Simulation de Monte Carlo par automate stochastique hybride. Application à un cas test pour la fiabilité dynamique

Gabriel Antonio Perez Castaneda, Jean-François Aubry, Nicolae Brinzei

8ème édition du congrès international pluridisciplinaire
QUALITA 2009 – Besançon (France)
Du 18 au 20 mars 2009

SIMULATION DE MONTE CARLO PAR AUTOMATE STOCHASTIQUE HYBRIDE, APPLICATION A UN CAS TEST POUR LA FIABILITE DYNAMIQUE

PEREZ CASTANEDA Gabriel Antonio [1,2], AUBRY Jean-François [1], BRINZEI Nicolae [1]

[1] *Centre de Recherche en Automatique de Nancy – CNRS UMR 7039,*
Nancy – Université, INPL, 2, avenue de la forêt de Haye, 54516, Vandœuvre-lès-Nancy, France
+33 (0)3 83 59 56 33 – +33 (0)3 83 59 56 44,
perezc76@ensem.inpl-nancy.fr, jean-francois.aubry@isi.u-nancy.fr, Nicolae.Brinzei@ensem.inpl-nancy.fr

[2] *Instituto Tecnológico de Tehuacán, Lib. Instituto Tecnológico s/n, 75770, Tehuacán, Puebla, Mexique*

Résumé :

Un système dynamique hybride est décrit par un ensemble de variables continues et un ensemble d'événements discrets interagissant mutuellement. La réalité impose en outre de prendre en compte les défaillances des composants ou les incertitudes sur la connaissance du système. Certains événements ou variables prennent alors un caractère stochastique. L'approche d'évaluation de la fiabilité dynamique par simulation de Monte Carlo d'un modèle de type automate d'état a déjà été présentée [Pérez1]. Nous avons ensuite défini et implémenté un Automate Stochastique Hybride pour modéliser un système dynamique hybride afin de prendre en compte les problèmes relatifs aux défaillances pour évaluer par simulation les paramètres de la sûreté de fonctionnement. Nous l'avons implémenté dans l'environnement de simulation Scicos – Scilab. Nous disposons maintenant d'un outil de simulation de Monte Carlo performant permettant d'accéder à l'évaluation des grandeurs de la sûreté de fonctionnement en contexte dynamique. Afin de confronter notre proposition à d'autres méthodes, nous l'avons appliquée au benchmark utilisé par différents auteurs (Réseaux de Petri stochastiques (RdPS), processus markoviens déterministes par morceaux (PMDPM) …). Notre objectif est donc d'évaluer la probabilité d'occurrence des deux événements redoutés du cas test : l'assèchement et le débordement d'un réservoir. Cet exemple a pour principal intérêt de mettre en lumière les problématiques de la sûreté de fonctionnement des systèmes dynamiques hybrides.

Abstract:

A dynamic hybrid system is described by a set of continuous variables and a set of discrete events interacting each other. The reality also requires taking into account component failures or uncertainties on knowledge of the system. Some events or variables then take a stochastic character. The approach for evaluating the dynamic reliability by Monte Carlo simulation of a state machine type model has already been submitted [Pérez1]. We also defined and implemented a Stochastic Hybrid Automaton by modeling a hybrid dynamic system to take into account problems related to failures to evaluate by simulation dependability parameters. We have implemented this approach in the simulation Scicos - Scilab environment. Now, we dispose off a tool for the Monte Carlo simulation that allows the evaluation of dependability parameters in dynamic context. To compare our approach to other methods, we have applied it to the benchmark used by some authors (Markov multiphase, stochastic Petri nets, piecewise deterministic Markov processes …). Our aim is to evaluate the occurrence probability of two feared events of the case test: drainage and the overflow of a tank. This example has the main interest of highlighting the problems of dependability and modeling of hybrid dynamic systems.

Mots clés : Automate stochastique hybride, fiabilité dynamique, simulation de Monte Carlo.

Keywords: Stochastic hybrid automaton, dynamic reliability, Monte Carlo simulation.

1. Introduction

La fiabilité dynamique est la discipline qui prend en compte les interactions entre le comportement dynamique et déterministe d'un système et le comportement stochastique de ses composants. La complexité mathématique de l'évaluation analytique de la fiabilité dynamique nous amène à recourir à la simulation [Pérez2]. L'approche d'évaluation de la fiabilité dynamique par simulation de Monte Carlo d'un modèle de type automate d'état a déjà été présentée [Pérez1]. Ensuite nous avons défini et implémenté un Automate Stochastique Hybride [Pérez3] pour modéliser un système dynamique hybride afin de prendre en compte les problèmes relatifs aux défaillances dans l'évaluation des paramètres de la sûreté de fonctionnement qui sont obtenus par statistiques sur un grand nombre de simulations (Méthode de Monte Carlo). L'importance de l'implémentation de l'automate stochastique hybride réside dans le fait qu'il prend en compte les différents modes de fonctionnement continus du système définis dans les différents états discret de l'automate et le passage de l'un à l'autre sur des événements déterministes ou stochastiques désignés par les transitions correspondantes. Afin de confronter notre proposition à d'autres méthodes, nous l'avons appliquée au benchmark utilisé par différents auteurs [Aldemir], [Dutuit], [Marseguerra], [Kermish] et [Zhang].

2. Automate stochastique hybride

L'automate stochastique hybride prend en compte les différents modes continus de fonctionnement du système et le passage de l'un à l'autre sur l'occurrence des événements déterministes et stochastiques. Les premiers sont produits par franchissement de seuils des variables continues, les seconds sont produits par les défaillances des composants simulées par un générateur aléatoire en fonction de leurs lois de probabilités. Les dynamiques continues du système sont définies à travers des équations différentielles ordinaires.

Un automate stochastique hybride est défini comme un 11-tuple :

$$ASH = \left(\mathcal{X}, \mathcal{E}, \mathcal{A}, X, A, \mathcal{H}, \mathcal{F}, p, x_0, x_0, p_0\right) \qquad (1.)$$

dans lequel :

- $\mathcal{X}$ est un ensemble fini d'états discrets,
- $\mathcal{E}$ est un ensemble fini d'événements,
- $\mathcal{A}$ est un ensemble fini d'arcs de la forme $(x, \mathrm{e}, \mathrm{G}, \mathrm{R}, x')$ où :
- x et x' sont les états origine et but de l'arc, e l'événement associé à l'arc, G la condition de garde et R est la fonction de réinitialisation. Sur occurrence de e si la condition de garde G est vérifiée, le système bascule de l'état x à l'état x' dans lequel R définit les valeurs initiales des variables continues du système,
- X est un ensemble fini des variables réelles,
- $A : \mathcal{X} \times X \to \left(\Re^+ \to \Re\right)$ est une fonction des « activités », qui associe à un élément de $\mathcal{X} \times X$ une fonction définie sur $\Re^+$ et à valeur dans $\Re$,
- $\mathcal{H}$ est un ensemble fini d'horloges,
- $\mathcal{F} : \mathcal{H} \to (\Re \to [0,1])$ est une application qui associe à chaque horloge une fonction de répartition de probabilité,
- p est une distribution de probabilités de transition d'état $p(x' | x, e)$. Par exemple, si on a le même événement e définissant les transitions de l'état discret x vers les états discrets x' et x'' (l'automate à états sous jacent n'est pas déterministe), on peut définir la probabilité p de passer de l'état x à l'état x' et la probabilité (1-p) de passer de l'état x à l'état x'',
- x_0, x_0 et p_0 correspondent respectivement à l'état discret initial, à la valeur initiale du vecteur d'état continu et à la distribution initiale des probabilités de transition.

Les éléments $\mathcal{X}$, $\mathcal{E}$ et $\mathcal{A}$ de l'automate stochastique hybride correspondent à l'automate à états finis définissant sa partie événementielle. En revanche, X et A définissent sa partie continue. Finalement, $\mathcal{H}$ et p expriment son aspect temporel et stochastique. La figure 1 montre le modèle de l'automate stochastique hybride.

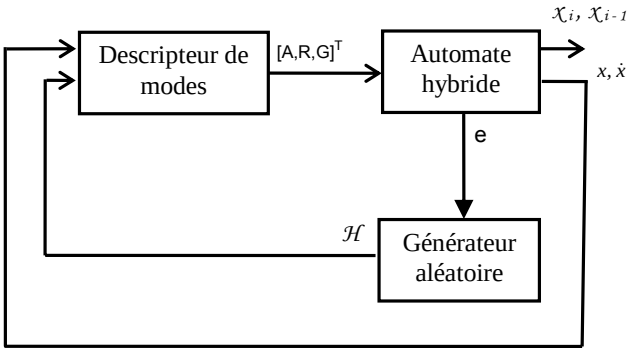


Figure 1. *Modèle de l'automate stochastique hybride*

L'*automate hybride* est un bloc Scicos [Najafi]. Il est constitué (figure 1) de i ports d'entrée (à gauche du bloc) et de deux ports de sortie (à droite du bloc). La sortie notée « $x, \dot{x}$ » fournit les valeurs des variables d'état continu x aussi que leurs dérivées $\dot{x}$. La sortie notée « x_i, x_{i-1} » fournit l'état discret courant du système ainsi que l'état précédent. La sortie notée « e » produit un événement lorsque toute transition d'état discret est effectuée.

Le *descripteur de modes* du modèle de l'automate stochastique hybride correspond aux différentes dynamiques continues du système. Il y a autant de dynamiques continues que d'états discrets. Il a deux entrées : la première correspond aux variables d'état continues et à leurs dérivées provenant de l'automate hybride. La deuxième reçoit les valeurs tirées par le générateur aléatoire. Par ailleurs, le descripteur de modes a i ports de sortie chacun étant défini par le vecteur $[A, R, G]^T$.

Le *générateur aléatoire* correspond à la structure temporisée stochastique $\mathcal{H}$ de l'équation (1.). Le générateur aléatoire réalise des tirages aléatoires correspondant aux transitions aléatoires vers les états concernés à travers sa sortie. Chaque fois qu'une transition d'état discret se produit la sortie « e » du bloc automate hybride, génère un événement activant le bloc générateur aléatoire à travers son entrée (au dessus du bloc). A ce moment a lieu le tirage des valeurs aléatoires.

3. Le cas test

Le cas test consiste en un réservoir contenant un liquide dont le niveau h doit être maintenu à l'aide d'une pompe principale P1, d'une pompe de secours P2 et d'une vanne de vidange V. Chacun de ces trois composants est commandé par une boucle de contrôle contenant un détecteur de niveau (figure 2).

La vanne V permet de vider le réservoir avec un débit donné, tandis que les pompes P1 et P2 en assurent le remplissage. La mission à remplir par cette installation est de maintenir le niveau de liquide à l'intérieur d'un intervalle $h \in [6,8]$, afin d'éviter deux situations extrêmes : l'assèchement et le débordement. L'un de ces cas, par exemple, est susceptible de se produire lorsque les débits des pompes P1 et P2 ne compensent plus celui de la vanne V. Pour tenter d'éviter ces modes de défaillance, des capteurs de niveau indépendants sont associés à chacun des composants. Lorsque le niveau descend sous un seuil (h<6) les deux pompes sont normalement mises en marche, tandis que la vidange de l'eau par la vanne V est arrêtée. Dans le cas contraire où le niveau excède le seuil (h>8), ce sont les pompes qui sont arrêtées alors que la vidange du réservoir est maintenue (tableau 1).

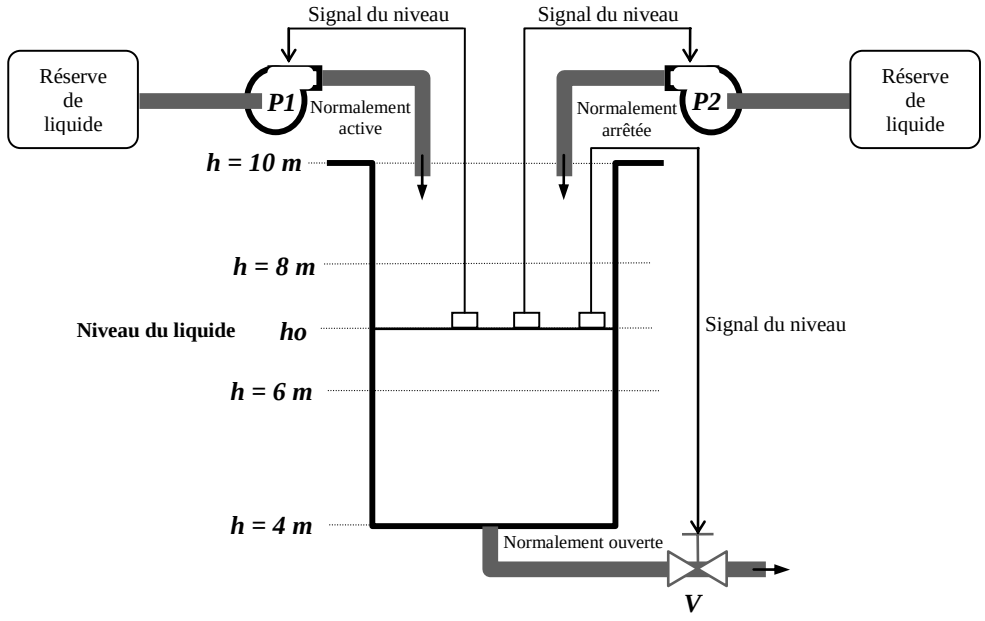


Figure 2. *Le réservoir et sa régulation de niveau*

Les trois composants sont mutuellement indépendants et non réparables. Les différents modes de défaillance pour chaque composant sont pris en compte (figure 3) : le comportement intempestif et le blocage en l'état. Leurs durées de fonctionnement avant défaillance sont des variables aléatoires qui suivent des lois exponentielles de paramètres respectifs :

- $\lambda_{P1} = 2{,}2831.10^{-3}h^{-1}$; $\lambda_{P2} = 2{,}8571.10^{-3}h^{-1}$; $\lambda_V = 1{,}5625.10^{-3}h^{-1}$

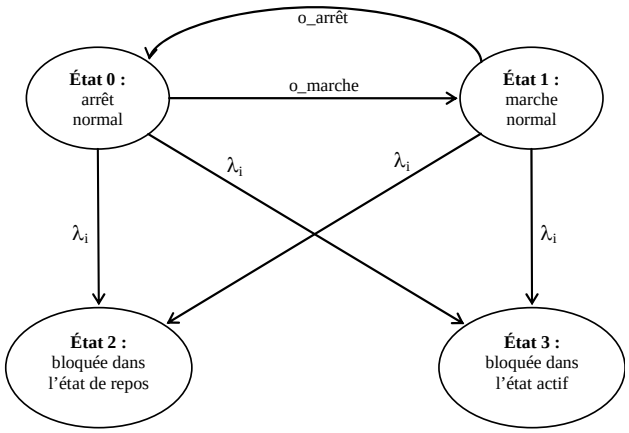


Figure 3. *Etats des composants et transitions entre états*

Niveau *h*	**Pompe 1**	**Pompe 2**	**Vanne**
$h < 6$ m	active	active	fermée
$6 \text{ m} \leq h \leq 8$ m	active	arrêtée	ouverte
$h > 8$ m	arrêtée	arrêtée	ouverte

Tableau 1. Conditions de fonctionnement nominal

La variable continue pour le système est le niveau du liquide *h* lequel est fonction de l'état des composants. Ainsi, l'équation différentielle pour le système est donnée par :

$$\frac{dh(t)}{dt} = \gamma(\upsilon) \tag{2.}$$

où $\upsilon = (\upsilon_{P1}, \upsilon_{P2}, \upsilon_V)$ dont les composants $c \in \{P1,P2,V\}$. Ainsi,

$$\upsilon_c = \begin{cases} 0 & si\ c\ est\ OFF\ ou\ bloqué\ en\ OFF \\ 1 & si\ c\ est\ ON\ ou\ bloqué\ en\ ON \end{cases} \tag{3.}$$

avec $\gamma(\upsilon) = (\upsilon_{P1} + \upsilon_{P2} - \upsilon_V)G$, où G est le débit des composants.

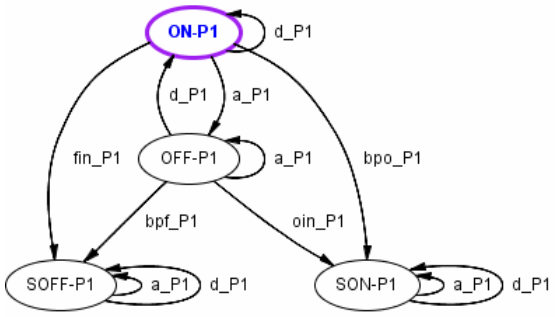
L'équation généralisée (2.) reflète les différents modes opératoires possibles du processus. Elle fait apparaître l'influence des phénomènes discrets sur l'évolution du processus au travers des termes υ_c. Ces derniers peuvent prendre la valeur 1 si l'actionneur associé est commandé en ouverture ou active ou bien si une défaillance de cet actionneur le bloque dans la position ouverte ou active, et la valeur 0 dans le cas contraire, comme l'exprime l'équation (3.). En conditions nominales, le débit de P1 est égal au débit de P2 et de V. Ainsi G = 1,5 m^3h^{-1} pour P1, P2 et V. Au temps *t = 0*, le niveau du liquide *h* = 7 m, la pompe P1 fonctionne, P2 est à l'arrêt et la vanne V est ouverte.

4. Implémentation

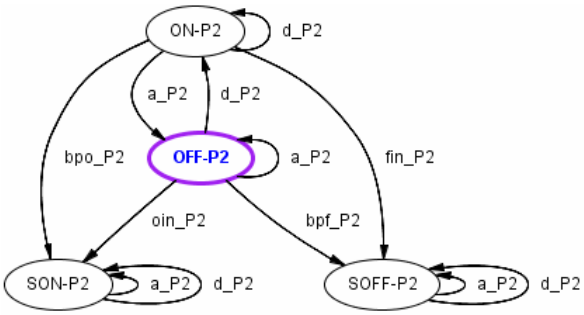
Pour implémenter l'automate stochastique hybride du système, nous avons défini d'abord cinq automates à états finis élémentaires : trois pour les composants, un pour le réservoir et un dernier pour la commande (figure 4). A l'aide du logiciel DESUMA [DESUMA], nous avons réalisé la composition synchronisée de ces cinq automates afin d'obtenir formellement l'automate global. Cette composition synchronisée des cinq automates a donné comme résultat un automate global de 873 états. Avant de le transformer en automate stochastique hybride, nous avons simplifié l'automate résultant à partir de règles simples : d'abord, le but de notre application étant de déterminer la probabilité d'arriver aux états redoutés, nous avons regroupé tous les états qui correspondent à l'assèchement du réservoir. Nous avons aussi appliqué la même procédure pour le débordement. De plus, nous avons agrégé tous les états fugitifs chaque fois que cela était possible (exemple séquence d'événements de commande). Comme résultat de ces règles simples, nous avons obtenu un automate global final de 83 états. A partir de cet automate, nous avons implémenté l'automate stochastique hybride.

L'ensemble des événements associés à la pompe P1, à la pompe P2, à la vanne V et à la commande est :

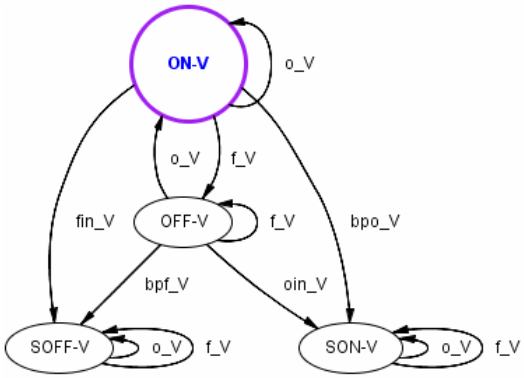
- bpo_P1, bpo_P2 et bpo_V : pompes bloquées dans l'état actif et vanne bloquée dans l'état ouvert,
- bpf_P1, bpf_P2 et bpf_V : pompes bloquées dans l'état d'arrêt et vanne bloquée dans l'état fermé,
- oin_P1, oin_P2 et oin_V : démarrage intempestif des pompes et ouverture intempestive de la vanne,
- fin_P1, fin_P2 et fin_V : arrêt intempestif des pompes et fermeture intempestive de la vanne,
- a_P1 et a_P2 : arrêt des pompes P1 et P2,
- d_P1 et d_P2 : démarrage des pompes P1 et P2,
- o_V : ouverture de la vanne et
- f_V : fermeture de la vanne.



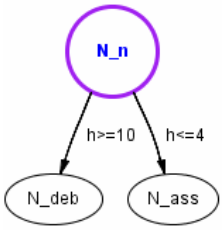
(a) Automate de la pompe 1



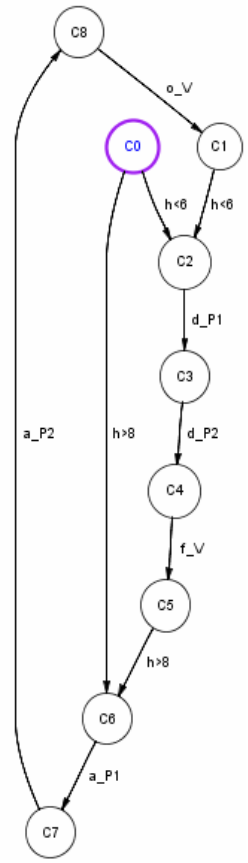
(b) Automate de la pompe 2



(c) Automate de la vanne



(d) Automate du réservoir



(e) Automate de commande

Figure 4. *Automates à états finis élémentaires*

Nous distinguons pour les composants P1, P2, V les états suivants :

- ON-P1, ON-P2 et ON-V : pompes actives et vanne ouverte,
- OFF-P1, OFF-P2 et OFF-V : pompes en arrêt et vanne fermée,
- SON-P1, SONP2 et SON-V : pompes bloquées dans l'état actif et vanne bloquée dans l'état ouvert et
- SOFF-P1, SOFF-P2 et SOFF-V : pompes bloquées dans l'état en arrêt et vanne bloquée dans l'état fermé.

Pour le réservoir nous avons les états ;

- N_n : niveau normal du réservoir ($6 \le h \le 8$),
- N_ass : niveau d'assèchement ($h \le 4$) et
- N_deb : niveau de débordement ($h \ge 10$).

Les lois de contrôle de la commande (tableau 1):

- initial : C0 – P1 active, P2 arrêtée et V ouverte,
- si h<6 : C2 → C3, P1 active ; C3 → C4, P2 active et C4 → C5, V fermée,
- si h>8 : C6 → C7, P1 arrêtée ; C7 → C8, P2 arrêtée et C8 → C1, V ouverte,
- C1 – état stable de la commande quand h>8 et
- C5 – état stable de la commande quand h<6.

5. Résultats

Pour évaluer la probabilité d'arriver dans les états redoutés (assèchement et débordement du réservoir) nous avons procédé à une série de simulations de Monte Carlo. La simulation est arrêtée si les conditions suivantes sont vérifiées :

- l'apport d'une i-ème histoire simulée sur la valeur du résultat est inférieur à la précision cherchée. Ce critère est donné par l'équation suivante :

$$\left| \frac{v_{m(i)} - v_{m(i-1)}}{v_{m(i)}} \right| \leq \varepsilon \qquad (4.)$$

  où $v_{m(i)}$ et $v_{m(i-1)}$ représentent la valeur moyenne de la probabilité mesurée après i histoires et respectivement après (i-1) histoires simulées. ε correspond à la précision de calcul désirée,

- la condition précédente est vérifiée pour un nombre k suffisant d'histoires par rapport au total des histoires i effectuées. L'équation suivante exprime ce critère. θ est la probabilité de convergence :

$$\frac{k}{i} \geq \theta \qquad (5.)$$

Nous avons utilisé une valeur de ε = 0,0001 et de θ = 0.8 (80% des histoires ont vérifié le critère). Le tableau 2 montre les résultats que nous avons obtenus (ASH) ainsi que les résultats obtenus par Zhang *et al.* [Zhang] (PMDPM et RdP).

Temps (heures)	**Débordement**			**Assèchement**		
	PMDPM	**RdP**	**ASH**	**PMDPM**	**RdP**	**ASH**
200	0,213	0,202	0,1913	0,026	0,023	0,0253
400	0,368	0,364	0,3682	0,068	0,067	0,0669
600	0,439	0,438	0,4365	0,097	0,096	0,0970
800	0,472	0,471	0,4687	0,111	0,110	0,1199
1000	0,486	0,486	0,4757	0,118	0,118	0,1178

Tableau 2. Probabilités d'accès aux états redoutés

Les résultats obtenus sont très proches de ceux présentés par Zhang et permettent de conclure à la validité de l'approche sur cet exemple. Cependant, il faut noter que les temps de simulation restent élevés (de l'ordre d'une journée avec un ordinateur PC de bureau standard). Ce temps important est en fait lié à la structuration actuelle de Scicos non adaptée à la simulation de Monte Carlo. Un travail important doit être mené pour améliorer cette performance de Scilab – Scicos pour une telle approche.

6. Conclusion

Notre approche nous a permis d'évaluer la probabilité d'occurrence des événements redoutés du cas test. Nous constatons une bonne convergence des résultats pour la probabilité de débordement et d'assèchement. Pour confirmer cette première impression, le pas suivant sera d'appliquer notre approche au même benchmark mais en considérant que la température évolue et influe sur les taux de défaillance λ_c. Le benchmark inclus aussi un nouvel événement redouté si la température dépasse un seuil dangereux. Ce travail est en cours. Il suppose d'ajouter l'automate décrivant l'événement dépassement de température, de générer le nouvel automate global, de réduire cet automate et de modifier le descripteur de modes et le générateur aléatoire pour incorporer la dépendance des taux de défaillance à la température. Les temps de simulation ne devraient pas augmenter sensiblement. On peut ajouter que les hypothèses très restrictives imposées par les auteurs du benchmark (débit constant et identique pour les pompes et la vanne) ne sont pas impératives dans notre approche. Les relations de dépendances (débit de vanne fonction de la pression par exemple) peuvent être intégrées sans difficulté grâce aux fonctionnalités de Scilab et sans accroissement sensible du temps de simulation.

Références

[Aldemir] Aldemir. *Computer Assisted Markov Failure Modelling of Process Control Systems*. IEEE Trans. on Reliability, vol. R-36 (1), pp. 133-144, April 987.

[DESUMA] http://www.eecs.umich.edu/umdes/toolboxes.html.

[Dutuit] Dutuit, Châtelet, Signoret et Thomas. *Dependability modelling and evaluation by using stochastic Petri nets : applications to two test cases*. Reliability Engineering and System Safety 55, pp. 117 – 124, 1997.

[Kermish] Kermish et Labeau. *Approche dynamique de la fiabilité des systèmes*. Projet 6/2000 de l'ISdF. Tâche n°1 : établissement de l'état de l'art en fiabilité dynamique. Université Libre de Bruxelles, 2000.

[Marseguerra] Marseguerra et Zio. *Monte Carlo approach to PSA for dynamic process systems*. Reliability Engineering and System Safety 52, pp. 227-241, 1996.

[Najafi] Najafi and Nikoukhah. *Modeling Hybrid Automata in Scicos*. Multi-conference on Systems and Control (MSC), Singapore, 1 – 3 October, 2007.

[Pérez1] Pérez Castaneda, Aubry et Brinzei. *Modélisation et simulation d'un système dynamique hybride pour calculer sa fiabilité en utilisant le toolbox Scicos de Scilab*. 7ième édition du Congrès International Pluridisciplinaire Qualita 2007, pp. 311 – 318, Tanger, Maroc, du 20 au 22 mars 2007.

[Pérez2] Pérez Castaneda, Aubry et Brinzei. *Etat de l'art en fiabilité dynamique*. 2èmes Journées Doctorales du GDR MACS JDMACS, Reims, France, du 9 au 11 juillet 2007.

[Pérez3] Pérez Castaneda, Aubry et Brinzei. *Automate Stochastique hybride*. 7e Conférence International de Modélisation et Simulation, pp. 386-395, Paris, France, 31 mars, 1er et 2 avril 2008.

[Zhang] Zhang, Gonzalez, Dufour et Dutuit. *Piecewise deterministic Markov processes and dynamic reliability*. Mathematical methods in reliability, Glasgow, 1 – 4 july, 2007.