Reliability Engineering and System Safety 152 (2016) 115–136

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Modeling and simulation of a controlled steam generator in the context of dynamic reliability using a Stochastic Hybrid Automaton☆

Génia Babykina [a,b,*,1], Nicolae Brînzei [a,b], Jean-François Aubry [a,b], Gilles Deleuze [c]

[a] Université de Lorraine, CRAN, UMR 7039, 2, avenue de la forêt de Haye, Vandœvre-lès-Nancy 54516, France
[b] CNRS, CRAN, UMR 7039, France
[c] Électricité de France (EDF) R&D Management des Risques Industriels, 1, avenue de Général de Gaulle, 92141 Clamart, France

ARTICLE INFO

Article history:
Received 28 January 2013
Received in revised form
7 March 2016
Accepted 13 March 2016
Available online 21 March 2016

Keywords:
Dynamic reliability
Stochastic Hybrid Automaton
Automata composition
Monte Carlo simulations
Sequence analysis
Reliability assessment
Power plant subsystem
Steam generator dynamics

ABSTRACT

The paper proposes a modeling framework to support Monte Carlo simulations of the behavior of a complex industrial system. The aim is to analyze the system dependability in the presence of random events, described by any type of probability distributions. Continuous dynamic evolutions of physical parameters are taken into account by a system of differential equations. Dynamic reliability is chosen as theoretical framework. Based on finite state automata theory, the formal model is built by parallel composition of elementary sub-models using a bottom-up approach. Considerations of a stochastic nature lead to a model called the Stochastic Hybrid Automaton. The Scilab/Scicos open source environment is used for implementation. The case study is carried out on an example of a steam generator of a nuclear power plant. The behavior of the system is studied by exploring its trajectories. Possible system trajectories are analyzed both empirically, using the results of Monte Carlo simulations, and analytically, using the formal system model. The obtained results are show to be relevant. The Stochastic Hybrid Automaton appears to be a suitable tool to address the dynamic reliability problem and to model real systems of high complexity; the bottom-up design provides precision and coherency of the system model.

1. Introduction

Most real-world industrial systems have a significant complexity level. The complexity lies in a variety of elements such as system size, number and structure of interactions between system components and of interactions between the system and its dynamic operational environment, and varying mechanisms for the aging of components. Due to this complexity, elaborated methods are needed to study the behavior of a system, to evaluate its performance and to assess the system reliability. In this sense conventional approaches to reliability assessment, such as event and fault trees, and reliability block diagrams, are often not adapted. Indeed, these methods are not designed to account for the dynamic structure function of a system. The dynamic reliability approach, in its turn, covers a wide range of problems and phenomena mentioned above and is thus a relevant framework to model complex systems operating in dynamic environment.

Numerous methods have been developed to address dynamic reliability, such as analytical solutions of systems of stochastic differential equations, their approximations using numerical methods, and Monte Carlo simulations. Methodologically attractive analytical solutions are very complex; thus, possible applications are limited to only very simple cases. Monte Carlo simulations, in their turn, allow us to capture detailed system behavior, and are thus a more realistic alternative to analytical methods when dealing with complex real-world systems. Moreover, simulations provide a variety of data, thus allowing a comprehensive statistical analysis.

☆This work was supported by the Groupement d'Intérêt Scientifique “Surveillance, Sûreté et Sécurité des Grands Systèmes” (GIS 3SGS, a French research network in the “Surveillance, Safety and Security of large systems”) under APPROches de la fiabilité DYNamique pour modéliser des systèmes critiques (APPRODYN) Grant.

* Corresponding author. Now with: Université de Lille, CERIM, E.A. 2694, 42, rue Ambroise Paré, Loos 59120, France.
E-mail addresses: evgeniya.babykina@univ-lille2.fr (G. Babykina), nicolae.brinzei@univ-lorraine.fr (N. Brînzei), jean-francois.aubry@univ-lorraine.fr (J.-F. Aubry), gilles.deleuze@edf.fr (G. Deleuze).
[1] G. Babykina was with the Université de Lorraine when this work was accomplished.

http://dx.doi.org/10.1016/j.ress.2016.03.009
0951-8320/

Monte Carlo simulations require an underlying input model that describes the behavior of the system. Different input models, or representation schemes, are available in the framework of dynamic reliability, such as stochastic Petri nets, graphical Markov models, and state-transition graphs (see [1] for comparison and a detailed review).

In this paper Monte Carlo simulations in the context of dynamic reliability are used to analyze the behavior of part of a nuclear power plant, more precisely, a sub-system involved in water level control of a steam generator. As highly critical and complex systems, the installations issued from the nuclear energy production industry are frequently used as case studies for reliability and safety assessment methodologies. Different methods are proposed for analysis. One can refer to [2] for the Petri Nets approach, [3,4] for the Markov/cell-to-cell mapping, [5–7] for the Discrete Dynamic Event Trees, [8] for the continuous-time Markov models combined with Reliability Block Diagrams, and [9] for other state-space models.

In this paper the Stochastic Hybrid Automaton (SHA) is proposed as the main tool for the reliability analysis of a system. The SHA is used as an input model for Monte Carlo simulations carried out to generate data for further statistical analysis of system reliability. The SHA is built using a formal "*bottom-up*" approach, which insures the completeness and relevance of the model.

The objectives of the present study are two-fold:

1. From a methodological point of view, the work aims to present the SHA as a tool for dynamic reliability assessment, to emphasize the advantage of using formal model construction methods when dealing with complex systems and to present the types of results that can be obtained with the proposed tools.
2. From a practical point of view, the work aims to address dynamic reliability in an applied context, employing the SHA to a large real-world system and to provide a rather detailed description of the analyzed system, thus enabling its further exploitation as a case study.

The paper is organized as follows. Section 2 covers the theoretical background for dynamic reliability. A formal model construction method and a definition of the SHA are given in Section 3. Section 4 details how the Scicos/Scilab software can be used to implement the SHA. The case study is addressed in Section 5 (a general description of the considered system) and in Section 6 (a formal system model and its implementation in Scicos/Scilab). The results are presented and discussed in Section 7.

2. Dynamic reliability: theoretical background

2.1. The concept of dynamic reliability

Generally, dynamic reliability as defined in [1,10,11] is a part of probabilistic safety analysis, studying the behavior of human–machine interface systems affected by underlying dynamic evolution. The general mathematical formulation for dynamic reliability is described in [12–14]. An overview of existing models is provided in [1]. A survey of dynamic reliability methodologies specifically used in the sphere of nuclear energy can be found in [15]. In general, the model for dynamic reliability is described as follows. We suppose that a system (for example, an industrial installation) is represented by a state-transition graph, where the system state is a combination of the states of its components. This system operates in a dynamic environment, represented by a set of continuous variables, which are called physical or process variables. Deterministic dynamics of these variables are formalized by a system of differential equations. It is assumed that the coefficients of these equations depend on the system states.

In the context of safety analysis, dynamic reliability can be seen as an extension of system reliability assessment methods to the case in which the structure function changes in time with a discrete evolution (*e.g.* in the case of a phased-mission system) and with a continuous evolution (*e.g.* in the case of dependency between the reliability of components and continuous physical variables). The structure function is meant to be a function describing the link between the states of system components, usually represented by their failures and repairs, and the state of the system itself.

The dynamic reliability accounts for the following phenomena:

- dynamic behavior of system components (aging and fatigue of different types);
- importance of the order of occurring events (ordered sequences of events are considered in place of cut sets);
- multiple natures (stochastic and deterministic) of events driving the transitions between states.

Building a mathematical model accounting for these phenomena implies specifying an analytical expression of the temporal evolution of physical variables and an explicit link between the system reliability parameters and these variables. Thus, mathematical formulation of the dynamic reliability problem is a complex set of equations.

2.2. Mathematical formulation for dynamic reliability

Following, for example, [10], the mathematical model for dynamic reliability is represented in the form of Chapman–Kolmogorov equations (for a detailed interpretation of model terms one can refer to [16, Section 3]). Initially relying on the Markovian assumption (the future of the system depends on its present state and not on event sequences leading to this present state), this model has been extended to a non-Markovian framework, allowing non-exponential temporal distributions for stochastic transitions and also deterministic transitions. The model gives an analytical expression of equations providing the probabilities of a system to be in a certain state at a certain time, given the environmental conditions or, more precisely, the values of physical variables affecting the system.

Another widely used representation of the dynamic reliability problem is a Piecewise Deterministic Markov Process (PDMP), originally defined by Davis [17] as a general class of non-diffusion dynamic stochastic hybrid models, *i.e.* deterministic motions punctuated by random jumps. Its formal definition is given below.

Definition 2.1 (*Piecewise Deterministic Markov Process*). Piecewise Deterministic Markov Process PDMP is a process $Y_t = (m_t, \boldsymbol{x}_t)$, where

- t indicates time and will further be omitted in subscripts for simplicity;
- $m \in \mathbb{M}$, with $\mathbb{M}$ being a countable set, are discrete modes;
- $\boldsymbol{x} \in \mathbb{R}^n$ is a set of real state variables representing physical variables of the system.

The PDMP is determined by a set of local characteristics in each mode m:

- E_m an open subset of $\mathbb{R}^n$ with its boundary ∂E_m and its closure $\overline{E}_m$;
- $\phi_m(\boldsymbol{x}, t) : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n$ is a flow corresponding to the deterministic dynamics of physical variables;