_t$ are listed, in columns 4 and 5 the variability range of the normalized input Δx_k (as explained in Section 2.2) and the variability range $\Delta \hat{y}_t$ of the normalized $\hat{y}_t$, are listed respectively, when only the simulations when each input variable is kept fixed are considered. Finally, in the last column, the value of the sensitivity index I_{x_k} computed for each input variable is shown.

In Table 18, the results of the sensitivity analysis referred to the

Table 15
DPSM for the communication between the sensor and the PID controller.

		N	β_2 "Bracketing" γ_2 =0.05	β_2 "Coverage"	γ_2 "Bracketing" β_2 =0.95	γ_2 "Coverage"	$\hat{y}_t$ [s]
	All simulations values of $x_{1,comm}$, $x_{2,comm}$ and $x_{3,comm}$ accounted	90	0.98	0.94	0.04	0.03	213
$x_{1,\ comm}$ Time is kept fixed	1	21	0.43	0.29	0.16	0.14	213
	2	18	0.36	0.24	0.18	0.16	318
	3	18	0.36	0.24	0.18	0.16	307
	4	20	0.41	0.27	0.17	0.15	335
$x_{2,comm}$ Magnitude is kept fixed	0	13	0.24	0.14	0.25	0.22	213
	1	77	0.96	0.90	0.05	0.04	213
$x_{3,comm}$ Order is kept fixed	1	19	0.39	0.25	0.18	0.15	544
	2	26	0.54	0.38	0.13	0.12	266
	3	19	0.39	0.25	0.18	0.15	213
	4	13	0.24	0.14	0.25	0.22	307

Table 16
DPSM for the safety valve.

		N	β_2 "Bracketing" $\gamma_2 =0.05$	β_2 "Coverage"	γ_2 "Bracketing" $\beta_2 =0.95$	γ_2 "Coverage"	$\hat{y}_t$ [s]
	All simulations values of $x_{1.safety}$, $x_{2.safety}$ and $x_{3.safety}$ accounted	90	0.98	0.94	0.04	0.03	213
$x_{1, safety}$ Time is kept fixed	1	18	0.36	0.24	0.18	0.16	213
	2	27	0.56	0.40	0.13	0.11	253
	3	19	0.39	0.25	0.18	0.15	312
	4	23	0.48	0.33	0.15	0.13	213
$x_{2,safety}$ Magnitude is kept fixed	0	3	0.02	0.01	0.71	0.67	9000
	1	13	0.24	0.14	0.25	0.22	1253
	2	23	0.48	0.33	0.15	0.13	213
	3	28	0.58	0.42	0.12	0.11	312
	4	23	0.48	0.33	0.15	0.13	213
$x_{3,safety}$ Order is kept fixed	1	25	0.52	0.37	0.14	0.12	1221
	2	17	0.34	0.22	0.20	0.17	307
	3	29	0.6	0.44	0.12	0.1	213
	4	16	0.31	0.2	0.11	0.18	213

failure events of the steam valve are presented. The steam valve failure time $x_{1,steam}$ is the input that most affects the grace time $\hat{y}_t$ available, whereas the failure magnitude $x_{2,steam}$ and the order of the failure $x_{3,steam}$ along the accidental sequence of events have almost the same (low) influence on the output $\hat{y}_t$.

In Table 19, the results of the sensitivity analysis referred to the failure of the communication between the sensor and the PID controller are shown.

The failure magnitude $x_{2,comm}$ appears to be irrelevant for the $\hat{y}_t$, ($\Delta\hat{y}_t$ =0), in both cases of communication working ($x_{2,comm}$=0) or failed ($x_{2,comm}$=1). However, the order $x_{3,comm}$ at which communication fails along the accidental sequence is the most important input for the quantification of $\hat{y}_t$.

The results of sensitivity analysis referred to the safety valve failure are shown in Table 20. The failure magnitude $x_{2,safety}$ and the failure order along the accidental sequence $x_{3,safety}$ have a large influence on $\hat{y}_t$,

Table 18
Sensitivity analysis for the steam valve.

x_k	$x_{k,i}$	$\hat{y}_t$	Δx_k	$\Delta\hat{y}_t$	I_{x_k}
$x_{1,steam}$	1	213	0.75	0.61	**0.81**
	2	544			
	3	266			
	4	544			
$x_{2,steam}$	1	318	0.67	0.33	0.49
	2	213			
	3	253			
$x_{3,steam}$	1	253	0.75	0.31	0.41
	2	213			
	3	307			
	4	266			

Table 17
DPSM for the PID.

		N	β_2 "Bracketing" $\gamma_2 =0.05$	β_2 "Coverage"	γ_2 "Bracketing" $\beta_2 =0.95$	γ_2 "Coverage"	$\hat{y}_t$ [s]
	All simulations values of $x_{1.PID}$, $x_{2.PID}$ and $x_{3.PID}$ accounted	90	0.98	0.94	0.04	0.03	213
$x_{1,PID}$ Time is kept fixed	1	18	0.36	0.24	0.19	0.16	213
	2	27	0.56	0.4	0.13	0.11	544
	3	19	0.39	0.25	0.18	0.15	503
	4	23	0.48	0.33	0.15	0.13	1253
$x_{2,PID}$ Magnitude is kept fixed	0	0	0	0	0	0	0
	1	10	0.16	0.09	0.31	0.28	544
	2	10	0.16	0.09	0.31	0.28	213
	3	12	0.21	0.13	0.26	0.23	307
	4	19	0.39	0.25	0.18	0.15	266
	5	10	0.16	0.09	0.31	0.28	253
	6	9	0.14	0.08	0.34	0.3	1503
	7	15	0.29	0.18	0.22	0.19	1253
	8	5	0.05	0.03	0.52	0.48	1253
$x_{3,PID}$ Order is kept fixed	1	21	0.43	0.29	0.16	0.14	213
	2	23	0.48	0.33	0.15	0.13	253
	3	14	0.26	0.16	0.23	0.2	503
	4	32	0.65	0.49	0.11	0.09	1253

Table 19
Sensitivity analysis for the communication between the sensor and the PID controller.

x_k	$x_{k,i}$	$\hat{y}_t$	Δx_k	$\Delta \hat{y}_t$	I_{x_k}
$x_{1,comm}$	1	213	0.75	0.36	0.49
	2	318			
	3	307			
	4	335			
$x_{2,comm}$	0	213	1	0	0
	1	213			
$x_{3,comm}$	1	544	0.75	0.61	**0.81**
	2	266			
	3	213			
	4	307			

Table 20
Sensitivity analysis for the safety valve.

x_k	$x_{k,i}$	$\hat{y}_t$	Δx_k	$\Delta \hat{y}_t$	I_{x_k}
$x_{1,safety}$	1	213	0.75	0.32	0.42
	2	253			
	3	312			
	4	213			
$x_{2,safety}$	1	1253	0.75	0.83	**1.10**
	2	213			
	3	312			
	4	213			
$x_{3,safety}$	1	1221	0.75	0.83	**1.10**
	2	307			
	3	213			
	4	213			

Table 21
Sensitivity analysis for the PID.

x_k	$x_{k,i}$	$\hat{y}_t$	Δx_k	$\Delta \hat{y}_t$	I_{x_k}
$x_{1,PID}$	1	213	0.75	0.83	**1.10**
	2	544			
	3	503			
	4	1253			
$x_{2,PID}$	1	544	0.875	0.86	0.98
	2	213			
	3	307			
	4	266			
	5	253			
	6	1503			
	7	1253			
	8	1253			
$x_{3,PID}$	1	213	0.75	0.83	**1.10**
	2	253			
	3	503			
	4	1253			

whereas the failure time $x_{1,safety}$ has smaller influence on $\hat{y}_t$.

The results for the failure of the PID are shown in Table 21. Although the failure magnitude $x_{2,PID}$ is relevant for the quantification of $\hat{y}_t$, the failure time $x_{1,PID}$ and the failure order along the accidental sequence $x_{3,PID}$ affect $\hat{y}_t$ with a larger extent.

In conclusion, we can claim that dynamic aspects are critical for the estimation of $\hat{y}_t$ for the UTSG system: sensitivity analysis results, indeed, show that, among the different inputs considered ($x_{1,comp}$, $x_{2,comp}$, $x_{3,comp}$), the failure time $x_{1,steam}$ affects the quantification of $\hat{y}_t$ when the failure of the steam valve is considered, the failure magnitude

$x_{2,safety}$ and the failure order $x_{3,safety}$, affects $\hat{y}_t$ when the failure of the safety valve is considered, the failure time $x_{1,PID}$ and the failure order $x_{3,PID}$ affects $\hat{y}_t$ when the failure of the PID is considered and finally, the failure order $x_{3,comm}$ influences $\hat{y}_t$ when the failure of the communication between the sensor and the PID controller is taken into account. Although a comprehensive analysis should consider all the number of possible sequences of events originated by the MVL approximation of Section 3.2.1, the results here provided based on only N =90 randomly selected sequences of events are sufficient to conclude that a DET analysis is needed rather than a static ET analysis. In next Section, we will briefly show the advantages of a DET, that accounts for the different times, magnitude and order of failure events, with respect to a static ET for the case study here considered.

3.2.3. The Dynamic Event Tree

In this Section, supported by the outcomes of the sensitivity analysis of Section 3.2.2.2, a DET methodology is used to account for the system dynamics along the accidental sequences progression (considering the timing $x_{1,comp}$, the magnitude $x_{2,comp}$ and the order $x_{3,comp}$ of failure events for the different components) and to compute the probability of occurrence of the accidental scenarios.

A DET is in principle similar to a static ET (where the sequence of system responses following an initiating event is predetermined by the analyst) except that, in a DET, both the timing and sequence of system responses are determined by a time-dependent model of system evolution, and only the branching rules are determined by the analyst [1]. The time-dependent model of the systems allows for a MVL description of components states which, therefore, accounts for different timing, order and magnitude of the possible failure events, leading, consequently, to a multitude of possible scenarios much larger than for a static ET analysis.

Among the scenarios, the identification of Prime Implicants (PIs) is fundamental for the calculation of the probability of failure of the system and for the analysis of such a system. PIs correspond, indeed, to the Minimal Cut Sets (MCS) of the static ET, but are also supplied with the information of time, sequence and magnitude of failures occurrences. [7,9,24]. Moreover, PIs identification allows for a more accurate characterization of failure sequences of non−coherent systems, that are those systems where both the failed or the working states of a component can lead to the system failure [6], as it is for the UTSG hereafter analyzed.

Another important category of sequences arises when dynamics is considered in the analysis that are the so called Near Misses, which are sequences (among safe scenarios), whose sequences of events lead the safety parameter values close to, but not exceeding, the corresponding acceptable thresholds [33]. For the UTSG, we rely on the classification of the sequences in Safe, Near Misses and PIs as presented in [6].

In what follows, we compare the advantages of a DET with respect to a static ET by assuming a failure probability equal to 10^{-3} for the PID ($P_{fail, PID}$) and for the communication between the sensor and the PID failure ($P_{fail, comm}$), 10^{-2} for the steam valve ($P_{fail, steam}$) and 10^{-4} for the safety valve ($P_{fail, safety}$). Fig. 6 shows a static ET for the scenario events related to safety valve, communication, PID and steam valve. The probability of each branch of the ET is given in Fig. 6. Dashed branches are the MCS for this scenario as identified in [6], whose total probability of occurrence turns out to be equal to 1.097E-02.

However, it is important to notice that the results of the static ET might be invalidated when a different combination of failures times, order, and magnitudes occur. As we will show, indeed, a single branch (scenario) of the static ET corresponds effectively to more different branches in the DET, which are all the possible combinations of timing, order and magnitude of the components that fail during the considered static scenario. Consequently, a branch of static ET lumps together safe, near miss and PI scenarios, that would be otherwise spooned out if the system dynamics was modelled within a DET.
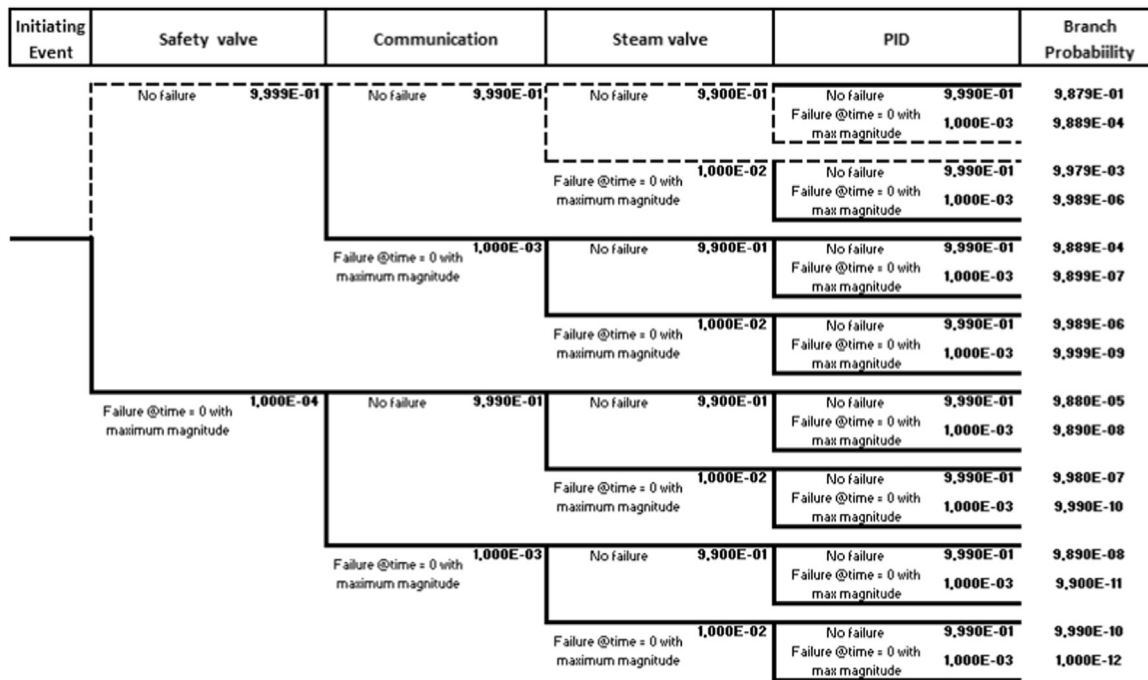
Fig. 6. Event Tree.

To show this, without loss of generality, we focus on a selection of MVL sequences of the UTSG that, incidentally, are three safe sequences, four NMs and four PIs, among the 100509 possible sequences. Table 22 lists the selected sequences (defined in terms of order and discrete magnitude and timing of failure events of each component).

For each dynamic sequence, times of failures and magnitudes have been sampled from the corresponding intervals that have been introduced in Section 3.2.1 (e.g., if the time of failure is labeled as 1, it is sampled from the interval [1,1000]; similarly, for magnitudes), and the SIMULINK model has been run.

Fig. 7 plots the dynamic sequences listed in Table 22 as branches of a DET (where dashed branches are left unsolved and only the failure magnitudes m generate alternative paths, whereas the effects of timing and order are not shown, for the sake of the Figure clarity and to avoid the combinatorial explosion of the number of branches to be plotted). Fig. 7 reports, for each sequence, the values of the probability of the corresponding branch calculated in the static ET of Fig. 6. It is important to mention that, for the DET, we have considered the PID

failure probability $P_{fail, PID}$ equal to 1.25E-04 (i.e, 1/8 of the $P_{fail, PID}$ in the static ET), the safety valve failure probability $P_{fail, SV}$ equal to 2.5E-05 (i.e, 1/4 of the $P_{fail, SV}$ in the static ET), the steam valve failure probability $P_{fail, ST.V}$ equal to 3.33E-03 (i.e., 1/3 of the $P_{fail, ST.V}$), and $P_{fail, COMM}$ has been assumed equal to 10^{-2}, being only one the possible magnitude of the communication.

In Fig. 7, the evidence of the effects of timing and failure order on the accidental scenarios consequences is shown. For example, let us consider the sequence with safety valve failure magnitude equal to 3, failure magnitude of the communication equal to 1, steam valve not failed (failure magnitude equal to 0) and, finally, failure magnitude of the PID controller equal to 3. These events are resumed into the second and the tenth sequence of Table 22, that means that the originated DET branch correspond to two different sequences differing only for timing and order of failure events (and, thus, not shown) but leading to two opposite consequences, i.e., in one case safe and in the other PI.

Moreover, results of Fig. 7 show that each failure sequence evolves with a larger probability in the ET, than in the DET. However, further efforts should be devoted to investigate whether a static ET branch envelopes (or

Table 22
The MVL dynamic sequences considered for the DET.

Sequence	Safety valve			Communication			PID			Steam valve		
	Time	Mag	Order	Time	Mag	Order	Time	Mag	Order	Time	Mag	Order
SAFE	0	0	0	4	1	2	4	8	1	0	0	0
SAFE	1	3	2	1	1	1	4	3	3	0	0	0
SAFE	4	3	4	2	1	3	2	5	1	2	2	2
NM	3	3	2	4	1	3	2	4	1	0	0	0
NM	4	4	3	4	1	2	1	4	1	0	0	0
NM	4	3	4	4	1	3	1	4	1	2	1	2
NM	4	2	3	2	1	2	1	4	1	0	0	0
PI	1	1	1	0	0	0	3	4	2	0	0	0
PI	1	4	1	3	1	3	1	2	2	0	0	0
PI	2	3	1	4	1	2	4	3	3	0	0	0
PI	2	4	1	3	1	4	3	4	3	2	3	2

Fig. 7. Comparison of ET and DET results for the dynamic sequences of Table 22.

not) all the possible dynamic sequences that would be generated by a DET. It may happen, in fact, that, when considering all the dynamic sequences (lumped in the same branch in an ET) the ET may not necessarily overestimate, but it may even underestimate the failure probability (if the system modelled in not-coherent, for which both failed and working states of the same components can lead the system to failure [8]).

4. Conclusions

In this work, a sensitivity analysis method has been presented, to determine which input variables of a TH codes affect most the safety margin quantification of a dynamic system. Safety margin has been computed according to a dynamic probabilistic definition, which allows for the quantification of the uncertainties affecting the safety parameter evolution along an accidental scenario and, at the same time, accounts

also for the earliest time needed to reach the estimated safety margin. Based on the results of this analysis, it is possible to conclude whether dynamic aspects influence (or not) the safety margin quantification. This can be used to decide the most correct probabilistic model to be used for the system safety assessment and the computation of the probability of occurrence of the accidental scenarios considered: a static analysis (i.e., a static ET) or a dynamic analysis (i.e., a DET). The method has been applied to two different cases of study: an SBO followed by a Seal LOCA and the UTSG in which four components are supposed to fail. Concerning the first case of study, the sensitivity analysis allows us to conclude that simulated boiled up water level in the core whose dynamic evolution with MAAP5 TH code is not sensitive to the dynamic inputs (i.e., time of operators actions, time of the onset of the increased leakage rate). Therefore, a static analysis has been performed to evaluate the probabilities of core damage based only on the failure probabilities of static events (i.e., seal stages). On the contrary, in the second case of study, dynamic inputs of the SIMULINK model of the UTSG (i.e., time, magnitude and order of the steam valve, the communication, the safety valve and the PID) result to be relevant for the variability of the water narrow range level fluctuation during the accidental scenarios considered. Consequently, a simplified DET has been built and a comparison between the results of a static ET and the DET have been presented. The comparison has shown, in particular, that a single branch of the static ET corresponds to many branches of the DET and that, consequently, a static scenario of the ET can correspond, in reality, simultaneously to safe scenario, a

NM, or a PI, in the DET, that would lead to a wrong quantification of the system failure if dynamic aspects are neglected.

From the applications to the two cases of study, some limits for the proposed method arise:

1. The estimation of the values of y_{γ_1} and $y_{t_{\gamma_2}}$ through OS suffers the limited number of available TH code simulations, when the analyst is required to ensure both the value of the percentile and of the confidence on its estimate. One possible solution can consist in utilizing other methods, such as Finite Mixture Models [20] that have been proven in [8] to require a lower number of simulations than OS while, at the same time, to allow for estimating the entire distribution of the parameter rather than only few given percentiles, as it is for OS.
2. The sensitivity index I_x, here defined gives an indication of which is the input that most affects the DPSM. However, it does not consider any non-linear system response to the accidental progressions that are simulated and, therefore, further efforts should be devoted to fill this gap, in future research works.

Therefore, we can conclude that further studies are necessary in order to overcome these limits and improve, consequently, the methodology presented for the selection of the probabilistic model to be used for the safety assessment of a NPP.

Appendix A

The real values of y_{γ_1} and $y_{t_{\gamma_2}}$ are unknown, because the distributions of y and y_t are also unknown. Order Statistics (OS) is a non parametric model used to determine $\hat{y}_{\gamma_1}$ and $\hat{y}_{t_{\gamma_2}}$, which are the estimation of y_{γ_1} and $y_{t_{\gamma_2}}$, with a confidence β_1 and β_2, respectively [23]. A limited number N TH simulations is available, where $\bar{y} = \{y_1,\dots,y_N\}$ is the vector of the output safety variable and $\bar{y}_t = \left\{y_{t_1},\dots,y_{t_N}\right\}$ is the vector containing the time to reach the corresponding output values of $\bar{y}$. OS ensures that the mth value (usually the first) of the N sorted output has a certain probability β of exceeding (undershooting) the unknown true value of the γth percentile of its distribution. This is valid for both y and y_t [10].

Two different approaches, namely "Bracketing" and "Coverage", are possible, depending on the assumptions done on the relationship between γ, β and N. "Bracketing" approach [23], with Assuming $m = 1$ and referring to uncorrelated outputs y and y_t, defines:

$$\beta = (1 - \gamma^N)^2 \tag{A1}$$

And, thus, ensures γ_1 to be the probability that y lies below y_{γ_1} in any of the N runs, whatever the value of y_t, and γ_2 to be the corresponding probability for y_t [10].

"Coverage" approach, with uncorrelated output y and y_t, defines [23]:

$$\beta = 1 - \gamma^N + N\gamma^N \ln(\gamma) \tag{A2}$$

Usually, Eqs. α and (A2) are used to get the optimal number N of simulations needed to estimate the $\gamma=0.95$ percentile with a confidence $\beta=0.95$, as required by the regulation guidance: with this settings two approaches give $N=72$ for "Bracketing" and $N=89$ for "Coverage". As we can notice, "Coverage" approach requires a larger number of runs as compared to the "Bracketing" approach. This is because in the "Coverage" approach (contrarily to the "Bracketing" approach) one output (e.g., y) is sorted jointly with the other output (e.g., y_t) and both percentiles y_{γ_1} and $y_{t_{\gamma_2}}$ are required to simultaneously lie within the estimated percentiles $\hat{y}_{\gamma_1}$ and $\hat{y}_{t_{\gamma_2}}$ to guarantee the confidence β_1 and β_2 [10].

References

[1] Aldemir T. A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plant. Ann Nucl Energy 2013;52:113–24.

[2] Alvarenga MAB, Frutuoso e Melo PF. Including Severe Accidents in the Design Basis of Nuclear Power Plants: an Organizational Factors Perspective after the Fukushima Accident. In Annals of Nuclear Energy Vol. 79 20159 (May) Elsevier p. 68–77.d.

[3] Borgonovo E, Plischke E. Sensitivity analysis: A review of recent advances European Journal of Operational Research, Article in Press; 2015.

[4] Cojazzi G. The DYLAM approach to the dynamic reliability analysis of systems. Reliab Eng Syst Saf 1996;52:279–96.

[5] Deterministic safety analysis for nuclear power plants: safety guide — Vienna: International Atomic Energy Agency, 2009. p.; 24 cm. — (IAEA safety standards series, ISSN 1020–525X; no. SSG-2) STI/PUB/1428 ISBN978–92–0–113309–0.

[6] Di Maio F, Vagnoli M, Zio E. Risk-based clustering for near misses identification in integrated deterministic and probabilistic safety analysis, (2015). Sci Technol Nucl Install 2015, [art.693891].

[7] Di Maio F, Baronchelli S, Zio E. Hierarchical differential evolution for minimal cut sets identification: application to nuclear safety systems. Eur J Oper Res 2014;238(2):645–52.

[8] Di Maio F, Nicola G, Zio E, Yu Y. Finite mixture models for sensitivity analysis of thermal hydraulic codes for passive safety system analysis. Nucl Eng Des 2015;289:144–54.

[9] Di Maio F, Baronchelli S, Zio E. A computational framework for prime Implicants Identification in non-coherent dynamic systems. Risk Anal 2015;35(1):142–56.

[10] Di Maio F, Rai A, Zio E. A dynamic probabilistic safety margin characterization approach in support of integrated deterministic and Probabilistic Safety analysis. Reliab Eng Syst Saf 2016;145(5400):9–18.

[11] Habibiyan H, Setayeshi S, Arab-Alibeik H. A fuzzygain-scheduled neural controller for nuclear steam generators. Ann Nucl Energy 2004;31(15):1765–81.

[12] Hofer E, Kloos M, Krzykacz-Hausmann B, Peschke J, Sonnenkalb M. Dynamic Event Trees for Probabilistic Safety Analysis. Garsching, Germany: GRS; 2014.

[13] Iooss B, Lemaître P. A review on global sensitivity analysis methods. Oper Res/Comput Sci Interfaces Ser 2015;59:101–22.

[14] Karanki DR, Dang VN, Kim T-W, "Discrete dynamic event tree analysis of mloca using ads-trace", (2011) International Topical Meeting on Probabilistic Safety Assessment and Analysis 2011, PSA 2011, 1, pp. 610–622. 5.

[15] Karanki DR, Kim T-W, Dang VN. A dynamic event tree informed approach to probabilistic accident sequence modeling: dynamics and variabilities in medium LOCA. Reliab Eng Syst Saf 2015;142:78–91.

[16] Kothare MV, Mettler B, Morari M, Bendotti P, Falinower C-M. Level control in the steam generator of a nuclear power plant. IEEE Trans Control Syst Technol 2000;8(1):55–69.

[17] Light Water VVAA. Reactor sustainability Research and development program plan, Fiscal year 2009–2013. DOE Off Nucl Energy 2009.

[18] Marseguerra M, Zio E, Cadini F. Optimized adaptive fuzzy controller of the water level of a pressurized water reactor steam generator. Nucl Sci Eng 2007;155(3):386–94.

[19] McKay MD. Variance-based methods for Assessing uncertainty importance in NUREG-1150 analyses, LA-UR-96-2695. Los Alamos Natl Lab 1996:7–27.

[20] McLachlan G, Peel D. Finite mixture models. New York: John Wiley & Sons Inc; 2000.

[21] Metzroth K, Denning RS, Aldemir T Dynamic event tree analysis of competing creep failure mechanisms in a station blackout accident, (2011) International Topical Meeting on Probabilistic Safety Assessment and Analysis 2011, PSA 2011, 1, pp. 623–634.

[22] Modular Accident Analysis Program 5 (MAAP5) Applications Guidance: Desktop Reference for Using MAAP5 Software - Phase 1 Report. EPRI, Palo Alto, CA: 2014. 3002003113.

[23] Nutt WT, Wallis GB. Evaluation of nuclear safety from the outputs of computer codes in the presence of uncertainties. Rel Eng Sys Saf 2004;83:57–77.

[24] Quine WV. The problem of simplifying truth functions", Am. Math, Monthly, Volume 59, p. 521– 531, 1952.

[25] Retrieved from ⟨http://www.power-technology.com/projects/tomari-3/tomari-38.html⟩.

[26] Ruger CJ, WJ Lucas, Jr. "Technical Findings Related to Generic Issue 23: Reactor Coolant Pump Seal Failure", NUREG/CR-4948, Division of Safety Issue Resolution, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, March; 1989.

[27] Saltelli A, Chan K, Scott E. Sensitivity analysis. NewYork: John Wiley & Sons Inc; 2000.

[28] Shaukat SK, Jackson JE, Thatcher DF. "Regulatory Analysis for Generic Issue 23: Reactor Coolant Pump Seal Failure", NUREG/1401, Division of Safety Issue Resolution, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, April; 1991.

[29] Smidts C. Probabilistic dynamics: a comparison between continuous event trees and a discrete event tree model. Reliab Eng Syst Saf 1994;44(2):189–206.

[30] Sobol IM. Sensitivity estimates for nonlinear mathematical models. Math Model Comput Exp 1993;1:407–14.

[31] WOG2000, Reactor Coolant Pump Seal Leakage Model for Westinghouse PWRs, WCAP-15603, Revision 1, May 2002.

[32] Zio E, Di Maio F. Bootstrap and Order Statistics for Quantifying Thermal-Hydraulic Code Uncertainties in the Estimation of Safety Margins. In Science and Technology of Nuclear Installations, Vol. 2008, Article ID 340164. Hindawi Publishing Corporation; 2008.

[33] Zio E, Maio F Di. Processing dynamic scenarios from a reliability analysis of a nuclear power plant digital instrumentation and control system. Ann Nucl Energy 2009;36:1386–99.

[34] Zio E, Di Maio F, Tong J. Safety Margins Confidence Estimation for a Passive Residual Heat Removal System. In Reliability Engineering & System Safety, Vol. 95, pp. 828–836. Elsevier, August 2010.

[35] Zio E. Computational methods for reliability and risk analysis. Ser Qual, Reliab Eng Stat 2009;14.

[36] Zio E. Integrated deterministic and probabilistic safety assessment: concepts, challenges, research directions. Nucl Eng Des 2014. http://dx.doi.org/10.1016/j.nucengdes.2014.09.004.