Advanced RESTART method for the estimation of the probability of failure of highly reliable hybrid dynamic systems

Pietro Turati, Nicola Pedroni, Enrico Zio

Advanced RESTART method for the estimation of the probability of failure of highly reliable hybrid dynamic systems

Pietro Turati[1], Nicola Pedroni[1], Enrico Zio[1,2,*]

[1] Chair on Systems Science and the Energetic Challenge, Fondation Electricite' de France (EDF), Laboratoire Genie Industriel, CentraleSupélec, Université Paris-Saclay, Grande voie des Vignes, 92290 Chatenay-Malabry, France.

[2] Energy Department, Politecnico di Milano, Via La Masa 34, Milano, 20156, Italy.

[*] Corresponding author: enrico.zio@polimi.it, enrico.zio@ecp.fr, enrico.zio@supelec.fr

ABSTRACT

The efficient estimation of system reliability characteristics is of paramount importance for many engineering applications. Real world system reliability modeling calls for the capability of treating systems that are: *i*) dynamic, *ii*) complex, *iii*) hybrid and *iv*) highly reliable. Advanced Monte Carlo (MC) methods offer a way to solve these types of problems, which are feasible according to the potentially high computational costs. In this paper, the REpetitive Simulation Trials After Reaching Thresholds (RESTART) method is employed, extending it to hybrid systems for the first time (to the authors' knowledge). The estimation accuracy and precision of RESTART highly depend on the choice of the Importance Function (IF) indicating how close the system is to failure: in this respect, proper IFs are here originally proposed to improve the performance of RESTART for the analysis of hybrid systems. The resulting overall simulation approach is applied to estimate the probability of failure of the control system of a liquid hold-up tank and of a pump-valve subsystem subject to degradation induced by fatigue. The results are compared to those obtained by standard

MC simulation and by RESTART with classical IFs available in the literature. The comparison shows the improvement in the performance obtained by our approach.

Keywords: advanced Monte Carlo method; RESTART; Piecewise Deterministic Markov Process (PDMP); hybrid dynamic system; importance function; efficient failure probability estimation.

1. INTRODUCTION

In the performance-based design and operation of modern engineered systems, the accurate assessment of reliability characteristics is of paramount importance, and more so for nuclear, aerospace, chemical and energy transmission systems that are safety-critical and must be designed and operated within a risk-informed approach (USNRC, 2009), (EPA, 2009), (NASA, 2010).

In order to assess quantitatively the failure behavior of these systems, complex mathematical models are built and subsequently translated into detailed mechanistic computer codes that are used to simulate the response of the systems under various operational transient and accident scenarios. In practice not all the characteristics of the system under analysis can be fully described by the model, due to the presence of intrinsically stochastic events and to the analysts' incomplete knowledge about some phenomena. This leads to uncertainty on the values of model parameters and on the hypotheses supporting the model structure. These uncertainties must be taken into account to conduct a realistic assessment of the system failure behavior and the associated reliability characteristics.

In practice real-world systems are: 1) *dynamic*, i.e., their state changes (deterministically and/or stochastically) in time; 2) *hybrid*, i.e., they are characterized by both discrete and continuous variables (e.g., components' discrete states, like functioning, failed, standby, and continuous

physical quantities, like temperatures and pressures); 3) *complex*, i.e., they are described by a large number of variables and parameters related by highly nonlinear dependences; 4) *highly reliable*, i.e., their failure probability is very low.

These real-world system features rarely allow solving the models for reliability assessment with uncertainty propagation analytically. On the other hand, Monte Carlo Simulation (MCS) methods offer a feasible means (Zio, 2013). The basic idea is to randomly generate a large number of possible system evolutions and estimate the failure probability as the fraction of the number of simulations that end in a failure state. Obviously, the smaller the failure probability, the larger the number of simulations needed to achieve an acceptable estimation accuracy and precision. As a consequence, the resulting computational cost may be very high and at times impractical (e.g., repeated realizations of system response by the computer code RELAP5-3D, which is used to describe the thermal-hydraulic behavior of nuclear systems, may take up to twenty hours per run in some applications). This calls for new simulation techniques that allow performing failure probability estimations, with as few as possible model calls and, thus, as low as possible computational time.

This can be obtained by resorting to advanced Monte Carlo Simulation techniques (Bucklew, 2004), (Robert and Casella, 2004), (Rubino and Tuffin, 2009). Examples of these methods include Stratified Sampling (Helton and Davis, 2003), (Cacuci and Ionescu-Bujor, 2004), (Munoz Zuniga M. et al., 2011); Importance Sampling (IS) (Au and Beck, 2003a), (Au, 2004), (Asmussen and Glynn, 2007), (Dupuis et al., 2007), (Asmussen et al., 2011) and its variants, such as the cross-entropy method (Rubinstein and Kroese, 2004), (De Boer et al., 2005), (Asmussen and Glynn, 2007), (Botev and Kroese, 2008) or the recent Markov Chain Monte Carlo (MCMC) IS (Botev et al., 2013a); Subset Simulation (Au and Beck, 2001), (Au and Beck, 2003b), (Ching et al., 2005), (Au et al., 2007), (Cadini et al., 2012), (Au and Wang, 2014); Line Sampling (Schuëller and

Pradlwarter, 2007), (Zio and Pedroni, 2010), (Valdebenito et al., 2010) and Splitting Methods (Kahn and Harris, 1951), (Garvels, 2011), (Botev and Kroese, 2012), (Botev et al., 2013b), (Murray et al., 2013). These algorithms have shown to provide outstanding performances in *static* problems, whereas their *applicability* to complex *dynamic* systems is not fully demonstrated.

Methods explicitly designed for dynamic reliability analyses have been proposed in the literature (Labeau, 1996), and consistently developed through years (Labeau et al., 2000). In (Zhu et al., 2006) advancements in the dynamic reliability field have been brought by including software behavior into the analysis and using an entropy-driven criterion to force the simulation of scenarios of interest. (Čepin and Mavko, 2002) and (Rao et al., 2009) evaluate system failure probabilities by resorting to dynamic fault trees. A method exploiting Dynamic Event Tree (DET) and Monte Carlo simulation is proposed in (Li et al., 2010) and (Li et al., 2011) to force the stochastic system simulation to a failure state and to retrieve the corresponding probability by means of a biasing approach similar to that of Importance Sampling. In (Catalyurek et al., 2010) and (Aldemir, 2013) an efficient framework is proposed for the exploration of the state space of dynamic, hybrid and complex systems and the assessment of the corresponding state probabilities; however, an acceptance threshold on the probabilities is introduced to avoid an explosion of the number of system analysis, making these approaches exposed to neglecting events with small failure probabilities. Finally, Sequential Monte Carlo simulation has recently captured the attention of many researchers due to its rigorous consistent mathematical formulation and its possibility of dealing with static rare events (Cérou et al., 2012) and large hybrid dynamic systems (Blom et al., 2006), (Cassandras and Lygeros, 2006).

However, in this paper, we consider the REpetitive Simulation Trials After Reaching Thresholds (RESTART) method, an advanced MCS technique taking its root in splitting theory, which has shown promising performance in the analysis of dynamic, *discrete* systems (Villén-Altamirano and

Villén-Altamirano, 1991), (Villén-Altamirano and Villén-Altamirano, 1994), (Görg and Schreiber, 1996), (Garvels and Kroese, 1998), (Tuffin and Trivedi, 2000) and which can be potentially extended to dynamic, *hybrid* systems. The method is based on the random generation of many possible realizations of the life of the dynamic system. Such trajectories are split (i.e., "multiplied") when they get close to "interesting" regions of the system state space (i.e., the failure region); on the contrary, the trajectories are stopped if they tend to go far from the failure region. This way of proceeding, coupled with a proper weight assigned to each path allows a more efficient exploration of the system state space and, thus, a reduction of the variance of the corresponding failure probability estimator (Villén-Altamirano and Villén-Altamirano, 2002). The indication of which trajectories should be split (i.e., of which regions of the state space should be explored more deeply) is given by a properly selected scalar Importance Function (IF) which is crucial for the overall performance of the method (Garvels et al., 2002), (Villén-Altamirano and Villén-Altamirano, 2006), (Lagnoux, 2006), (Cérou and Guyader, 2007), (Amrein and Künsch, 2011). In particular, the possibility of embedding the discrete and continuous variables of a hybrid system within a single scalar importance function is of interest for the use of this method.

In this view, the objective of the paper is to show the feasibility of efficiently employing this technique for hybrid, dynamic, highly reliable systems. To this aim, we apply the RESTART method to evaluate the failure probability of two hybrid dynamic systems in the literature, whose mathematical models contain both discrete and continuous time-dependent variables: the first is a control system of a liquid hold-up tank (Marseguerra and Zio, 1996) and the second is a system composed by a pneumatic valve and a centrifugal pump subject to degradation (Lin et al., 2014). The systems are modeled via Piecewise Deterministic Markov Processes (PDMPs). Although suggestions and guidelines for the construction of proper Importance Functions (IFs) for discrete dynamic systems are given in literature (Villén-Altamirano, 2007), (Villén-Altamirano, 2010b),

(Villén-Altamirano, 2014), *no* indications have been given yet with reference to *hybrid* systems: our developments in this represent the main contribution of the present paper.

The rest of the paper is organized as follows: in section 2, a recall of the RESTART method and of the performance index for evaluating it, is given; section 3 reports some references regarding the PDMP modeling technique used in both case studies; section 4 introduces general guidelines for the definition of the importance function; section 5 presents an application of the RESTART for estimating the failure probability of a control system of a liquid tank; section 6 shows the RESTART performance on a pump-valve subsystem of a liquid delivery system; finally in section 7 some conclusions are drawn.

2. THE RESTART METHOD

The REpetitive Simulation Trials After Reaching Thresholds (RESTART) method is a splitting technique that takes its origins in (Bayes, 1970) and has been developed mainly by (Villén-Altamirano and Villén-Altamirano, 2002); (Villén-Altamirano and Villén-Altamirano, 2006); (Villén-Altamirano and Villén-Altamirano, 2011). The method has been introduced to efficiently estimate small failure probabilities of dynamic systems: it relies on the observation that a (small) failure probability can be expressed as a product of (larger) probabilities conditional on some chosen "intermediate" and, thus, more frequent events. The problem is, thus, tackled by performing a sequence of *retrial* simulations of (more frequent) intermediate events in their conditional probability spaces. Such retrial simulations are carried out by sequentially *splitting* the evolution trajectory of the dynamic system each time it "enters" these intermediate conditional regions. In this way, the split trajectories gradually populate all the intermediate conditional regions until the final failure region is reached.

For the sake of brevity, in what follows only the main elements and concepts underlying the RESTART algorithm are recalled for self-containment and better comprehension of the paper; the reader is referred to the cited references for further technical details.

2.1. The Algorithm

Let Ω be the state space of the stochastic process $X(t)$ describing the evolution of the dynamic system of interest and A be the rare failure event, whose probability has to be estimated. A scalar function $\phi: \Omega \to \mathbb{R}$, called Importance Function (IF), is introduced to identify a sequence of nested "intermediate" states sets $C_i \subset \Omega$, $(C_1 \supset C_2 \supset \cdots \supset C_M)$: these sets are of the form $C_i = \{x(t) \in \Omega : \phi(x(t)) > T_i\}$, where $T_1 < \cdots < T_M$ is a given sequence of predefined thresholds. This generates a partition of Ω in regions $C_i - C_{i+1} = \{x(t) \in \Omega : T_i \leq \phi(x(t)) < T_{i+1}\}$, such that the higher i, the closer the system to the failure region A, i.e., the higher the "importance" of the system states belonging to that region.

By way of example, assume that the system of interest is a nuclear reactor which is assumed to fail when the fuel cladding temperature $\theta_f(t)$ exceeds the safety threshold $\theta_f^{max} = T_A$. In this case, the stochastic process $X(t)$ is represented by the ensemble of the (discrete) variables describing the state of the components of the nuclear reactor system (e.g., pumps, valves, safety systems, etc.) and of the (continuous) variables describing the evolution of the physical quantities that are critical for the reactor safety (e.g., temperature, pressure, mass flow rate, etc.). The importance function $\phi(X(t))$ can be simply chosen as the "natural" indicator of the condition of the fuel cladding, i.e., its temperature $\theta_f(t)$: in other words, $\phi(X(t)) = \theta_f(t)$. Finally, since the system fails when $\phi(X(t))$ exceeds θ_f^{max}, then three possible "intermediate" thresholds can be chosen as $T_1 < T_2 < T_3 < T_A$.

The algorithm proceeds as follows. A certain number N of initial simulation paths (trajectories), called *main trials*, is generated by crude Monte Carlo simulation. The starting point of these trajectories is represented by the initial condition of the system of interest and it lies in region $C_0 - C_1 = \{x(t) \in \Omega : \phi(x(t)) < T_1\}$. When the IF associated to a simulation path started from a given region C_i exceeds a threshold T_{i+k} of higher level at time t^*, $k = 1, \dots, M - i$, the corresponding system state $X(t^*)$ is saved and $R_{i+k} - 1$ new paths, called *retrials*, are generated having the saved state $X(t^*)$ as origin (hence, if we count also the original path that has exceeded threshold T_{i+k}, we have R_{i+k} trials starting from state $X(t^*)$). On the contrary, every time the IF of a trial born in C_i falls below threshold T_i, that trial is interrupted. This is the main difference between RESTART and the "classical" splitting (Garvels et al., 2002), where the paths are split only the first time they cross a more important threshold T_{i+k} and, then, they are maintained for the rest of the simulation, even if their trajectories fall below the "generating" threshold T_{i+k}. On the contrary, RESTART keeps only one of the R_{i+k} trials (e.g. the one that has crossed the threshold) as the representative path for exploring less important regions (i.e., those regions lying below the threshold T_{i+k} from which the R_{i+k} retrials are generated): obviously in such a case the representative path has to be re-split in case threshold T_{i+k} is again exceeded.. The reason behind the truncation of the trajectories that tend to move farther from failure region A is to reduce as much as possible the computational cost associated to the exploration of regions of the state space that are not of interest. At the same time, the unbiasedness of the estimates is guaranteed by associating a proper weight to each path/retrial on the basis of the region $C_i - C_{i+1}$ explored. Intuitively, less important regions are visited by a lower number of paths with higher weights whereas more important regions are explored by a potentially larger number of retrials, but with correspondingly lower weights. An analytical demonstration of the unbiasedness of the RESTART estimators can be found in (Villén-

Altamirano and Villén-Altamirano, 2002). In addition, it must be remembered that one trajectory may exceed more than one threshold at the same time (even if not frequently). For example, consider a trial with origin in $X_i(t^*) \in C_i - C_{i+1}$ which exceeds T_{i+1} and T_{i+2} at the same time. In such a case, $R_{i+1} \cdot R_{i+2} - 1$ retrials should be generated from the new state $X_{i+2}(t^*)$, as if all the $R_{i+1} - 1$ retrials that should have been generated due to the exceedance of threshold T_{i+1} and the one with origin in $X_i(t^*)$ had reached T_{i+2}. In summary, we should take into account: i) the initial trial started from $X_i(t^*)$ which is terminated when it falls below T_i; ii) $(R_{i+1} - 1)$ retrials which are generated due to the exceedance of threshold $T_{i+1}$and that are terminated when they fall below T_{i+1}; iii) $R_{i+1} \cdot (R_{i+2} - 1)$ retrials which take into account the possible exceedance also of threshold T_{i+2} and that are stopped when they fall below T_{i+2}.

The simulation path of each retrial ends due to either the rules explained above or to the occurrence of a process "end condition"; on the contrary, the simulation path of the main trials is terminated only due to the occurrence of the "end condition". "End conditions" are given as in crude Monte Carlo simulations (e.g., reaching of the mission time t_{miss}, occurrence of absorbing events, etc.). Figure 1 shows possible evolutions of the retrials (dashed and/or dotted lines) associated to a single main trial (bold line) in a RESTART simulation with three thresholds ($M = 3$), retrials $R_1 = 3, R_2 = 4, R_3 = 2$, a mission time (i.e., time horizon of system observation) t_{miss} and failure region defined by $\phi\big(X(t)\big) \geq T_A$.

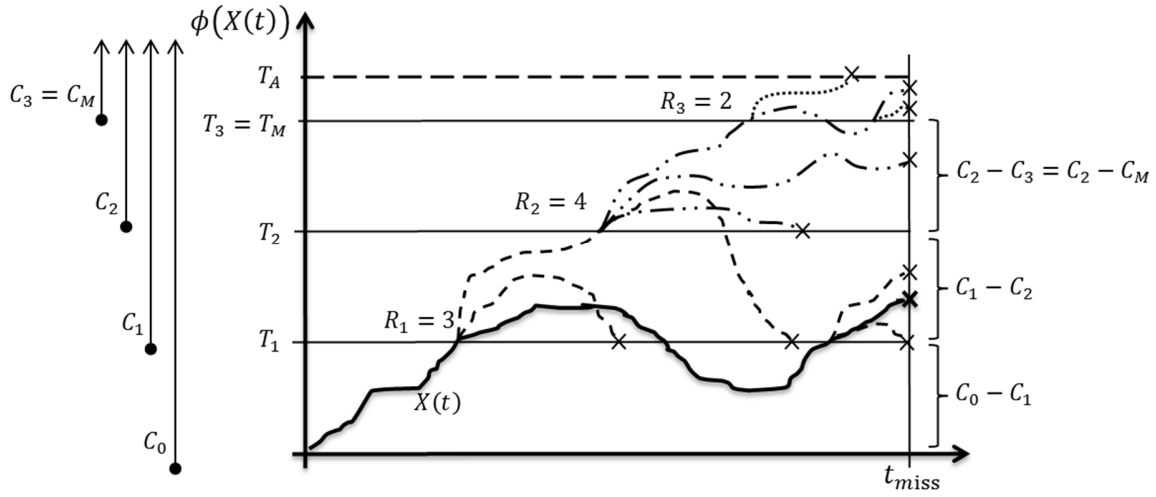

Figure 1 Possible evolutions of RESTART trajectories relative to a single main trial (bold) in a simulation with $M = 3, R_1 = 3, R_2 = 4, R_3 = 2$.

For the evaluation of statistics based on all simulation trials, the weights associated to the each trial need to be computed. The weight of a trajectory is obviously related to the region $C_i - C_{i+1}$ in which the trial lies; in particular it is related to the product $r_i = \prod_{j=1}^{i} R_j$ of the splitting factors necessary to reach threshold T_i and to the number of main trials N. In details, if $X(t)$ is in $C_i - C_{i+1}$, its weight w_i will be $w_i = \frac{1}{N \cdot r_i} = \frac{1}{N \cdot \prod_{j=1}^{i} R_j}$. Notice that, the higher is the importance of the region, the lower is its statistical weight. For example, considering the situation depicted in Figure 1, where the number N of main trials is 1, the trajectories in region $C_1 - C_2$ have weights $w_1 = \frac{1}{R_1} = \frac{1}{3}$, since the main trial is split into three retrials every time it exceeds threshold T_1; similarly, trajectories in region $C_2 - C_3$ have weights $w_2 = \frac{1}{R_1 \cdot R_2} = \frac{1}{3 \cdot 4} = \frac{1}{12}$, since they are the results of two successive splittings, related to the crossing of thresholds T_1 (splitting into three retrials) and T_2 (splitting into four retrials). Then, the estimator $\hat{P}(A)$ of the probability of failure $P(A)$ is $\hat{P}(A) = \sum_{i=1}^{M} w_i \cdot N_A^i = \sum_{i=1}^{M} \frac{N_A^i}{r_i}$, where N_A^i is the number of occurrences of the failure event A when the

system has a state $X(t)$ lying in region $C_i - C_{i+1}$. Furthermore, if $A \subset C_M$ (i.e., failures occur only if the system has a state in C_M), the estimator becomes simply $\hat{P}(A) = \frac{N_A^M}{N \cdot r_M} = \frac{N_A}{N \cdot \prod_{j=1}^{M} R_j}$. In (Villén-Altamirano and Villén-Altamirano, 2002) the unbiasedness of the estimators is proven and details concerning the variance of this estimator are given.

As in all Monte Carlo-based methods, the higher the correlation among the generated trajectories, the higher the variance $V\left[\hat{P}(A)\right]$ of the failure probability estimator. In the RESTART method, each retrial shares a part of the "simulation path" with the trial from which it is generated: thus, there is correlation between them. In (Villén-Altamirano and Villén-Altamirano, 2002), optimal and quasi-optimal values for the number of retrials $R_i, i = 1, \dots, M$, have been derived analytically for a fixed number of thresholds M in order to minimize the variance of $\hat{P}(A)$: on one side, R_i should be large enough to widely explore the system state space by generating the possible trajectories of evolution of the process; on the other side, R_i has to be small enough to avoid a significant increase in the correlation among the retrials and, thus, a dramatic decrease in the efficiency of the method. The analytical results derived in (Villén-Altamirano and Villén-Altamirano, 2002) demand for information that is typically not available a priori, such as the value of $P_{i|0}$, i.e., the probability that the system reaches region C_i knowing that it is in region C_0. However, rough estimations via crude Monte Carlo or expert judgement are usually enough to obtain satisfying results. Another crucial parameter for the algorithm is the number M of thresholds. If the IF is continuous, it is possible to identify the optimal value for M as the largest possible value that guarantees $P_{i|i-1} < 0.5$, where $P_{i|i-1}$ is the conditional probability that the system reaches region C_i, given that it lies in region C_{i-1}, i.e., $P(X(t) \in C_i | X(t) \in C_{i-1})$. On the contrary, if the state space is discrete or hybrid (which is the case of the present paper), the IF is discontinuous and, thus, optimal values for M and R_i cannot be obtained easily. Applications of the RESTART

method to reliability problems in discrete state spaces have been already shown in the literature; also, suggestions for the choice of the corresponding IFs have been proposed (Villén-Altamirano, 2007); (Villén-Altamirano, 2010a); (Villén-Altamirano, 2014). However, to the best of the authors' knowledge, applications and related IFs for hybrid systems have not been proposed yet.

2.2. Performance Index

The performance of the RESTART method can be assessed by means of the well-known Figure of Merit (FoM) $C \cdot V(\hat{P})$, where C is the computational cost associated to the method and $V\left(\hat{P}(A)\right)$ the variance of the failure probability estimator $\hat{P}(A)$: this indicator takes into account both the precision (i.e., the variance) of the estimator and the computational effort needed to obtain it. The gain or speedup G of RESTART can be defined as the ratio between the FoM of crude Monte Carlo simulation and the FoM of RESTART. A formula for the ideal (i.e., maximal) gain has been derived in (Villén-Altamirano and Villén-Altamirano, 2002):

$$G = \frac{1}{P(A)(-\ln P(A) + 1)^2}, \quad (1)$$

where $P(A)$ is the failure probability to be estimated.

3. PIECEWISE DETERMINISTIC MARKOV PROCESS (PDMP) FOR MODELING HYBRID DYNAMIC SYSTEMS

Piecewise Deterministic Markov Process is a modeling technique that allows to describe systems whose variables evolve accordingly to physical laws (typically by Ordinary Differential Equations-ODEs), which could stochastically change in time. PDMPs were firstly introduced by (Davis, 1984)

and (Davis, 1993) for describing systems with deterministic motion and random jumps; recently PDMP have been treated in (Jacobsen, 2006) and used in (Lin et al., 2014).

PDMPs are suitable, e.g., for modeling the process of degradation of physical systems which present interdependencies among their variables (Lin et al., 2014). Let

$$\vec{X}(t) = \begin{bmatrix} \vec{Y}(t) \\ \vec{Z}(t) \end{bmatrix} \in E = \mathbb{R}^d \times S \quad (2)$$

be the vector representing the state of the system on the support E: for simplicity of the presentation of the method, the d-dimensional vector $\vec{Y}(t)$ contains all the continuous variables (typically related to the system physical quantities like temperatures and pressures), whereas $\vec{Z}(t)$ has a discrete support S and contains all the discrete variables (e.g., those related to the functioning, partially functioning or failed states of mechanical components). A continuous variable is commonly used either in a continuous time monitoring or physics-based modeling framework. On the contrary, discrete variables are used either when it is not necessary or it is not possible to build a more detailed continuous model. This can be due to the lack of information, (e.g., it is not possible to continuously monitor the system state), or to the fact that it is sufficient to know a range in which the variables lie: for example, if the vibrations are over a certain value, then the pump is considered partially degraded, otherwise it is in normal conditions.

In PDMPs, $\vec{Y}(t)$ follows a piecewise deterministic process whose interruptions are brought by Markovian transitions of the discrete variables $\vec{Z}(t)$ at time t_k. Letting $\vec{X}_k = \vec{X}(t_k)$ be the state of the system at transition time t_k, then the random jumps of the discrete variable $\vec{Z}(t)$ are driven by the following transition probability:

$$P\left(\vec{X}_{k+1} = \vec{j}, t_{k+1} \in [t_k, t_k + \Delta t] | \{\vec{X}_n, t_n\}_{n \le k}\right) = P\left(\vec{X}_{k+1} = \vec{j}, t_{k+1} \in [t_k, t_k + \Delta t] | \vec{X}_k = \vec{i}\right) \quad (3)$$
$$\forall k \ge 0, \Delta t \ge 0, \vec{i}, \vec{j} \in E, \vec{i} \ne \vec{j}.$$

The transition probability in (3) depends on the state of both the continuous and discrete variables. Between two consecutive transition times t_k and t_{k+1}, the evolution of the system is deterministic, i.e., $\vec{X}(t) = \vec{\psi}(\vec{X}_k,\ t - t_k)$ for $t \in [t_k, t_{k+1}), \forall k \in \mathbb{N}$, where $\vec{\psi}: \mathbb{R}^d \times S \to \mathbb{R}^d \times S$ is a deterministic function in which $\vec{Z}(t)$ is constant and $\vec{Y}(t)$ takes a specific value. It is not rare that different values of the discrete variables $\vec{Z}(t)$ imply different deterministic evolutions for the continuous variables $\vec{Y}(t)$ (i.e., the shape of $\vec{\psi}$ is itself dependent on the value of $\vec{Z}(t)$.

4. IMPORTANCE FUNCTION DEFINITION

In what follows, general guidelines and procedural steps for defining efficient importance functions are reported.

4.1. System Analysis

The scope of this step is to identify the components and the continuous variables involved in the (failure) event of interest: for example, those states that the components should visit to cause system failure (i.e., the minimal cut sets) and the values that the continuous variable should assume in those conditions (e.g., liquid level in a hold-up tank or the pressure in a nuclear reactor vessel). Dependencies among components and variables could be also identified (if possible) at this step: for example, specific sequences of events that lead the system to failure.

4.2. Components And Variables Ranking

Based on the information collected at the previous step, a possibly rough and qualitative ranking of the components and variables that contribute most to the failure event should be performed. In particular, variables and component configurations that are *necessary* to lead to system failure (e.g., a specific configuration or failure mode of the valves in the system) should be ranked at the top.

4.3. Definition of the Importance Function

The definition of a proper Importance Function is typically problem- and system-dependent: see (Villén-Altamirano, 2010b), (Villén-Altamirano, 2014). Thus, in accordance with the analyses conducted in the previous two steps, an importance function should be conceived by considering first the elements (i.e., the components and the continuous variables) in the top positions of the ranking, i.e., those that contribute most to system failure. For example, in the case study that follows (Section 5), firstly, the state of three valves is considered since their failure is the necessary condition to lead the system to an uncontrolled situation; secondly, the level of the liquid in the tank is taken into account, since it gives information about the remaining time available to perform repair on the failed components.

However, it has to be admitted that an automatic general procedure for the definition of the Importance Function is not yet available, especially for complex systems. In this view, the previous guidelines could serve as a starting point for future works.

5. CASE STUDY 1: HOLD UP TANK

The RESTART method has been applied to a well-known case study in the literature for dynamic reliability analysis (Aldemir, 1987), (Siu, 1994), (Marseguerra and Zio, 1996).

5.1. The Model

The system consists of a tank containing a fluid whose level is controlled by suitable sensors, which govern three active components (Figure 2).

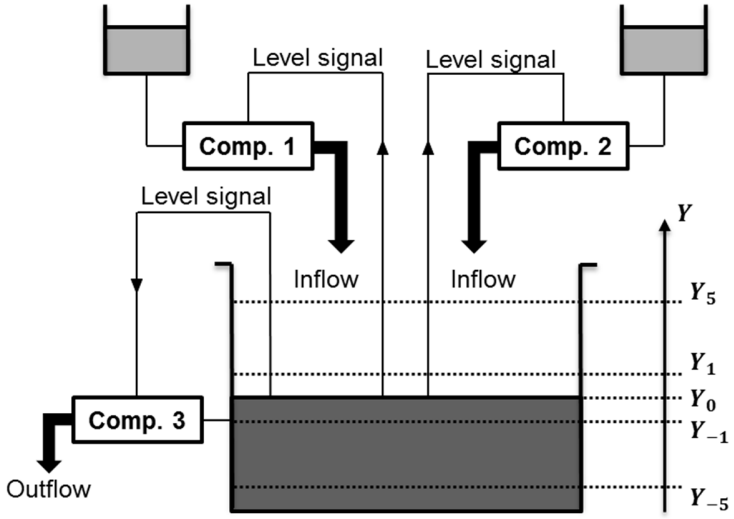

Figure 2 Tank containing a liquid, whose level is controlled by three active components

Input inflow is provided by components 1 and 2 (e.g., pumps) that produce equal and constant rates of liquid level variation $Q_1 = Q_2 = 0.6\,m/h$. Outflow is, instead, provided by a valve with constant level variation rate $Q_3 = -0.6\,m/h$. All the components are independent and can fail either Stuck Open (SO) or Stuck Closed (SC); after failure, a repair strategy that brings the components back to an "as-good-as-new" state is implemented. Exponential probability distributions are used to model all types of stochastic transition. The Mean Time To Failures (MTTFs) of components 1, 2 and 3 are $219h$, $175h$ and $320h$, respectively, for both types of failures (SO and SC), whereas the Mean Time To Repair (MTTR) for each component is $5h$. In this case study, the continuous variable $Y(t)$ represents the level of liquid in the tank; and there are 3 discrete variables $\vec{Z} = (Z_1, Z_2, Z_3)$ for the components states (-1: operating; 0: SC; 1: SO).

The initial liquid level is set to $Y(t = 0) = Y_0 = 0$. The whole system fails either for overflow (i.e., when the liquid level exceeds threshold $Y_5 = Y_0 + 5$) or for dry-out (i.e., when the liquid level falls below threshold $Y_{-5} = Y_0 - 5$). In addition, two alarm thresholds, namely, Y_{-1} and Y_1, are set to $Y_0 \pm 1$, respectively. Every time the level $Y(t)$ reaches one of these two alarm thresholds, the

possibly failed components are detected and put under repair; at the same time, the control system modifies the working configuration of the active components so as to drive the liquid level towards a safe condition. Between two consecutive (stochastic) transition times t_k and t_{k+1}, the liquid level evolution is described by the following deterministic law:

$$Y(t) = Y_{t_k} + (a_1 Q_1 + a_2 Q_2 + a_3 Q_3) \cdot (t - t_k); \forall t_k \leq t \leq t_{k+1} \quad (4)$$

where Y_{t_k} is the value of the liquid level at (random) transition time t_k and $\vec{a} = (a_1, a_2, a_3)$ is a Boolean vector such that:

$$a_i = \begin{cases} 1 \; if \; component \; i \; is \; open \; or \; SO \\ 0 \; if \; component \; i \; is \; closed \; or \; SC \end{cases} \quad (5)$$

With reference to Figure 2**,** the initial configuration of the system is in equilibrium, i.e., the inflow equals the outflow and $\vec{a} = (1,0,1)$. We divide the liquid level in three working states: 1) $Y(t) \leq Y_{-1}$; 2) $Y_{-1} < Y(t) < Y_1$; 3) $Y_1 \leq Y(t)$. If $Y(t)$ passes from 2) to 1), due to any kind of component failure, the controller will set $\vec{a} = (1,1,0)$ to increase the liquid level; otherwise, if $Y(t)$ passes from 2) to 3), the controller will set $\vec{a} = (0,0,1)$ to reduce the liquid level. Once the liquid level reaches one of the failure thresholds $Y_{\pm 5}$, the system remains failed and no repair can be conducted within a time comparable with the mission time t_{miss}. For simplicity of presentation, in this paper we consider only the assessment of the probability of dry-out failures, i.e., $U = P\left(t_{dryout} \leq t_{miss}\right)$, where t_{dryout} is the time at which dryout occurs and t_{miss} $(= 500h)$ is the mission time. Notice that the event of interest occurs when the following two events occur consecutively: *i*) all the components fail in the configuration of minimal cut set (*mcs*) $a_{dryout} = (0,0,1)$, (i.e., component 1 *SC*, component 2 *SC*, component 3 *SO*); *ii*) the repair strategy fails to restore at least one component before the liquid level reaches Y_{-5}.

5.2. **Importance Functions**

Two Importance Functions (IFs) have been considered in this case study: the first one ϕ_1 has already been proposed in the literature to evaluate multi-components failure probability (Villén-Altamirano, 2014); the second one ϕ_2 is introduced for the first time in this paper and takes into account both the presence of multiple discrete components states and the information associated to the continuous physical variable $Y(t)$.

Since in this case we have only one minimal cut set (*mcs*) a_{dryout} that leads to the failure event of interest, the IF $\phi_1(t)$ introduced in (Villén-Altamirano, 2014) becomes:

$$\phi_1(t) = fc(t)/n, \quad (6)$$

where $fc(t)$ is the number of components in the *mcs* which are failed at time t and n is the cardinality of the *mcs* (i.e., $n = 3$ in this case): obviously, the higher the number of failed components, the closer the system to failure and the higher the importance of the corresponding state. Notice that once the *mcs* configuration is obtained at time t, the system is *not* guaranteed to fail instantaneously at time t. Actually, there is still a safety margin given by the time needed by liquid level $Y(t)$ to move from the alarm threshold Y_{-1} to the failure one Y_{-5}: in this time window repairs "could" occur and avoid system failure. Thus, three thresholds $(T_1, T_2, T_3) = (1/3\,, 2/3, 1)$ are used in our RESTART implementation, instead of the two admissible if no repair strategy had been planned (actually, if no repairs were allowed, $\phi_1(t) = 1$ would automatically imply system failure at t).

The second IF $\phi_2(t)$ considers two aspects: (i) during the process components could fail in a state different from that of the *mcs* and (ii) once the *mcs* is reached, repair processes still happen stochastically. The importance function $\phi_2(t)$ is defined as follows:

$$\phi_2(t) = \frac{2 \cdot fc(t) - f(t)}{3} + \max\left(0, \ln \frac{Y_5 - Y(t)}{Y_5 - Y_{-1}}\right), \quad (7)$$

where $f(t)$ is the number of failed components at the current time t. The first "discrete" term considers that if a component fails stuck in a position opposite to the one "required" by the *mcs* a_{dryout}, it gives a negative contribution to (i.e., it reduces) the importance of that state (since the component needs to be repaired before it can reach the configuration "required" by the *mcs*). In other words, ϕ_2 gives less importance to those configurations where components are failed, but not in the state according to the *mcs*. In addition, the second term introduces a continuous part into the IF, when the alarm threshold Y_{-1} has been down-crossed. This allows introducing additional intermediate thresholds to increase the frequency of trajectory splitting; i.e., to make the exploration of the system state space more thorough, which increases the performance of the method by reducing the variance of the estimator of the conditional probability $P(Y(t) < Y_{-5} \mid Y(t) < Y_{-1})$. In the case under analysis, we introduce only one intermediate threshold that corresponds to the configuration of the system where the *mcs* has been reached and the liquid level is $Y(t) = -3$, i.e., it is at half position between the alarm Y_{-1} and the failure threshold Y_{-5}: thus, $(T_1, T_2, T_3, T_4) = (1/3\,, 2/3, 1\,, 1.287)$.

5.3. **Results**

The RESTART method has been applied with both importance functions ϕ_1 and ϕ_2 and its efficiency compared to that of standard MCS. It is worth recalling that accelerated Monte Carlo methods are typically used when the computational cost associated to a single run of the dynamic system model is prohibitive (e.g., hours or days): in this view, it is interesting to compare the performance of the two methods by keeping fixed the total time of simulation of the system model. Thus, the results produced by RESTART have been compared to the estimates obtained by the crude Monte Carlo method using the same Total Simulation Time (TST) t_S (in this case, $t_S =$

$80000h$, i.e., the total number of hours of liquid tank evolution). As performance indices, we have considered the Mean $\left(E\left[\widehat{U}\right]\right)$ of the failure probability estimator $\widehat{U}$, its Standard Deviation $\left(Std\left[\widehat{U}\right]\right)$, the Figure of Merit (FoM) introduced in section 2.2 and the average Number of System Analyses $(E[NSA])$ (i.e., the average number of complete or partial paths used to evaluate the estimator). The number of retrials R_i for each threshold T_i has been fixed to $(7, 7, 40)$ and $(7, 7, 7{,}10)$, respectively for ϕ_1 and ϕ_2, following the guidelines provided by (Villén-Altamirano and Villén-Altamirano, 2002).

Table 1 reports the values of the performance indices $E\left[\widehat{U}\right]$, $Std\left[\widehat{U}\right]$, FoM and $E[NSA]$ obtained as average over 100 estimates. The true value U of the failure probability is 5.40×10^{-4}. The Std of the estimator obtained using IF ϕ_2 is one order of magnitude smaller than the one obtained by crude Monte Carlo and almost 30% smaller than the one provided by ϕ_1. In addition, the FoM given by the new IF ϕ_2 is two orders of magnitude lower than that of standard MC and half of that of ϕ_1. The values of $E[NSA]$ show that RESTART employs more system analyses than standard MC, but it must be considered that part of some system analysis is shared by different retrials and, then, it does not imply additional computational cost. Indeed, the real total computational cost required by the different methods (which matters in the analysis) is the same by construction and is represented by the TST.

Table 1 System probability of dry-out failure obtained as average over 100 estimates by crude Monte Carlo (MC) and by the RESTART method with two different Importance Functions (IFs), ϕ_1 and ϕ_2.

	MC	**RESTART ϕ_1**	**RESTART ϕ_2**
$E\left[\widehat{U}\right]$	4.91×10^{-4}	5.36×10^{-4}	5.38×10^{-4}
$Std\left[\widehat{U}\right]$	1.70×10^{-3}	2.40×10^{-4}	1.69×10^{-4}
$FoM\left[\widehat{U}\right]$	2.25×10^{-1}	4.74×10^{-3}.	2.30×10^{-3}
$E[NSA]$	1.63×10^{2}	2.00×10^{3}	2.26×10^{3}

6. CASE STUDY 2: PUMP AND VALVE SUBSYSTEM

In this artificial case, the fluid delivery system between two plants is considered. It consists of two subsystems: the former pushes fluid from plant A to plant B, whereas the latter pushes fluid in the opposite direction. The subsystems are identical and consist of a pneumatic valve and a centrifugal pump. Part of the pipes is shared between the two subsystems, so that they have to work in alternating way (Figure 3): every hour, the fluid flow has to be inverted; thus, every hour the operating (resp., the switched off) pump is switched off (resp., on) and the associated valve is closed (resp., opened). Since the two subsystems are identical, we focus our attention on the analysis of a single pump-valve subsystem whose actual operating time is considered (i.e., only the time during which the subsystem is actually delivering the fluid). Indeed, components' degradation develops due to wear.

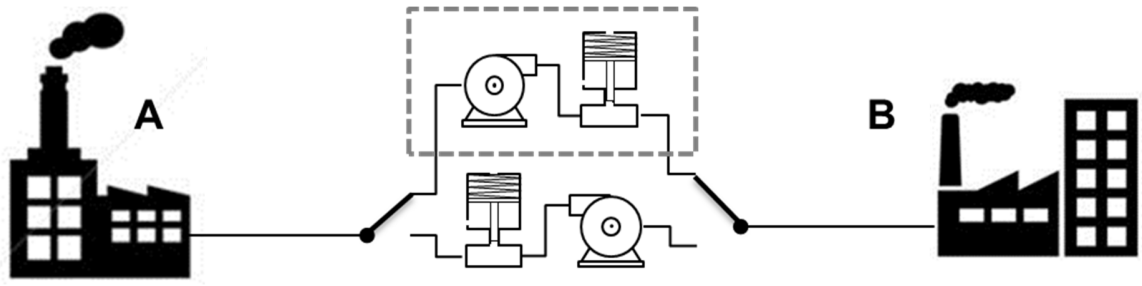

Figure 3 Fluid delivery system, where the pump-valve subsystem under analysis is highlighted by the dash box.

6.1. Model

The model of the subsystems' components (centrifugal pump and pneumatic valve) takes its roots from (Lin et al., 2014), where a Piecewise Deterministic Markov Process is used to describe the dependences between the degradation processes of the two components and the effect of the abrasive particles present in the fluid. In particular, the authors consider the influence that the

degradation state of the pump has on the degradation process of the valve. We recall here the main characteristics of the model and refer the interested reader to (Lin et al., 2014) for more details.

6.1.1. Pump

The degradation process of the centrifugal pump is described by a continuous-time homogeneous Markov chain $Z(t)$. The state space consists of a state of normal functioning, namely $Z(t) = 3$, two degradation states (namely, $Z(t) = 2$ and $Z(t) = 1$) and a failure one (namely, $Z(t) = 0$). This classification is based on the intensity of the vibrations produced by the pump. In other words, state 3 specifies the normal condition (i.e., small vibrations), state 2 medium vibrations, state 1 high vibrations and state 0 specifies the failure state. No repairs are planned, except those performed at the mission time and the corrective ones, i.e., those carried out when the component is failed. Figure 4 shows synthetically the state space of the Markov process modeling the stochastic degradation of the pump. The transition rate λ has been changed from that of (Lin et al., 2014) in favor of a more realistic value of $\lambda = 4.68 \times 10^{-5}\ h^{-1}$, which already takes into account the relative increment caused by the abrasive particles.

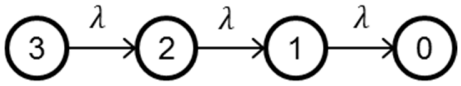

Figure 4 State space of the Markov process modeling the degradation of the pump

6.1.2. Valve

The pneumatic valve is a gas-actuated valve with a linear cylinder actuator described by a physics-based model. A system of Ordinary Differential Equations (ODEs) describes the evolution of the state variables of the valve. These variables are: (i) the position and the velocity of the piston, $x(t)$ and $v(t)$, respectively; (ii) the mass of gas at the top and bottom chamber of the valve, $m_t(t)$ and $m_b(t)$, respectively, and (iii) the equivalent orifice area of the internal leakage of the piston, $L(t)$.

The differential equation describing the deterministic time evolution of the leakage $L(t)$ (i.e., the variable pinpointing the degradation state of the valve, which depends on the vibration state of the pump) is as follows:

$$\dot{L}(t) = w(1 + \alpha_v)\left(1 + \beta_{Z(t)}\right) r v(t)^2, \quad (8)$$

where w is the wear coefficient, α_v is a constant that characterizes the relative increment of the degradation rate due to the abrasive particles in the fluid, r is the coefficient of kinetic friction and $\beta_{Z(t)}$ is a variable that characterizes the relative increment of the internal leakage caused by the vibrations of the pump: the higher the vibrations, the larger the value of $\beta_{Z(t)}$. Table 2 reports the value of the model parameters that have been here modified with respect to (Lin et al., 2014).

Table 2 Parameters of the physical valve model modified with respect to (Lin et al., 2014)

Parameters	Value
$\boldsymbol{w}$	$4.17 \times 10^{-11}\ m\ N^{-1}$
$\boldsymbol{\alpha_v}$	0.2
$\boldsymbol{\beta_3}$	0
$\boldsymbol{\beta_2}$	0.2
$\boldsymbol{\beta_1}$	0.4
$\boldsymbol{\beta_0}$	0

If $L(t)$ reaches the value $3.20 \times 10^{-6} m^2$, then the valve can be considered failed, since it can not get to the fully opened position within the safety time limit of 15s from the opening command.

With reference to the notation used in section 3, the subsystem is described by the following vector of variables:

$$\vec{X}(t) = \begin{bmatrix} \vec{Y}(t) \\ Z(t) \end{bmatrix} = \begin{bmatrix} x(t) \\ v(t) \\ m_b(t) \\ m_t(t) \\ L(t) \\ Z(t) \end{bmatrix} \in E = \mathbb{R}^5 \times \{3, 2, 1, 0\}, \quad \textbf{(9)}$$

where $Z(t)$ represents the state of the pump. The objective is the evaluation of the failure probability U of the subsystem up to the mission time $t_{miss} = 1848h$, since at that time components are put under maintenance and they are restored.

6.2. Importance Functions

Two Importance Functions (IFs) have been considered to apply the RESTART method and compare its performance to that of the crude Monte Carlo method. IF ϕ_1 is based only on the state of the pump and exploits the fact that the pump is the only source of (aleatory) uncertainty in the subsystem. Thus, two intermediate thresholds $(T_1, T_2) = (1/3\,, 2/3)$ are set (Villén-Altamirano, 2014):

$$\phi_1\left(t, \vec{X}\right) = \frac{3 - Z(t)}{3}. \quad \textbf{(10)}$$

The second IF ϕ_2 tries to consider the contribution of valve failures to the failure of the whole subsystem. Since the speed of degradation of the valve is dependent on the degradation of the pump (i.e., the higher the pump vibrations, the higher the degradation speed of the valve), the new IF takes into account also the pump transition times. Indeed, it can be seen that the mission time t_{miss} of the experiment is such that if the pump remains in state 3 (i.e., the normal functioning state), no valve failure can occur, because the leakage cannot reach the failure level. However, if the first transition time $t_{3\to2}$ of the pump occurs before a certain time $\bar{t}_{3\to2} = 629h$, then, valve failure could happen. This also depends on the time $t_{2\to1}$, when the second transition $2 \to 1$ occurs. It is

reasonable that the sooner transition $3 \rightarrow 2$ occurs (i.e., the smaller $t_{3\rightarrow 2}$), the larger the time window within which $2 \rightarrow 1$ can occur and can lead to valve failure. Thus, we can identify the set of pump transition times that can lead to the failure of the valve within the mission time. Figure 5 reports the function $t_{2\rightarrow 1} = f(t_{3\rightarrow 2})$ (black line), which gives the maximum time $t_{2\rightarrow 1}$ within which transition $2 \rightarrow 1$ must happen so that the valve failure occurs before t_{miss}: in other words, given the first pump transition time $t_{3\rightarrow 2}$, if $t_{2\rightarrow 1} < f(t_{3\rightarrow 2})$, then the system is going to fail before t_{miss}, either due to a deterministic degradation of the valve or to a possible third stochastic transition of the pump.

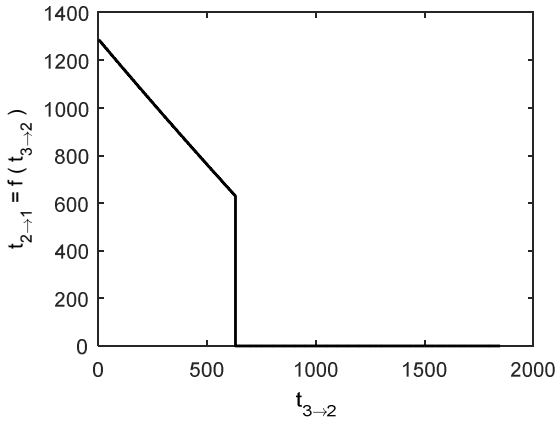

Figure 5 Maximum value that $t_{2\rightarrow 1}$ can assume to guarantee valve failure within t_{miss}

The new IF ϕ_2 is, then, based on the observation that the smaller is the number of transitions needed by the pump to lead the subsystem to failure, the higher should be the corresponding IF associated to that particular pump state. Thus, ϕ_2 can be expressed as follows:

$$\phi_2\left(t, \vec{X}\right) = \begin{cases} \dfrac{3 - Z(t)}{3}, & Z(t) \neq 2 \\ \dfrac{3 - Z(t)}{3} + \dfrac{1}{3} I_{(t \leq f(t_{3\rightarrow 2}))}, & Z(t) = 2 \end{cases} \quad (11)$$

The second term in (11) shows that if $t_{3\rightarrow 2} < \bar{t}_{3\rightarrow 2}$, then, ϕ_2 jumps directly from 0 to the second intermediate threshold T_2 equal to $2/3$, due to the high probability of valve failure. If the second

transition of pump state does not occur at time $t \leq f(t_{3\to 2})$, the possibility of valve failure ceases and the IF correspondingly decreases.

6.3. Results

Differently from Case Study 1 (Section 5), the RESTART and the MC methods are here compared by fixing the maximum variance of the estimator $\widehat{U}(t)$ for every time step t within a time window of interest. Thus, the performance index introduced in Section 2.2 practically "reduces" to the computational time (CPU) or to the Total Simulation Time (TST), i.e., the "number of hours" simulated by the dynamic system model. To this aim, the independent replication method with a non-fixed number of replicas has been used to evaluate, each time a new path is simulated during an experiment, the width of the 90% Confidence Interval (CI) of the Relative Error (RE) of the estimator $\widehat{U}(t)$ at every time step t (Villén-Altamirano, 2014). The replication of new paths in an experiment is interrupted when the widths of the CIs of the RE are lower than a given threshold (10%, in this paper) for all the time steps in the time window of interest. In this paper, the time window considered is $[t_{check1}, t_{check2}] = [1700h, 1848h]$, which includes the time where the contribution of valve failures to the failure of the subsystem starts to become relevant and where, thus, our attention is focused. Figure 6 reports the mean value $E[\widehat{U}]$ and the 0.05 and 0.95 percentiles of $\widehat{U}$ obtained using 100 estimators produced by crude MC and RESTART using the two different IFs ϕ_1 and ϕ_2 described in Section 6.2. All the methods return almost the same average estimate confirming that the corresponding estimators are unbiased. In Figure 6 (middle right), a zoom on the critical time window shows how the three methods obtain the desired precision for the failure probability estimates around $1700h$, where the RE reaches its maximum value within the time window of interest. The other two zooms (top and bottom) show that the MC

Simulation tends to present respectively the largest Confidence Intervals (CIs) before $1700h$ and the smallest after that time; the opposite behavior is obtained for ϕ_1. On the contrary, the CIs obtained by ϕ_2 take average values showing a higher robustness according to the chosen stopping criterion.

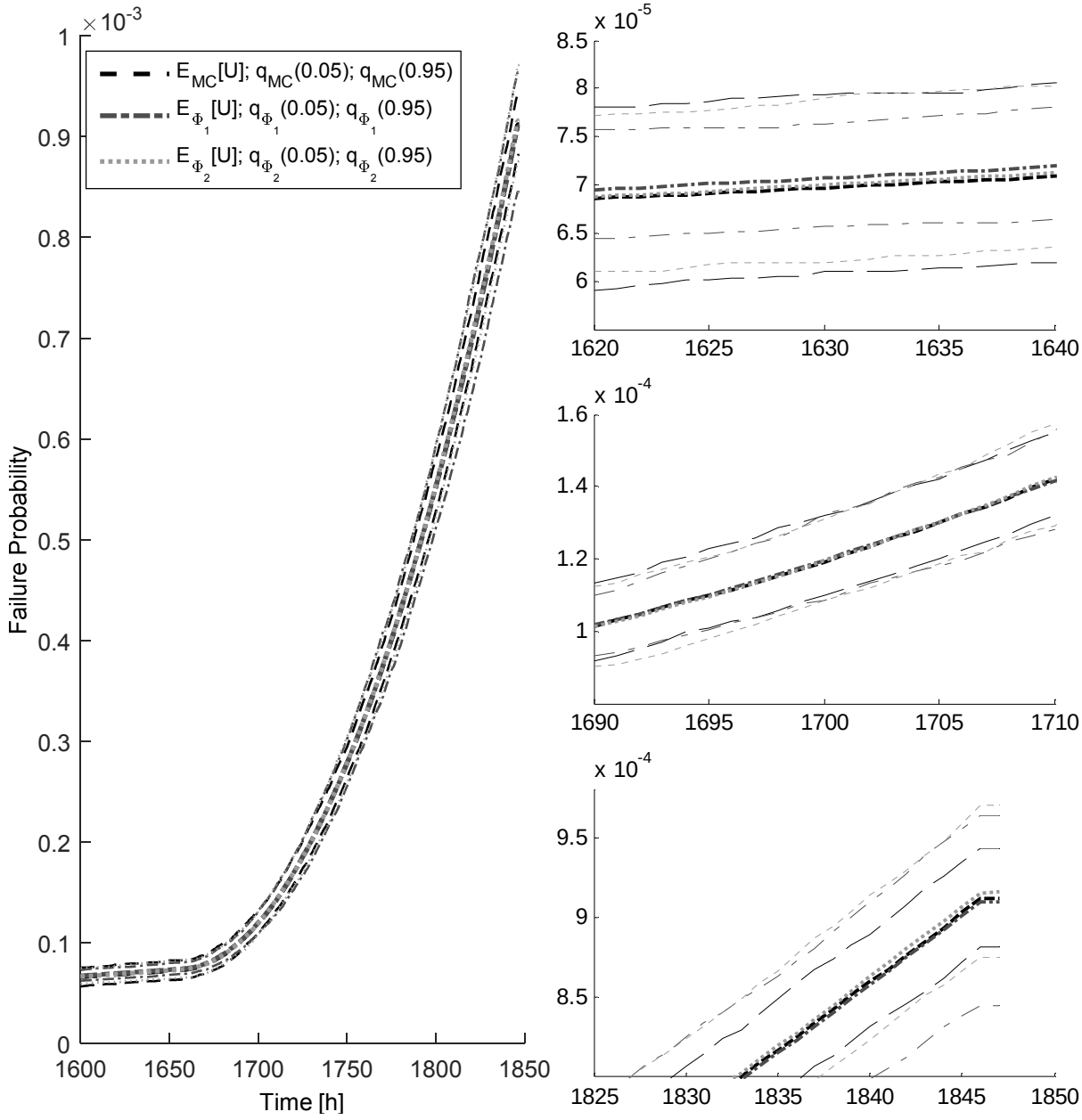

Figure 6 Left column: average failure probability and respective 0.05 - 0.95 percentiles obtained by 100 estimators of the subsystem evolution with crude Monte Carlo (MC, dashed lines), RESTART $\boldsymbol{\Phi_1}$ (dashed-dotted lines) and RESTART $\boldsymbol{\Phi_2}$ (dotted lines). Right column: zoom on different time windows of the same quantities.

In Table 3 the Total Simulation Times (TSTs) needed by the different methods to get the desired precision are proposed. Both the RESTART methods save at least 90% of the TST compared to the crude Monte Carlo, obtaining gains G larger than 10. Furthermore ϕ_2 outperforms ϕ_1, getting on average a gain of 17.89 (larger than 16.56), which is closer to the optimal gain G (1) introduced in section 2.2 which, in this case study, is around 18. The number of retrials R_i starting from each threshold T_i has been chosen via a trial-and-error technique that has led to $R_{\phi_1} = [R_1(\phi_1), R_2(\phi_1)] = [20, 4]$ and $R_{\phi_2} = [R_1(\phi_2), R_2(\phi_2)] = [8, 8]$. It is worth noting that ϕ_2 presents the same number of retrials at both thresholds, in accordance with the quasi-optimal results proposed in (Villén-Altamirano and Villén-Altamirano, 2002). On the contrary, the disparity between the retrials of ϕ_1 is caused by the different probabilities that the IF has of crossing a given threshold, given the actual state of the subsystem.

Table 3 Mean Total Simulation Time (TST) and gain obtained by 100 replications, respectively, with crude Monte Carlo (MC); RESTART with ϕ_1 and ϕ_2 as Importance Functions.

	MC	**RESTART ϕ_1**	**RESTART ϕ_2**
TST	4.51×10^9	2.72×10^8	2.52×10^8
$Gain, G$	-	16.56	17.89

7. CONCLUSIONS

The RESTART method has been here used, for the first time, for the estimation of the failure probability of hybrid dynamic systems due to its capability of thoroughly exploring, by means of sequences of retrials, paths that could potentially lead to rare failure events and also for the possibility of embedding discrete and continuous variables (typically describing a hybrid system) within a single scalar IF. For this reason, an extension of the IF definition has been necessary. Two case studies have been considered: the first concerns the control system of a liquid hold-up tank;

the second deals with a pump-valve subsystem subject to degradation induced by fatigue. The two case studies have shown how the performance of the RESTART method (quantified in terms of estimation accuracy, precision and associated computational cost) can be increased by properly taking into account the contribution of both the continuous and the discrete variables (characterizing the hybrid system) in the definition of the Importance Function (IF).

In the first case study, it has been shown that taking into account the contribution of continuous variables in the construction of the IF allows increasing the performance of the RESTART by an order of magnitude with respect to crude Monte Carlo simulation and by a factor of 2 with respect to RESTART employing classical, “discrete” IFs already available in the literature.

In the second case study, some preliminary knowledge about the possible failure sequences has led to the introduction of a new IF capable of considering the dependences between the degradation of the two process components of the system. By so doing, the performance of the RESTART has been found to be close to the optimal theoretical one derived in (Villén-Altamirano and Villén-Altamirano, 2002). Although in this paper it has been shown, by means of two case studies, that the introduction of an IF considering both continuous and discrete variables can increase the performance of the RESTART method in the analysis of hybrid, dynamic systems, it has to be admitted that a *general* procedure for an *automatic* design of an efficient IF is not yet available, especially for complex, multi-components, multi-state systems.

8. REFERENCES

(Aldemir, 1987) Aldemir T. "Computer-assisted Markov failure modeling of process control systems." Reliability, IEEE Transactions on 36.1 (1987): 133-144.

(Aldemir, 2013) Aldemir, Tunc. "A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants." Annals of Nuclear Energy 52 (2013): 113-124.

(Amrein and Künsch, 2011) Amrein M. and H. R. Künsch. "A variant of importance splitting for rare event estimation: Fixed number of successes." ACM Transactions on Modeling and Computer Simulation (TOMACS) 21.2 (2011): 13.

(Asmussen and Glynn, 2007) Asmussen S. and P. W. Glynn. “Stochastic Simulation: Algorithms and Analysis: Algorithms and Analysis.” Vol. 57. Springer, 2007, New York, NY.

(Asmussen et al., 2011) Asmussen S. et al. "Efficient simulation of tail probabilities of sums of correlated lognormals." Annals of Operations Research 189.1 (2011): 5-23.

(Au and Beck, 2001) Au S.-K. and J. L. Beck. "Estimation of small failure probabilities in high dimensions by subset simulation." Probabilistic Engineering Mechanics 16.4 (2001): 263-277.

(Au and Beck, 2003a) Au S. K. and J. L. Beck, "Important sampling in high dimensions." Structural Safety 25.2 (2003): 139-163.

(Au and Beck, 2003b) Au S. K. and J. L. Beck, "Subset simulation and its application to seismic risk based on dynamic analysis." Journal of Engineering Mechanics 129.8 (2003): 901-917.

(Au and Wang, 2014) Au S. K. and Y. Wang. Engineering Risk Assessment with Subset Simulation. John Wiley & Sons, 2014, Singapore Pte. Ltd.

(Au et al., 2007) Au, S. K., J. Ching and J. L. Beck. "Application of subset simulation methods to reliability benchmark problems." Structural Safety 29.3 (2007): 183-193.

(Au, 2004) Au S. K. "Probabilistic failure analysis by importance sampling Markov chain simulation." Journal of Engineering Mechanics 130.3 (2004): 303-311.

(Bayes, 1970) Bayes A. J. "Statistical techniques for simulation models." Australian computer journal 2.4 (1970): 180-184.

(Blom et al., 2006) Blom, H. A.P. et al. Stochastic hybrid systems: theory and safety critical applications. Vol. 337. Heidelberg: Springer, 2006.

(Botev and Kroese, 2008) Botev Z. I., and D. P. Kroese. "An efficient algorithm for rare-event probability estimation, combinatorial optimization, and counting." Methodology and Computing in Applied Probability 10.4 (2008): 471-505.

(Botev and Kroese, 2012) Botev Z. I., and D. P. Kroese. "Efficient Monte Carlo simulation via the generalized splitting method." Statistics and Computing 22.1 (2012): 1-16.

(Botev et al., 2013a) Botev Z. I., P. L’Ecuyer and B.Tuffin. "Markov chain importance sampling with applications to rare event probability estimation." Statistics and Computing 23.2 (2013): 271-285.

(Botev et al., 2013b) Botev Z. I. et al. "Static network reliability estimation via generalized splitting." INFORMS Journal on Computing 25.1 (2013): 56-71.

(Bucklew, 2004) Bucklew J. “Introduction to rare event simulation.” Springer, 2004, New Yorkl.

(Cacuci and Ionescu-Bujor, 2004) Cacuci D. G. and M. Ionescu-Bujor. "A comparative review of sensitivity and uncertainty analysis of large-scale systems. II: statistical methods." Nuclear Science and Engineering 147.3 (2004): 204-217.

(Cadini et al., 2012) Cadini F., et al. "Subset Simulation of a reliability model for radioactive waste repository performance assessment." Reliability Engineering & System Safety 100 (2012): 75-83.

(Cassandras and Lygeros, 2006) Cassandras, C. G. and J. Lygeros. Stochastic hybrid systems. Boca Raton: CRC Press, Taylor & Francis group, 2006.

(Catalyurek et al., 2010) Catalyurek U., et al. "Development of a code-agnostic computational infrastructure for the dynamic generation of accident progression event trees." Reliability Engineering & System Safety 95.3 (2010): 278-294.

(Cérou and Guyader, 2007) Cérou F. and A. Guyader. "Adaptive multilevel splitting for rare event analysis." Stochastic Analysis and Applications 25.2 (2007): 417-443.

(Cérou et al., 2012) Cérou, F. et al. "Sequential Monte Carlo for rare event estimation." Statistics and Computing 22.3 (2012): 795-808.

(Čepin and Mavko, 2002) Čepin, M. and B. Mavko "A dynamic fault tree." Reliability Engineering & System Safety 75.1 (2002): 83-91.

(Ching et al., 2005) Ching J., S. K. Au and J. L. Beck. "Reliability estimation for dynamical systems subject to stochastic excitation using subset simulation with splitting." Computer methods in applied mechanics and engineering 194.12 (2005): 1557-1579.

(Davis, 1984) Davis M. H. "Piecewise-deterministic Markov processes: A general class of non-diffusion stochastic models." Journal of the Royal Statistical Society. Series B (Methodological) (1984): 353-388.

(Davis, 1993) Davis M. H. "Markov Models & Optimization". Vol. 49. CRC Press, 1993, Boca Ranton, Florida.

(De Boer et al., 2005) De Boer P.-T. et al. "A tutorial on the cross-entropy method." Annals of operations research 134.1 (2005): 19-67.

(Dupuis et al., 2007) Dupuis P., K. Leder, and H. Wang. "Importance sampling for sums of random variables with regularly varying tails." ACM Transactions on Modeling and Computer Simulation (TOMACS) 17.3 (2007): 14.

(EPA, 2009) "Guidance on the Development, Evaluation, and Application of Environmental Models" Council for Regulatory Environmental Modeling, U.S. Environmental Protection Agency, Washington DC 20460, 2009.

(Garvels and Kroese, 1998) Garvels M. JJ, and D. P. Kroese. "A comparison of RESTART implementations." Simulation Conference Proceedings, 1998. Winter. Vol. 1. IEEE, 1998.

(Garvels et al., 2002) Garvels Marnix JJ, Jan-Kees C.W. Van Ommeren, and Dirk P. Kroese. "On the importance function in splitting simulation", European Transactions on Telecommunications 13.4 (2002): 363-371.

(Garvels, 2011) Garvels M. JJ. "A combined splitting-cross entropy method for rare-event probability estimation of queueing networks." Annals of Operations Research 189.1 (2011): 167-185.

(Görg and Schreiber, 1996) Görg C. and F. Schreiber, "The RESTART/LRE method for rare event simulation." Proceedings of the 28th conference on Winter simulation. IEEE Computer Society, 1996.

(Helton and Davis, 2003) Helton J. C. and F. J. Davis, "Latin hypercube sampling and the propagation of uncertainty in analyses of complex systems." Reliability Engineering & System Safety 81.1 (2003): 23-69.

(Jacobsen, 2006) Jacobsen M. "Point process theory and applications." Birkhũser Boston, 2006.

(Kahn and Harris, 1951) Kahn H. and T. E. Harris. "Estimation of particle transmission by random sampling." National Bureau of Standards applied mathematics series 12 (1951): 27-30.

(Labeau, 1996) Labeau, P.-E. "Probabilistic dynamics: estimation of generalized unreliability through efficient Monte Carlo simulation." Annals of Nuclear Energy 23.17 (1996): 1355-1369.

(Labeau et al., 2000) Labeau, P.-E., C. Smidts, and S. Swaminathan. "Dynamic reliability: towards an integrated platform for probabilistic risk assessment." Reliability Engineering & System Safety 68.3 (2000): 219-254.

(Lagnoux, 2006) Lagnoux A. "Rare event simulation." Probability in the Engineering and Informational Sciences 20.01 (2006): 45-66.

(Lin et al., 2014) Lin Y.H., Y.F. Li and E. Zio. "Dynamic Reliability Models for Multiple Dependent Competing Degradation." Proceedings of the European Safety and Reliability Conference ESREL 2014.

(Marseguerra and Zio, 1996) Marseguerra M. and E. Zio. "Monte Carlo approach to PSA for dynamic process systems." Reliability Engineering & System Safety 52.3 (1996): 227-241.

(Li et al., 2010) Li J., A. Mosleh and R.Kang. "From Blind to Guided Simulation: Biased Monte Carlo Based on Entropy and Zero Variance for Dynamic PSA Applications." Proceedings of the 10th International Conference on Probabilistic Safety Assessment and Management (PSAM-10) 2010.

(Li et al., 2011) Li J., A. Mosleh and R. Kang. "Likelihood ratio gradient estimation for dynamic reliability applications." Reliability Engineering & System Safety 96.12 (2011): 1667-1679.

(Munoz Zuniga M. et al., 2011) Munoz Zuniga M., et al. "Adaptive directional stratification for controlled estimation of the probability of a rare event." Reliability Engineering & System Safety 96.12 (2011): 1691-1712.

(Murray et al., 2013) Murray L., H. Cancela, and G. Rubino. "A splitting algorithm for network reliability estimation." IIE Transactions 45.2 (2013): 177-189.

(NASA, 2010) "Risk-Informed Decision Making Handbook." NASA/SP-2010-576, Version 1.0, 2010.

(Rao et al., 2009) Rao, K. D., et al. "Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment." Reliability Engineering & System Safety 94.4 (2009): 872-883.

(Robert and Casella, 2004) Robert C. P. and G. Casella. "Monte Carlo statistical methods." Vol. 319. New York: Springer, 2004.

(Rubino and Tuffin, 2009) Rubino, G. and B. Tuffin, eds. Rare event simulation using Monte Carlo methods. New York: Wiley, 2009.

(Rubinstein and Kroese, 2004) Rubinstein R. Y., and D. P. Kroese. "The cross-entropy method: a unified approach to combinatorial optimization, Monte-Carlo simulation and machine learning." Springer, 2004, New York, NY.

(Schuëller and Pradlwarter, 2007) Schuëller G. I. and H. J. Pradlwarter. "Benchmark study on reliability estimation in higher dimensions of structural systems–an overview." Structural Safety 29.3 (2007): 167-182.

(Siu, 1994) Siu N. "Risk assessment for dynamic systems: an overview." Reliability Engineering & System Safety 43.1 (1994): 43-73.

(Tuffin and Trivedi, 2000) Tuffin B. and K. S. Trivedi. "Implementation of importance splitting techniques in stochastic Petri net package." Computer Performance Evaluation. Modelling Techniques and Tools. Springer Berlin Heidelberg, 2000. 216-229.

(USNRC, 2009) "Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making." NUREG-1855, US Nuclear Regulatory Commission, Washington DC, 2009.

(Valdebenito et al., 2010) Valdebenito M. A., H. J. Pradlwarter and G. I. Schuëller. "The role of the design point for calculating failure probabilities in view of dimensionality and structural nonlinearities." Structural Safety 32.2 (2010): 101-111.

(Villén-Altamirano and Villén-Altamirano, 1991) Villén-Altamirano M. and J. Villén-Altamirano, "RESTART: A Method For Accelerating Rare Event Simulations." Analysis 3 (1991): 3.

(Villén-Altamirano and Villén-Altamirano, 1994) Villén-Altamirano M. and J. Villén-Altamirano, "RESTART: a straightforward method for fast simulation of rare events." Simulation Conference Proceedings, 1994. Winter. IEEE, 1994.

(Villén-Altamirano and Villén-Altamirano, 2002) Villén-Altamirano M. and J. Villén-Altamirano, "Analysis of RESTART simulation: Theoretical basis and sensitivity study." European Transactions on Telecommunications 13.4 (2002): 373-385.

(Villén-Altamirano and Villén-Altamirano, 2006) Villén-Altamirano M. and J. Villén-Altamirano, "On the efficiency of RESTART for multidimensional state systems." ACM Transactions on Modeling and Computer Simulation (TOMACS) 16.3 (2006): 251-279.

(Villén-Altamirano and Villén-Altamirano, 2011) Villén-Altamirano M. and J. Villén-Altamirano. "The rare event simulation method RESTART: efficiency analysis and guidelines for its application." Network performance engineering. Springer Berlin Heidelberg, 2011. 509-547.

(Villén-Altamirano, 2007) Villén-Altamirano J., "Importance functions for RESTART simulation of highly-dependable systems." Simulation 83.12 (2007): 821-828.

(Villén-Altamirano, 2010a) Villén-Altamirano J. "RESTART simulation of non-Markov consecutive-*k*-out-of-*n*: F repairable systems." Reliability Engineering & System Safety 95.3 (2010): 247-254.

(Villén-Altamirano, 2010b) Villén-Altamirano J., "Importance functions for restart simulation of general Jackson networks", European Journal of Operational Research 203.1 (2010): 156-165.

(Villén-Altamirano, 2014) Villén-Altamirano J., "Asymptotic optimality of RESTART estimators in highly dependable systems", Reliability Engineering & System Safety 130 (2014): 115-124.

(Zhu et al., 2006) Zhu D., A. Mosleh, and C. Smidts. "A framework to integrate software behavior into dynamic probabilistic risk assessment." Reliability Engineering & System Safety 92.12 (2007): 1733-1755.

(Zio and Pedroni, 2010) Zio E. and N. Pedroni. "An optimized Line Sampling method for the estimation of the failure probability of nuclear passive systems." Reliability Engineering & System Safety 95.12 (2010): 1300-1313.

(Zio, 2013) Zio E., “The Monte Carlo Simulation Method for System Reliability and Risk Analysis”, Springer, 2013.