3e Conférence Francophone de MOdélisation et SIMulation "Conception, Analyse et Gestion des Systèmes Industriels"
MOSIM'01 – du 25 au 27 avril 2001 - Troyes (France)

CONCEPTION ET SURETE DE FONCTIONNEMENT : DEUX ACTIVITES INDISSOCIABLES

Didier JAMPI, Edwige GUILHEM

PSA Peugeot Citroën
18, rue des Fauvelles
92256 La Garenne Colombes Cedex, France
Mél : guilhem1, jampi1@mpsa.com

Jean-François AUBRY

CRAN/INPL
2, avenue de la Forêt de Haye
54 516 Vandoeuvre-Lès-Nancy Cedex, France
Mél : jfaubry@ensem.inpl-nancy.fr

RESUME : *L'introduction massive de l'électronique dans le secteur automobile a permis, d'une part une amélioration conséquente des services rendus par le véhicule, et d'autre part une réduction des coûts, qui s'explique par le caractère moins onéreux de l'électronique par rapport à la mécanique. Néanmoins, de nombreux systèmes contrôlés et commandés par l'électronique, tels que le freinage, doivent répondre à de sévères critères de fiabilité et requièrent donc, lors de leur conception, une attention particulière en terme de sûreté de fonctionnement.*
Cet article présente une méthodologie dont l'objectif majeur est la prise en compte de la sûreté de fonctionnement lors de la conception de systèmes de contrôle commande numériques.

MOTS-CLES : *Système de contrôle commande numérique, Sûreté de fonctionnement, Réseau de Petri*

CONTEXTE

L'introduction de l'électronique dans le secteur automobile (citons par exemple les coussins gonflables de sécurité, l'embrayage piloté (Trotin, 1997) ou le contrôle moteur) a permis de répondre à une exigence grandissante des clients vis-à-vis des fonctionnalités que doit remplir leur véhicule et ce en terme de sécurité, agrément de conduite, pollution.
Les systèmes alliant mécanique et électronique, dits mécatroniques, requièrent une attention particulière lors de leur conception en ce qui concerne leur sûreté de fonctionnement. En effet, la prise en compte de la sûreté de fonctionnement au plus tôt dans le cycle de développement d'un système permet une localisation et une correction aisées des erreurs assurant ainsi une diminution des délais et des coûts de conception. De plus, un constructeur se doit de livrer un véhicule dont la fiabilité ne peut être remise en question.

Dans cet article nous décrirons une méthodologie permettant l'introduction de concepts de sûreté de fonctionnement au cours de la conception de système de contrôle commande d'organes mécaniques.

INTRODUCTION

Calvez présente un modèle conceptuel à trois composantes (Calvez, 1990) :

- une composante fonctionnelle qui caractérise les fonctions du système,
- une composante comportementale qui décrit l'évolution des fonctions,
- une composante exécutive qui spécifie la partie matérielle du système.

Parallèlement aux études fonctionnelles, comportementales et exécutives, pourront être menées des études de sûreté de fonctionnement. Nous nous intéresserons essentiellement à la composante comportementale du modèle conceptuel. Au cours de la description comportementale du système de contrôle commande, nous introduirons successivement quatre concepts de sûreté de fonctionnement :

- une vérification ayant pour objectif de s'assurer de la bonne formalisation du système de commande (Laprie et al., 1989) c'est-à-dire de certaines propriétés de la formalisation, résultant de qualités propres aux systèmes modélisés,
- une validation dont le but est de s'assurer de la formalisation du bon système c'est-à-dire de l'adéquation du comportement du système modélisé au cahier des charges,
- une étude qualitative de sûreté de fonctionnement qui permet d'identifier les faiblesses du système et d'y remédier en introduisant entre autres des reconfigurations de la commande,
- une étude quantitative de sûreté de fonctionnement dont l'objectif est d'évaluer les paramètres de la sûreté du système spécifié (probabilités…).

1 VERIFICATION

Pour modéliser le comportement du système de contrôle commande numérique, nous avons utilisé les réseaux de Petri interprétés (Brams, 1983), (David et Alla, 1989), (Peterson, 1981). Le choix de ce formalisme s'explique par :

- l'amélioration de la lisibilité et donc de la compréhension du système modélisé, de par le caractère graphique des réseaux de Petri,
- la conformité du caractère discret des systèmes de contrôle commande numériques à un formalisme à états transitions,
- la possibilité de garantir un certain nombre de propriétés de par le caractère formel des réseaux de Petri.

De plus, la complexité raisonnable des systèmes de contrôle commande à formaliser permet d'obtenir des réseaux de Petri de taille modérée (quelques dizaines de nœuds).

La vérification consiste à s'assurer de la bonne formalisation du système modélisé, en l'occurrence ici d'un système de contrôle commande numérique. Certaines propriétés propres aux systèmes de commande, telles que l'absence d'états bloquants, la réinitiabilité et le déterminisme lors du fonctionnement nominal ou dégradé, devront être vérifiées.

Les qualités de réinitiabilité et d'absence de blocage, que vérifie le système de contrôle commande numérique, se déclinent en la propriété de vivacité pour les réseaux de Petri formalisant ce système. Vérifier la réinitiabilité et l'absence de blocage de la commande revient donc à s'assurer de la vivacité des réseaux de Petri modélisant cette commande.

Un découpage fonctionnel approprié du système de contrôle commande permet d'obtenir plusieurs sous fonctions sans parallélisme (deux actions d'une même sous fonction ne pourront être simultanées). Chacune de ces fonctions se modélise en réseau de Petri sous forme de graphe d'états interprété à jeton unique.

Une condition nécessaire pour que le système de contrôle soit réinitialisable et sans blocage est que chacune des sous fonctions le soit également. Nous cherchons donc, dans un premier temps, à construire des graphes d'états interprétés vivants à jeton unique. Il sera nécessaire, dans un second temps, de vérifier la conservation de la vivacité une fois les réseaux réunis, réunion qui traduit le parallélisme des actions de la commande.

1.1 Vivacité d'un graphe d'états à jeton unique

Deux approches sont envisageables pour s'assurer de la vivacité des graphes d'états :

- le réseau est tout d'abord construit puis sa vivacité est a posteriori vérifiée,
- la vivacité du réseau est a priori assurée par une technique de construction par raffinement fondée sur l'utilisation de primitives (Tankoano, 1988), (Moitessier, 1991) et l'application de certaines règles simples.

Cette seconde approche, décrite dans (Jampi et al., 2000), a l'avantage d'assurer dès la première construction la vivacité de graphes d'états, contrairement à la première approche qui peut nécessiter un nombre indéterminé de constructions jusqu'à obtention d'un réseau ayant les propriétés requises.

1.2 Conservation de la vivacité une fois les réseaux réunis

La réunion des graphes d'états interprétés peut faire apparaître des phénomènes, tels que l'interblocage et l'indéterminisme, altérant les qualités désirées de la commande. Une vérification de la conservation de la vivacité doit donc être entreprise.

L'application de techniques classiques telles que l'utilisation du graphe des marquages est envisagée. Un problème se pose quant à la détermination de ce graphe des marquages, ce dernier devant prendre en compte l'interprétation des réseaux. Dans l'hypothèse restrictive d'une commande ne dépendant que d'événements indépendants et de variables aux valeurs dénombrables (par exemple des variables booléennes), une approche similaire à celle utilisée pour la définition du graphe d'occurrence des réseaux de Petri colorés (Jensen, 1997) est envisageable. Le graphe d'accessibilité est alors construit en fonction du marquage, de l'occurrence des événements et des valeurs des variables. L'exemple de la figure 1 illustre cette démarche.

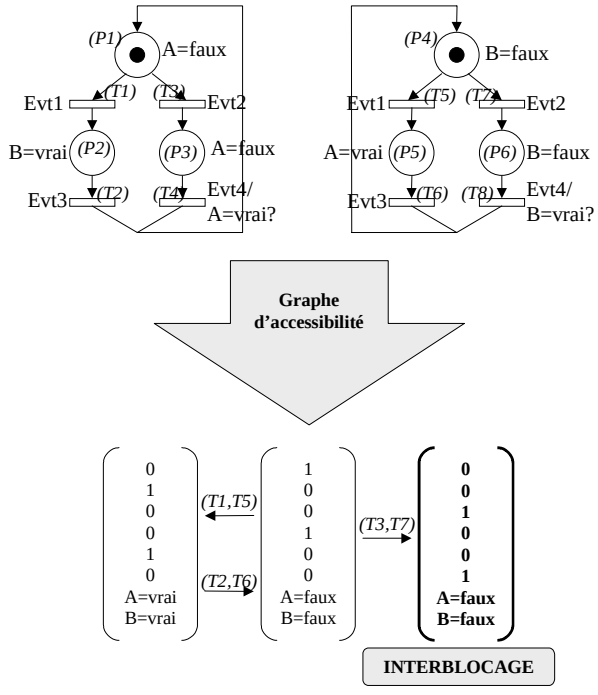

Figure 1. Détermination du graphe d'accessibilité

Cette approche n'est applicable qu'à une classe bien particulière de systèmes. Une étude est menée pour définir une démarche systématique et exhaustive permettant l'analyse du déterminisme et de l'absence de blocage des fonctions réunies, quelles qu'elles soient.

A l'issue de l'étape de vérification, nous obtenons des réseaux de Petri interprétés vivants et sans conflits, formalisant une commande réinitialisable, déterministe et sans états bloquants ou non atteignables. Cette formalisation sert de support à l'étude qualitative de sûreté de fonctionnement à venir.

2 ETUDE QUALITATIVE DE SURETE DE FONCTIONNEMENT

L'originalité de l'approche proposée est de réaliser une étude qualitative de sûreté de fonctionnement à partir de la formalisation du système de contrôle commande, système le plus à même à réagir à d'éventuelles défaillances. Cette approche, qui peut s'apparenter à une AMDEC (Analyse des Modes de Défaillance, de leur Effet et de leur Criticité) (Villemeur, 1988) a deux avantages :

- elle aide le concepteur à définir des recommandations à mettre en œuvre pour minimiser la fréquence d'occurrence d'un événement redouté (par détection précoce des causes de défaillance et reconfiguration logicielle par exemple) et/ou la gravité des conséquences d'une défaillance,
- elle permet d'identifier aisément dans le système de commande les états à partir desquels doivent être mises en œuvre les reconfigurations logicielles.

Cette étude repose sur le fait que l'apparition d'une défaillance affectant le système de contrôle commande se traduira toujours par une évolution anormale du réseau de Petri modélisant la commande, soit au niveau de la place, soit au niveau de la transition (Aubry, 1987).

Pour une AMDEC traditionnelle, les éléments de départ de l'analyse sont les composants du système. Ici, les éléments de départ sont les places et les transitions du réseau de Petri formalisant le système de contrôle commande. Ainsi, nous définissons quatre modes de défaillances :

a) Transition franchie avec retard

b) Transition franchie en avance

Ces deux modes de défaillance traduisent le fait que, bien que l'état du process permette (resp. ne permette pas) une évolution de la commande, le changement d'état de cette dernière ne s'opèrera qu'ultérieurement (resp. s'opère intempestivement). Ce phénomène peut s'expliquer, par exemple, par l'obtention d'une image biaisée du processus induite par une dérive de capteur.

c) Transition devenue infranchissable :

Ce mode de défaillance traduit le fait que l'état de la partie opérative (par exemple une défaillance capteur) ne permet plus l'obtention de la véracité d'une condition ou l'occurrence d'un événement.

d) Action erronée :

Ce mode de défaillance est révélateur d'une non-conformité de la commande à l'état de la partie commandée.

Le concepteur s'interrogera sur les causes, les conséquences, la gravité et la fréquence d'occurrence des différents modes de défaillance et ce, pour chaque transition et chaque place du réseau de Petri formalisant le système de contrôle commande. Cette étude conduira à définir des recommandations à mettre en œuvre afin d'améliorer globalement la sûreté de fonctionnement du système. Parmi les recommandations, nous trouvons notamment les besoins en reconfiguration du système de contrôle commande dont l'objet est de réagir aux défaillances du système. Le dossier de spécification est ainsi complété et la mise en œuvre des reconfigurations nécessite l'introduction de nouvelles places et de nouvelles transitions dans la formalisation de la commande. Afin d'assurer les propriétés d'absence d'états bloquants, de réinitiabilité et de déterminisme de la commande, la formalisation des reconfigurations se fait à l'aide des primitives de construction telle qu'énoncée dans le paragraphe 1.

Les résultats de l'étude qualitative de sûreté de fonctionnement pourront être répertoriés dans un tableau semblable au tableau 1.

NŒUD	**Mode de défaillance**	**Causes**	**Conséquences**	**G**	**O**	**Recommandations**	**G'**	**O'**
Pi	Action erronée							
Tj	Franchie prématurément							
	Franchie avec retard							
	Devenue infranchissable							

Tableau 1. Récapitulatif de l'étude de type AMDEC

Le concepteur réalise ainsi de façon méthodique une étude qualitative exhaustive de sûreté de fonctionnement, exhaustive en ce sens que toutes les transitions et toutes les places du réseau de Petri formalisant le système de contrôle commande seront étudiées.

Le système de commande obtenu à l'issue de l'étude qualitative de sûreté de fonctionnement intègre un fonctionnement en mode nominal ainsi qu'en mode dégradé par reconfiguration suite à une défaillance. Il faut dorénavant prouver que le comportement du système de commande et de la partie opérative modélisés répond à celui décrit dans le cahier des charges.

3 VALIDATION

La validation consiste à s'assurer que le comportement du système modélisé correspond bien à celui du système spécifié et ce, en terme de dynamique et de sûreté.
A ce niveau du développement, la validation ne peut être réalisée que par simulation. Les systèmes à simuler font cohabiter partie continue (évolution de variables continues comme la vitesse) et partie discrète (occurrence d'un événement) et sont alors dits hybrides. Effectivement, le comportement de la partie commande est conditionné par l'état de la partie opérative dont l'évolution est fonction de la commande. Une validation du système par simulation nécessite donc la prise en compte conjointe de la commande et de la partie commandée.
De nombreux travaux sur la simulation des systèmes hybrides ont été réalisés (Champagnat et al.,1998), (Ibrahim, 1993), (Wieting et Sonnenschein, 1995) et ne seront pas plus amplement développés ici.

La validation permet de s'assurer que le comportement des solutions retenues pour réaliser le système spécifié est conforme à celui décrit dans le cahier des charges. Plusieurs choix technologiques sont souvent envisageables. Des critères tels que le coût mais également la sûreté (fiabilité, sécurité) déterminent la solution à mettre en œuvre. C'est pourquoi une étude quantitative de sûreté de fonctionnement visant à déterminer la fiabilité du système est menée.

4 ETUDE QUANTITATIVE DE SURETE DE FONCTIONNEMENT

L'originalité de l'approche envisagée est de réaliser une étude de sûreté de fonctionnement à l'aide du système de contrôle commande, ce qui permet lors de l'évaluation quantitative de prendre en compte les différentes reconfigurations logicielles qui fiabilisent le fonctionnement du système global.
L'étude qualitative de sûreté de fonctionnement a permis d'identifier un certain nombre de défaillances affectant le fonctionnement du système. Chaque composant, dont la panne est à l'origine d'une défaillance, sera modélisé par un réseau de Petri stochastique dont l'évolution pourra conditionner celle du réseau de Petri interprété de commande par passage dans un état de non-conformité ou de reconfiguration.
Dans l'hypothèse où les processus de commande et d'apparition des défaillances sont assimilés à des systèmes markoviens homogènes, nous cherchons à extraire du réseau de Petri, formalisant le fonctionnement et le dysfonctionnement du système global, un graphe de Markov à partir duquel seront réalisées les études quantitatives de sûreté de fonctionnement (Pagès et Gondran, 1980). Le graphe de Markov obtenu est confronté au problème d'explosion combinatoire. C'est pourquoi, une réduction de ce graphe doit être réalisée. L'approche de réduction envisagée repose sur le fait que les graphes sont caractérisés par deux échelles de temps : une dynamique rapide pour la commande, une dynamique lente pour les défaillances. La réduction consistera en un regroupement d'états fondé sur la notion de classes de transition caractérisées par l'ordre de grandeur des taux de franchissement.

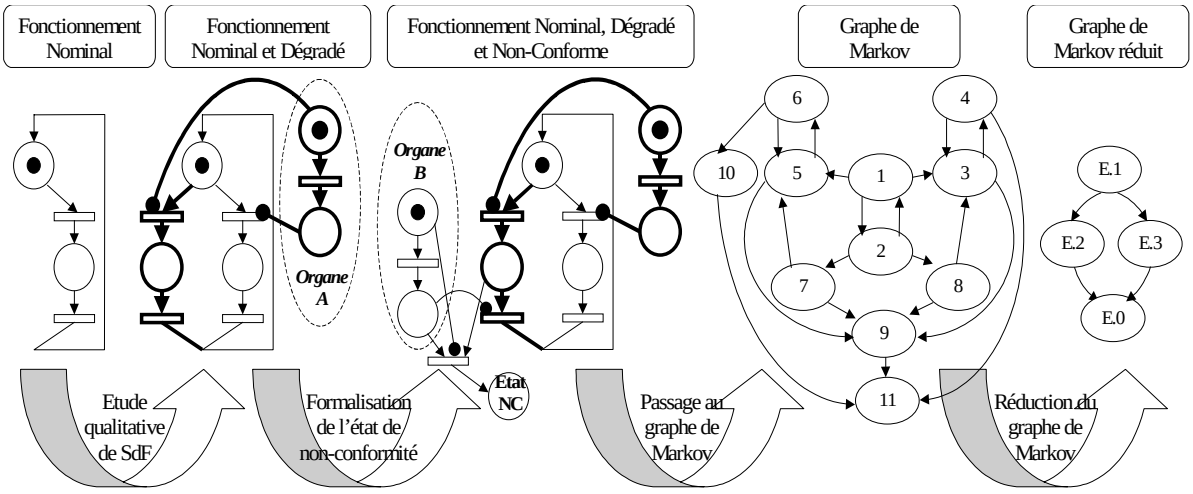

Figure 2. Démarche pour l'étude quantitative

La démarche globale proposée est représentée schématiquement par la figure 2. Nous y reconnaissons :

- la mise en œuvre d'une reconfiguration à l'issue de l'étude qualitative menée à l'aide de la formalisation du système de contrôle commande ainsi que la mo-

délisation des états des composants induisant le passage à ce mode de fonctionnement,
- la modélisation de l'état de non-conformité et la formalisation des composants conditionnant le passage de la commande à cet état,
- l'obtention du graphe de Markov à partir du réseau de Petri formalisant le comportement du système de commande en fonction de l'état des composants,
- la réduction du graphe de Markov obtenu.

L'étude quantitative de sûreté de fonctionnement permet de justifier le choix des concepteurs en terme de sûreté et non plus seulement en terme de coût.

5 EXEMPLE

Nous proposons d'illustrer notre approche à l'aide d'un exemple de régulation de hauteur de caisse par un dispositif de suspension hydraulique. L'exemple proposé n'a pas la prétention d'exposer une étude exhaustive de la suspension. Cet exemple est d'ailleurs adapté et simplifié pour répondre à un objectif didactique et n'est donc pas nécessairement le reflet de la réalité.

5.1 Présentation

L'objectif de la régulation inscrit dans le cahier des charges est de maintenir la caisse à une hauteur proche d'une valeur Ho tout en assurant le confort du conducteur, c'est-à-dire en interdisant toute variation brusque de hauteur. Cette hauteur est assurée par un système de vérin hydraulique alimenté en fluide par l'intermédiaire d'une pompe et d'un dispositif faisant varier les débits que nous nommerons vanne (Figure 3). Pour effectuer la régulation, une commande de position Uv du volet de la vanne, calculée en fonction de la hauteur de caisse est envoyée à chaque changement de période d'échantillonnage (CPE).

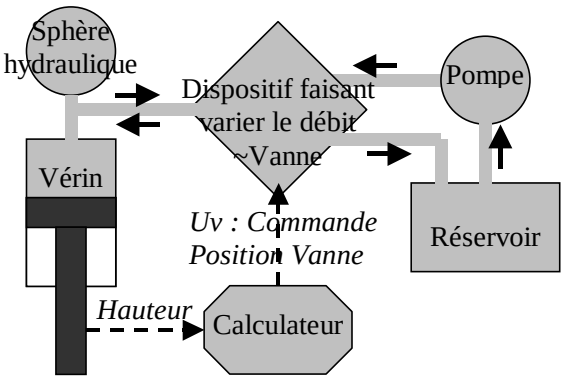

Figure 3. Dispositif de suspension

5.2 Vérification

La fonction de régulation étant élémentaire, la construction à l'aide des primitives est triviale puisqu'il suffit d'utiliser le réseau embryonnaire pour modéliser cette commande (Figure 4). Il apparaît clairement que cette fonction est réinitialisable sans blocage et déterministe.

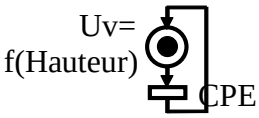

Figure 4. Formalisation de la fonction de régulation

Nous allons fiabiliser la régulation de hauteur en réalisant, à partir de la formalisation de cette fonction, l'étude qualitative de sûreté de fonctionnement préconisée au paragraphe 2.

5.3 Etude qualitative de sûreté de fonctionnement

Pour illustrer l'étude « de type AMDEC » proposée, intéressons nous au mode de défaillance « action erronée » de l'unique place, c'est-à-dire à la fausseté de la commande Uv=f(hauteur).

Les causes de ce mode de défaillance peuvent être entre autres :
- une valeur erronée de la variable d'entrée, à savoir l'information de hauteur, due par exemple à une défaillance du capteur de hauteur,
- une non-conformité de la commande à l'état de l'actionneur (par exemple une défaillance de la vanne).

Une des conséquences de très grande gravité de ce mode de défaillance peut être une casse de la suspension.
La fréquence d'occurrence de la défaillance du capteur de hauteur est supposée suffisamment élevée pour que nous recommandions l'utilisation d'un capteur de type hystérésis fournissant une information de niveau haut et bas (Tableau 2). Sur occurrence d'une de ces informations, une reconfiguration, correspondant à un ordre d'ouverture (Uv=OUVRIR) ou de fermeture (Uv=FERMER) de la vanne, sera mise en œuvre.

Comme mentionné dans le paragraphe 2, la reconfiguration proposée peut être construite et modélisée, à partir de la formalisation de la commande en fonctionnement nominal, par la technique de construction à l'aide des primitives Séquence (SEQ qui permet l'insertion d'une place et d'une transition) et Fourche (FOU qui relie deux places par une nouvelle transition) (figure 5). L'utilisation de ces primitives permet d'obtenir, dès la première construction, une fonction réinitialisable, exempte de blocage et dont tous les états sont atteignables.

NŒUD	Mode de défaillance	Causes	Conséquences	G	O	Recommandations	G'	O'
P1	Action erronée	- défaillance capteur de hauteur - défaillance vanne	Risque de casse de suspension	4	2	Utiliser un capteur hystérésis pour détecter un niveau haut et un niveau bas et ouvrir ou fermer la vanne en conséquence	4	1

Tableau 2. Extrait de l'étude de type AMDEC

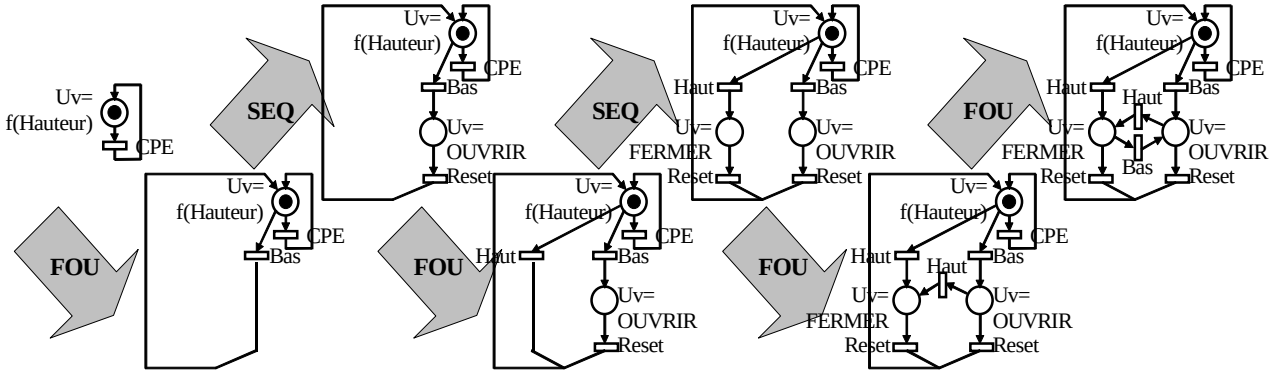

Figure 5. Mise en œuvre de la reconfiguration

Le réseau embryonnaire (réseau initial de la figure 5) formalise le fonctionnement nominal de la régulation de hauteur. Sur occurrence d'une information de niveau bas (ou haut) suite à une défaillance du capteur de hauteur, la commande passe en mode dégradé jusqu'à réparation du capteur. Cette réparation induit un retour en mode nominal. Nous expliquons ainsi l'utilisation de la première primitive Fourche pour débuter la formalisation du fonctionnement dégradé. Le franchissement de la nouvelle transition introduite est conditionné par l'occurrence de l'information de hauteur basse (BAS). L'action à mener suite au franchissement de cette transition est une commande d'ouverture de la vanne (Uv=OUVRIR). De plus, nous quitterons le fonctionnement dégradé pour un fonctionnement nominal sur occurrence du message reset qui signifie que la réparation du capteur de hauteur a été réalisée. Pour formaliser la commande d'ouverture et le retour en mode nominal, nous utilisons une primitive Séquence. De la même façon, des primitives Fourche et Séquence seront appliquées pour modéliser la commande de fermeture de la vanne sur occurrence d'un niveau haut et le retour au fonctionnement nominal suite à la réparation du capteur de hauteur. L'utilisation de la troisième (Resp. quatrième) primitive Fourche s'explique par le fait que lorsque la vanne est commandée en ouverture (Resp. fermeture), si un niveau haut (Resp. bas) de la caisse est détecté, une commande de fermeture (Resp. ouverture) de la vanne doit être effectuée.

La commande obtenue intègre un fonctionnement en mode nominal et un fonctionnement en mode dégradé suite à la défaillance du capteur de hauteur. Assurons nous maintenant que le système de commande et la partie opérative se comportent conformément au cahier des charges.

5.4 Validation

Par simulation conjointe de la partie opérative et de la partie commande, nous pouvons valider le comportement du système global.
La courbe de la figure 6 montre l'évolution de la hauteur en fonctionnement nominal puis lors du dysfonctionnement à la suite d'une défaillance du capteur de hauteur pour le système sans reconfiguration. La courbe de la figure 7 révèle le fonctionnement en mode nominal puis en mode dégradé du système avec reconfiguration. Le choix de Hmax et de Hmin doit faire l'objet d'un compromis entre le confort du conducteur et la capacité du matériel à réaliser la fonction dégradée.

Nous pouvons légitimement nous interroger sur la pertinence d'introduire un nouveau capteur et ce, en fonction du rapport coût/fiabilité. L'étude quantitative de sûreté de fonctionnement permettra d'évaluer la plus-value d'une solution par rapport à l'autre en terme de fiabilité.

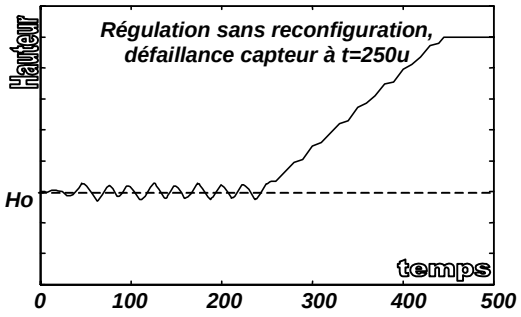

Figure 6. Evolution de la hauteur pour une régulation sans reconfiguration

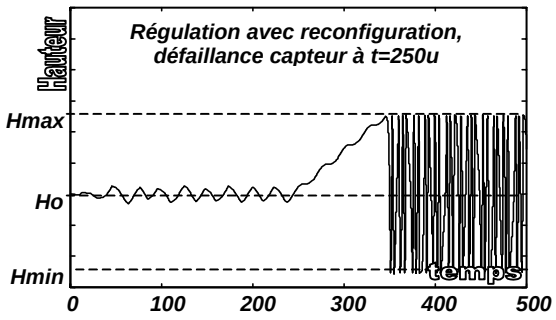

Figure 7. Evolution de la hauteur pour une régulation avec reconfiguration

5.5 Etude quantitative de sûreté de fonctionnement

Dans cette étude quantitative, par souci de simplification, nous ne prendrons en compte que les défaillances des capteurs et de la vanne. L'étude réalisée conformément à la démarche proposée au paragraphe 4 permet d'obtenir les graphes de Markov réduits des figures 8 et 9.

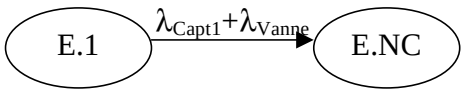

Figure 8. Graphe de Markov réduit pour un système sans reconfiguration de la commande

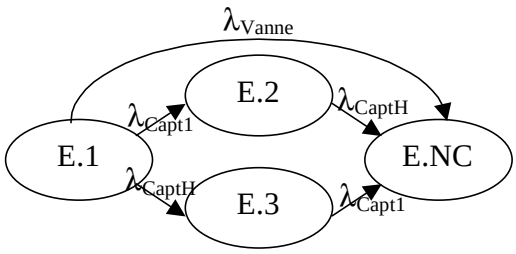

Figure 9. Graphe de Markov réduit pour un système avec reconfiguration de la commande

Le graphe de la figure 8 traduit le fait que, pour la commande sans reconfiguration, la non-réalisation de la régulation de hauteur est due, soit à une défaillance du capteur de hauteur, soit à une défaillance de la vanne.
En revanche, le graphe de la figure 9 montre que, pour la commande avec reconfiguration, la non-réalisation de la régulation est due, soit à une défaillance de la vanne, soit à une défaillance du capteur de hauteur et à une défaillance du capteur hystérésis.

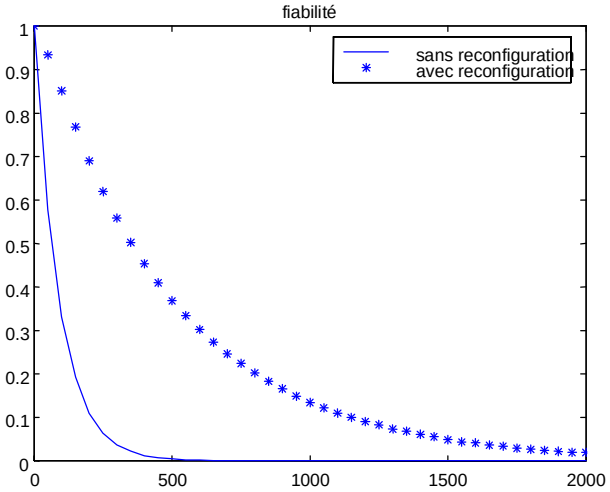

Figure 10. Courbes de fiabilité des systèmes régulés par une commande avec ou sans reconfiguration

Une étude quantitative à l'aide du système de contrôle commande permet donc une prise en compte des reconfigurations dans l'évaluation de la sûreté de fonctionnement. Il est alors possible de quantifier la plus-value d'une reconfiguration (Figure 10) et ainsi orienter le choix du concepteur et ce, en terme de coût et de sûreté.

CONCLUSION

Un des intérêts de la méthodologie proposée est de pouvoir réaliser plusieurs études de sûreté de fonctionnement à l'aide d'une même représentation de la commande enrichie par l'avancement de l'étude. Aucune perte d'information due au passage d'un formalisme à un autre, utile à une étude spécifique, n'est donc à déplorer.
Dans un contexte industriel, une telle approche n'est applicable que si elle est outillée. C'est pourquoi, un des objectifs actuels de nos travaux est de spécifier et de réaliser un outil de simulation supportant cette méthodologie.

REFERENCES

Aubry J.F., 1987 : « Conception des systèmes de commande numériques des convertisseurs électromécaniques : vers une méthodologie intégrant la Sûreté de fonctionnement ». Thèse de Doctorat de l'Institut National Polytechnique de Lorraine.

Brams G.W., 1983 : « Réseaux de Petri : Théorie et pratique. Tome 1 : Théorie et analyse ». MASSON

Calvez J.P., 1990 : « Spécification et conception des systèmes, une méthodologie ». Manuels informatiques. MASSON

Champagnat R., Esteban P., Pingaud H., Valette R., 1998 : « Modélisation et simulation d'un système hybride à l'aide d'un modèle RdP Pr/Tr-EAD ». ADPM'98. 3ème Conférence Internationale sur l'Automatisation des processus mixtes. Reims, mars 1998

David R., Alla H., 1989 : « Du grafcet aux réseaux de Petri ». Traité des Nouvelles Technologies Série Automatique. HERMES.

Ibrahim I., 1993 : « Vers un outil de simulation d'un processus dynamique hybride et sa commande ». Thèse de Doctorat de l'Institut National Polytechnique de Lorraine.

Jampi D., Aubry J.F., Porras J., Trotin D., Zanne C., 2000 : « Spécification de systèmes mécatroniques sûrs de fonctionnement ». 12ème colloque national de fiabilité et maintenabilité. λμ12 Montpellier, mars 2000.

Jensen K., 1997 : « Coloured Petri Nets, Basic concepts Volume 1 ». Springer.

Laprie J.C., Coutois B., Gaudel M.C., Powell D., 1989 : « Sûreté de fonctionnement des systèmes informatiques ». DUNOD informatique. BORDAS PARIS.

Moitessier F., 1991 : « MISTRAL : Méthodologie Interactive de conception et réalisation des Systèmes de commande Temps Réel répartis en Automatique : application à un processus éLectromécanique ». Thèse de Doctorat de l'Institut National Polytechnique de Lorraine.

Pagès A., Gondran M., 1980 : « Fiabilité des systèmes ». Collection de la Direction des Etudes et Recherches d'Electricité De France. Edition Eyrolles.

Peterson J.L., 1981 : « Petri net theory and the modeling of systems ». By Prentice-Hall, INC., Englewoog cliffs, New Jersey 07632

J. Tankoano J., 1988 : « M2C : Une approche méthodique pour la conception certifiée des systèmes de commande des automatismes industriels répartis ». Thèse de Doctorat de l'Université de Nancy I.

Trotin D., 1997 : « Contribution à l'amélioration du confort longitudinal et de l'agrément de conduite par la commande d'un embrayage ». Thèse de Doctorat de l'Université des Sciences et Technologies de Lille.

Villemeur A., 1988 : « Sûreté de fonctionnement des systèmes industriels. Fiabilité. Facteurs humains. Informatisation ». Collection de la Direction des Etudes et Recherches d'Electricité De France. Edition Eyrolles.

Wieting R., Sonnenschein M., 1995 : « Extending high-level Petri Nets for modeling hybrid systems ». In A. Sydow (Editor). Proceeding of the IMACS. Symposium on system analysis and simulation, Volumes 18-19. Berlin, June 1995. Gordon and Breach Publishers