# Evaluation des performances des systèmes intégrant des conflits dans un contexte de fiabilité dynamique. Prise en compte de la défaillance du système de détection de la température d'un four.

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

# Evaluation des performances des systèmes intégrant des conflits dans un contexte de fiabilité dynamique. Prise en compte de la défaillance du système de détection de la température d'un four

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
2 - Instituto Tecnológico de Tehuacán, Libramiento Instituto Tecnológico s/n, 75770
Tehuacán, Puebla, México
{perezc76, jean-francois.aubry, nicolae.brinzei}@ensem.inpl-nancy.fr

**Résumé** : Dans cet article nous présentons l'évaluation des grandeurs de la sûreté de fonctionnement par simulation de Monte Carlo dans un contexte de fiabilité dynamique. Pour cela nous modélisons le système par un Automate Stochastique Hybride que nous définissons formellement. Cet Automate Stochastique Hybride permet de prendre en compte un problème important de la fiabilité dynamique, celui des comportements différents sous l'occurrence d'un événement. Le conflit qui apparaît à un instant donné pendant la simulation représentant le choix d'un de ces comportements parmi les comportements possibles est résolu par un choix probabiliste, une distribution de probabilités étant associée pour chaque conflit. Nous illustrons cette approche sur un cas-test représenté par le système de régulation de la température d'un four.

**Mots clefs** : fiabilité dynamique, automate stochastique hybride, conflit probabiliste, simulation de Monte Carlo, évaluation.

## Introduction

Le concept de fiabilité dynamique a pour objet de prendre en compte les interactions entre le comportement fonctionnel dynamique et déterministe d'un système et le comportement dysfonctionnel stochastique de ses composants. Les études d'évaluation prévisionnelle de la sûreté de fonctionnement des systèmes dans un tel contexte doivent prendre en compte les aspects suivants (Kermish et al., 2000), (Labeau et al., 2000), (Dufour et Dutuit, 2002) :

- 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 ;
- modèle non binaire 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 complexité mathématique de l'évaluation analytique de la sûreté de fonctionnement (Kermish et al. 2000) est telle qu'elle n'est possible que sous certaines hypothèses ou lorsque le système n'est pas trop complexe (Belhadj et al., 1996), (Cocozza-Thivent et al., 2006). Afin de pallier cette complexité mathématique, une voie possible, que nous explorons, est d'avoir recours à la simulation de Monte Carlo.

Dans cet article nous proposons de prendre en compte d'autres aspects de la fiabilité dynamique et notamment la prise en compte des comportements différents sous l'occurrence d'un événement. Ainsi, les interactions entre les variables physiques continues et l'occurrence des événements, l'évolution de la structure fiabiliste dans le temps ne peuvent pas être prise en compte dans les modèles combinatoires classiques tels que les arbres de défaillances. Pour ces raisons nous nous orientons vers des modèles de type états-transitions, tels que les automates. Dans ces modèles certains événements sont non-déterministes, c'est-à-dire que sur leur occurrence le système peut évoluer vers des états différents. C'est le cas par exemple d'un événement qui représente le franchissement d'un seuil par une variable physique. Lorsque cet événement se produit et si le composant qui réalise le diagnostic fonctionne et le détecte, le système passe dans un état de fonctionnement sûr. Par contre si l'événement n'est pas diagnostiqué (le composant est défaillant), le système continue à

évoluer vers un état potentiellement dangereux. C'est un problème typique de la fiabilité dynamique, la structure fiabiliste étant différente dans les deux cas.

La première partie de cet article présente le modèle formel d'un Automate Stochastique Hybride qui permet de prendre en compte tous les aspects de la fiabilité dynamique. La deuxième partie présente un cas-test qui nous sert à illustrer l'utilisation de l'Automate Stochastique Hybride pour la modélisation des systèmes en fiabilité dynamique. Il s'agit d'un système de régulation de la température d'un four. La troisième partie présente la simulation de Monte Carlo du modèle obtenu, ainsi que l'évaluation des grandeurs de la sûreté de fonctionnement. Ensuite nous concluons ce travail et nous présentons des perspectives.

## 1. Automate stochastique hybride

Les automates hybrides ont été définis formellement par (Alur et al., 1992), dans le but de la spécification et de la vérification des systèmes dynamiques hybrides (Alur et al., 1992), des systèmes temps réel (Alur et al., 1995). Ces automates modélisent les systèmes dynamiques hybrides comme un automate à états finis temporisé muni de variables qui évoluent continument avec le temps.

Ayant été intéressés par la prise en compte des défaillances (phénomènes aléatoires) et par l'évaluation quantitative des paramètres de la sûreté de fonctionnement, nous avons introduit et implémenté une extension du modèle d'Allur : l'automate stochastique hybride (Perez Castaneda et al., 2008).

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 caractérisés par des lois de répartition de probabilités. Les dynamiques continues du système sont définies à travers des équations différentielles ordinaires.

Nous l'avons défini comme un 11-tuple :

$$\left(\mathcal{X}, \mathcal{E}, \mathcal{A}, \mathrm{X}, \mathrm{A}, \mathcal{H}, \mathcal{F}, p, x_0, \mathrm{x}_0, p_0\right) \qquad (1)$$

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 $\left(x, \mathrm{e}, \mathrm{G}, \mathrm{R}, x'\right)$ 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 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 de variables réelles ;
- $A : X \times X \to \left(\mathbb{R}^+ \to \mathbb{R}\right)$ est une fonction des « activités », qui associe à un élément de $X \times X$ une fonction définie sur $\mathbb{R}^+$ et à valeur dans $\mathbb{R}$ ;
- $\mathcal{H}$ est un ensemble fini d'horloges ;
- $\mathcal{F} : \mathcal{H} \to \left(\mathbb{R} \to [0,1]\right)$ 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 $x''$ ; la distribution de probabilité p est une distribution de probabilité discrète sur l'ensemble de transitions en conflit sortant de l'état $x$ ;
- $x_0$, $\mathrm{x}_0$ et $p_0$ correspondent respectivement à l'état discret initial, à la valeur initiale de la variable d'état continue 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. En revanche, X et A définissent sa partie continue. Finalement, $\mathcal{H}$ et $p$ expriment son aspect temporisé et stochastique.

La distribution des probabilités $p$ permet de modéliser des comportements différents du système sous l'occurrence d'un même événement, le non-déterminisme étant résolu par un choix probabiliste.

Cet automate stochastique hybride a été implémenté dans Scilab-Scicos. La figure 1 montre le modèle de l'automate stochastique hybride.

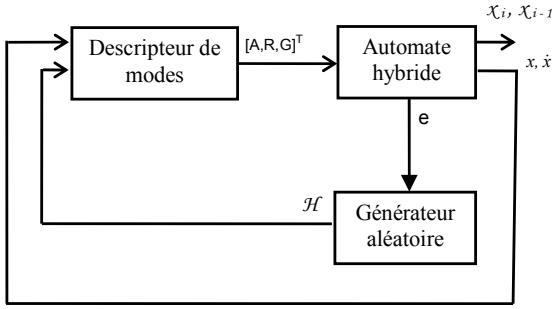


*Figure1 : Modèle de l'automate stochastique hybride*

L'*automate hybride* est un bloc Scicos (Najafi et al., 2007). Il est constitué de *i* ports d'entrée (à gauche du bloc) et de deux ports de sortie (à droite du bloc). La sortie en bas donne la valeur des

variables d'état continue x ainsi que leur dérivée $\dot{x}$. La sortie en haut donne l'état discret courant du système ainsi que l'état discret précédent. L'unique sortie (en bas du bloc) est une sortie d'événements discrets e. Elle génère un événement quand une transition d'état discret se produit.

Le *descripteur de modes* 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 physiques et à leurs dérivées qui viennent de l'automate hybride. La deuxième fournit les valeurs aléatoires du tirage produit par le générateur aléatoire afin de les injectés vers les états discrets concernés. Par ailleurs, le descripteur de modes a *i* ports de sortie dont chaque sortie est définie par le vecteur $[A, R, G]^T$.

Le *générateur aléatoire* correspond à la structure temporisée stochastique $\mathcal{H}$ et $p$ 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 d'événements discrets du bloc automate hybride, génère un événement activant le bloc générateur aléatoire à travers son entrée en haut. Dans ce moment-là, le tirage des valeurs aléatoires se fait.

Afin de montrer les différentes caractéristiques et les avantages qu'offrent l'utilisation et l'application de l'automate stochastique hybride à l'évaluation de la sûreté de fonctionnement dans un contexte de fiabilité dynamique, nous allons présenter un cas test sur lequel nous effectuons une simulation de Monte Carlo.

## 2. Système de régulation de la température d'un four

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

### *2.1. 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.

### *2.2. 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 le contrôleur tombe en panne (avec un taux ($\lambda_{PI}$) 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 ($x_{\inf TOR} \leq x \leq x_{\sup TOR}$). 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 $\mu_{PI}$). Cependant, la possibilité de défaillance du TOR existe, après une durée également aléatoire ($\lambda_{TOR}$). 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 ($\mu_{TOR}$). On a considéré que le four n'est pas défaillant.

Le système de détection du franchissement de seuil par la température du four est à son tour soumis aux défaillances. Lorsque l'événement franchissement de seuil se produit, le système est soumis à une probabilité de non fonctionnement. Afin de pallier cette situation, on ajoute un deuxième capteur (seuil de température plus élevé). Celui-ci à son tour peut ne pas détecter la dérive de la température du four. On supposera que les deux capteurs sont identiques et soumis à la même probabilité de bon fonctionnement p. Lorsque les deux capteurs ont défailli, le système atteint un état de danger.

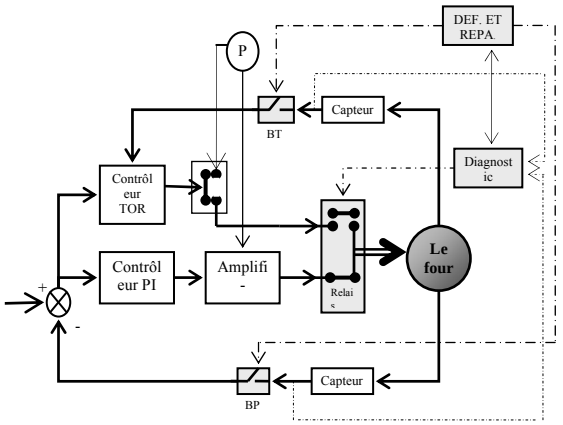


*Figure 2 : Diagramme structurel du système de régulation de la température d'un four*

### *2.3 Automate stochastique hybride du système de régulation de la température*

L'automate stochastique hybride de la figure 3 résume le comportement du système. L'automate a 11 états discrets dont l'état 1 est l'état initial. Dans chaque état il y a une équation différentielle qui représente la dynamique continue du système. Sur chaque transition sont indiqués e, G, et R.

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 défaillant, mais toujours actif. Soit la détection du franchissement de seuil fonctionne et on va alors dans l'état 3, soit celle-ci est défaillante et on se rend dans l'état 9.
- **États 3 et 4** : le contrôleur TOR est actif à la suite de la bonne détection de la défaillance du PI ; le contrôleur PI est en réparation.
- **État 5** : la défaillance du TOR est arrivée, mais il est toujours actif.
- **Etat 6** : la détection de la défaillance du TOR a fonctionné.
- **Etat7** : le PI est réparé et redevient actif ; on est en attente de la réparation du TOR.
- **Etat 8** : défaillance du PI qui vient d'être réparé, mais il est toujours actif.
- **Etat9** : le premier capteur de détection a défailli ; soit le deuxième capteur détecte la panne et on se rend dans l'état 3, soit il est également en défaut et on atteint l'état redouté 11.
- **Etat10** : les deux contrôleurs sont défaillants et on est en attente de la détection de la panne par le deuxième capteur le premier état en défaut à l'arrivée dans cet état).
- **Etat 11** : le système de détection a complètement défailli et on est dans l'état redouté où le four est incontrôlable.

Chaque transition des paires de transitions suivantes : {2→3 et 2→9}, {5→6 et 5→10}, {8→6 et 8→10} se produit sous l'occurrence du même événement et, par conséquent, elles sont en conflit. La résolution de ce conflit est faite par un choix probabiliste avec la probabilité $p$ de bonne détection ou la probabilité $(1-p)$ de défaillance de la détection.

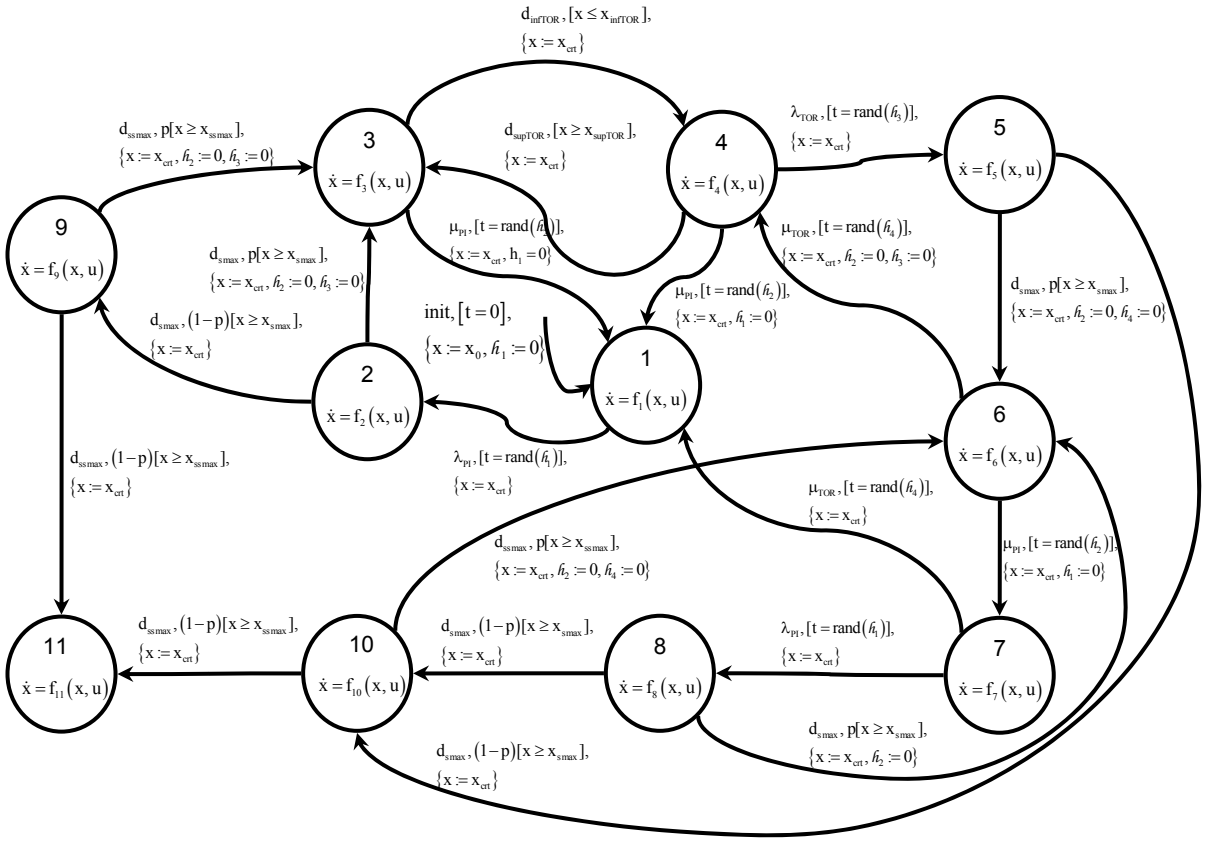


*Figure : 3 Automate stochastique hybride du système de contrôle de la température d'un four*

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

$$\mathcal{X} = \{1,2,3,4,5,6,7,8,9,10,11\} \quad (2)$$

$$\mathcal{E} = \{\lambda_{PI}, \lambda_{TOR}, \mu_{PI}, \mu_{TOR}, d_{s\,max}, d_{ss\,max}, d_{infTOR}, d_{supTOR}\} \quad (3)$$

dont

- $\lambda_{PI}, \lambda_{TOR}, \mu_{PI}$ et $\mu_{TOR}$ sont respectivement les taux de défaillance du PI et du TOR ainsi que leur taux de réparation. Ces taux correspondent aux transitions stochastiques du système. Ces événements correspondants seront produits par le générateur aléatoire dans la simulation.
- $d_{s\,max}$ et $d_{ss\,max}$ sont les seuils de température au-delà desquels on identifie la défaillance des contrôleurs PI et TOR
- $d_{infTOR}$ et $d_{supTOR}$ sont les seuils du TOR et quand ils sont détectés le four s'allume ou s'éteint.
- les conditions de garde des différentes transitions sont :

$$G = \{\ t = rand(h_1);\ t = rand(h_2);\ t = rand(h_3);\ t = rand(h_4);\ x \le x_{s\,max};\ x \ge x_{ss\,max};\ x \le x_{infTOR};\ x \ge x_{supTOR}\ \} \quad (4)$$

- $X = \{x\}$, représente la variable physique du système : la température
- $A = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9, f_{10}, f_{11}\}$ (5)
- $R = \{x = x_{crt}\}$. 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.
- $\mathcal{F}(h_i) = 1 - e^{-\lambda h_i}$. Nous avons utilisé la loi exponentielle pour $i = 1 \ldots 4$.
- lorsque le système de détection de franchissement de seuil est sollicité (dépassement des $d_{s\,max}$ et $d_{ss\,max}$) il peut fonctionner avec une probabilité $p$ ou défaillir avec une probabilité $(1 - p)$.

### *2.4 Paramètres pour la modélisation et la simulation*

Du point de vue fiabiliste, le système a trois composants : le contrôleur PI, le contrôleur TOR et le système de détection du franchissement de seuil par la température. Pour les deux contrôleurs on considère que 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 :

$$\begin{aligned} &x_{smax} = 240\ °C\ ; \quad x_{ssmax} = 300\ °C \\ &x_{infTOR} = 170\ °C\ ; \quad x_{supTOR} = 210\ °C \\ &\lambda_{PI} = 13 \cdot 10^{-05}\ h^{-1};\ \lambda_{TOR} = 8 \cdot 10^{-05}\ h^{-1} \\ &\mu_{PI} = 21 \cdot 10^{-03}\ h^{-1};\ \mu_{TOR} = 14 \cdot 10^{-03}\ h^{-1} \end{aligned} \quad (6)$$

Concernant le système de détection du franchissement de seuil par la température, on considère que chaque fois qu'il est sollicité il répond avec une probabilité $p = 0.8$.

Les équations différentielles associées aux différents états discrets sont :

État 1 :

$$\dot{x} + 0.0015x - 0.0015u_{ref} = 0 \quad (7)$$

État 2 :

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

États 3 et 4 :

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

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

État 5 :

$$1500\dot{x} + x - u_{mip} = 0 \quad (11)$$

État 6 :

$$1500\dot{x} + e^{1/1500}x - u_s = 0 \quad (12)$$

État 7 :

$$\dot{x} + 0.0015x - 0.0015u_{ref} = 0 \quad (13)$$

État 9, 10 et 11 :

$$1500\dot{x} + x - u_{map} = 0 \quad (14)$$

où : $u_{ref} = 190°C$ (température de référence),

$u_{map} = 400°C$ (température de puissance maximale),

$u_{mip} = 25°C$ (température de puissance minimale),

$u_s = 25°C$ (température ambiante).

## 3. Simulation et évaluation de la sûreté de fonctionnement

### *3.1 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 11 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 réinitialisation $R_3 = \{x = x_{crt}\}$ et la troisième aux conditions de garde associées aux transitions de sortie de l'état discret $G_3$.

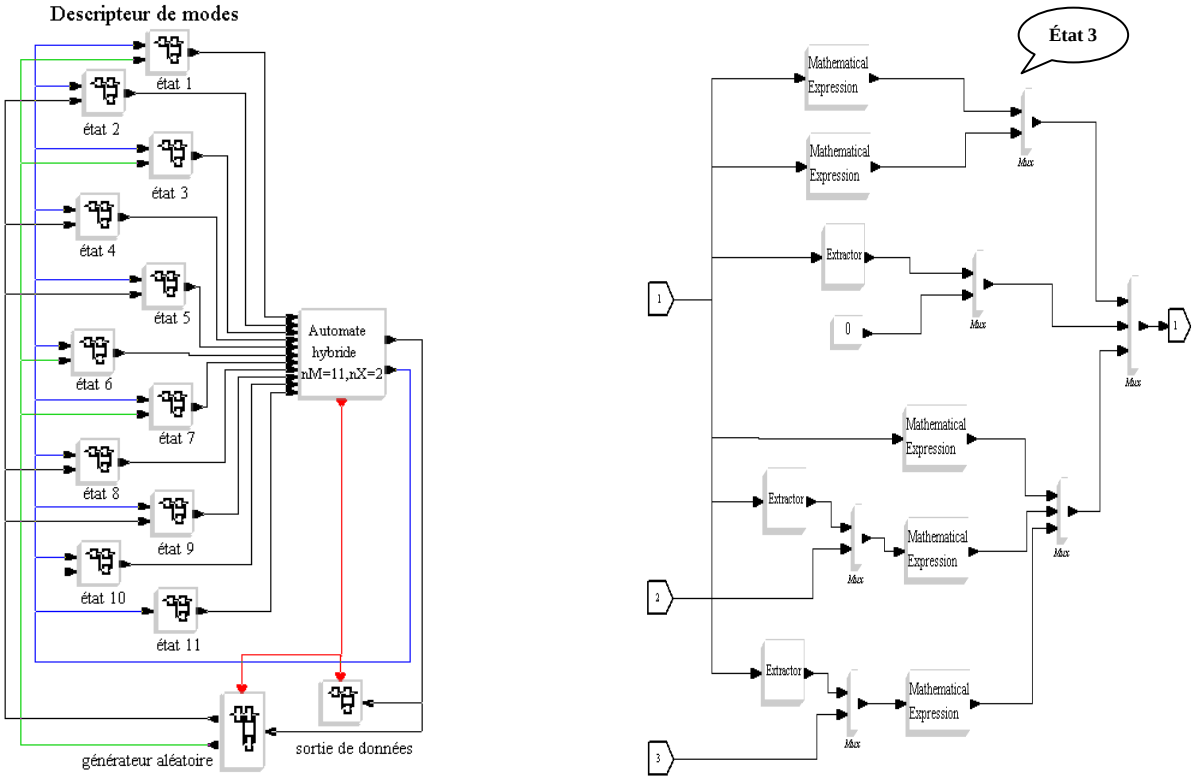


*Figure 4 : Modèle Scicos du système hybride représentant le système de régulation de la température*

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. Après la réparation du régulateur PI et sa remise en fonctionnement, à l'instant $t_3$ celui-ci retombe en panne. A l'instant $t_4$ la température dépasse le premier seuil de danger, mais cet événement n'est pas détecté et le système entre dans l'état numéro 9. Ensuite le système de détection identifie le passage du deuxième seuil de danger par la température et le régulateur TOR prend le contrôle du système. A l'instant $t_5$ le régulateur PI tombe à nouveau en panne, le système entre dans l'état 2. Le dépassement du premier seuil de danger par la température n'est pas identifié et le système entre dans l'état numéro 9. Le système de détection ne fonctionne cette fois ni lors du dépassement du deuxième seuil de température et à l'instant $t_6$ le système entre dans l'état redouté 11 dans lequel la température est hors contrôle. Dans cet état le système reste jusqu'à la fin de la mission, car cet état est un état absorbant (selon l'automate de la figure 3).

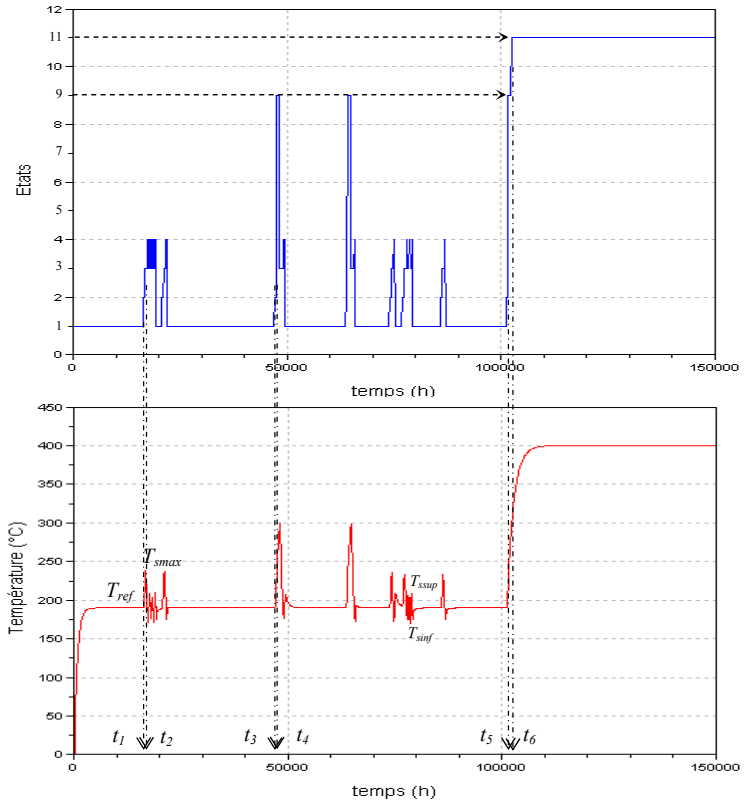


*Figure 5 : Simulation du système hybride avec l'automate stochastique hybride*

### *3.2 Evaluation des grandeurs de la sûreté de fonctionnement*

Pour obtenir les grandeurs de la sûreté de fonctionnement nous avons utilisé l'Automate Stochastique Hybride implémenté sous Scicos-Scilab et effectué une simulation de Monte Carlo.

*3.2.1 Probabilité de l'état redouté*

L'état numéro 11 de l'Automate Stochastique Hybride représente l'état redouté du système, état dans lequel la température du four est hors contrôle. Du point de vue de la sûreté de fonctionnement il est important d'évaluer la probabilité que le système puisse atteindre cet état redouté. Pour estimer cette probabilité nous faisons une simulation de Monte Carlo sur 10000 histoires et pour une durée de fonctionnement de $10^6$ heures et nous avons représenté graphiquement l'évolution de cette probabilité en fonction du temps (figure 6).
Nous avons effectué plusieurs simulations de Monte Carlo avec un nombre d'histoires par simulation de 1000, 5000, 10000 et 12000. Les résultats sont assez proches les uns des autres, ce qui a tendance à montrer qu'il n'est peut être pas nécessaire de faire un nombre très important d'histoires.

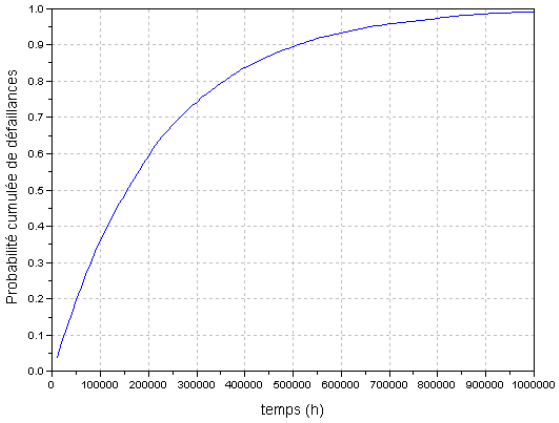


*Figure 6 : Probabilité cumulée de défaillance du système de régulation de la température*

*3.2.2 Durée moyenne de fonctionnement avant défaillance globale du système de régulation*

Une autre grandeur importante de la sûreté de fonctionnement est la durée moyenne de fonctionnement avant défaillance. Puisque nous nous intéressons au système global de régulation de la température du four, ce système est non réparable une fois que le système a atteint l'état numéro 11, et, par conséquent, cette durée représente la durée moyenne de fonctionnement avant la première défaillance (MTTFF – mean time to first failure). Cette grandeur est estimée comme la moyenne du temps d'accès à l'état numéro 11soit en simulant un nombre prédéfini d'histoires soit en arrêtant la

simulation lorsque les deux critères suivants sont vérifiés :

- 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 :

$$\left| \frac{v_{mg(i)} - v_{mg(i-1)}}{v_{mg(i)}} \right| \leq \varepsilon \qquad (15)$$

où $v_{mg(i)}$ et $v_{mg(i-1)}$ représentent la valeur moyenne de la grandeur de sûreté de fonctionnement mesurée (ici le temps moyen d'accès à l'état redouté) après i histoires et respectivement après (i-1) histoires simulées. $\varepsilon$ correspond à la précision de calcul désirée.

- lorsque l'équation (15) est vérifiée un nombre k suffisant de fois par rapport au total des histoires i effectuées. L'équation suivante exprime ce critère. $\theta$ est la probabilité de convergence :

$$\frac{k}{i} \geq \theta \qquad (16)$$

Nous obtenons ainsi :

$$\text{MTTFF} = 212058 \text{ heures} \qquad (17)$$

Sachant que les grandeurs de la sûreté de fonctionnement sont définies soit comme une somme de probabilités d'état sur un sous-ensemble des états discrets $\sum_{x_i \in \mathcal{X}_S \subset \mathcal{X}} P(x_i)$, soit comme une somme de temps de séjour dans un sous-ensemble d'états discrets $\sum_{x_i \in \mathcal{X}_S \subset \mathcal{X}} t(x_i)$, toutes ces grandeurs peuvent être obtenus à partir d'une simulation de Monte Carlo de l'Automate Stochastique Hybride. En effet, celle-ci rend disponible pour chaque état discret différents indicateurs tels que la probabilité d'être dans l'état ou le temps de séjour. Il reste à définir simplement les sous-ensembles d'états discrets qui correspond aux états de disponibilité, d'indisponibilité, de maitenabilité, etc. pour en évaluer ces grandeurs.

## 4. Conclusions

Nous avons pu modéliser grâce à l'automate stochastique hybride un problème important de la fiabilité dynamique : des comportements différents d'un système sous l'occurrence d'un événement. Le conflit généré est résolu par un choix probabiliste, en associant une distribution de probabilités pour toutes les transitions validées par l'événement. Notre approche nous a permis d'évaluer la probabilité d'atteindre un état redouté, ainsi que le MTTFF. D'autres grandeurs de la sûreté de fonctionnement peuvent être également évaluées, car par la simulation de Monte Carlo de l'Automate Stochastique Hybride on est capable d'obtenir les probabilités de tous les états du système, ainsi que les temps de séjour dans ces états.

Nous avons pu montrer la faisabilité de l'approche et nous voudrons prendre en compte dans la suite de notre travail, des systèmes avec des composants dont leur comportement sera non binaire (plus de deux transitions en conflit). Une autre perspective intéressante sera d'attribuer des distributions de probabilité pour les transitions en conflit en fonction du temps et de déterminer une allocation de ces distributions de probabilités afin de minimiser la probabilité d'occurrence des événements dangereux.

## Références


Alur R., Courcoubetis C., Henzinger T.A., Ho P.H., "Hybrid automata: an algorithmic approach to the specification and verification of hybrid systems", *Lecture Notes in Computer Science* 736, pp. 209-229. Spinger-Verlag, 1992.

Alur R., Hill M., Dill D., "Automata theoretic verification of real-time systems", *Formal Methods for Real-Time Computing,* Trends in Software Series, John Wiley & Sons Publishers, pp. 55-82, 1995.

Belhadj M., Aldemir T., "Some computational improvements in process system reliability and safety analysis using dynamic methodologies", *Reliability Engineering System Safet*, 52, pp. 339-347, 1996.

Cocozza-Thivent C., Eymard R., "Algorithmes de fiabilité dynamique", *LambdaMu15*, Lille, 2006.

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

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

Labeau P. E., Smidts C., Swaminathan S., "Dynamic reliability: towards an integrated platform for probabilistic risk assessment", *Reliability Engineering and System Safety*, 68, pp. 219-254, 2000.

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

Perez Castaneda G.A., Aubry J.F., Brinzei N., "Automate Stochastique hybride appliqué à l'évaluation de la fiabilité dynamique", *7e Conférence Internationale de Modélisation et Simulation (MOSIM'08)*, Paris, pp. 386-395, 31 mars, 1er et 2 avril 2008.