7e Conférence Internationale de MOdélisation et SIMulation - MOSIM'08 - du 31 mars au 2 avril 2008 – Paris- France
« Modélisation, Optimisation et Simulation des Systèmes : Communication, Coopération et Coordination.».

AUTOMATE STOCHASTIQUE HYBRIDE APPLIQUÉ À L'ÉVALUATION DE LA FIABILITÉ DYNAMIQUE

G. A. PÉREZ CASTANEDA[1, 2], J. - F. AUBRY[1]

[1]CRAN CNRS UMR 7039
Nancy – Université, INPL – ENSEM
2, avenue de la forêt de Haye
54516 Vandœuvre-lès-Nancy, France
jean-francois.aubry@isi.u-nancy.fr
nicolae.brinzei@ensem.inpl-nancy.fr

N. BRINZEI[1]

[2]Instituto Tecnológico de Tehuacán
Libramiento Instituto Tecnológico s/n, 75770
Tehuacán, Puebla, México
perezc76@ensem.inpl-nancy.fr

RÉSUMÉ : *Un système dynamique hybride (SDH) 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. Pour cette raison, nous avons défini et implémenté un Automate Stochastique Hybride pour modéliser un SDH afin de prendre en compte les problèmes relatifs aux défaillances pour évaluer par simulation les paramètres de la sûreté de fonctionnement. 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. L'automate nous permet d'accéder aux grandeurs de la sûreté de fonctionnement, lesquelles sont obtenues par statistique sur un grand nombre de simulations (Méthode de Monte Carlo). Après la définition formelle de l'automate stochastique hybride, nous présenterons un cas test permettant d'inclure la majorité des problèmes posés par l'évaluation des paramètres de la sûreté de fonctionnement en contexte dynamique.*

MOTS-CLÉS : *Automate stochastique hybride, fiabilité dynamique, simulation des systèmes dynamiques hybrides.*

1. INTRODUCTION

Une caractéristique importante de nombreux systèmes industriels est que leur comportement, comme par exemple la réponse à une perturbation, change en fonction du temps en raison des interactions entre les composants de ce système ou avec l'environnement (Siu, 1994). 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). En plus de l'hybridité (continu + événements discrets), il faut donc tenir compte du caractère stochastique du système imposé par les défaillances des composants ou par les incertitudes sur la connaissance du système. Pour cette raison, actuellement, il est très important de pouvoir évaluer la fiabilité de ces types de systèmes. Cependant, pour son évaluation, il faut surmonter les problèmes qu'elle pose.

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. Pour cette raison, dans ce papier, nous présentons un Automate Stochastique Hybride (ASH) permettant de modéliser les interactions entre les défaillances des composants et les dynamiques continues du système, dans le but d'accéder à l'évaluation de la fiabilité d'un système dynamique par la simulation.

Nous avons implémenté l'automate stochastique hybride pour évaluer non seulement la fiabilité du système, mais aussi sa disponibilité et sa maintenabilité. L'automate stochastique hybride nous permet de tenir compte des interactions entre les composants et les variables du processus physique et aussi de l'interaction avec les défaillances des composants du système. De même, nous présentons les résultats de la modélisation et de la simulation d'un cas test au moyen de cet automate stochastique hybride. Pour évaluer la fiabilité d'un système, ainsi que sa disponibilité et sa maintenabilité, nous avons appliqué une simulation de Monte Carlo. En ce qui concerne à la fiabilité du système, nous avons

considéré le MTTF (mean time to failure), c'est-à-dire la durée moyenne de fonctionnement avant défaillance. Pour la disponibilité nous avons d'abord considéré l'indisponibilité du système et à partir de celle-ci nous avons calculé sa disponibilité. Finalement, nous avons considéré pour la maintenabilité le MTTR (mean time to repair), c'est-à-dire, la durée moyenne de réparation. Le MTTF et le MTTR, nous permettent de donner une estimation en termes de temps de la fiabilité et de la maintenabilité du système (Villemeur, 1988).

2. LA FIABILITÉ DYNAMIQUE

Afin de dimensionner et mesurer l'importance de l'implémentation de l'automate stochastique hybride et son application à l'évaluation de la fiabilité d'un système dynamique et des autres grandeurs de la Sûreté de Fonctionnement (SdF), nous allons définir de façon générale ce qu'on entend par fiabilité dynamique, quels sont les principaux problèmes qu'elle pose et comment nous allons les surmonter. Il existe par ailleurs des méthodes qui ont été développées pour l'évaluer. Un état de l'art de la fiabilité dynamique et de ces méthodes a déjà été présenté (Pérez-Castaneda *et al.*, 2007b). De même, nous avons aussi proposé une approche pour l'évaluation de la fiabilité dynamique dans (Pérez Castaneda *et al.*, 2007a).

2.1. Définition

La fiabilité dynamique est l'évaluation prévisionnelle de la fiabilité d'un système dont la structure fiabiliste (ce qui exprime comment la défaillance du système dépend des défaillances de ses composants) évolue dans le temps. On peut donc dire en général que la « fiabilité dynamique » est le problème de l'évaluation probabiliste de la défaillance d'un système dynamique hybride. On peut la représenter sous la forme suivante :

$$R_S(t) = P[\,S(X(T),Q(T),V(T)) = 1\,] \quad 0 \le T \le t \qquad (1)$$

Cette expression exprime que la fiabilité $R_S(t)$ d'un système non réparable se mesure par la probabilité que le système fonctionne pendant un intervalle de temps [*0, t*]. *S* est la fonction de structure du système qui vaut *1* si le système fonctionne et *0* dans le cas contraire. *X(T)* le vecteur d'état continu et *Q(T)* le vecteur d'état discret. *V(T)* est le vecteur des variables aléatoires « état de fonctionnement » des composants.

2.2. Les principaux problèmes que pose la fiabilité dynamique

Le premier problème à traiter est de prendre en compte les interactions dynamiques existant entre les paramètres physiques et le comportement nominal ou dysfonctionnel des composants du système. Un deuxième problème (parfois lié au précédent) est de prendre en compte le temps et notamment l'ordre d'occurrence des événements, notamment des défaillances. Un troisième problème, consiste à prendre en compte les défaillances progressives des composants dues à l'usure (Soro, 2006).

Si on désire traiter les problèmes relatifs à la fiabilité dynamique à travers un formalisme mathématique, cela nécessite d'intégrer dans le modèle les interactions entre les phénomènes probabilistes et le processus physique. L'expression mathématique proposée par (Kermish et Labeau, 2000) prend en compte cet aspect sur la base des équations de Chapman – Kolmogorov pour un système markovien. C'est la densité de probabilité $\pi(\bar{x},i,t)$ de trouver le système au temps *t* dans l'état discret *i* où le vecteur $\bar{u}$ des variables physiques prend la valeur $\bar{x}$:

$$\boldsymbol{\pi}(\bar{x},i,t) = \int \boldsymbol{\pi}(\bar{u},i,0).\boldsymbol{\delta}\left(\bar{x} - \bar{g}_i(t,\bar{u})\right).e^{-\int_o^t \boldsymbol{\lambda}_i(\bar{g}_i(s,\bar{u}))ds} d\bar{u}$$
$$+ \sum_{j \neq i} \int d\bar{u} \int_o^t d\boldsymbol{\tau}\, \boldsymbol{\pi}(\bar{u},j,\boldsymbol{\tau})\, p(j \to i \mid \bar{u})\, \boldsymbol{\delta}\left(\bar{x} - \bar{g}_i(t-\boldsymbol{\tau},\bar{u})\right)$$
$$\cdot e^{-\int_\tau^t \boldsymbol{\lambda}_i(\bar{g}_i(s-\boldsymbol{\tau},\bar{u}))ds} \qquad (2)$$

$\bar{g}_i(t,\bar{u})$ 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 $\bar{x}$ à l'instant *t*. $\lambda_i(\bar{g}_i(s,\bar{u}))$ est le taux global de sortie de l'état *i* qui dépend des variables physiques (et donc de la trajectoire). $p(j \to i \mid \bar{u})$ est la probabilité de transition de l'état *j* vers l'état *i* au point $\bar{u}$. 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.

Cependant, la résolution de (2) n'est possible qu'au niveau de cas-test. D'autres méthodes analytiques sont aussi proposées (Dufour et Dutuit, 2002), (Desgrouas et Mercier, 2005), (Cocozza-Thivent et Eymard, 2006) et (Mercier, 2006), pour citer quelques exemples. Néanmoins, elles sont limitées à des cas-test en considérant certaines hypothèses, ce qui limite la possibilité de prendre en compte toute la problématique posée par la fiabilité dynamique dans le modèle mathématique. Les autres méthodes montrent un degré élevé de complexité mathématique. Finalement, (Cocozza-Thivent *et al.,* 2006) expriment que pour certains systèmes parfois très « simples », il n'existe aussi aucune méthode analytique pour calculer des quantités usuelles comme la disponibilité.

En conséquence, étant donnée la complexité et les limites mathématiques pour évaluer la fiabilité d'un système dynamique hybride, nous pouvons conclure qu'elle n'est souvent accessible que par simulation. En résumé, le modèle à simuler doit prendre en compte les éléments suivants :

a) Système hybride : combinaison d'équations d'état continu et d'automate d'états finis.

b) Reconfiguration des équations d'état continu sur l'occurrence des événements (entraînant donc une modification de la structure fiabiliste).

c) Caractère déterministe ou stochastique des variables et des événements.

d) Injections des défaillances.

e) Diagnostic de ces défaillances et réaction à ces défaillances en temps réel.

f) Prise en compte des lois de probabilités quelconques (et notamment en fonction du temps) et l'interaction entre ces lois de probabilités et l'état continu du système.

2.3. La fiabilité dynamique et l'automate stochastique hybride

A l'heure actuelle, il existe plusieurs approches développées pour évaluer la fiabilité dynamique. Mais, elles ne prennent pas en compte tous les aspects mentionnés ci dessus. Par exemple l'approche DYLAM (Dynamic Logical Analytical Methodology) (Cojazzi, 1996). Elle est utilisée surtout par les spécialistes du domaine nucléaire. Cette méthodologie est un outil puissant qui prend en compte les événements déterministes et les défaillances. Pour une analyse plus détaillée de la fiabilité, l'idée basique de cette méthode est de fournir un outil pour coupler les comportements probabilistes et déterministes d'un système d'une part et les comportements physiques et événementiels d'autre part. Mais DYLAM est une méthode de simulation qui discrétise le temps et modélise explicitement l'évolution des variables du processus physique. Un autre inconvénient de DYLAM, est la logistique un peu lourde qu'elle utilise pour démarrer l'évaluation de la fiabilité.

Une autre approche dite de modélisation « hybride » est proposée par (Chabot *et al.,* 1998). Celle-ci intègre les phénomènes continus et les événements discrets. Le modèle du système à étudier est réalisé sous la forme d'un réseau de Petri stochastique interprété qui sert de support à une simulation de Monte Carlo classique en s'appuyant sur le logiciel MOCA-RP®. Les inconvénients de cette approche sont d'abord qu'il faut écrire deux procédures qui décrivent les lois spéciales relatives aux transitions d'activité continue et aux transitions discrètes à délai nul. Ensuite, on définit un fichier texte contenant les données pour le calcul continu permettant de définir les valeurs initiales des paramètres continus pour chaque nouvelle histoire de la simulation de Monte Carlo. Finalement, la complexité pour implémenter le réseau de Petri du système physique est conséquente. Cela est dû aux différents types de transitions définies afin de distinguer celles qui correspondent à la partie continue de celles de la partie discrète. De même pour les différents types de place.

Afin d'intégrer tous les problèmes posés par la fiabilité dynamique, nous avons donc défini un automate stochastique hybride. 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 de l'automate et le passage de l'un à l'autre sur des événements déterministes ou stochastiques désignés par les transitions correspondantes. Les événements déterministes sont produits par un franchissement de seuils des variables continues et les événements stochastiques sont produits par un générateur aléatoire, en fonction de leurs lois de probabilités. Les dynamiques continues du système sont définies à travers des équations différentielles ordinaires.

Notre approche ne discrétise pas le temps car elle prend en compte les changement d'état au cours de la simulation à n'importe quel instant. Nous avons implémenté dans la même simulation tous les paramètres physiques et stochastiques afin de les traiter en temps réel et durant la même simulation. Un autre avantage que nous offre l'automate stochastique hybride par rapport aux autres approches, réside dans le fait qu'il nous permet de gérer les dynamiques continues du système à travers des fonctions de transitions appelées « zero-crossing » en détectant l'occurrence des événements qui se produisent soit par le franchissement des seuils des variables physiques soit par les défaillances ou les réparations aléatoires des composants.

3. L'AUTOMATE STOCHASTIQUE HYBRIDE

Nous avons commencé à traiter les problèmes relatifs à la fiabilité dynamique de façon progressive. L'automate stochastique hybride prend en compte les différents éléments présentés (§ 2.2) :

- Un automate à états finis nous permet de définir la partie événementielle. En plus, dans chaque état nous spécifions le mode de fonctionnement (la dynamique continue) du système. Cela nous amène à transformer l'automate à états finis en automate hybride pour gérer la partie continue et la partie événementielle, c'est-à-dire, pouvoir piloter les événements qui se produisent dans la partie continue en fonction des événements qui se produisent dans la partie discrète (points a et b § 2.2).
- Compte tenu du caractère déterministe et stochastique des variables et des événements, nous avons introduit dans l'automate hybride l'aspect stochastique à travers un générateur aléatoire afin de modéliser les défaillances et les réparations du système. Une fonction de « zero-crossing » nous permet de déterminer les franchissements des seuils soit des variables du processus, soit des variables stochastiques pour les défaillances et réparations des composants (points c, d et e §2.2).

3.1. Définition de l'automate stochastique hybride

Ce sont (Alur *et al.,* 1993) qui ont introduit la structure mathématique de l'automate hybride comme un modèle et un langage de spécification pour les systèmes hybrides. (Alur *et al.,* 1995) modélisent les systèmes dynamiques hybrides comme un automate fini muni de

variables qui évoluent continuellement avec le temps conformément aux lois dynamiques physiques. Étant donné que de nombreuses applications de sécurité critique sont des systèmes hybrides, des analyses de fiabilité rigoureuses sont requises exigeant une modélisation formelle (Henzinger, 1996).

Définition :

Un Automate Stochastique Hybride est un 11-tuple

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

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 $(x, e, \mathrm{G}, \mathrm{R}, x')$ 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,
- $\mathrm{A} : \mathcal{X} \times X \to (\Re^+ \to \Re)$ 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,
- 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'' (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 à l'état discret initial x, à la valeur initial de la variable d'état continu x et à la probabilité de transition initiale, respectivement.

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 temporisé et stochastique.

3.2. Réalisation de l'automate stochastique hybride

L'outil informatique utilisé pour implémenter l'automate stochastique hybride afin d'évaluer la fiabilité d'un système dynamique hybride est la boîte à outils Scicos de Scilab. Nous avons implémenté l'automate stochastique hybride sur la base de l'automate hybride proposé par (Najafi et Nikoukhah, 2007).

L'automate stochastique hybride est composé d'un automate hybride et d'un générateur aléatoire liés aux différents modes de fonctionnement à travers un « descripteur de modes ». Il est présenté dans la figure 1.

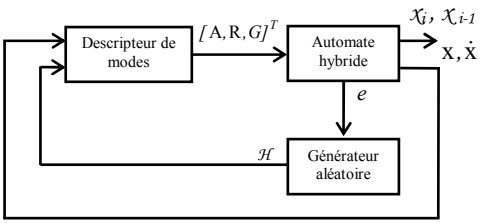

Figure 1. Modèle de l'automate stochastique hybride

L'*automate hybride* dont la définition est donnée par (Najafi et Nikoukhah, 2007) est un bloc Scicos. Il est constitué de *i* ports d'entrée (à gauche du bloc) et de deux ports de sortie (à droite du bloc). L'unique sortie (en bas du bloc) est une sortie d'événements discrets *e*. Celle-ci est activée quand une transition d'état se produit. En ce qui concerne les entrées, il y a autant d'entrées que d'états (ou modes de fonctionnement) permettant de décrire le système. Chaque entrée correspond à un vecteur donné par l'équation 3 :

$$V_i = \begin{bmatrix} \mathrm{A}_i(\dot{\mathrm{x}}, \mathrm{x}, u, t) \\ \mathrm{R}_i(\dot{\mathrm{x}}, \mathrm{x}, u, t) \\ \mathrm{G}_i(\dot{\mathrm{x}}, \mathrm{x}, u, t) \end{bmatrix} \quad (3)$$

où le premier élément du vecteur correspond à la dynamique $\mathrm{A_i}$ du système dans l'état courant x_i, laquelle est exprimée par une équation différentielle de la forme :

$$0 = \mathrm{A}_i(\dot{\mathrm{x}}, \mathrm{x}, u, t) \quad (4)$$

x et $\dot{\mathrm{x}}$ étant respectivement la variable d'état continu et sa dérivée, u le vecteur des variables d'entrée et t le temps. Le deuxième élément R_i du vecteur V_i d'entrée correspond aux valeurs qui sont utilisées pour réinitialiser les variables d'état continu lors de l'entrée dans un nouvel état discret. Enfin, le troisième élément G_i du vecteur V_i correspond aux conditions de garde associées aux transitions de sortie de l'état x_i. En ce qui concerne les deux sorties de l'automate hybride, la première (au-dessus) est un vecteur qui indique le numéro d'état discret courant x_i et le précédent x_{i-1}. La deuxième sortie (au-dessous) correspond au vecteur des variables d'état continu x et de leurs dérivées $\dot{\mathrm{x}}$.

Le *générateur aléatoire* de la figure 1 correspond à la structure temporisée stochastique $\mathcal{H}$ de la définition donnée. Le générateur aléatoire réalise des tirages aléatoires correspondant aux transitions aléatoires. Le générateur aléatoire est activé chaque fois qu'il y a un changement d'état discret grâce à la sortie des

événements discrets de l'automate hybride. Le générateur aléatoire est constitué de deux blocs Scicos : le premier où on pourra définir les fonctions aléatoires spécifiques à tous les états et le deuxième qui permettra de mémoriser la valeur aléatoire générée à chaque tirage afin d'être mise à la disposition de l'automate.

Le *descripteur de modes* du modèle de l'automate stochastique hybride de la figure 1 correspond aux différentes dynamiques continues du système. Il y a autant de dynamiques continues que d'états discrets.

Afin de montrer les différentes caractéristiques et les avantages qu'offre l'utilisation et l'application de l'automate stochastique hybride à l'évaluation de la fiabilité d'un système dynamique, nous allons présenter un cas test sur lequel nous avons effectué une simulation de Monte Carlo dont les résultats statistiques permettent de déterminer les paramètres de sûreté de fonctionnement.

4. LE CAS TEST

Il s'agit de modéliser et simuler le comportement d'un système dynamique hybride constitué d'un four et de son système de contrôle de température.

4.1. Description du système

Le système présenté figure 2 contient deux boucles de régulation. La première contient un contrôleur Proportionnel-Intégral (PI) dont le rôle est de contrôler la température du four en fonction de la température de référence. La deuxième boucle est de type Tout ou Rien (TOR), elle permet de maintenir la température du four aux alentours de la température de référence +/- ΔT. Les deux boucles ne peuvent pas fonctionner en même temps. Pour cela, un relais bascule ses deux contacts permettant ainsi d'activer soit le PI soit le TOR. L'ordre de basculement est donné par le composant « diagnostic » dont le rôle est de détecter les défaillances.

4.2. Comportement du système

Le système fonctionne de la manière suivante : au démarrage la température x du four est contrôlée par le contrôleur PI. Au bout d'un certain temps aléatoire (λ_{PI}) le contrôleur tombe en panne (avec un taux (λ_{PI}) et la température du four augmente rapidement. Le diagnostic détecte que la température du four a atteint une valeur dangereuse ($x \geq x_{s\,max}$) déduisant ainsi que la température du four est hors contrôle. Il donne alors l'ordre au relais de basculer sur la boucle TOR. La boucle du contrôleur PI est maintenant ouverte et la boucle TOR fermée. La température du four est contrôlée maintenant par le TOR ($x_{inf\,TOR} \leq x \leq x_{supTOR}$). Dès que le diagnostic a détecté que la température est hors contrôle, il a donné l'ordre de basculer au relais vers la boucle du TOR et enclenché le processus de réparation du contrôleur PI (on considère une réparation de durée aléatoire μ_{PI}). Cependant, la possibilité de défaillance du TOR existe, après une durée également aléatoire (λ_{TOR}). Une fois que le contrôleur PI est réparé, le diagnostic bascule le relais sur la boucle de celui ci et ouvre la boucle du TOR. La température du four est maintenant à nouveau régulée par le contrôleur PI. On inclut également le processus de réparation du TOR (μ_{TOR}). On a considéré que le four n'est pas défaillant.

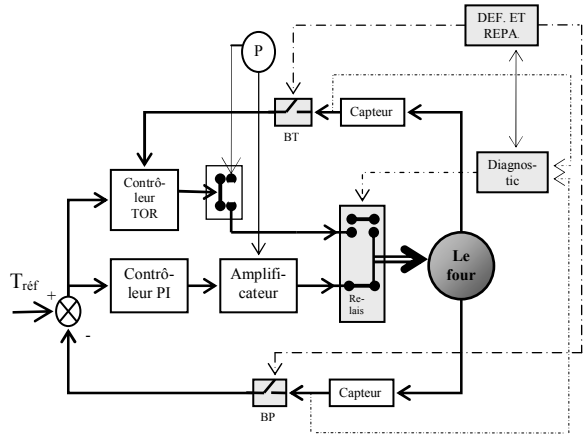

Figure 2. Diagramme structurel du système de contrôle de la température d'un four

$T_{réf}$ – Température de référence P – Alimentation de puissance

L'automate stochastique hybride de la figure 3 résume le comportement du système. L'automate a 9 états dont l'état 1 est l'état initial. Dans chaque état il y a une équation différentielle de la forme donnée par (4) laquelle représente la dynamique continue du système. Sur chaque transition sont indiqués e, G et R .

En partant de la définition de l'automate stochastique hybride nous avons les expressions suivantes pour le cas test :

$$\mathcal{X} = \{1,2,3,4,5,6,7,8,9\}$$
$$\mathcal{E} = \{\lambda_{PI}, \lambda_{TOR}, \mu_{PI}, \mu_{TOR}, d_{smin}, d_{smax}, d_{infTOR}, d_{supTOR}\}$$

dont

- $\lambda_{PI}, \lambda_{TOR}, \mu_{PI}$ et μ_{TOR} sont respectivement les taux de défaillance du PI et du TOR ainsi que leurs taux de réparation. Ces taux correspondent aux transitions stochastiques du système. Ces événements correspondants seront produits par le générateur aléatoire dans la simulation.
- d_{smin} et d_{smax} sont les seuils de température minimum et maximum au-delà de laquelle le diagnostic identifie la défaillance des contrôleurs PI et TOR.
- d_{infTOR} et d_{supTOR} sont les seuils du TOR et quand ils sont détectés par le diagnostic, le four s'allume ou s'éteint.

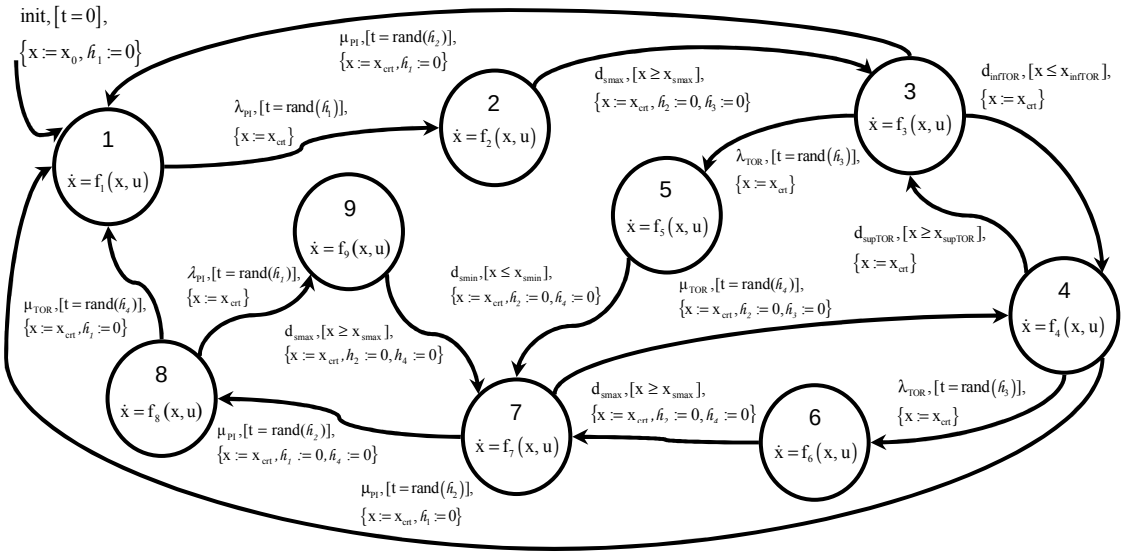

Figure 3. Automate stochastique hybride du système de contrôle de la température d'un four

$G = \{\ t = rand(h_1);\ t = rand(h_2);\ t = rand(h_3);$
$t = rand(h_4);\ x \le x_{smin};\ x \ge x_{smax};$
$x \le x_{infTOR};\ x \ge x_{supTOR}\ \}$

$X = \{x\}$, représente la variable physique du système : la température.

$A : \mathcal{X} \times X \to \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9\}$

$R = \{x = x_{crt}\}$. La valeur de la température x à l'entrée dans chaque état est la même quand le système a quitté l'état précédant (température courante x_{crt}).

$R = \{h_2 := 0\}$ représente la réinitialisation de l'horloge h_2 qui modélise le temps de réparation du contrôleur PI.

$\mathcal{H} = \{h_1, h_2, h_3, h_4\}$, h_1 et h_2 représentent le temps de bon fonctionnement et, respectivement, le temps de réparation du contrôleur PI. h_3 et h_4 représentent le temps de bon fonctionnement et, respectivement, le temps de réparation du contrôleur TOR.

$\mathcal{F}(h) = 1 - e^{-\lambda h}$. Nous avons utilisé la loi exponentielle pour $i = 1 \ldots 4$.

Pour le cas test il n'y a pas besoin d'utiliser p, parce il n'y a pas de transition en conflit.

Nous donnons une brève description des états du système correspondant à l'automate stochastique hybride de la figure 3 :

- État 1, le contrôleur PI est actif et il contrôle la température du four.
- État 2, le contrôleur PI est actif mais défaillant alors que le contrôleur TOR n'est pas sollicité.
- États 3 et 4, le contrôleur TOR est actif et le contrôleur PI est en réparation.
- État 5 et 6, le TOR est défaillant mais toujours actif. Le temps de détection de la défaillance est très bref et l'occurrence de l'événement « fin de réparation du PI » pendant ce temps est hautement improbable. En conséquence, on néglige l'occurrence de cet événement lors du séjour du système dans les états 5 et 6.
- État 7, la défaillance du TOR est détectée par le diagnostic. Dans cet état les deux boucles sont défaillantes et inactives, mais le PI est en réparation.
- État 8, le TOR est maintenant en réparation. Le PI est réparé et il est maintenant actif.
- État 9, le PI est actif mais défaillant alors que le TOR est en réparation.

Les transitions : 2→3, 3→4, 4→3, 5→7, 6→7 et 9→7 sont déterministes, elles correspondent aux franchissements de seuils de température. Les autres transitions sont aléatoires : défaillances ou réparations de contrôleurs.

4.3. Paramètres pour la modélisation et la simulation

Du point de vue fiabiliste, le système a deux composants : le contrôleur PI et le TOR. Les taux de défaillance ainsi que les taux de réparation sont constants (distribution exponentielle des durées de fonctionnement et de réparation). Les événements correspondants sont produits par le générateur aléatoire. Les paramètres utilisés pour la simulation sont:

- $x_{smax} = 240$ °C ; $x_{smin} = 140$ °C
- $x_{infTOR} = 170$ °C ; $x_{supTOR} = 210$ °C
- $\lambda_{PI} = 13 \cdot 10^{-05}\ h^{-1}$; $\lambda_{TOR} = 8 \cdot 10^{-05}\ h^{-1}$
- $\mu_{PI} = 21 \cdot 10^{-03}\ h^{-1}$; $\mu_{TOR} = 14 \cdot 10^{-03}\ h^{-1}$

Les équations différentielles associées aux différents états discrets sont :

- État 1 :

$$\dot{x} + 0.0015x - 0.0015u_{ref} = 0 \qquad (5)$$

- État 2 :

$$1500\dot{x} + x - u_{map} = 0 \quad (6)$$

- États 3 et 4 :

$$1500\dot{x} + x - u_{mip} = 0 \quad (7)$$

$$1500\dot{x} + x - u_{map} = 0 \quad (8)$$

- État 5 :

$$1500\dot{x} + x - u_{mip} = 0 \quad (9)$$

- État 6 :

$$1500\dot{x} + x - u_{map} = 0 \quad (10)$$

- État 7 :

$$1500\dot{x} + e^{1/1500}x - u_s = 0 \quad (11)$$

- État 8 :

$$\dot{x} + 0.0015x - 0.0015u_{ref} = 0 \quad (12)$$

- État 9 :

$$1500\dot{x} + x - u_{map} = 0 \quad (13)$$

où :

- $u_{\text{ref}} = 190°C$ (température de référence)
- $u_{map} = 300°C$ (température de max puissance)
- $u_{mip} = 25°C$ (température de min puissance)
- $u_s = 25°C$ (température ambiante)

5. RÉSULTATS

5.1. Le modèle et la simulation du système dynamique

La boîte à outils Scicos de Scilab offre une structure modulaire pour construire des systèmes dynamiques hybrides en utilisant un éditeur de blocs-diagrammes.

La figure 4.a présente le modèle Scicos du système dynamique du contrôle de la température du four dont le comportement a été présenté par la figure 3. Le modèle Scicos est constitué des blocs suivants : l'automate hybride, le générateur aléatoire et le descripteur de modes. Ce modèle correspond au modèle de l'automate stochastique hybride de la figure 1. Dans la figure 4.a, le descripteur de modes a 9 blocs : un bloc pour chaque état discret. La figure 4.b présente le détail du descripteur de modes correspondant à l'état discret 3 : La première entrée du bloc « Mux », située à l'extrême droite, correspond aux équations différentielles A_3 définissant le comportement dynamique du système. La deuxième entrée correspond à la fonction de

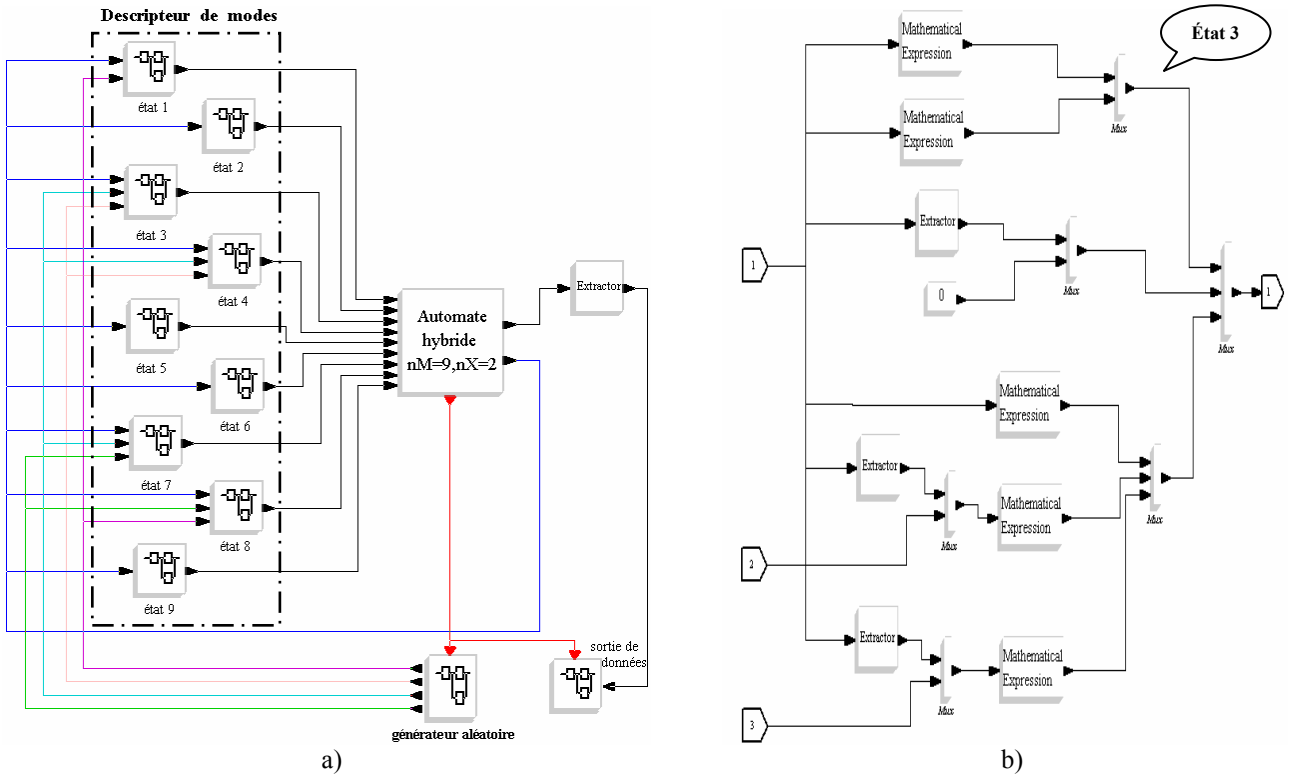

Figure 4. Modèle Scicos du système hybride (cas test)

réinitialisation $R_3 = \{x = x_{crt}\}$ et la troisième aux conditions de garde associées aux transitions de sortie de l'état discret G_3. Les résultats graphiques de la simulation du système sont montrés sur la figure 5. La courbe du haut montre l'évolution de l'état courant du système au cours du temps (selon l'automate de la figure 3) alors que la courbe du bas présente l'évolution de la

température du four. Cette dernière courbe montre la réponse à l'échelon de référence au démarrage, puis la défaillance de la boucle PI (à t_1) identifiée par le passage du seuil de danger (à t_2) et ensuite la régulation TOR (de t_2 à t_3). On peut aussi voir la défaillance du TOR qui tombe en panne (à t_3). La température monte à nouveau vers le seuil de danger (à t_4) détecté par le diagnostic qui bascule le relais. L'automate est alors dans l'état 7, où ni le contrôleur PI, ni le TOR ne contrôlent la température. Le four est débranché, la température chute vers zéro jusqu'à la réparation du contrôleur PI (à t_5) qui reprend le contrôle et ainsi de suite. Bien entendu, il aurait pu arriver que la réparation du TOR arrive avant celle du contrôleur PI.

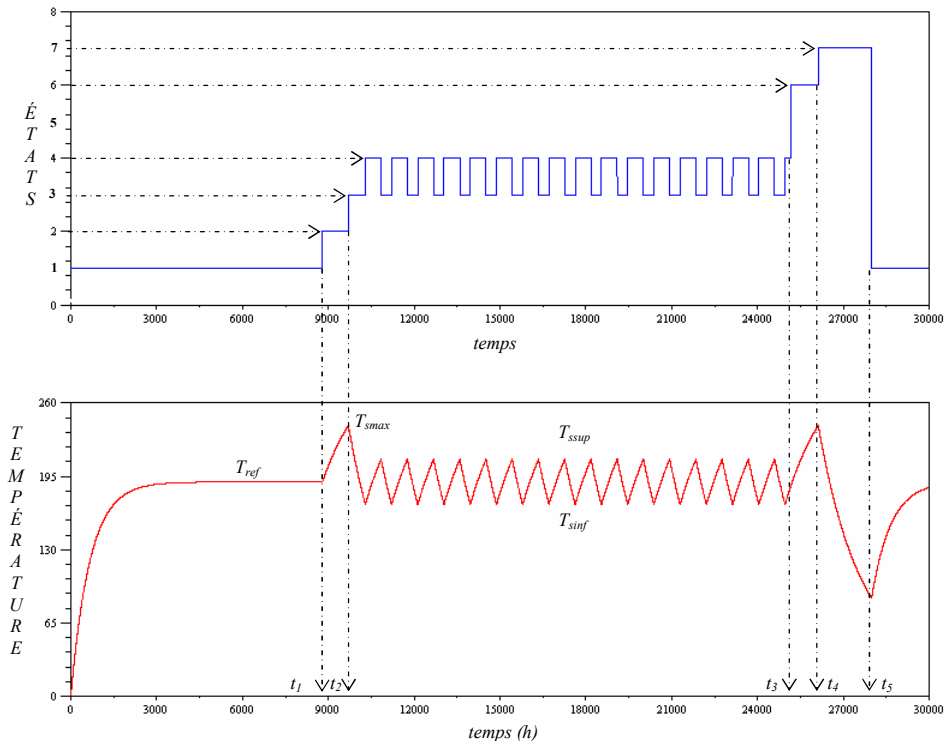

Figure 5. Simulation du système hybride avec l'automate stochastique hybride

5.2. Évaluation des grandeurs de la sûreté de fonctionnement

Pour obtenir les grandeurs de la SdF nous avons utilisé l'ASH implémenté sous Scicos – Scilab et effectué une simulation de Monte Carlo. La simulation est arrêtée quand l'apport d'une *i-ème* histoire simulée sur la valeur du résultat est insignifiant par rapport aux *(i-1)* histoires précédentes. Ce critère d'arrêt est donné par l'équation suivante :

$$\left| \frac{v_{mg(i)} - v_{mg(i-1)}}{v_{mg(i)}} \right| \leq \varepsilon \qquad (14)$$

où $v_{mg(i)}$ et $v_{mg(i-1)}$ représentent la valeur moyenne de la grandeur de SdF mesurée après i histoires et respectivement après $(i-1)$ histoires simulées. ε est la précision de calcul désirée.

5.2.1 La fiabilité du système

Pour l'étude de la fiabilité du système, nous avons effectué une simulation de Monte Carlo en rendant absorbant l'état 7 de l'automate stochastique hybride de la figure 3. La fiabilité du système est la probabilité qu'il soit dans les états 1, 2, 3, 4, 5 et 6. Nous avons donc approché le MTTF (mean time to failure) par *la moyenne du temps d'accès à l'état absorbant (MoyTAEA)* sur l'ensemble des histoires simulées (une histoire est le passage du système par une suite d'états de bon fonctionnement avant d'arriver à l'état de défaillance du système, l'état 7). Nous avons considéré une précision $\varepsilon = 0.001$, équation (14), pour la mesure considérée MoyTAEA qui approche de manière asymptotique le MTTF. On obtient ainsi :

$$MTTF = 1{,}8 \cdot 10^6 \; h$$

Les résultats montrent qu'il n'est pas nécessaire de faire plus de 33 histoires, la durée de simulation étant de l'ordre de trois minutes. La figure 6 présente ces résultats.

5.2.2 La disponibilité du système

Comme nous avons mentionné, la disponibilité du système est la probabilité que le système soit en état d'accomplir une fonction requise dans des conditions

données à un instant donné. Nous avons déterminé l'indisponibilité $\overline{A} = 1 - A$. L'état 7 est l'état d'indisponibilité du système lorsque ni le contrôleur PI, ni le contrôleur TOR ne contrôlent plus la température du four. Pour approcher la disponibilité asymptotique, on considère comme mesure *le temps moyen de séjour dans l'état d'indisponibilité (TmoySEI)* et on lui applique le critère d'arrêt donné par l'équation (14) avec une précision $\varepsilon = 0.001$ (chaque fois que le système passe dans l'état 7, on vérifie si l'équation (14) est satisfaite). Quand ce critère d'arrêt de la simulation est satisfait, on considère que le régime asymptotique est atteint et on détermine l'indisponibilité du système $\overline{A}$ comme le rapport entre le temps de séjour cumulé dans l'état d'indisponibilité (état 7) et le temps de séjour cumulé dans tous les états, y compris l'état d'indisponibilité. Ensuite, on obtient la disponibilité du système :

$$A = 1 - \overline{A} = 99.99\%$$

Les résultats montrent qu'il n'est pas nécessaire de faire plus de 58 histoires, la durée de simulation étant de l'ordre de quatre minutes. La figure 7 présente ces résultats.

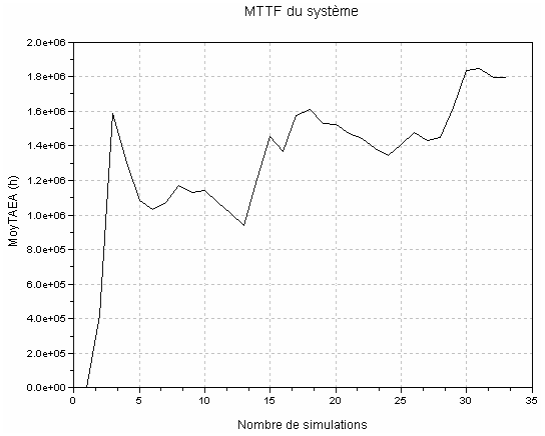

Figure 6. Temps moyen d'accès à l'état de défaillance

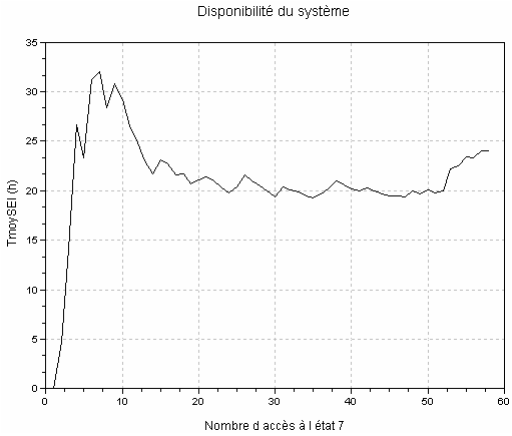

Figure 7. Temps moyen de séjour dans l'état d'indisponibilité

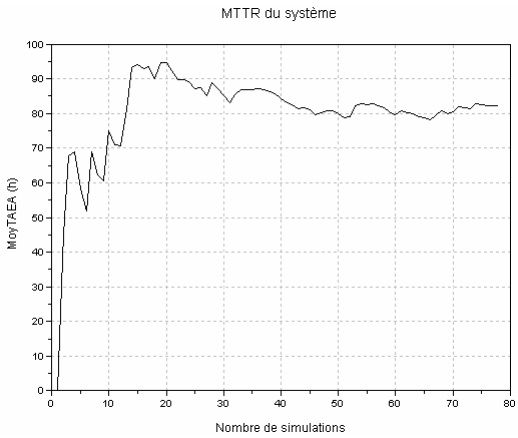

Figure 8. Temps moyen d'accès à l'état de fonctionnement

5.2.3 La maintenabilité du système

La maintenabilité est l'aptitude d'une entité à être rétablie à l'instant t dans un état dans lequel elle peut accomplir une fonction requise, sachant qu'elle est en panne depuis l'instant initial. Nous avons calculé le MTTR (mean time to repair) comme l'espérance mathématique de la durée de réparation. Nous avons donc approché le MTTR par *la moyenne du temps d'accès aux états de fonctionnement (MoyTAEF)* sur l'ensemble des histoires simulées (une histoire est le passage du système de l'état défaillant 7 vers l'état de bon fonctionnement 1). Nous avons considéré une précision $\varepsilon = 0.001$, équation (14), pour la mesure considérée MoyTAEF qui approche de manière asymptotique le MTTR. On obtient ainsi :

$$MTTR = 82\ h$$

Les résultats montrent qu'il suffit de simuler 78 histoires, la durée de simulation étant de l'ordre de trois minutes pour atteindre la précision désirée. La figure 8 présente ces résultats.

6. CONCLUSIONS ET PERSPECTIVES

La modélisation et la simulation d'un système dynamique hybride simple avec l'automate stochastique ont permis d'évaluer les grandeurs de la sûreté de fonctionnement. L'intérêt du formalisme est bien entendu vis-à-vis de l'impossibilité à trouver une solution analytique pour les grandeurs de la SdF. Nous avons pu prendre en compte les interactions entre fonctionnement et dysfonctionnement pour une évaluation fine de ces paramètres de SdF. Nous pouvons remarquer que le modèle Scicos du système est simple et l'approche est systématique et réutilisable. Par ailleurs, nous avons pu visualiser les changements d'état de l'automate au cours de la simulation. Finalement, nous avons pu constater la capacité de l'automate stochastique hybride à piloter la simulation malgré le comportement déterministe et stochastique. Les temps de simulations sont courts, ce qui permet de prendre en compte de nombreux systèmes technologiques. D'autres aspects peuvent être simplement pris en compte comme par exemple des lois de vieillissement avec dépendance éventuelle de l'état discret ou les caractéristiques probabilistes du diagnostic. Un effort doit être fait pour rechercher les modalités d'accélération de la simulation particulièrement pour la fiabilité, notamment en mettant à profit les différentes échelles de temps présentes entre les aspects fonctionnels et dysfonctionnels.

RÉFÉRENCES

Alur, R., C. Courcoubetis, T. A. Henzinger and P. H. Ho, 1993. Hybrid automata: an algorithmic approach to the specification and verification of hybrid systems. In R. L. Grossman, A. Nerode, A. P. Ravn, and H. Rischel, editors, Hybrid Systems I, *Lecture Notes in Computer Science* 736, p. 209 – 229. Spinger-Verlag.

Alur, R., C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P. H. Ho, X. Nicollin, A. Olivero, J. Sifakis and S. Yovine, 1995. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138; p. 3 – 34.

Chabot, J. L., F. Ducamp, J-M. Mattei, Y. Dutuit, T. Hutinet et P. Joulain, 1998. Simulation hybride, méthode de modélisation intégrant phénomènes continus et discrets. *11eme Colloque National de Fiabilité et Maintenabilité-Lambda-mu 11*, Arcachon, France, p. 126 - 136.

Cocozza-Thivent, C. et R. Eymard, 2006. Algorithmes de fiabilité dynamique. *15eme Colloque National de Fiabilité et Maintenabilité-Lambda-mu 15*, Lille, France.

Cocozza-Thivent, C., M. Desgrouas et S. Mercier, 2006. *15eme Colloque National de Fiabilité et Maintenabilité-Lambda-mu 15*, Lille, France.

Cojazzi, G., 1996. The DYLAM approach for the dynamic reliability analysis of systems. *Reliability Engineering and System Safety* 52, p. 279-296.

Dufour, F. and Y. Dutuit, 2002. Dynamic Reliability : A new model. *Lambda-mu 13 – ESREL European Conference*, Lyon, France, p. 350 - 353.

Desgrouas, M. et Mercier, 2005. *6ème Congrès International pluridisciplinaire Qualita et Sûreté de Fonctionnement,* Bordeaux, France.

Henzinger, T. A., 1996. The theory of hybrid automata. *Proceedings of the 11th Annual IEEE Symposium on Logic in Computer Science (LICS)*, pp. 278 – 292.

Kermish, C. et P. E. Labeau, 2000. *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.

Mercier, S., 2006. Encadrement de quantités fiabilistes pour un gros système markovien. *15eme Colloque National de Fiabilité et Maintenabilité-Lambda-mu 15*, Lille, France.

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

Pérez Castaneda, G. A., J-F. Aubry et N. Brinzei, 2007a. Modélisation et simulation d'un système dynamique hybride pour calculer sa fiabilité dynamique en utilisant le toolbox Scicos de Scilab. *7ème édition du Congrès International pluridisciplinaire Qualita 2007* – Tanger (Maroc), p. 311 – 318.

Pérez Castaneda, G. A., J-F. Aubry et N. Brinzei, 2007b. Etat de l'art en fiabilité dynamique. *2èmes Journées Doctorales du GDR MACS JDMACS 2007*, Reims, France.

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

Soro, I. W., M. Nourelfath, D. Aït-Kadi, 2006. Évaluation des indices de performance d'un système multi-états dégradable. *6e Conférence francophone de Modélisation et Simulation MOSIM 06*, du 3 au 5 d'avril, Rabat, Maroc, p.184 – 193.

Villemeur A., 1988. *Sûreté de fonctionnement des systèmes industriels.* Collection de la Direction des Études et Recherches d'Électricité de France. Éditions Eyrolles.