

# AIDE A LA CONCEPTION DE SYSTEMES MECATRONIQUES SURS DE FONCTIONNEMENT

## Extraction de scénarios critiques à partir d'un modèle réseau de Petri à l'aide de la logique Linéaire

Sarhane KHALFAOUI<sup>1</sup>

Directeurs de thèse: Hamid DEMMOU\* et Robert VALETTE\*

Responsable industriel: Edwige Guilhem\*\*

Laboratoire d'accueil:

\*Laboratoire d'Analyse et d'Architecture des Systèmes  
LAAS CNRS  
7, avenue du Colonel Roche  
31077 Toulouse Cedex 4

Etablissement d'inscription:

Institut National  
Polytechnique de Toulouse,  
6, allée Emile Monso, BP  
4038, 31029 Toulouse  
Cedex 4

Entreprise d'accueil:

\*\*PSA Peugeot Citroën  
Direction des Systèmes  
d'Information,  
18, rue des Fauvelles 92256  
La Garenne Colombes Cedex

---

### Résumé

*La connaissance des scénarios critiques est indispensable, dès la phase de conception des systèmes mécatroniques, afin d'estimer leur sûreté de fonctionnement. Ceci permet de valider les reconfigurations et d'orienter le choix de l'architecture de ces systèmes. Cet article présente une méthode de recherche de scénarios potentiellement dangereux dans un cadre formel (logique Linéaire) à partir d'un modèle réseau de Petri.*

### Mots clés

*Réseau de Petri, logique Linéaire, mécatronique, sûreté de fonctionnement*

---

## 1 Problématique

La part croissante de l'électronique dans le secteur automobile a considérablement amélioré et diversifié les services rendus par le véhicule. Toutefois, cela a rendu difficile la conception des systèmes mécatroniques sûrs, alliant mécanique, hydraulique et électronique ainsi qu'un calculateur.

Par ailleurs, la phase de conception doit être rapide et peu coûteuse (le moins de prototypes possibles, le plus tard possible) avec un niveau de sûreté garanti. De plus, les ressources en moyens matériels étant limitées (pour des raisons de coûts, de poids, de mise en œuvre...), les concepteurs évitent au maximum les redondances matérielles.

Des études de Sûreté de Fonctionnement réalisées dès la phase de conception permettent une meilleure maîtrise des risques et de la fiabilité des systèmes conçus. En effet, si des points faibles sont mis en évidence lors de l'évaluation du niveau de sûreté (fiabilité, sécurité) des systèmes conçus, cela permet aux concepteurs d'apporter des compléments de spécification des stratégies de pilotage et des modes de reconfiguration avant les essais sur banc.

---

<sup>1</sup> sarhane.khalfaoui@mpsa.com

Actuellement, les études de sûreté prévisionnelle des systèmes automobiles sont réalisées par une succession d'analyses classiques décrites dans [1]. En particulier, l'estimation quantitative de la Sûreté de Fonctionnement de ces systèmes est réalisée à l'aide de méthodes telles que les Arbres de Défaillances ou les Diagrammes de Fiabilité. Or, en ce qui concerne les systèmes mécatroniques, l'utilisation des Arbres de Défaillance pour évaluer la probabilité d'apparition d'un événement redouté n'est pas toujours suffisante. En effet, cette méthode ne permet pas de prendre en compte les phénomènes temporels liés à leurs dynamiques de fonctionnement (possibilité de reconfigurations et de fonctionnements dégradés) et à leur aspect hybride (existence de variables d'états discrètes et continues).

C'est dans ce contexte que des recherches sont menées au sein du groupe PSA Peugeot Citroën sur le thème « Conception sûre de fonctionnement ». L'estimation de la Sûreté de Fonctionnement des systèmes mécatroniques dans la phase de conception nécessite la détermination de tous les types de comportement amenant à des états pour lesquels la sécurité des automobilistes n'est plus assurée. Dans sa thèse (Cifre entre PSA et le LAAS) [2], Gilles Moncelet a mis en évidence d'une part, que l'analyse qualitative visant la mise en évidence des scénarios critiques dans les systèmes mécatroniques est confrontée au problème de l'explosion combinatoire du nombre d'états du graphe d'accessibilité (ensemble de tous les états atteignables du système), et d'autre part que la rareté des scénarios critiques rend inefficaces les méthodes basées seulement sur la simulation.

Afin de contourner le problème de l'explosion combinatoire, nous utilisons directement le modèle réseau de Petri pour établir les scénarios possibles, plutôt que d'utiliser le graphe d'accessibilité associé, qui contient bon nombre d'informations sans intérêt du point de vue sûreté de fonctionnement car décrivant des comportements sans défaillances. La logique Linéaire [3] offre une approche logique permettant d'interpréter les transitions d'un réseau de Petri comme une relation de causalité et de construire les scénarios sous forme d'un graphe d'ordre partiel entre les événements. La nature dynamique et hybride des systèmes mécatroniques est respectée contrairement aux méthodes classiques de Sûreté de Fonctionnement [10].

## 2 Cadre des travaux

La thèse sous convention CIFRE a débuté le 1<sup>er</sup> octobre 2000. Le laboratoire d'accueil est le Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS) de Toulouse. Les responsables scientifiques sont Hamid DEMMOU et Robert VALETTE. La responsable industrielle (PSA) est Edwige GUILHEM.

Mon travail de thèse se déroule suivant trois étapes :

- Etablir une méthode de modélisation spécifique aux systèmes mécatroniques basée sur les réseaux de Petri (RdP) et respectant leur caractère hybride.
- Elaborer une méthode d'analyse qualitative consistant à :
  - Déterminer les scénarios conduisant à l'événement redouté par une analyse des causalités (à l'aide de la logique Linéaire) à partir du modèle RdP du système mécatronique étudié.
  - Spécifier un outil informatique permettant d'implémenter cette méthode dans un outil de modélisation RdP en vue d'obtenir un démonstrateur supportant différents cas d'études du monde automobile.

Le but ultime est de permettre une analyse quantitative efficace pour déterminer la probabilité d'occurrence des événements redoutés en utilisant éventuellement la simulation de Monte Carlo et en s'appuyant sur la connaissance des scénarios critiques.

## 3 Travaux réalisés

### 3.1. Définition d'une méthode de modélisation des systèmes mécatroniques

Les systèmes mécatroniques font partie de la famille des systèmes dynamiques hybrides [4]. En effet, la dynamique continue est associée à la partie énergétique et la dynamique discrète est liée à la commande numérique et à l'existence d'événements discrets tels que les défaillances, les dépassements de seuils ou les reconfigurations.

De ce fait, nous avons choisi une modélisation associant réseau de Petri et équations différentielles [4]. Ce modèle représente le fonctionnement nominal et le comportement en présence de défaillances de chaque composant du système mécatronique ainsi que les interactions entre ces composants. Le réseau de Petri décrit les changements de configuration, tandis que les équations différentielles décrivent la dynamique continue. Cette modélisation hybride présente l'avantage de séparer clairement les aspects discrets et continus.

Au cours de la première année de thèse nous avons montré que cette méthode était effectivement applicable aux systèmes que nous étudions. Cela a donné lieu à la publication [6].

### 3.2. Développement d'une méthode d'extraction des scénarios critiques

Une fois la méthode de modélisation choisie, nous avons commencé la seconde phase du travail consistant à élaborer une méthode d'extraction des scénarios critiques. Son but est de mettre en évidence les suites de changements d'états des composants et d'interactions entre ces composants qui conduisent aux états redoutés et d'analyser plus précisément ce qui fait que le système quitte le fonctionnement normal pour aller vers l'état redouté. Notre méthode est basée sur une analyse qualitative à partir d'un modèle réseau de Petri. Il s'agit donc d'extraire et de rendre explicite les scénarios redoutés à partir d'une analyse d'un modèle agrégeant un ensemble de connaissances sur le fonctionnement du système.

Nous ne voulons pas travailler directement sur le graphe d'accessibilité des états globaux de tout le système (explosion combinatoire). Nous ne considérons donc que des états partiels (des ensembles de jetons) et nous interprétons les transitions comme des relations de causalité.

#### 3.2.1. Cadre formel

Une façon de traiter l'accessibilité dans les réseaux de Petri est de résoudre l'équation caractéristique  $M' = M + C \cdot \bar{s}$ . Cette équation ne fournit qu'une condition nécessaire (mais non suffisante) d'accessibilité du marquage  $M'$  à partir de  $M$  et ne donne aucun ordre de franchissement des transitions du vecteur caractéristique  $\bar{s}$ .

Basée sur le calcul des séquents<sup>2</sup>, la logique Linéaire [3] permet d'obtenir une condition nécessaire et suffisante d'accessibilité entre deux marquages partiels grâce à l'équivalence entre prouvabilité de séquent et accessibilité dans le réseau de Petri correspondant [6].

La traduction d'un réseau de Petri en logique Linéaire a été présenté dans [7]. Une formule logique est associée à chaque marquage et à chaque transition. Il est nécessaire que la partie gauche du séquent initial contienne la liste de toutes les transitions permettant d'atteindre un marquage  $M'$  à partir d'un marquage donné  $M$ .

Notre approche se base sur cette traduction d'un réseau de Petri en logique Linéaire. Mais notre problème se pose différemment. En effet, ce qui nous intéresse c'est de trouver une suite d'actions (tirs de transitions) avec le contexte nécessaire correspondant (les jetons nécessaires) qui

---

<sup>2</sup> Un séquent est une expression de la forme :  $\Gamma, X \mid - Y, \Delta$  qui se lie : «  $\Gamma et X$  » permet de déduire «  $Y ou \Delta$  ».  $\Gamma, X, Y et \Delta$  sont des formules logiques.

aboutit à l'apparition d'un jeton dans la place représentant l'état partiel jugé dangereux. On ne connaît donc pas le marquage initial, et du marquage final on ne connaît que le fragment correspondant à l'état partiel dangereux. On ne sait pas quelles sont les transitions qui doivent être franchies. Le problème qui se pose n'est donc pas simplement de prouver un séquent, il est surtout de trouver les séquents intéressants.

La première chose est de pouvoir écrire la liste des transitions à considérer sans savoir a priori combien de fois elles seront franchies. La logique linéaire dispose d'un connecteur pour exprimer cela, c'est le connecteur exponentiel "!". Ecrire  $!t$  dans un séquent, cela veut dire que l'on peut franchir la transition  $t$  zéro fois, une fois ou  $k$  fois au gré des besoins lors de la construction de l'arbre de preuve.

Si  $M_d$  représente l'état partiel dangereux, alors lors de la recherche des causalité vers l'arrière (que l'on appelle raisonement arrière), le séquent sera  $M, !t_1, \dots, !t_n \multimap M_d, \Gamma$  où  $\Gamma$  correspond à un contexte qui accompagnera nécessairement  $M_d$  pour le scénario produisant  $M_d$  (c'est-à-dire que  $\Gamma$  et  $M_d$  seront produits simultanément).

Pour un raisonement avant, on aura de même  $M_n, \Gamma, !t_1, \dots, !t_n \multimap M'$  lorsque l'on recherchera tout ce qui peut être une conséquence logique d'un état partiel normal  $M_n$ .

### 3.2.2. Principe de la méthode

Le principe de cette méthode, qui a donné lieu aux communications [9] et [11], consiste à remonter la chaîne de causalité dans le modèle réseau de Petri du système étudié, par un raisonement arrière partant de l'état redouté. Ce raisonement est poursuivi jusqu'à ce que l'on arrive à un état de fonctionnement normal. Ensuite un raisonement avant est mené afin de voir toutes les évolutions possibles à partir de l'état partiel normal obtenu. On doit trouver un ou plusieurs fonctionnements normaux et retrouver le comportement menant à l'état redouté. En plus de la mise en évidence de la bifurcation entre le comportement normal et le comportement redouté (qui doit apparaître sous la forme d'un conflit entre deux transitions), on doit également avoir enrichi le contexte (rajouter des jetons dans des places) ce qui permet d'appréhender dans quelles conditions exactes le comportement redouté a lieu.

Cet enrichissement du contexte se fait progressivement en étudiant les comportements partageant un lien de causalité avec le comportement redouté. Partant d'une connaissance très partielle des conditions d'occurrence de ce comportement (par exemple le déclenchement d'une alarme suite au franchissement d'un seuil de sécurité), on s'intéresse aux comportements qui sont en conflit avec ce dernier (transitions en conflit) et qui permettent d'éviter d'aboutir à l'état partiel redouté. L'étude des conditions de tirs de ces transitions en conflit nous informe de manière plus complète sur les conditions d'occurrence du comportement redouté. Pour garantir la non occurrence de ce comportement, certaines conditions sont nécessaires, par exemple la disponibilité d'une ressource de reconfiguration ou la présence du système dans un état de fonctionnement bien déterminé. La non satisfaction de ces conditions nous conduit inévitablement vers l'état redouté. De façon récursive, l'étude des comportements qui sont en conflit avec ceux en conflit avec le comportement critique (et qui favorisent par conséquent l'occurrence du comportement redouté) nous informe plus précisément sur le contexte dans lequel a eu lieu l'événement redouté.

Nous avons élaboré une méthode générale (une première ébauche est donnée dans la communication [8]) basée sur 4 étapes qui a pour but de déterminer les conditions de marquages d'un ensemble de places donné (qu'on appelle état cible). Cela consiste à déterminer de manière systématique et formelle comment marquer et démarquer cet ensemble de places.

Cette méthode est composée de 4 étapes :

1. Détermination des états normaux
2. Détermination des états cibles (états partiels redoutés ou états à étudier)
3. Raisonnement arrière à partir de l'état cible (peut être un état redouté ou n'importe quel autre état partiel du modèle RdP)
4. Raisonnement avant à partir des états conditionneurs (mettre en évidence les conflits : bifurcation entre fonctionnement normal et scénarios redoutés).

La première étape consiste à déterminer les places dont le marquage représente un état de fonctionnement normal. Ces places nominales seront utilisées comme critère d'arrêt du raisonnement arrière. Cette étape peut être réalisée de deux manières : soit en utilisant une connaissance a priori des états de bon fonctionnement du système, soit en effectuant une simulation de Monte Carlo du modèle sur une courte fenêtre temporelle pour déterminer la probabilité de marquage des places du réseau. Celles qui auront une probabilité de marquage non négligeable seront assimilées à des places normales.

La deuxième étape détermine l'état cible à étudier. Cet état cible peut être soit un état partiel redouté soit un autre état partiel ayant un lien de causalité direct ou indirect avec cet état redouté (par exemple une place qui représente la disponibilité d'une ressource pour assurer un fonctionnement dégradé évitant l'occurrence de l'événement redouté).

La troisième étape génère l'ensemble des chemins qui mènent vers l'état partiel redouté. On effectue un raisonnement arrière sur le modèle RdP. On prend comme marquage initial le seul état redouté et l'on cherche de façon exhaustive tous les scénarios minimaux [9] (aucun franchissement de transition non nécessaire n'est effectué) permettant de consommer le marquage initial et aboutissant à un marquage final uniquement formé de places associées au fonctionnement normal. Au cours de cette étape, on est en général amené à enrichir le marquage initial (ajouter des jetons dans certaines places). Cela se fera chaque fois que pour consommer un jeton dans une place non associée à un fonctionnement normal il faut franchir une transition non sensibilisée par un marquage accessible à partir du marquage initial non enrichi. Les jetons ajoutés lors du processus d'enrichissement du marquage correspondent à des états partiels qui sont des conséquences logiques des scénarios redoutés et qui seront donc nécessairement observés lors de l'évolution du système vers l'état redouté. En inversant les scénarios obtenus lors de cette étape, nous aurons les suites d'actions possibles menant d'un état normal à l'état redouté. Cet état normal est nommé état conditionneur.

La dernière étape de la méthode consiste à construire un raisonnement avant en partant de chaque état conditionneur déterminé à l'étape précédente. Cela a pour objectif de localiser les bifurcations entre le comportement redouté et le fonctionnement normal du système ainsi que les conditions (de marquage de certaines places du réseau) impliquées dans ces bifurcations.

### **3.3. Cas d'étude**

Deux systèmes, dont les principes peuvent être identifiés à des systèmes automobiles existants, ont été étudiés. Il s'agit du conjoncteur-disjoncteur électromécanique et un système de régulation du volume de deux réservoirs. Ces exemples ont été traités dans trois articles acceptés et présentés dans des congrès nationaux et internationaux. Le conjoncteur-disjoncteur a été le support de deux publications : la première a eu lieu en mai 2001 dans [8] et la deuxième à l'occasion du [9] en octobre 2001. Quant au système de régulation de deux réservoirs, il a été choisi pour illustrer l'apport de notre méthode de recherche de scénarios critiques par rapport aux Arbres de Défaillances, et a été présenté au mois de mars à l'occasion du Colloque Européen de Sécurité de Fonctionnement [10].

## 4 Perspectives

La suite de notre travail va consister à formaliser la méthode de recherche de scénarios critiques sous la forme d'un algorithme en vue de son automatiser de façon à prendre en compte des systèmes de plus en plus complexes. Cela nous permettra de spécifier l'outil démonstrateur.

A plus long terme, nous envisageons de traiter un exemple industriel pour préparer le transfert de la méthode au sein de PSA Peugeot Citroën.

### Références

- [1] V. Hénault, « Méthodologie de développement des systèmes électroniques embarqués automobiles, matériels et logiciels, sûrs de fonctionnement », thèse présentée à l'IRESTE, septembre 1996.
- [2] G. Moncelet, « Application des réseaux de Petri à l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile », Thèse de Doctorat, N°3076, Université Paul Sabatier, Toulouse.
- [3] J.Y. Girard, « Linear Logic », *Theoretical Computer Science*, 50, 1987, p.1-102.
- [4] Systèmes dynamiques hybrides, ouvrage collectif sous la direction de J. Zaytoon, édition Hermes, ISBN 2-7462-0247-6.
- [5] R. Champagnat, P. Esteban, P. Pingaud, R. Valette, « Modeling and simulation of a hybrid system through Pr/Tr PN DAE model », ADPM'98 3<sup>rd</sup> International Conference on Automation of Mixed Processes, 19-20 March 1998, Reims, France p. 131-137.
- [6] F. Girault, « Formalisation en logique Linéaire du fonctionnement des réseaux de Petri », Thèse de Doctorat, N°2870, Université Paul Sabatier, Toulouse.
- [7] B. Pradin-Chézalviel, R. Valette, L.A. Künzle, « Scenario duration characterization of t-timed Petri nets using linear logic », *IEEE PNPM'99, 8th International Workshop on Petri Nets and Performance Models*, Zaragoza, Spain, September 6-10, 1999, p.208-217.
- [8] S. Khalfaoui, E. Guilhem, H. Demmou, R. Valette, « Modeling critical mechatronic systems with Petri Nets and feared scenarios derivation », *ECM2S5 5<sup>th</sup> Workshop on Electronics, Control, Modeling, Measurement and Signals*, 30-31 May, 1<sup>er</sup> Juin, 2001, Toulouse, France p. 55-59.
- [9] S. Khalfaoui, E. Guilhem, H. Demmou, N. Riviere, « Extraction de scénarios critiques à partir d'un modèle RdP à l'aide de la logique Linéaire », *MSR'2001 Modélisation des systèmes réactifs*, 17-19 Octobre 2001, Toulouse, France p. 409-424.
- [10] S. Khalfaoui, E. Guilhem, H. Demmou, R. Valette, « Une méthode pour obtenir des scénarios critiques dans les systèmes mécatroniques », *Colloque Européen de Sûreté de Fonctionnement (Im13)*, Palais des Congrès - Lyon - France - 18 au 21 Mars 2002.
- [11] H. Demmou, S. Khalfaoui, N. Riviere, R. Valette, E. Guilhem, « A method for deriving critical scenarios from mechatronic systems », *Journal Européen des Systèmes Automatisés (soumis)*.