Reliability Engineering and System Safety 154 (2016) 117–126

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

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

Pietro Turati [a], Nicola Pedroni [a], Enrico Zio [a,b,*]

[a] 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
[b] Energy Department, Politecnico di Milano, Via La Masa 34, Milano 20156, Italy

ARTICLE INFO

Article history:
Received 9 December 2014
Received in revised form
8 June 2015
Accepted 19 April 2016
Available online 6 June 2016

Keywords:
Advanced Monte Carlo method
RESTART
Piecewise Deterministic Markov Process (PDMP)
Hybrid dynamic system
Importance function
Efficient failure probability estimation

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.

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 [56,31,48].

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 [69]. 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

* Corresponding author at: Energy Department, Politecnico di Milano, Via La Masa 34, Milano 20156, Italy.
E-mail addresses: enrico.zio@polimi.it, enrico.zio@ecp.fr, enrico.zio@supelec.fr (E. Zio).

http://dx.doi.org/10.1016/j.ress.2016.04.020
0951-8320/

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 [18,50,51]. Examples of these methods include Stratified Sampling [36,19,46]; Importance Sampling (IS) [7,11,4,30,5] and its variants, such as the cross-entropy method [52,29,4,14] or the recent Markov Chain Monte Carlo (MCMC) IS [16]; Subset Simulation [6,8,26,10,20,9]; Line Sampling [53,68,57] and Splitting Methods [38,34,15,17,47]. 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 [39], and consistently developed through years [40]. In [67] 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. In [25], and [49] the authors evaluate system failure probabilities by resorting to dynamic fault trees. A method exploiting Dynamic Event Tree (DET) and Monte Carlo simulation is proposed in [44,45] 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 [22,2] 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 [24] and large hybrid dynamic systems [13,21].

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 [58,59,35,32,55] 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 [60]. 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 [33,61,41,23,3]. 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 [43] and the second is a system composed by a pneumatic valve and a centrifugal pump subject to degradation [42]. 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 [63,65,66], 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 [12] and has been developed mainly in [60–62]. 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 $\phi : \Omega \rightarrow \mathbb{R}$, called Importance Function (IF), is introduced to identify a sequence of nested "intermediate" states sets $C_i \subset \Omega$, $(C_1 \supset C_2 \supset \ldots \supset C_M)$: these sets are of the form $C_i = \{ x(t) \in \Omega : \phi(x(t)) > T_i \}$, where $T_1 < \ldots < T_M$ 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