

EXTRACTION DES SCENARIOS CRITIQUES POUR L'EVALUATION DE LA SURETE DE FONCTIONNEMENT DES SYSTEMES MECATRONIQUES

Approche hybride basée sur un modèle réseau de Petri et la logique linéaire

Malika MEDJOUJ¹

Directeur(s) de thèse: Hamid DEMMOU* et Robert VALETTE*

Laboratoire d'accueil:

*Laboratoire d'Analyse et
d'architecture des Systèmes
LAAS-CNRS
7, avenue du Colonel Roche
31077 Toulouse Cedex4

Etablissement d'inscription:

Université Paul Sabatier
UPS
118 route de Narbonne
31062 Toulouse cedex 4

Résumé

Afin de concevoir les systèmes mécatroniques et de valider leurs reconfigurations et leurs modes dégradés, il est nécessaire d'estimer leur sûreté de fonctionnement en connaissant les scénarios critiques dès la phase de conception. L'objectif à long-terme est d'évaluer la fiabilité (sûreté) dynamique de ces systèmes. On propose une nouvelle version d'un algorithme qui permet la construction des scénarios critiques à partir d'un modèle Réseau de Petri. Elle est plus précise car elle tient compte partiellement de l'aspect continu du système hybride étudié. Ces scénarios caractérisent comment le système quitte le fonctionnement normal pour évoluer vers l'état redouté en déterminant la suite d'actions et les changements d'états conduisant à l'état critique.

Mots clés

Sûreté de fonctionnement, systèmes mécatroniques, fiabilité dynamique, réseau de Petri, logique linéaire.

1 INTRODUCTION

L'intégration progressive de l'électronique dans le secteur automobile a amélioré le confort et les services rendus par le véhicule. Toutefois, cela a complexifié la conception des systèmes mécatroniques combinant des technologies mécaniques, hydrauliques, électroniques et informatiques, ce qui rend difficile la maîtrise de leur fiabilité.

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 sécurité garantie. De plus, les ressources en moyens matériels étant limitées, pour des raisons de coûts et 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, les points faibles mis en évidence lors de l'évaluation du niveau de sûreté des systèmes conçus permettent aux

¹mmedjoud@laas.fr

concepteurs de spécifier des stratégies de pilotage et des modes de reconfiguration avant les premiers essais sur un prototype réel.

Les systèmes mécatroniques sont hybrides : 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 (défaillances, dépassements de seuils). L'étude de la sûreté de fonctionnement de tels systèmes doit nécessairement tenir compte des interactions existantes entre leurs paramètres physiques (température, pression, vitesse...) et le dysfonctionnement de leurs composants. Les méthodes classiques de la sûreté de fonctionnement, comme les arbres de défaillances [1] sont insuffisantes pour de tels systèmes complexes et hybrides car ils sont dynamiques. La sûreté de ces systèmes doit tenir compte du temps et de l'ordre d'apparition des événements[2].

La rareté de ces scénarios redoutés rend inefficaces les méthodes basées seulement sur la simulation[3]. En plus de ce point, dans sa thèse (Cifre entre PSA et le LAAS) [4], Gilles Moncelet a démontré que l'analyse qualitative visant la mise en évidence des scénarios critiques dans les systèmes mécatronique est confrontée au problème de l'explosion combinatoire du nombre d'états de graphe d'accessibilité. Afin de contourner ce problème, dans la suite des travaux avec PSA et le LAAS [5], Sarhane Khalfaoui a utilisé directement le modèle Réseau de Petri (RdP) pour extraire les scénarios redoutés sans générer le graphe d'accessibilité associé et la logique linéaire pour représenter les modèles RdP et en extraire des scénarios. L'avantage est que la logique linéaire permet de construire un ordre partiel de franchissement des transitions et focalise la recherche sur les parties intéressantes du modèle pour l'analyse de la sûreté de fonctionnement [6]. Cette approche est basée sur l'équivalence entre l'accessibilité dans les RdP et la prouvabilité du séquent associé en logique linéaire[7]. La nature hybride et dynamique des systèmes mécatroniques est respectée par le choix d'une modélisation associant RdP et équations différentielles[8]. Le modèle RdP décrit le fonctionnement nominal, les défaillances et les mécanismes de reconfiguration. Les équations différentielles représentent l'évolution des variables continues de la partie énergétique du système.

L'avantage de son approche est de séparer clairement l'aspect continu de l'aspect discret. Cela permet une analyse logique (en utilisant la logique linéaire) des causalités associées aux changements d'état concernant l'aspect discret. Partant de l'état redouté, il est possible de revenir en arrière à travers la chaîne des relations de cause à effet et d'extraire tous les scénarios possibles menant vers l'état dangereux (critique). Chaque scénario est donné sous la forme d'un ordre partiel entre les événements nécessaires à l'apparition de l'évènement redouté ce qui diffère d'un arbre de défaillance qui donne un ensemble de combinaisons statiques des états partiels nécessaires pour l'obtention de l'état redouté [9]. Cette approche a conduit au développement d'un algorithme pour générer automatiquement des scénarios critiques à partir d'un modèle RdP [10]. Comme cet algorithme opère uniquement sur l'aspect discret du modèle, de nombreux scénarios incohérents avec la dynamique continue sont générés.

Afin d'éliminer ces scénarios incohérents vis-à-vis de la dynamique continue du système, nous proposons une approche pour une analyse qualitative de la sûreté de fonctionnement des systèmes mécatroniques d'un point de vue fiabilité dynamique[11]. Cette approche a conduit à l'élaboration d'une nouvelle version de l'algorithme qui tient partiellement compte de l'aspect continu et plus particulièrement des seuils associés à certaines transitions dans le modèle RdP. Cela permet de déterminer plus précisément les conditions exactes de l'occurrence de l'évènement redouté ; ce qui pousse le système à quitter son fonctionnement normal et à évoluer vers l'état redouté.

La méthode et l'algorithme sont illustrés sur un cas d'étude: système de régulation de deux réservoirs. Nous avons montré comment un grand nombre de scénarios cohérents vis-à-vis de la partie discrète du modèle hybride mais incohérents vis-à-vis de sa partie continue ne sont plus générés.

2 METHODE DE RECHERCHE DES SCENARIOS CRITIQUES

On appelle scénario un ensemble d'événements (ici franchissements de transition) menant d'un état partiel (ici marquage partiel) à un autre et vérifiant un ordre partiel. Comme on l'a cité dans l'introduction, on suppose que le système est constitué d'un ensemble de composants. Un état partiel est l'ensemble des états d'un sous-ensemble de ces composants.

Définition: un ordre partiel peut être défini par un graphe de précédence (graphe orienté) (E, A) ou E est un ensemble de franchissements de transitions (ti) et A un ensemble de paires (ti, tj) telles que ti précède tj (ti et tj étant des franchissements de transitions).

Le principe de la méthode est d'enrichir progressivement le contexte dans lequel s'est produit l'évènement conduisant à l'état redouté en étudiant les conflits de comportements ayant un lien de causalité avec l'occurrence de l'évènement redouté. Partant d'une connaissance partielle des conditions d'occurrence de cet évènement, on s'intéresse aux comportements qui permettent d'éviter le chemin critique et qui correspondent à des bifurcations représentées par des conflits de transitions. L'étude des conditions de tir de ces transitions de bifurcation nous informe de manière plus complète sur les conditions d'occurrence de l'évènement redouté.

Cette méthode est composée de 2 étapes : un raisonnement arrière et un raisonnement avant. Le raisonnement arrière prend comme marquage initial dans le réseau de Petri inversé le seul état cible et cherche de façon exhaustive tous les scénarios permettant de consommer le marquage initial et aboutissant à un marquage final formé uniquement de places associées au fonctionnement normal. Le raisonnement avant prend comme état initial ces places de fonctionnement normal dans le réseau de Petri initial. Son objectif est de localiser les bifurcations entre le comportement redouté et le fonctionnement normal du système ainsi que les conditions impliquées dans ces bifurcations.

Avant de présenter l'algorithme permettant de générer les scénarios redoutés, on introduit le cas d'étude sur lequel on illustre les différentes étapes de l'algorithme.

3 CAS D'ETUDE

3.1. PRESENTATION

L'exemple, dont le principe peut être identifier à un système automobile existant, est basé sur un système de régulation du volume de deux réservoirs. Il est constitué d'un calculateur, de deux pompes, de trois électrovannes (tout ou rien), de deux capteurs de volume et des deux réservoirs régulés (Réservoir 1, Réservoir 2) et d'un troisième réservoir de vidange. Les deux réservoirs régulés alimentent des utilisateurs selon un besoin prédéfini (fonction du temps).

Le volume dans chaque réservoir (1 ou 2) doit rester dans un intervalle donné $[V_{\min}, V_{\max}]$ ($i = 1$ ou 2). Le contrôle s'opère à l'aide du calculateur qui décide, selon la valeur du volume (délivrée par le capteur), d'approvisionner (ou non) le réservoir en question en alimentant (ou non) l'électrovanne concernée.

Pour chaque réservoir, on distingue donc deux phases de fonctionnement selon que l'électrovanne alimentant ce réservoir est ouverte ou fermée :

Une phase de conjonction lorsque l'électrovanne est ouverte. Le volume dans le réservoir est croissant durant cette phase, et cela quelle que soit la valeur du débit de sortie vers l'utilisateur (le débit d'alimentation de l'électrovanne est bien supérieur, par hypothèse, au débit de sortie).

Une phase de disjonction lorsque l'électrovanne est fermée. Le volume dans le réservoir est par conséquent décroissant.

La loi de contrôle du calculateur pour chaque réservoir est telle que lorsque le volume dépasse la limite supérieure de commande V_{\max} pendant la phase de conjonction, alors le calculateur

commande la fermeture de l'électrovanne. Lorsque le volume devient inférieur à V_{imin} (limite inférieure de commande) durant la phase de disjonction alors le calculateur commande à l'électrovanne de s'ouvrir et on change par conséquent de phase de fonctionnement.

Ce système doit assurer l'approvisionnement des utilisateurs tout en évitant le débordement de l'un des réservoirs. Une troisième électrovanne de secours est prévue pour cet effet. Elle est partagée entre les deux réservoirs et assure leur vidange quand ils débordent. Elle ne peut être utilisée que par un seul réservoir à la fois. Quand le volume dans l'un des réservoirs dépasse la limite supérieure de sécurité (V_{iL}), alors le calculateur commande l'ouverture de cette électrovanne du côté du réservoir qui risque de déborder, et ce jusqu'à ce que le volume devienne inférieur à V_{imin} .

Pour simplifier nous supposons que seules les électrovannes peuvent subir des défaillances. Les électrovannes 1 et 2 (prévues pour l'alimentation des réservoirs) peuvent être bloquées en ouverture. En cas de défaillance de l'électrovanne 3 (de secours), celle ci est mise hors service (on ne peut pas l'ouvrir pour faire la vidange).

Maintenant, supposant que l'une des électrovannes (ex EV1) est bloquée en ouverture c'est-à-dire qu'on ne peut pas la fermer, alors le volume dans le réservoir 1 continue de croître jusqu'à atteindre V_{iL} . Dans ce cas on doit ouvrir l'électrovanne EV3 de secours pour vidanger le réservoir 1. Si l'électrovanne EV3 est aussi hors service (on ne peut pas l'ouvrir) ou si elle est occupée par la vidange du réservoir 2 (EV1 bloquée et EV3 hors service ou occupée), alors le volume dans le réservoir 1 dépassera V_{iL} pour atteindre V_{iS} qui est l'événement redouté qu'on considère (débordement de réservoir 1).

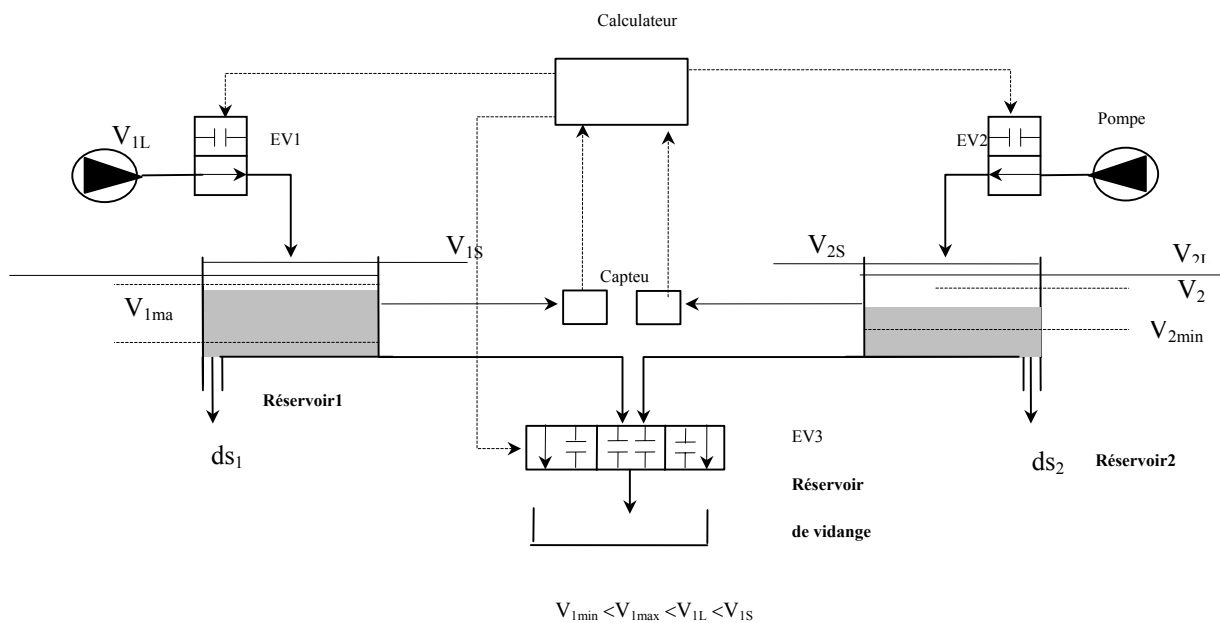


Figure 1: Cas d'étude

3.2. MODELE DU SYSTEME SOUS LA FORME D'UN RESEAU DE PETRI

Dans le réseau de Petri de la figure 2 : La place $V1_dec$ représente la phase de disjonction (le volume décroît); la place $V1_cr$ représente la phase de conjonction pendant laquelle le volume

croît. La place EV1_OK modélise le bon fonctionnement de l'électrovanne 1. La transition t11 représente la commande de fermeture de l'électrovanne 1 quand le volume dépasse V1max. La transition t12 représente la commande d'ouverture de la même électrovanne quand le volume devient inférieur à V1min. La transition def1 représente le fait que l'électrovanne puisse rester bloquée en ouverture, et que la transition rep1 peut être réparée. Le réservoir 2 est modélisé de la même façon. Quand le volume dans le réservoir 1 dépasse la limite supérieure de sécurité (V1L), et si l'électrovanne de secours est disponible (la place EV3_OK est marquée) alors t14 devient franchissable et on commence la procédure de vidange du réservoir 1 via l'électrovanne 3 en marquant la place EV3_oc1. Cette phase dure le temps que met le volume pour atteindre le seuil bas V1min. Ensuite on libère l'électrovanne 3 (on marque de nouveau EV3_OK) et on recommence une phase de conjonction (on remet un jeton dans la place V1_cr) en tirant la transition t15. L'électrovanne 3 peut subir une défaillance (tir de la transition def3). Dans ce cas, la place EV3_HS est marquée et l'électrovanne est mise hors service.

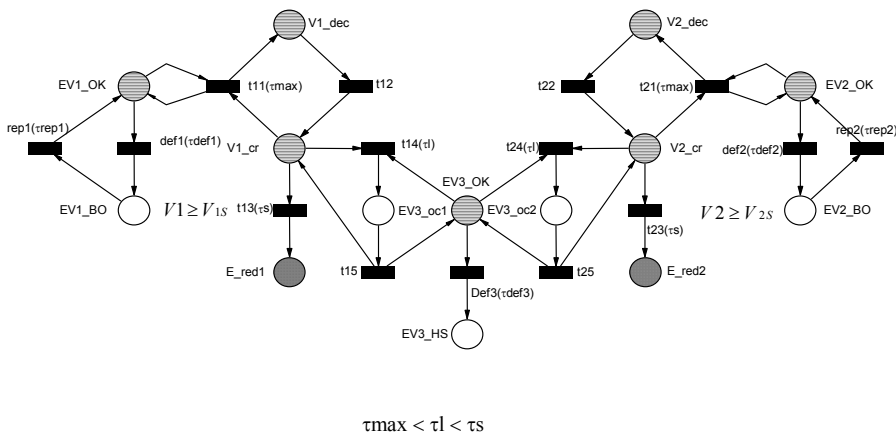


Fig.1. Figure 2. Réseau de Petri décrivant le système

4 ALGORITHME

Comme décrit dans [10] l'algorithme est constitué de différentes procédures et structures de données manipulant des ensembles de transitions qui peuvent être en conflit pour pouvoir générer tous les scénarios possibles.

La nouvelle version de l'algorithme [12] prend en compte explicitement les conditions associées au franchissement de certaines transitions. Ces conditions sont des seuils impliquant des variables continues. Elles sont représentées dans l'algorithme par des durées qui correspondent au temps que met le système pour atteindre ces seuils (approximation temporelle d'un système hybride).

Cette version de l'algorithme introduit une nouvelle liste de données (Lint2) qui est une liste de transitions franchissables ou potentiellement franchissables à ne pas franchir car elles sont en conflit avec des transitions qui doivent être franchies avant elles (à cause de l'aspect continu). La prise en compte de ces relations de précedence provenant de la dynamique continue et non spécifiées par le réseau de Petri permet d'éliminer un certain nombre de scénarios incohérents vis-à-vis de la dynamique continue dans cette nouvelle version de l'algorithme.

5 APPLICATION DE L'ALGORITHME SUR LE CAS D'ETUDE

En appliquant l'algorithme à l'exemple, l'ancienne version génère 23 ordres partiels dans lesquels quatre correspondent aux scénarios redoutés du réservoir 1, neuf à son fonctionnement

normal et dix sont incohérents en tenant compte de l'aspect continu. L'utilisation de la nouvelle version élimine les dix scénarios incohérents.

La conséquence de la prise en compte des seuils associés aux transitions t_{11} , t_{14} et t_{13} , est que la transition t_{13} sera franchie uniquement si t_{11} et t_{14} ne sont pas franchies. Cela signifie que les scénarios redoutés sont composés de fragments contenant les transitions en conflit avec t_{11} et t_{14} , et par le franchissement de t_{13} .

Par exemple le scénario suivant $\{t_{13}, def_1, t_{23}, def_2\}$ donné par l'ancienne version n'est pas produit dans la nouvelle version car la transition t_{14} qui est en conflit avec t_{13} a un seuil de franchissement inférieur, donc elle est franchie avant et interdit le franchissement de t_{13} .

6 CONCLUSION ET TRAVAIL FUTUR

Nous avons présenté et illustré un algorithme pour générer des scénarios à partir d'un modèle réseau de Petri. Cette nouvelle version de l'algorithme qui tient compte de l'aspect continu du système permet d'éviter la génération de scénarios incohérents. C'est une réelle amélioration mais les travaux doivent continuer car on obtient encore un nombre important de scénarios. Nous avons deux problèmes majeurs à résoudre à court terme: certains scénarios générés ne sont pas minimaux et d'autres sont redondants. Par exemple dans le système précédant, nous avons trouvé quatre scénarios redoutés recouvrant deux comportements redoutés minimaux. En effet, parfois l'algorithme produit des scénarios qui ne sont pas minimaux c'est-à-dire qui contiennent des événements qui sont la conséquence d'événements pris en compte dans le scénario, mais qui ne sont pas strictement nécessaires à l'obtention finale de l'état critique redouté. De même que la notion de coupe minimale a été définie dans le cadre des arbres de défaillance, il nous faut donc définir ce qu'est un scénario redouté minimal et soit prendre en compte cette définition dans l'algorithme afin de l'arrêter lorsque le scénario n'est pas minimal, soit l'utiliser à posteriori pour extraire un scénario minimal d'un scénario qui ne l'est pas. Rappelons d'abord ce qu'est une coupe minimale dans un arbre de défaillance.

Une coupe est un ensemble d'événements entraînant l'événement indésirable [13]. *Une coupe minimale* est la plus petite combinaison d'événements entraînant l'événement redouté ; ainsi le retrait d'un événement de la coupe ne produit plus l'événement indésirable. La recherche des coupes minimales se fait traditionnellement à partir d'une transformation d'un arbre de défaillances (AdD) en une expression booléenne, et l'utilisation des lois de l'algèbre de Boole pour obtenir une expression booléenne réduite de l'événement redouté. Une autre méthode plus récente, est basée sur les Diagrammes de Décision Binaires (BDD) codant L'AdD [14].

Dans notre approche, la représentation du scénario sous forme logique ne se fait pas à l'aide d'une expression booléenne. Elle se fait par un séquent de logique linéaire. Dans un tel séquent, la liste des franchissements de transition est commutative (comme les éléments d'un monôme booléen avec l'opérateur "et"), mais grâce au fait qu'en logique linéaire les propositions logiques sont consommées lorsqu'elles sont utilisées dans une déduction, l'ordre partiel entre les franchissements peut être déduit à partir d'une preuve quelconque du séquent. La notion de séquent caractéristique d'un ordre partiel (d'un scénario) a été introduite par N. Rivière [15]. Toutes les preuves d'un tel séquent produisent alors le même ordre partiel. Si l'on écrit le séquent associé à un scénario redouté sous la forme du séquent caractéristique de l'ordre partiel associé au scénario, alors il sera minimal s'il est impossible de le décomposer (au cours d'une preuve) par une règle du calcul des séquents en deux sous scénarios tels que l'un des deux mène encore d'un ensemble d'états partiels normaux à un ensemble d'états partiels comprenant l'état redouté. Nous comptons explorer cette piste. Actuellement, nous travaillons sur la notion de minimalité pour nos scénarios, qui est exprimée dans notre contexte sous la forme d'un séquent en logique linéaire. Cette notion sera intégrée à l'algorithme pour préciser le critère d'arrêt.

A long terme, nous envisageons une analyse quantitative pour estimer la probabilité d'occurrence d'évènement redouté dans des systèmes plus complexes.

Références

- [1] Lee, W. S.; Grosh, D. L.; Tillman, F. A., Lie, C. H., «Fault tree analysis, methods, and applications – A review », IEEE Transactions on Reliability, August 1, 1985; ISSN 0018-9529; r-34, page 194-203.
- [2] Chris J. GARRET, Sergio B. Guarro, George E. APOSTOLAKIS, « The Dynamic Flowgraph Methodology for Assessing the Dependability of Embedded Software Systems », IEEE Transactions On Systems, Man, and Cybernetics, Vol. 25, No. 5, May 1995.
- [3] P.E. Labeau: “A Survey on Monte Carlo Estimation of Small Failure Risks in Dynamic Reliability”. In International Journal of Electronics and Communications, Vol. 52, pp. 205-211, 1998.
- [4] G.Moncelet, « Application des réseaux de Petri à l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile », thèse de Doctorat, No 3076, Université Paul Sabatier, Toulouse.
- [5] S. Khalfaoui, « Méthode de recherche des scénarios redoutés pour l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile », thèse de Doctorat, No 03574, Institut National Polytechnique, Toulouse.
- [6] 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.
- [7] S. Khalfaoui, E.Guilhem, H. Demmou, R. Valette, “Une méthode pour obtenir des scénarios critiques dans les systèmes mécatroniques”, λμ13-ESREL2002 European Conférence, Lyon - France - 18 au 21 mars 2002.
- [8] R. Champagnat, P. Esteban, H. Pingaud, R. Valette, “Modelling and simulation of a hybrid system through Pr/Tr PN DAE model”, ADPM'98 3rd International Conference on Automation of Mixed Processes, 19-20 March 1998, Reims, France p. 131-137.
- [9] H. Demmou, S. Khalfaoui, N. Rivière, E. Guilhem, “Extracting critical scenarios from a Petri net model using linear logic” Journal.
- [10] S. Khalfaoui, H. Demmou, E. Guilhem, R. Valette “An algorithm for deriving critical scenarios in mechatronic systems” IEEE SMC (System Man and Cybernetic)2002, 6-9 october, Hammamet Tunisie
- [11] F. Dufour, Y. Dutuit, “Dynamic Reliability: A new model”, λμ13-ESREL2002 European Conference, Lyon - France - 18 au 21 Mars 2002.
- [12] M. Medjoudj, H. Demmou, R. Valette, « Un algorithme pour l'extraction des scénarios critiques dans les systèmes hybrides », Formalisation des Activités Concurrentes (FAC'2004), Toulouse (France), 9-10 Mars 2004, 12p.
- [13] Alain Villemeur « Sûreté de fonctionnement des systèmes industriels », 1988
- [14] Eric Niel, Etienne Craye « Maîtrise des risques et sûreté de fonctionnement des systèmes de production », Chapitre 7 Yves Dutuit et Antoine RAUZY, 2002
- [15] N. Rivière, "Modélisation et analyse temporelle par réseaux de Petri et logique linéaire", thèse de l'INSA de Toulouse, le 26 novembre 2003.

