HAL
open science

Sûreté de fonctionnement prévisionnelle en contexte dynamique

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

To cite this version:

Nicolae Brinzei, Gabriel Antonio Perez Castaneda, Jean-François Aubry. Sûreté de fonctionnement prévisionnelle en contexte dynamique. 2ème Workshop Surveillance, Sûreté et Sécurité des Grands Systèmes, 3SGS'09, Jun 2009, Nancy, France. pp.CDROM. hal-00436410

HAL Id: hal-00436410

https://hal.science/hal-00436410v1

Submitted on 26 Nov 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Sûreté de fonctionnement prévisionnelle en contexte dynamique

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

[2]Instituto Tecnológico de Tehuacán, Libramiento Instituto Tecnológico s/n, 75770, Tehuacán, Puebla, México

{Nicolae.Brinzei, perezc76, Jean-Francois.Aubry}@ensem.inpl-nancy.fr

Résumé – Un système dynamique hybride est décrit par un ensemble de variables continues et un ensemble d'événements discrets interagissant mutuellement. De plus, certains événements ou variables continues présentent un caractère stochastique. Cet article présente une approche d'évaluation de la fiabilité dynamique par simulation de Monte Carlo. Nous avons défini un Automate Stochastique Hybride pour modéliser un système dynamique hybride et nous l'avons implémenté dans l'environnement Scicos-Scilab. Cet outil permet d'accéder à l'évaluation des paramètres de la sûreté de fonctionnement en contexte dynamique. Nous l'avons appliqué au benchmark de référence dans le domaine de la fiabilité dynamique pour évaluer la probabilité d'occurrence des événements redoutés.

Abstract – One hybrid dynamic system is described by a set of continuous variables and as well as by a set of discreet events interacting mutually. Moreover, some continuous variables and events are the stochastic ones. This work describes an evaluation approach of dynamic reliability by Monte Carlo simulation. We are defined an Hybrid Stochastic Automaton in order to modeling an hybrid dynamic system which was implemented in the Scicos-Scilab software. This automaton allowed achieving the evaluation of dependability parameters in the dynamic context. It was applied in the reference benchmark in the field of dynamic reliability in order to evaluate the probability of the top events.

1. Introduction

Une caractéristique importante de nombreux systèmes industriels est que leur comportement change en fonction du temps en raison des interactions entre les composants de ce système ou avec l'environnement [1]. Chaque comportement donné du système est défini par les lois de la physique qui lui sont propres ; le passage d'un comportement à un autre peut être dû à plusieurs causes : l'intervention humaine, l'action de l'organe de contrôle agissant sous l'influence des variables physiques qui décrivent l'état du système (détection d'une alarme…), une discontinuité propre au système (diode dans un circuit, couplage intermittent…) ou encore une défaillance de composant (auquel cas le système peut lui-même être dans un état de défaillance). Ainsi l'évaluation prévisionnelle des grandeurs de la sûreté de fonctionnement (fiabilité, disponibilité, maintenabilité ou sécurité) des systèmes doit prendre en compte tous les aspects caractéristiques à ces systèmes et notamment :

- les interactions dynamiques existant entre les paramètres physiques (représentées généralement par des variables continues) et le comportement nominal ou dysfonctionnel des composants (représenté généralement par l'occurrence d'événements) ;
- le caractère déterministe ou stochastique des événements et des variables physiques ;
- la structure fiabiliste qui évolue dans le temps (reconfiguration du modèle) ;
- les modes de vieillissement multiples des composants selon l'état discret du système ;
- les modèles non binaires du comportement des composants ;
- l'instant et l'ordre d'occurrence des événements associés aux changements de l'état discret, qu'ils soient liés aux défaillances des composants ou aux franchissements de seuils des variables continues.

La prise en compte de tous ces aspects n'est pas possible avec les outils classiques de la sûreté de fonctionnement (arbre des défaillances, diagrammes de fiabilités, chaînes de Markov continues ou discrètes, réseaux de Petri stochastiques, etc.). Ainsi, un nouveau concept est devenu nécessaire pour définir tous les aspects pouvant intervenir dans l'évaluation de la sûreté de fonctionnement. Ce concept est celui de la fiabilité dynamique [2]. Nous présentons, dans la première partie de cet article, le concept de fiabilité dynamique tel qu'il a été formalisé par Labeau Smidts et Swaminathan dans [2], quelques outils qui ont été développés pour répondre à certains aspects de la fiabilité dynamique, ainsi que le point de vue concernant la modélisation des systèmes qui nous permettra d'étudier ces aspects. Suite à ce point de vue, nous proposons comme outil de modélisation, de

simulation et d'évaluation un automate stochastique hybride que nous avons défini formellement et implémenté. Il sera présenté dans la partie deux de cet article. La troisième partie présente l'application de l'automate stochastique hybride à l'étude d'un cas test qui fait office de benckmark dans le domaine de la fiabilité dynamique. Nous illustrons le mode de construction de l'automate qui nous permettra, ensuite, par une simulation de Monte-Carlo d'accéder à l'évaluation de la probabilité d'occurrence des événements redoutés. Ensuite, nous concluons ce travail en évoquant également les perspectives qu'il ouvre.

2. Fiabilité dynamique

La fiabilité prévisionnelle d'un système est traditionnellement l'activité qui consiste à évaluer a priori la probabilité pour qu'un système accomplisse sa fonction sur un intervalle de temps donné. Cette probabilité dépend des fiabilités de chacun de ses composants et de la manière dont ils concourent ensemble à la réalisation de la fonction du système. C'est la conception « statique » de la fiabilité prévisionnelle. La relation qui exprime la dépendance entre l'état binaire du système (marche ou panne) et l'état binaire de ses composants peut prendre des formes diverses (arbres des causes, équation booléenne, diagrammes et réseaux de fiabilité…). On peut l'appeler génériquement fonction de structure du système :

$$y = \varphi\left(x_1, x_2, ..., x_n\right) \tag{1}$$

où y et les x_i sont les états binaires du système et de ses n composants.

A partir de certaines formes de cette fonction, on peut utiliser un certain nombre de théorèmes de la théorie des probabilités permettant d'établir une relation entre la fiabilité du système et celles de ses composants :

$$R_S = f\left(R_1, R_2, ..., R_n\right) \tag{2}$$

Les notions de coupes ou de liens, sous-ensembles de l'ensemble des composants du système suffisants à assurer pour les premiers la défaillance du système et pour les seconds son fonctionnement, aident à trouver cette relation, notamment lorsque la fonction de structure est monotone. On peut dans ce cas se contenter de connaître les coupes ou les liens minimaux. Le théorème de Sylvester Poincaré, le théorème des probabilités totales ou le théorème d'expansion de Shannon permettent alors l'écriture d'une expression analytique de la fiabilité du système.

En contexte statique, la fonction de structure est unique et invariante dans le temps, elle ne dépend que de l'état des composants.

La complexité grandissante des systèmes amène à reconsidérer cette hypothèse. En effet, les systèmes complexes sont susceptibles de reconfigurations, de modes d'exploitation divers impliquant des sollicitations différentes des composants si bien que leur fiabilité n'évolue pas toujours avec la même loi au cours de leur vie et on ne peut plus considérer que les conditions d'exploitation garantissent la constance des paramètres d'une loi de vieillissement. La probabilité de défaillance d'un composant évolue ainsi avec les variables physiques fonctionnelles du système de manière difficile à prévoir. Il faut donc tenir compte de l'évolution dynamique de ces variables fonctionnelles dans l'étude du comportement dysfonctionnel des composants. De plus, les modes opératoires d'un système complexe changent dans le temps et les conditions de ces changements sont dues aussi bien à l'évolution des variables fonctionnelles qu'à l'apparition d'événements aléatoires comme les défaillances de composants. Enfin, on a constaté souvent qu'en présence d'une même coupe d'événements, un danger peut être présent ou non selon l'ordre dans lequel les événements se produisent. Ainsi, en contexte de *fiabilité dynamique* l'équation de Chapman-Kolmogorov généralisée [2] exprime la densité de probabilité $\pi(\overline{\mathbf{x}}, i, t)$ de trouver le système, au temps *t*, dans l'état discret *i* où le vecteur ***u*** des variables physiques prend la valeur $\overline{\mathbf{x}}$:

$$\begin{aligned}\pi(\overline{x}, i, t) &= \int \pi(\overline{u}, i, 0).\delta\left(\overline{x} - \overline{g}_i(t, \overline{u})\right).e^{-\int_o^t \lambda_i(\overline{g}_i(s,\overline{u}))ds} d\overline{u} \\ &+ \sum_{j \neq i} \int d\overline{u} \int_o^t d\tau\, \pi(\overline{u}, j, \tau) p(j \to i \mid \overline{u}) \delta\left(\overline{x} - \overline{g}_i(t-\tau, \overline{u})\right). \\ &e^{-\int_\tau^t \lambda_i(\overline{g}_i(s-\tau,\overline{u}))ds}\end{aligned} \tag{3}$$

$\mathbf{g_i}(t, \mathbf{u})$ représente la trajectoire suivie par les variables physiques dans l'état discret *i* jusqu'à l'instant *t*. δ est la fonction de Dirac qui permet de ne retenir que les trajectoires menant à ***x*** à l'instant *t*. $\lambda_i\left(\mathbf{g}_i\left(s, \mathbf{u}\right)\right)$ est le taux global de sortie de l'état *i* qui dépend des variables physiques (et donc de la trajectoire). $p(j \to i \mid \mathbf{u})$ est la probabilité de transition de l'état *j* vers l'état *i* au point ***u***. Cette expression est la somme de deux contributions : la première correspond au cas où le système est resté dans l'état *i* pendant l'intervalle [*0, t*]. La deuxième correspond aux cas où le système est passé d'un autre état *j* à l'état *i* à l'instant τ.

Différents outils, tels que les processus de Markov déterministes par morceaux (PDMP) [3] [4], les arbres de défaillances dynamiques (ADD) [5], ou pilotés par des chaînes de Markov (Boolean Driven Markov Process – BDMP) [6] ont été proposés pour résoudre les problèmes qui se posent en fiabilité dynamique. Ces approches analytiques basées sur la résolution des équations différentielles associées sont difficilement applicables lorsque la taille des systèmes étudiés augmente.

Ainsi, dans ce papier, nous considérons que la fonction de structure peut alors prendre la forme d'un automate à états finis dont les états représenteront les modes du système et les transitions correspondront aux différents événements déterministes ou probabilistes. Chaque mode sera caractérisé par sa dynamique continue et sa fonction de transition. Cette dernière dépendra à la fois de la

dynamique continue et des distributions probabilistes des événements de défaillances.

L'avantage de cette modélisation est multiple. Il permet déjà sans difficulté d'intégrer la maintenabilité du système et donc de passer à l'évaluation de tous les paramètres de sûreté de fonctionnement (FMDS). En outre, il met en évidence la possibilité de modes distincts pour une même combinaison de composants défaillants mais accessibles par des séquences d'événements différentes. Le langage de l'automate est le moyen d'accès à toutes les séquences menant à n'importe quel sous-ensemble d'états caractéristiques (disponibilité, danger, etc.). Enfin, si cette modélisation ne peut elle-même prétendre à une évaluation analytique des paramètres de la SdF dans le cas général (sous quelques hypothèses simplificatrices, on peut retrouver certaines des solutions analytiques partielles citées ci-dessus), elle permet l'accès à une évaluation par simulation.

Nous avons défini, ainsi, le concept d'automate stochastique hybride [7] que nous présentons ensuite.

3. 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. Nous l'avons définit comme un 11-tuple :

$$\left(\mathcal{X}, \mathcal{E}, \mathcal{A}, \mathrm{X}, \mathrm{A}, \mathcal{H}, \mathcal{F}, p, x_0, \mathrm{x}_0, p_0\right) \qquad (4)$$

où :

- $\mathcal{X}$ 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 $\left(x, \mathrm{e}, \mathrm{G}, \mathrm{R}, x'\right)$ 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 et 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 ;
- $\mathrm{A} : \mathcal{X} \times \mathrm{X} \rightarrow \left(\Re^{+} \rightarrow \Re\right)$ est une fonction des « activités », qui associe à un élément de $\mathcal{X} \times \mathrm{X}$ une fonction définie sur $\Re^{+}$ et à valeur dans $\Re$;
- $\mathcal{H}$ est un ensemble fini d'horloges ;
- $\mathcal{F} : \mathcal{H} \rightarrow \left(\Re \rightarrow [0,1]\right)$ est une application qui associe à chaque horloge une fonction de répartition ;
- p est une distribution de probabilités de transition d'état $p(x' \mid x, \mathrm{e})$. Par exemple, si on a le même événement e définissant les transitions de l'état discret x vers les états discrets x' et x'' (on dit qu'il y a des transitions en conflit), 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 probabilité de transition initiale.

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 (discrète). En revanche, X, A, R et G définissent sa partie continue. Finalement, $\mathcal{H}$ et p expriment son aspect temporisé et stochastique.

Nous avons implémenté cet automate dans l'environnement de simulation Scicos-Scilab (figure 1).

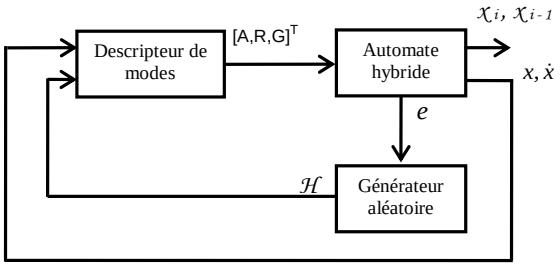

FIG. 1 : Modèle Scicos de l'automate stochastique hybride

L'automate hybride est un bloc Scicos [8]. Il est constitué de i entrées (il y a autant d'entrées que des états discrets), de deux sorties (à droite du bloc) qui fournissent l'état discret courant x_i et précédent x_{i-1} et le vecteur des variables d'état continu et de leurs dérivées $\left[x, \dot{x}\right]^{\mathrm{T}}$. L'unique sortie est une sortie d'événements discrets e qui est activée lorsque n'importe quelle transition d'état discret se produit. Le générateur aléatoire correspond à la structure temporisée stochastique $\mathcal{H}$ et p. Le générateur aléatoire réalise des tirages aléatoires correspondant aux transitions stochastiques. Chaque fois qu'une transition d'état discret se produit la sortie d'activation du bloc automate hybride génère un événement e activant le bloc générateur aléatoire à travers son entrée d'activation. A ce moment le tirage des valeurs aléatoires est réalisé. Le bloc générateur aléatoire permet de choisir la loi de distribution de probabilité à utiliser : exponentielle, Weibull, etc. Le descripteur de modes correspond aux différentes dynamiques continues du système. Il y a autant de dynamiques continues que d'états discrets. Le descripteur a deux entrées : la première correspond aux variables physiques et à leurs dérivées qui viennent de l'automate hybride et la deuxième entrée reçoit les valeurs aléatoires du tirage produites par le générateur aléatoire. La sortie du descripteur de modes contient l'ensemble des valeurs des variables continues associées à chaque état discret du système. Cet ensemble est transmis aux entrées de l'automate hybride.

Dans ce papier nous appliquons ce concept d'automate stochastique hybride à la modélisation et à l'évaluation des paramètres de la sûreté de fonctionnement d'un cas test de référence dans la communauté fiabiliste [4].

4. Cas test en fiabilité dynamique

Le cas test (figure 2) consiste en un réservoir contenant un liquide dont le niveau *h* doit être maintenu à l'aide d'une pompe principale P_1, d'une pompe de secours P_2 et d'une vanne d'évacuation V. La vanne V permet de vider le réservoir avec un débit donné, tandis que les pompes P_1 et P_2 en assurent le remplissage. La mission à remplir par cette installation est de maintenir le niveau de liquide dans l'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 P_1 et P_2 ne compensent plus celui de la vanne V. Chacun de ces trois composants est commandé par une boucle de contrôle contenant un détecteur de niveau. Les trois composants sont mutuellement indépendants et non réparables.

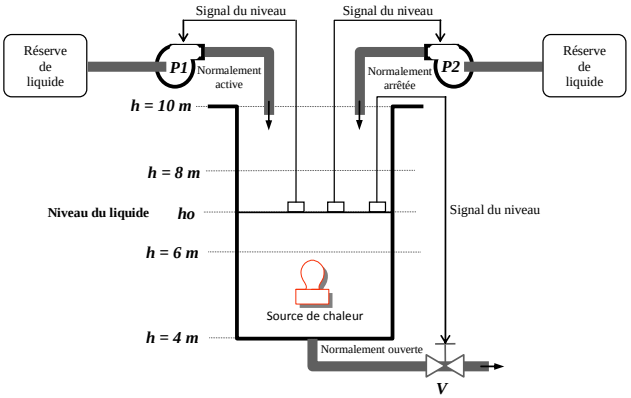

FIG.2 : Cas test étudié : réservoir et sa régulation de niveau

Une source de puissance thermique constante chauffe le liquide dont la température évolue ainsi avec les débits d'entrée et de sortie. On suppose de plus que les taux de défaillance des composants dépendent de la température suivant les relations suivantes :

$$\lambda^c = a(T)\hat{\lambda}^c \quad c = P_1, P_2, V \tag{5}$$

$$a(T) = \frac{b_1 e^{b_c(T-20)} + b_2 e^{-b_d(T-20)}}{(b_1 + b_2)} \tag{6}$$

où *a(T)* est une fonction de la température (figure 3) et les paramètres respectifs sont : $\lambda_{P1} = 2{,}2831.10^{-3}h^{-1}$, $\lambda_{P2} = 2{,}8571.10^{-3}h^{-1}$, $\lambda_V = 1{,}5625.10^{-3}h^{-1}$, $b_1 = 3{,}0295$, $b_2 = 0{,}7578$, $b_c = 0{,}05756$ et $b_d = 0{,}2301$.

En plus de l'assèchement et du débordement une troisième situation dangereuse peut se produire, celle d'une *surchauffe* lorsque la température du liquide devient supérieure à 100°C.

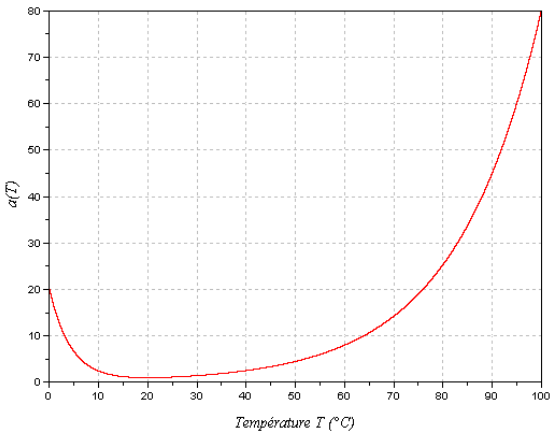

FIG. 3 : La fonction *a(T)* exprimant l'évolution du taux de défaillance des composants (courbe en baignoire)

Les variables continues pour le système sont : le niveau du liquide *h* et la température *T* du fluide lesquelles varient en fonction de l'état des composants. Ainsi, les variables *h(t)* et *T(t)* satisfassent les équations différentielles suivantes :

$$\begin{aligned} \frac{dh(t)}{dt} &= \gamma_1(\upsilon) \\ \frac{dT(t)}{dt} &= (\gamma_2(\upsilon) - \gamma_3(\upsilon)T)/h \end{aligned} \tag{7}$$

où $\upsilon = (\upsilon_{P1}, \upsilon_{P2}, \upsilon_V)$ et les composants $c \in \{P_1, P_2, V\}$. Ainsi :

$$\upsilon_c = \begin{cases} 0 & \text{si c est OFF ou bloqué en OFF} \\ 1 & \text{si c est ON ou bloqué en ON} \end{cases} \tag{8}$$

avec : $\gamma_1(\upsilon) = (\upsilon_{P1} + \upsilon_{P2} - \upsilon_V)G$,

$\gamma_2(\upsilon) = (\upsilon_{P1} + \upsilon_{P2})GT_{in} + 23{,}88915$, $\gamma_3(\upsilon) = (\upsilon_{P1} + \upsilon_{P2})G$, G = 1,5 m^3h^{-1} (débit des composants) et T_{in} = 15°C (température initiale du liquide).

Les équations généralisées (7) reflètent les différents modes opératoires possibles du processus. Elles font 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. La valeur 0 est prise dans le cas contraire, comme l'exprime l'équation (8). En conditions nominales, les débits pour les trois composants est le même. Au temps $t = 0$, le niveau du liquide *h* est 7 m, la température est 30,9261 °C, la pompe P_1 fonctionne, la pompe P_2 est à l'arrêt et la vanne V est ouverte.

Les lois de commande du système qui définissent l'état des pompes et de la vanne en fonction du niveau de liquide sont données dans le tableau suivant.

TAB.1 : Etat des composants en fonction du niveau de liquide

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

Les pompes P_1, P_2 ainsi que la vanne V présentent deux modes de défaillances : le comportement intempestif et le blocage dans l'état occupé. La figure 4 montre les états discrets de ces composants et les transitions entre ces états.

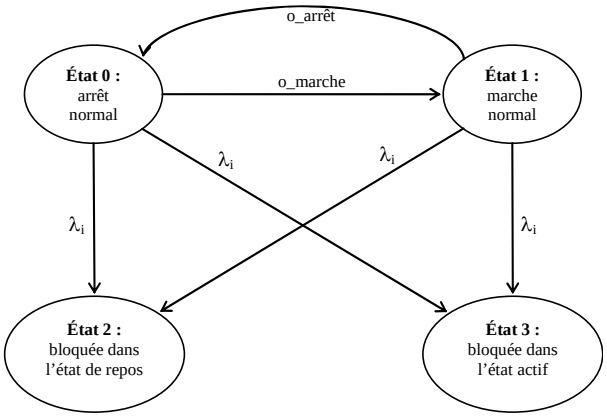

FIG. 4 : Etats des composants et transitions entre états

La mission du système est de maintenir le niveau et la température en évitant les trois événements redoutés : l'assèchement, le débordement et la surchauffe qui représentent les défaillances du système. Afin de montrer l'intérêt de l'utilisation de l'automate stochastique hybride dans les études de sûreté de fonctionnement en contexte dynamique, nous allons évaluer la probabilité d'occurrence de ces trois événements redoutés.

Tout d'abord il est nécessaire d'obtenir l'automate stochastique global du système modélisé. Nous construisons celui-ci par composition parallèle (synchronisation) des automates élémentaires de composants. Les automates élémentaires modélisant le fonctionnement des deux pompes et celui de la vanne s'obtiennent par déclinaison de l'automate de la figure 4. En plus de ces automates nous avons besoin de deux automates supplémentaires afin de modéliser l'évolution du niveau de liquide dans le réservoir et l'occurrence de deux événements redoutés, l'assèchement et le débordement, (figure 5.a), l'évolution de la température et le franchissement de seuil représentant l'événement redouté de surchauffe (figure 5.b), ainsi que d'un automate (figure 5.c) modélisant les ordres fournis par le système de commande aux différents composants en relation avec les lois de commande présentées dans le tableau 1.

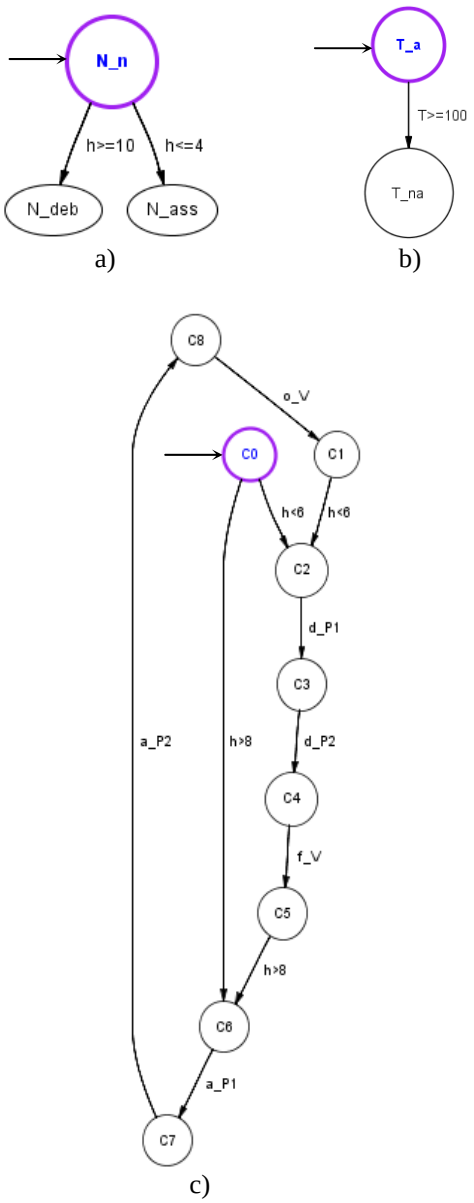

FIG. 5 : Automates élémentaires :
a) niveau de liquide
b) température du liquide
c) système de commande

La composition parallèle de ces automates nous a amené à un automate global à 1746 états. L'implantation de cet automate étant fastidieuse nous l'avons simplifié tout d'abord en considérant que notre objectif est l'évaluation de la probabilité d'occurrence des événements redoutés. Dans notre modélisation les défaillances sont représentées par des états bloquants dans lesquels le système est amené par l'occurrence des événements redoutés (conformément aux automates de la figure 5.a et 5.b). En conséquence la probabilité de défaillance peut se déterminer par la probabilité que le système se trouve dans l'état bloquant correspondant. De plus, nous nous intéressons à la probabilité de défaillance cumulée et non aux différentes manières d'atteindre l'état bloquant correspondant. Ainsi, nous fusionnons les états de

l'automate global qui contiennent les sous-états redoutés bloquants des composants.

Une deuxième règle de simplification consiste à regrouper les états fugitifs (dans lesquels le système ne passe pas de temps) avec le premier état ayant une durée de séjour non nulle obtenu après le passage par ces états fugitifs. Ces états fugitifs ont été introduits dans les automates élémentaires pour le besoin de la modélisation (pour modéliser l'action de la commande ont été introduits les séquences C2 → C3 → C4 → C5 lorsque le niveau de liquide atteint le seuil h<6 m et C6 → C7 → C8 → C1 lorsque le niveau du liquide atteint h>8 m), mais ils n'apportent rien à l'évaluation des probabilités de défaillance.

L'application de ces règles nous a permis de simplifier l'automate global du système. L'automate résultant présente 83 états Celui-ci a été implanté ensuite sous Scilab-Scicos.

Pour évaluer les probabilités de défaillances (assèchement, débordement et surchauffe) nous avons effectué une simulation de Monte-Carlo sur 10^4 histoires et nous avons tracé l'évolution de ces probabilités en fonction du temps nécessaire pour atteindre l'état correspondant. La figure 6 montre les probabilités cumulées de ces défaillances.

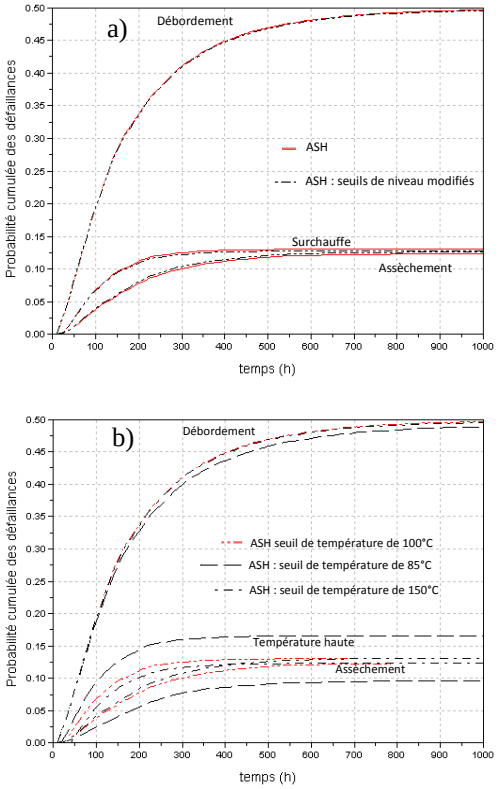

FIG. 6 : Probabilités cumulées de défaillances

Nous avons également fait varier les seuils de niveau représentant les événements de débordement et d'assèchement, ainsi que le seuil de température représentant l'événement de surchauffe. L'étude de la variation des paramètres du modèle montre une sensibilité faible aux paramètres de niveau. Sur la figure 6.a le seuil de débordement a été diminué d'un mètre et le seuil d'assèchement a été augmenté d'un mètre. Par contre, on note une sensibilité assez importante au paramètre température (figure 6.b). Avec un seuil de 85°C, la probabilité d'assèchement diminue sensiblement du fait que la probabilité d'avoir d'abord un dépassement de température augmente.

5. Conclusions

Dans ce papier nous avons présenté une approche d'évaluation prévisionnelle de la sûreté de fonctionnement en contexte dynamique. Afin de modéliser le système étudié nous avons défini un automate stochastique hybride qui permet de modéliser à la fois l'aspect événementiel (occurrence d'événements qui provoque un changement d'état discret) l'aspect continu (équations différentielles pour représenter l'évolution des variables physiques) et l'aspect temporisé et stochastique (horloges stochastiques). Cet automate stochastique hybride est implémenté dans l'environnement libre Scilab-Scicos. Pour valider notre approche, nous l'appliquons à l'étude d'un cas test qui présente deux variables continues : le niveau de liquide et la température et les interdépendances entre celles-ci sont prises en compte. De plus, la température agit également sur les taux de défaillances de composants. Il s'agit d'un cas typique de la fiabilité dynamique.

Les probabilités de défaillance (assèchement, débordement et surchauffe) sont évaluées par une approche de type simulation de Monte-Carlo. L'étude de la sensibilité de ces probabilités par rapport aux paramètres d'entrée du modèle montre qu'en réduisant le seuil de température représentant le phénomène de surchauffe on diminue également la probabilité d'assèchement du fait que la probabilité d'avoir d'abord un dépassement de température augmente. Nous touchons là un problème important de la fiabilité dynamique. En effet, on constate qu'il est indispensable de raisonner en termes de séquences possibles d'événements (dans notre modèle, le langage de l'automate) et non plus en termes de coupes. En effet, certains événements étant associés à des variables continues couplées, ils peuvent avoir lieu dans n'importe quel ordre (il n'y a pas d'occurrence simultanée dans un automate) et il convient de ne pas arrêter la simulation sur la détection du premier. Les probabilités à retenir seraient sans doute celles correspondant aux différentes séquences possibles. Par la construction de notre automate, nous pourrons identifier les états terminaux associés à chacune de ces séquences et par conséquent en déduire leur probabilité. Nous nous proposons de développer cet aspect dans une proche perspective.

Références

[1] Siu, N., 1994. Risk assessment for dynamic systems: An overview. *Reliability Engineering and System Safety* 43, p. 43-73.

[2] Labeau P. E., Smidts C., Swaminathan S., Dynamique reliability: towards an integrated plarform for probabilistic risk assessment, *Reliability Engineering and System Safety*, 68, 2000, p. 219-254.

[3] Cocozza-Thivent C., Desgrouas M. and Mercier S., Algorithme de calcul de disponibilité asymptotique en fiabilité dynamique, *Lambda mu 15*, Lille, 2006.

[4] Zhang H., Gonzalez K., Dufour F., Dutuit Y., Piecewise deterministic Markov processes and dynamic reliability, *Journal of Risk and Reliability*, vol. 222 (4), 2008.

[5] Bechta Dugan J., Sullivan K.J., Coppit D., Developing a low-cost high-quality software tool for dynamic fault-tree analysis, *IEEE Transactions on Reliability*, vol. 49(1), pp. 49–59, 2000.

[6] Bouissou M., Bon J.L., A new formalism that combines advantages of fault-trees and Markov models: Boolean logic Driven Markov Processes, *Reliability Engineering and System Safety*, vol. 82 (2), pp. 149-163, 2003.

[7] Pérez Castaneda G.A., Aubry J.F., Brinzei N., Automate Stochastique hybride, *7ème Conférence Internationale de Modélisation et Simulation (MOSIM)*, pp. 386-395, Paris, 2008.

[8] Najafi, M. and R. Nikoukhah, 2007. *Modeling Hybrid Automata in Scicos*. Multi-conference on Systems and Control (MSC), Singapore.