Modelling a feed-water control system of a steam generator in the framework of the dynamic reliability

Génia Babykina, Nicolae Brinzei, Jean-François Aubry, Gilles Deleuze

Modelling a feed-water control system of a steam generator in the framework of the dynamic reliability

G. Babykina, N. Brînzei, & J.-F. Aubry
CRAN CNRS UMR 7039, Université de Lorraine, ENSEM
2, avenue de la Fôret de Haye, 54516 Vandœuvre-les-Nancy, FRANCE
Tel.: +33(0)3 83 59 56 36, Fax: +33 (0)3 83 59 56 44
e-mail: {genia.babykina, nicolae.brinzei, jean-francois.aubry} @ univ-lorraine.fr

G. Deleuze
Électricité de France (EDF) R&D Management des Risques Industriels
1, avenue de Général de Gaulle, 92141 Clamart, FRANCE
e-mail: gilles.deleuze@edf.fr

ABSTRACT: The paper deals with the exploration of an industrial complex system behaviour and its probabilistic safety assessment (PSA). The main purposes are to build a model which realistically represents the system structure, to carry out the Monte Carlo study of the system behaviour and to perform the analysis of system reliability. The complexity of the system consists in its structure, size, dynamic operational behaviour, complex interactions between the system and its environment, *etc*. The theoretical framework chosen is the dynamic reliability approach allowing to account for all of these properties. The Stochastic Hybrid Automaton (SHA), seen as a flexible representation of the Piecewise Deterministic Markov Process, is a suitable tool to simultaneously represent continuous and discrete, stochastic and deterministic phenomena, and is thus employed as a formal model to draw the system structure and behaviour. This formal model (SHA) is effectively implemented in Scilab/Scicos open source freeware. This tool is efficient to simulate both the differential equations and discrete state changes when events occur. The differential equations represent the continuous evolution of physical variables describing the dynamic operational behaviour. The discrete states describe the various operating and dysfunctional modes of the system. A real-life system is used to perform a case study of the proposed approach. Precisely, within the French research project APPRODYN (APPROches de la fiabilité DYNamique pour modéliser des systèmes critiques - Dynamic reliability approaches to model critical systems), the feed-water control system of a steam generator of a pressurised water nuclear reactor is modelled. This system consists of different interacting components which simultaneously function according to the power demand. The power is a continuous variable representing operational behaviour. The built behavioural model and performed Monte Carlo simulations are used to study the trajectories of the system behaviour and to evaluate the probability of critical events occurrence.

1 INTRODUCTION

Real-world industrial systems are often complex in terms of their size, the structure of interactions between system components, the dynamic operational behaviour, ageing, *etc.* Thus, elaborated methods are needed to model behaviour of such systems and to assess their reliability. Traditional approaches to the reliability assessment not accounting for the dynamic structure function of a system (event and fault trees, reliability block diagrams, *etc.*) are often not suitable in this sense, whereas the dynamic reliability approach, covering a wide range of phenomena mentioned above, is a convenient framework to model the behaviour of complex systems operating in a dynamic environment.

The general solution for dynamic reliability can be approached by exact methods (finding analytical solutions of system equations) or by approximation (using numerical methods or by means of Monte Carlo simulations). Exact analytical solutions are rather complex and require simplifying hypotheses as for the modelled system, whereas Monte Carlo simulations allow realistic modelling and provide abundant data

for comprehensive statistical analysis.

In this paper two approaches to the dynamic reliability problem are presented: the Piecewise Deterministic Markov Process (PDMP) and the Stochastic Hybrid Automaton (SHA), which can be seen as an alternative and a more flexible formulation of the PDMP. A feed-water control system of a power plant steam generator is used as a case study to illustrate how the SHA can be applied to model a complex system operating in a dynamic environment and to assess its reliability. The paper is organized as follows. The theoretical framework of the employed methodology (dynamic reliability, PDMP and SHA) is summarised in Section 2. The system considered as a case study is described in Section 3. Section 4 deals with the implementation procedure, and some results are presented in Section 5. Conclusions and perspectives are given in Section 6.

2 THEORETICAL BACKGROUND

2.1 *Mathematical model for dynamic reliability*

The dynamic reliability is defined by Labeau et al. (2000) as a part of probabilistic safety analysis, studying the behaviour of human-machine interface systems affected by underlying dynamic evolution. More specifically, it is supposed that a system is represented by a state-transition graph, where the state is a combination of states of system components; the system's dynamic behaviour is represented by a set of continuous variables whose deterministic dynamics is formalised by a system of differential equations with coefficients depending on the system states (Cocozza-Thivent et al. 2006). Thus, the dynamic reliability allows accounting for numerous characteristics of complex systems, such as the interactions between continuous process variables and system components, for the dynamic behaviour of its components, stochastic and deterministic events characterising the transitions, *etc*.

The mathematical model for the dynamic reliability is proposed by Devooght and Smidts (1992) and is further approached by Devooght and Smidts (1996), Izquierdo et al. (1996), Marseguerra et al. (1998), Labeau et al. (2000). The model relies on the Markovian assumption and generally gives the analytical expression for the probability for a system to be in a certain state at a certain time, given the environmental conditions. The formal definition for the dynamic reliability problem is given below.

Definition 2.1 *(Mathematical model for dynamic reliability).*
Let:

- $i = (i(1), i(2), \cdots i(N))$ *be a vector of discrete states combination of* N *system components; this vector defines a state of the system;*
- $\boldsymbol{x} \in \mathbb{R}^n$ *be a vector of state variables describing the system behaviour and deterministically evolving in time* t *according to a state-specific systems of differential equations* $\boldsymbol{f}_i(\boldsymbol{x}(t), t) = d\boldsymbol{x}(t)/dt$*, with its solution* $\boldsymbol{x}(t) = \boldsymbol{g}_i(\boldsymbol{x}_0, t)$*,* $\boldsymbol{x}_0$ *being the initial values for state variables;*
- $\lambda_j(\boldsymbol{x})$ *be the global transition rate from the state* j *as a function of physical variables;*
- $p(j \to i \,|\, \boldsymbol{x})$ *be the specific transition rate from state* j *to state* i*, knowing the trajectory of physical variables, with* $\lambda_j(\boldsymbol{x}) = \sum_{j \neq i} p(j \to i \,|\, \boldsymbol{x})$*;*
- $\pi(\boldsymbol{x}, i, t)$ *be the probability density for a system to be in state* i *at time* t *with the physical variables vector* $\boldsymbol{u}$ *being equal to* $\boldsymbol{x}$*, obeying generalised Chapman-Kolmogorov equations (Devooght and Smidts 1992);*
- $\delta(\cdot)$ *be the Dirac delta function.*

The mathematical model for the dynamic reliability of a system is then defined as follows:

$$
\begin{aligned}
\pi(\boldsymbol{x}, i, t) \;=\; & \int_{\boldsymbol{x}_0}^{\boldsymbol{x}} \pi(\boldsymbol{u}, i, 0)\, \delta(\boldsymbol{x} - \boldsymbol{g}_i(\boldsymbol{u}, t)) \\
& \exp\left[- \int_0^t \lambda_i(\boldsymbol{g}_i(\boldsymbol{u}, s))\, \mathrm{d}s \right] \mathrm{d}\boldsymbol{u} \\
+ \; & \sum_{j \neq i} \int_{\boldsymbol{x}_0}^{\boldsymbol{x}} p(j \to i \,|\, \boldsymbol{u})\, \mathrm{d}\boldsymbol{u} \\
& \times \int_0^t \delta(\boldsymbol{x} - \boldsymbol{g}_i(\boldsymbol{u}, t - \tau)) \\
& \times \exp\left[- \int_0^{t-\tau} \lambda_i(\boldsymbol{g}_i(\boldsymbol{u}, s))\, \mathrm{d}s \right] \\
& \times \pi(\boldsymbol{u}, j, \tau)\, \mathrm{d}\boldsymbol{\tau}, \qquad (1)
\end{aligned}
$$

where $\pi(\boldsymbol{u}, i, 0)$ *is the probability for a system to be in state* i *at time* $t = 0$ *given the values of physical variables* $\boldsymbol{u}$*, the Dirac* δ *function* $\delta(\boldsymbol{x} - \boldsymbol{g}_i(\boldsymbol{u}, t))$ *indicates among all possible trajectories of physical variables those leading to values* $\boldsymbol{x}$ *at time* t*, and* $\exp\left[- \int_0^t \lambda_i(\boldsymbol{g}_i(\boldsymbol{u}, s))\, ds \right]$ *is the reliability at time* t*.*

The first additive term of Eq. (1) is interpreted as the probability to be in a discrete state i at time $t = 0$ and to remain in this state until time t; this term is integrated over all possible trajectories of physical variables. The second additive term of Eq. (1) is interpreted as the probability to go to the discrete state i from any other state $j \neq i$ at time $\tau < t$ and to remain in state i during the period $[\tau, t]$, regardless the trajectory followed by the system before entering the state j

(Markovian assumption); this term is integrated over all possible trajectories of physical variables and over all possible time instants τ.

Analytical solution of Eq. (1) is only possible for simple systems (Labeau et al. 2000), a review of approximative methods can be found in Labeau et al. (2000), Pérez Castañeda (2009), Aldemir (2013). Among these methods the Piecewise Deterministic Markov Process (PDMP) model (Dufour and Dutuit 2002, Zhang et al. 2008) and Monte Carlo simulations based on different types of state-transition models (Dutuit et al. 1997, Distefano et al. 2012, among others) are widely used.

2.2 *Piecewise Deterministic Markov Process*

The PDMP (Davis 1984) is used as a semi-analytical method to approximate the solution of Eq. (1). Its definition is given below.

Definition 2.2 *(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 $\mathbb{M}$ a countable set, are discrete modes corresponding to vector of states i in Definition 2.1;*
- *$\boldsymbol{X} \in \mathbb{R}^n$ is a set of real state variables corresponding to vector $\boldsymbol{x}$ in Definition 2.1.*

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 $\bar{E}_m$;*
- *$\phi_m : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n$ is a flow; the flow corresponds to the deterministic dynamics defined by $g_i(\cdot)$ in Definition 2.1;*
- *$\lambda_m : \bar{E}_m \to \mathbb{R}^+$ is an intensity of random jumps corresponding to $\lambda_i(\cdot)$ in Definition 2.1;*
- *Q_m is a Markov kernel on $\left(\bar{E}_m \mathcal{B}\left(\bar{E}_m\right)\right)$ with $\mathcal{B}(\cdot)$ a Borel set; the Markov kernel selects the post-jumps locations for the process and corresponds to the transition rate $p(\cdot)$ of Definition 2.1.*

Two types of jumps between modes are possible in the PDMP framework:

- *deterministic jumps at times $t^\star\,(m, \boldsymbol{X}) = \inf\{t > 0 : \phi_m(\boldsymbol{X}, t) \in \partial E_m\}$;*
- *stochastic jumps occurring according to a probability, for example, the probability of the first jump at time T_1, $\mathbb{P}_{(m,\boldsymbol{X})}(T_1 > t)$, or $\mathbb{P}(T_1)$ for simplicity, is*

$$\mathbb{P}(T_1) = \begin{cases} \exp\left[-\int_0^t \lambda_m\left(\phi_m(\boldsymbol{X}, s)\right) \mathrm{d}s\right] & \text{if } t < t^\star \\ 0 & \text{if } t \geq t^\star. \end{cases}$$

The PDMP is a theoretical model allowing the analytical or semi-analytical resolution of the dynamic reliability problem and analytical assessment of system reliability parameters. This model is however limited due to its complexity and is not suitable for large and complex systems. In this sense, the Stochastic Hybrid Automaton, which can be seen as an alternative formulation of the PDMP intented to perform the Monte Carlo simulations, is more convenient.

2.3 *Stochastic Hybrid Automaton*

We formally introduce the SHA in Definition 2.3, following Perez Castañeda et al. (2011).

Definition 2.3 *(Stochastic Hybrid Automaton SHA).*

The Stochastic Hybrid Automaton (SHA) is formally defined as an 11-uplet:

$$SHA = (\mathcal{X}, \mathcal{E}, \mathcal{A}, \boldsymbol{X}, \mathrm{A}, \mathcal{H}, \mathcal{F}, \mathrm{P}, \chi_0, \boldsymbol{X}_0, \boldsymbol{P}_0)$$

with:

- *$\mathcal{X}$ a finite set of discrete states $\{\chi^1, \cdots, \chi^m\}$;*
- *$\mathcal{E}$ is a finite set of deterministic or stochastic events $\{e_1, \cdots, e_r\}$;*
- *$\boldsymbol{X}$ is a finite set of real variables evolving in time $\{X_1, \cdots, X_n\}$;*
- *$\mathcal{A}$ is a finite set of arcs of the form $(\chi, e_j, G_k, R_k, \chi')$ where χ and χ' are respectively the origin and the goal discrete states of the arc k, e_j is the event associated to this arc, G_k is the guard condition on $\boldsymbol{X}$ in the state χ and R_k is the reset function of $\boldsymbol{X}$ in the state χ';*
- *$\mathrm{A} : \mathcal{X} \times \boldsymbol{X} \to (\mathbb{R}^{n+} \to \mathbb{R})$ is a function of "activities", describing the evolution of continuous variables in each discrete state;*
- *$\mathcal{H}$ is a finite set of clocks on $\mathbb{R}$;*
- *$\mathcal{F} : \mathcal{H} \to (\mathbb{R} \to [0, 1])$ is an application that associates a distribution function to each clock;*
- *$\mathrm{P} = \left[p_i^l\right]$ is a matrix of discrete probability distributions where p_i^l is a probability of transition from χ^i to χ^l on occurrence of event e: $p\left(\chi^i | \chi^l, e\right)$;*
- *$\chi_0, \boldsymbol{X}_0, \boldsymbol{P}_0$ are the initial conditions.*

Detailed interpretation of Definition 2.3 are given by Pérez Castañeda (2009) and Babykina et al. (2011).

The SHA can be seen as an alternative representation of the PDMP in the following:

- The set of discrete states $\mathcal{X}$ of the SHA corresponds to the modes $\mathbb{M}$ of the PDMP.
- Both frameworks (SHA and PDMP) are characterised by a set of physical variables, $\boldsymbol{X}$.
- The flow ϕ_m of the PDMP characterises the trajectories of physical variables in each state and corresponds to the activities function A of the SHA.
- The Markov kernel Q_m of the PDMP is a matrix $[Q_{ij}(t)]$ representing the probabilities of transitions from state i to state j in the time interval $[0, t]$. In this sense the Markov kernel of the PDMP contains a discrete probability part and a continuous probability part. The discrete probability part corresponds to the matrix $P = \left[p_i^j\right]$ of the SHA. We define: $Q_{ij}(\infty) = \left[p_i^j\right]$.

  The continuous probability part characterises the distribution functions of moments of jumps from state i to state j: $F_{ij}(t) = Q_{ij}(t)/p_i^j$. This part of the kernel corresponds to the $\mathcal{F}$ application of SHA.
- The guard conditions G of the SHA correspond to the definitions of deterministic times of jumps for the PDMP.

The SHA allows considering non exponential probability distributions, used to represent, for example, an intrinsic components ageing, as well as non temporal probability distributions, used to represent, for example, ageing by the number of a component solicitation (Perez Castañeda et al. 2011, Babykina et al. 2011).

The application of the SHA as a model for simulations is illustrated on a case study.

3 CASE STUDY DESCRIPTION

The considered case study is a system of water level regulation in the steam generator (SG) of a nuclear power plant. Several components provide this mission. The states of these components are conditioned by stochastic events, representing failures and reparations, and by deterministic evolution of a continuous variable, which is a demanded power. A brief description of the case study is given in the present section, for details one can refer to Aubry et al. (2012, the book chapter).

3.1 *Physical system*

The modelled system is composed of the following components:

- The turbo pumps (TPA) providing the feed water to the SG. There are two TPAs functioning at the same time. Each TPA is composed of in-turbine part (T) and out-of-turbine part (OT), serially operating: if one part (T or OT) of the TPA fails, the entire TPA is stopped.
- Feed water valves (ARE) controlling the incoming water flow to the SG. There are two AREs: a heavy-flow valve (ARE_{GD}) and a small-flow valve (ARE_{PD}) used to precise flow regulations.
- Extracting pumps (CEX) maintaining the vacuum under the condenser, providing the cooled feed water to the SG. There are three CEX pumps, operating in two-out-of-three (*2 oo 3*).
- The cylinder VVP, containing steam which provides the functioning of the TPAs and of the other not modelled components in case of the SG failure. The VVP is a passive system and its failures include the failures of other passive systems (tanks, heaters, dryers, *etc.*).

Finally, the control system responsible for water level regulation in the SG is accounted for in the model. This system is represented by the PID controller, defining the water flow rate Q_e needed to maintain the water level at a given reference value as a function of the actually measured water level N_{ge}.

The reliability diagram of the secondary circuit, considered in the present study, is given in Fig. 1.

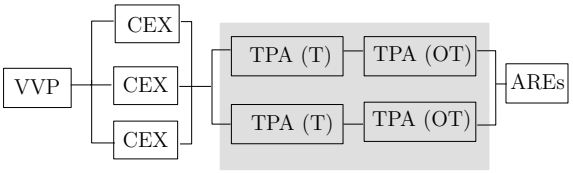

Figure 1: The reliability diagram of the modelled system.

Each of the mentioned sub-systems (components) is characterised by different failure modes, the failure may occur during operation or on demand (blocking of valves, refusal to open/close valves and pumps, *etc.*). The failures may be detected immediately or with a delay and reparation strategies depend on failure types.

3.2 *Operational behaviour and global system functioning*

The states of sub-systems are also conditioned by the power required from the power plant P. Power is a continuous time-dependent variable which represents

the dynamic operational environment of the system and which is expressed as a percent of a nominal power (P_n). A specific scenario of power evolution, corresponding to a normal cycle of the power plant, is considered in the case study: the start-up of the system is quite slow, once a full power reached, the system remains in a stationary position, and after a certain time period of duration T, the slow shut-down of the system is performed (we refer to Aubry et al. (2012, the book chapter, Section 8.4.3, scenario 1) for details on power evolution).

The interactions between the system components and between the system and its environment can be summarised as follows. We assume that the power required from the power plant defines the reference value for the water level in the SG. The PID controls the feed water flow rate necessary to attain this reference value, this command is sent to the ARE valve, which adapts its position according to the required flow rate. The water level in the SG is then adapted to the required power. The ARE valves can fail, thus not being able to provide the demanded flow rate, in this case the water level will not be adjusted to the required value. This process is represented in Fig. 2.

The nominal (without failures) operation of the global system, according to the power evolution scenario, is the following.

1. The power increases from $0\%P_n$ to $2\%P_n$ by $0.2\%P_n$ by hour. This power increase is provided by a security system not modelled in our case. At $2\%P_n$ the sub-systems are switched-on in a specific order:
   (a) Start-up of the the CEX pumps.
   (b) Start-up of the small-flow valve ARE_{PD} once the CEX are successfully launched.
   (c) Start-up of one of the TPA pumps once the ARE_{PD} is successfully launched.
2. The power increases from $2\%P_n$ to $10\%P_n$ by $0.8\%P_n$ by hour.
3. The power increases from $10\%P_n$ to $15\%P_n$ by $22.5\%P_n$ by hour. Once the power reaches $15\%P_n$, the sub-systems are demanded in a specific order:
   (a) Start-up of the heavy-flow valve ARE_{GD}.
   (b) Shut-down of the small-flow valve ARE_{PD} once the ARE_{GD} is successfully launched.
4. The power increases from $15\%P_n$ to $60\%P_n$ by $22.5\%P_n$ by hour. Once the power reaches $60\%P_n$, the sub-systems are demanded in a specific order:
   (a) Start-up of the second TPA.
   (b) The power increase is allowed once the second TPA is successfully launched.
5. The power increases from $60\%P_n$ to $100\%P_n$ by $22.5\%P_n$ by hour. Once the power reaches $100\%P_n$, the system operates normally during a certain time period T, after which the power decrease is carried out and the sub-systems are shut-down following the pattern symetric to this used during the power increase.

Note that the states of the ARE valves are directly linked to the system dynamics since the flow rate is adjusted according to the demanded power. The TPA pumps influence the power by their failures: when only one of the two TPA is functioning, the power (and thus the water level in the SG) is to be decreased to $60\%P_n$. Symmetrically, at this level of the required power, one TPA is sufficient. CEX pumps and VVP are independent systems. Some of their failures may however cause the automatic reactor shut-down (ARR), and thus the power forcing to 0%, requiring the shut-down of all other systems. The precise specification of the system functioning is given in Aubry et al. (2012, the technical report, Section 4.8).

4 IMPLEMENTATION OF THE CASE STUDY

4.1 *Model building*

The automata of the sub-systems are partially built by means of the parallel composition technique (Cassandras and Lafortune 1999). The idea is to model elementary sub-systems separately and combine those by a formal operation of synchronisation, using the alphabets (sets of events) of elementary automata. The parallel composition is employed to build the models of strongly linked components: the three CEX pumps and their interactions, in-turbine and out-of-turbine parts of the TPA pumps. The CEX global automaton is composed of three identical elementary CEX automata, accounting for pump failures during operation and during the stand-by period and of the specification automaton, coordinating the simultaneous functioning of these three CEX. The formal model for the TPA is composed of the in-turbine part of a TPA, its out-of-turbine part and the specification automaton coordinating their in-series functioning.

Functioning of the ARE valves and the VVP are represented by separate elementary automata.

The simultaneous functioning of different sub-systems in their operational environment is governed by a deterministic *control automaton*. The relevant behaviour of the whole system is provided by means of message sharing (Moalla et al. 1978, Dutuit et al. 1997). Precisely, the control automaton gives orders to and receives the responses from the sub-systems. These orders and responses are formalised by the variables shared between the different automata. The power evolution is modelled within the control automaton. This procedure is illustrated in Fig. 3 (normal failure-free power increase as described in Section 3.2) and in Fig. 4 (the case when one of the TPAs

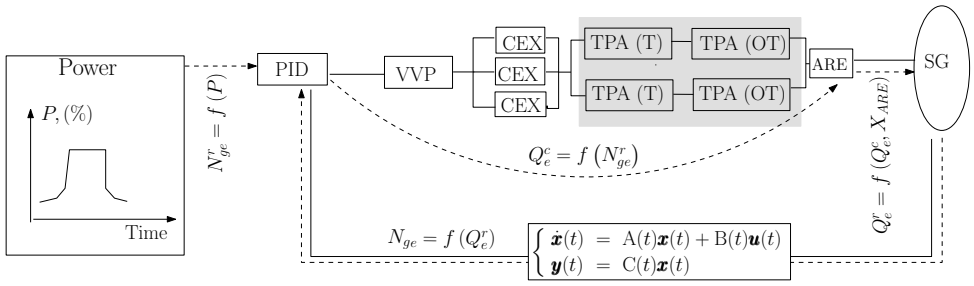

Figure 2: Case study system model and dynamics: scheme. N_{ge}: actual measured water level; N^r_{ge}: reference water level; Q^c_e: command value for feed water rate; X_{ARE}: state of the ARE; Q^r_e: real value of feed water rate. Dashed lines: modelled continuous variables.

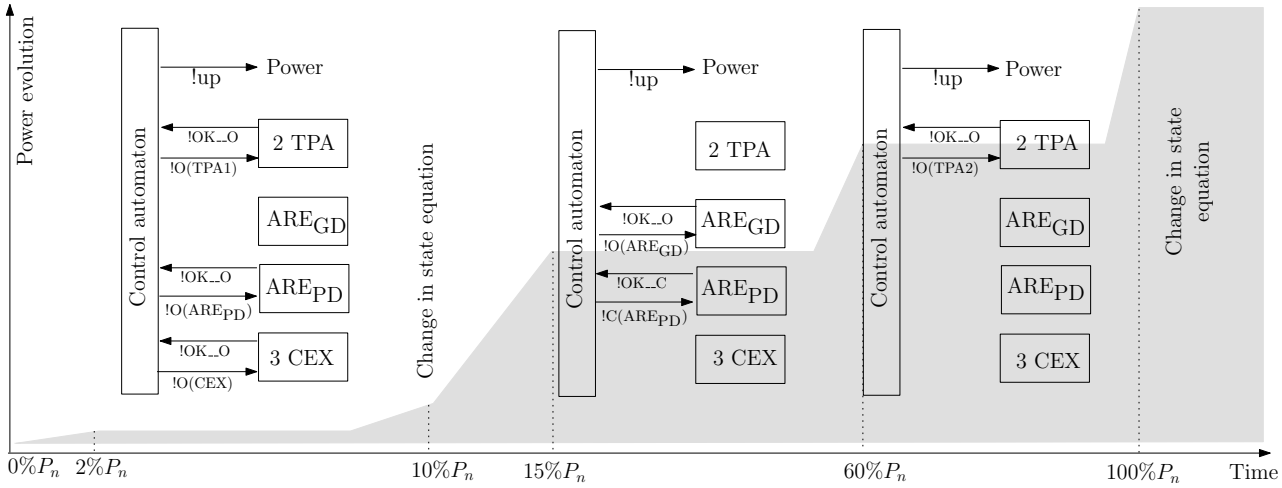

Figure 3: Simultaneous functioning of sub-systems during the power increase: schematic representation. "!O(X)": order to open for component X, "!OK__O": successful opening, "!C(X)": order to close for component X, "!OK__C": successful closure, "!up": order to start power increase, grey area represents power evolution. Boxes represent the automata of sub-systems.

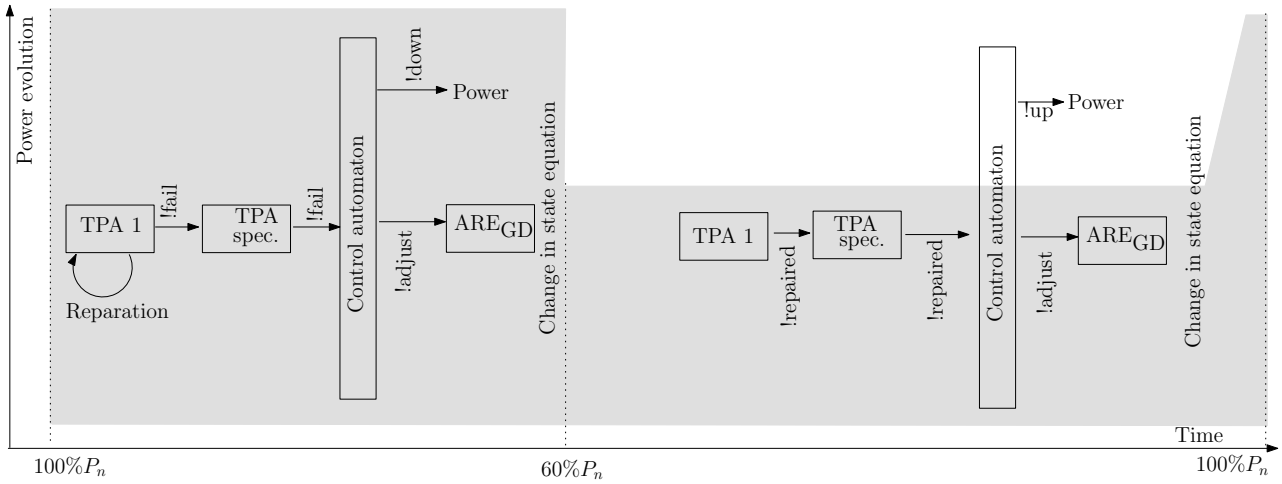

Figure 4: Simultaneous functioning of sub-systems in case of a failure in one of the TPA: schematic representation. "!fail": shared message indicating that TPA1 failed, "down": order to instantaneously decrease the power, "!adjust": order to adjust the water flow rate by valve position, "!up": order to start power increase, "Reparation": reparation procedure within the TPA1 automaton, grey area represents power evolution. Boxes represent the automata of sub-systems, "TPA spec." being the specification automaton which coordinates operation of the two TPA.

fails during operation at full-power). The Fig. 4 represents a simplified schema: it is supposed that other components do not fail during TPA reparation. The complete model accounts for failures of any component at any time instant.

4.2 *Monte Carlo simulations*

The constructed model is implemented in Scicos toolbox of Scilab (Campbell et al. 2010), using the AUTOMATON block for the SHA implementation (Najafi and Nikoukhah 2007). The details concerning the case study implementation using this Scicos are pro-

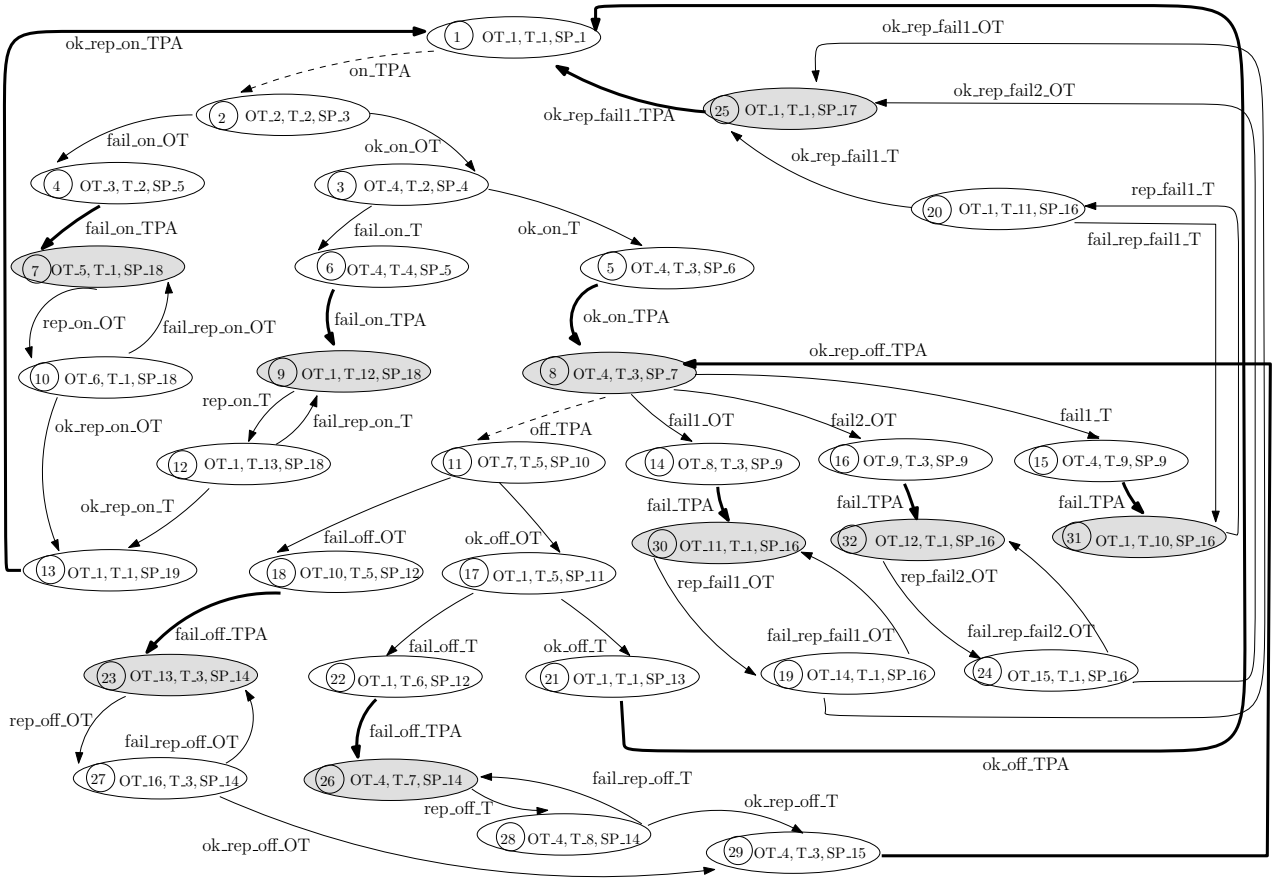

Figure 5: Global TPA automaton: result of parallel composition. Timed states are shaded, transitions representing messages sent to the automaton specifying the functioning of the two TPAs are in bold, transitions representing messages received from the automaton specifying the functioning of the two TPAs are dashed. Transitions characterised by variables shared with the control automaton are not represented for simplicity. The names of states correspond to combinations of elementary automata states (T: turbine, OT: out-of-turbine, SP: specification). The transitions are encoded as "aa_bb_cc_dd". dd: the concerned component (turbine, out-of-turbine or whole TPA), cc: type of failure/action occurred ("fail1" for type I failure, "fail2" for type II failure, "on" for switching on, "off" for switching off, "fail" for failure of any type on the whole TPA), bb: general type of event ("fail" for failure, "rep" for reparation), aa: result of reparation ("ok" for successful reparation, "fail" for failed reparation).

vided by Babykina et al. (2012, Section 4). The Monte Carlo simulations are carried out using certain parameters (Aubry et al. 2012, the technical report, Section 4.8) for the system (failure and reparation times, failure detection durations, probabilities of failure on demand, *etc.*)

5 RESULTS AND DISCUSSION

The conceived behavioural model of the case study and the results of Monte Carlo simulations based on its implementation as an SHA provide the data which allow the assessment of different safety and reliability parameters.

5.1 *The obtained model*

As a result we obtain a model composed of eight sub-systems: VVP, CEX, two TPAs, specification for the two TPAs, heavy- and small-flow AREs and the control automaton. These sub-systems exchange 62 shared variables, and the global system contains 488 states and 836 transitions. An example of the behavioural model of one TPA is given in Fig. 5.

5.2 *Safety and reliability assessment*

The behavioural model, partially built by means of the parallel automata composition, allows qualitative analysis of system trajectories and identification of dangerous scenarios, even if those are rare and difficult to capture by Monte Carlo simulations. In case of exponential probability distributions used for times of events, analytical evaluation of a specific scenario probability is also possible. For example, one can calculate the probability that an automatic reactor stopping (AAR) caused by failure of both TPA occurs during the power increase from 0% to $100\%P_n$. For more details on such calculations one can refer to (Babykina et al. 2012).

In more complicated cases, where the temporal probability distributions are not exponential, Monte Carlo simulations can be used to evaluate the frequency of different scenarios (Aubry et al. 2012, the book chapter, Section 8.3.5). For example, for a specific set of system parameters, using 111 simulated histories for a case study, one trajectory resulted in an AAR, in the large majority of cases the components operated without failure, with the exception of the TPA pumps. Only in approximately 20% of cases

the trajectories of TPA are failure-free, nearly half of the simulated trajectories had a failure while operating in the in-turbine part of TPA. Around 12% of trajectories contained a functioning failure of the out-of-turbine TPA. These failures are successfully repaired in the majority of cases.

A formal method of parallel automata composition, used for model building, provides a precise and a relevant representation of system behaviour and allows an analytical assessment of system safety and reliability. Nevertheless, this methodology results in a quite large and complicated model, leading to fastidious implementation and to time-consuming Monte Carlo simulations. It is however a price to pay for elaboration of a formal model not needing any verification techniques.

6 CONCLUSION

In this paper the Stochastic Hybrid Automaton (SHA) is proposed to model and to analyse the behaviour of a feed-water control system of a power plant steam generator. The SHA is a particular formulation of a Piecewise Deterministic Markov Process, widely used in the framework of dynamic reliability. The behavioural model of the considered system is built by means of parallel automata composition and shared variables, thus allowing a relevant simultaneous functioning of all the considered sub-systems. This behavioural model allows analytical assessment of system performance. Carried out Monte Carlo simulations provide data for empirical assessment of reliability parameters. The SHA shows to be a suitable tool to model large complex systems operating in dynamic environment. Such a model, thanks to its completeness, is absolutely essential to track critical event sequences. Further work is needed to optimise the implementation procedure and to accelerate the simulations.

REFERENCES

Aldemir, S. (2013). A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. *Annals of Nuclear Energy 52*, 113–124.

Aubry, J.-F., G. Babykina, A. Barros, N. Brinzei, G. Deleuze, B. de Saporta, F. Dufour, Y. Langeron, & H. Zhang (2012). Rapport final du projet APPRODYN : APPROches de la fiabilité DYNamique pour modéliser des systèmes critiques. Technical report, collaboration CRAN, EDF R&D, INRIA-CQFD, UTT-ICD.
URL: http://hal.archives-ouvertes.fr/hal-00740181 /PDF/Rapport_final_APPRODYN_v7a_NB.pdf.

Aubry, J.-F., G. Babykina, N. Brinzei, S. Medjaher, A. Barros, C. Bérenguer, A. Grall, Y. Langeron, D. Ngoc Nguyen, G. Deleuze, B. de Saporta, F. Dufour, & H. Zhang (2012, August). The APPRODYN project: dynamic reliability approaches to modeling critical systems. In Y. V. Nada Matta and J. Arlat (Eds.), *Supervision and Safety of Complex Systems*, pp. 181–222. Wiley-ISTE. Chapter 8.

Babykina, G., N. Brinzei, J.-F. Aubry, G. Deleuze, et al. (2012). Modélisation des systèmes complexes critiques en fiabilité dynamique par automates stochastiques hybrides, évaluation de leur comportement. *Congrès Lambda Mu 18*.

Babykina, G., N. Brinzei, J.-F. Aubry, & G. Perez Castañeda (2011). Reliability assessment for complex systems operating in dynamic environment. In *Proceedings of the European Safety and Reliability Conference ESREL 2011, Troyes, France*, pp. 327–334.

Campbell, S., J. Chancelier, & R. Nikoukhah (2010). *Modeling and Simulation in Scilab/Scicos with ScicosLab 4.4*. Springer.

Cassandras, C. & S. Lafortune (1999). *Introduction to discrete event systems*, Volume 11. Kluwer academic publishers.

Cocozza-Thivent, C., M. Desgrouas, & S. Mercier (2006). Algorithme de calcul de disponibilité asymptotique en fiabilité dynamique. In *Proceedings of Colloque National de Fiabilité et Maintenabilité - $\lambda\mu$ 15, Lille, France*, pp. 126–136.

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

Devooght, J. & C. Smidts (1992). Probabilistic reactor dynamics. I: The theory of continuous event trees. *Nuclear Science and Engineering 111*(3), 229–240.

Devooght, J. & C. Smidts (1996). Probabilistic dynamics as a tool for dynamic PSA. *Reliability Engineering & System Safety 52*(3), 185–196.

Distefano, S., F. Longo, & K. Trivedi (2012). Investigating dynamic reliability and availability through state–space models. *Computers & Mathematics with Applications 64*, 3701–3716.

Dufour, F. & Y. Dutuit (2002). Dynamic Reliability: A new model. In *Proceedings of 15éme Colloque National de Fiabilité et maintenabilité - $\lambda\mu$ 13 - ESREL 2002, Lyon, France*, pp. 350–353.

Dutuit, Y., E. Chatelet, J. Signoret, & P. Thomas (1997). Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases. *Reliability Engineering & System Safety 55*(2), 117–124.

Izquierdo, J., E. Melendez, & J. Devooght (1996). Relationship between probabilistic dynamics and event trees. *Reliability Engineering & System Safety 52*(3), 197–209.

Labeau, P., C. Smidts, & S. Swaminathan (2000). Dynamic reliability: towards an integrated platform for probabilistic risk assessment. *Reliability Engineering & System Safety 68*(3), 219–254.

Marseguerra, M., E. Zio, J. Devooght, & P.-E. Labeau (1998). A concept paper on dynamic reliability via Monte Carlo simulation. *Mathematics and Computers in Simulation 47*(2), 371–382.

Moalla, M., J. Pulou, & J. Sifakis (1978). Synchronized Petri nets: A model for the description of non-autonomous systems. *Mathematical Foundations of Computer Science 1978*, 374–384.

Najafi, M. & R. Nikoukhah (2007). Modeling hybrid automata in Scicos. In *Proceedings of Multi-conference on Systems and Control (MSC), Singapore*, pp. 1–3.

Perez Castañeda, G., J.-F. Aubry, & N. Brinzei (2011). Stochastic hybrid automata model for dynamic reliability assessment. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 225*(1), 28–41.

Pérez Castañeda, G. A. (2009). *Evaluation par simulation de la sûreté de fonctionnement de systèmes en contexte dynamique hybride*. Ph. D. thesis, Institut National Polytechnique de Lorraine, France.

Zhang, H., F. Dufour, Y. Dutuit, & K. Gonzalez (2008). Piecewise deterministic Markov processes and dynamic reliability. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 222*(4), 545–551.