HAL
open science

Modélisation et évaluation de la sûreté de fonctionnement d'un système d'autoroute automatisée

Ossama Hamouda, Mohamed Kaâniche, Karama Kanoun

To cite this version:

Ossama Hamouda, Mohamed Kaâniche, Karama Kanoun. Modélisation et évaluation de la sûreté de fonctionnement d'un système d'autoroute automatisée. 16ème Colloque de Maîtrise des Risques et de Sûreté de Fonctionnement. LAMBDA-MU 16, Oct 2008, Avignon, France. hal-00453029

HAL Id: hal-00453029

https://hal.science/hal-00453029v1

Submitted on 3 Feb 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

MODÉLISATION ET ÉVALUATION DE LA SÛRETÉ DE FONCTIONNEMENT D'UN SYSTÈME D'AUTOROUTE AUTOMATISÉE
DEPENDABILITY MODELING AND EVALUATION OF AN AUTOMATED HIGHWAY SYSTEM[1]

Ossama HAMOUDA, Mohamed KAANICHE, et Karama KANOUN
LAAS-CNRS; Université de Toulouse, 7, Avenue du Colonel Roche, F-31077 Toulouse, France
Tél. : 05 61 33 64 53 – Fax : 05 61 33 64 11, E-mail : {prénom.nom}@laas.fr

Résumé
Le trafic automobile est de plus en plus congestionné, surtout dans les zones urbaines. Une des solutions étudiées est l'automatisation du trafic. De nombreux programmes de recherche ont été conduits, ou sont en cours, relatifs à l'assistance à la conduite automobile qui constitue, à long terme, une voie vers la route ou l'autoroute automatisée. Un exemple consiste à former des convois, ou des pelotons de véhicules (« *Platoon* » en anglais) pouvant évoluer de façon autonome. La mise en œuvre de routes automatisées vise à améliorer la fluidité du trafic et la sécurité routière (grâce à la diminution des accidents), tout en réduisant la consommation de carburant et les nuisances (en particulier la pollution). Dans cet article, nous abordons le problème de l'évaluation de mesures quantitatives caractérisant la sûreté de fonctionnement dans le contexte d'un système d'autoroute automatisée, basé sur l'utilisation de pelotons de véhicules conduits par des agents plus ou moins autonomes, interagissant dans un même environnement multiagent.

Summary
The congestion of traffic has been increasingly growing, especially in urban areas. One of the investigated solutions for this problem is the automated traffic. Many research programs have been carried out or are currently underway regarding assistance for driving, which is in the long run a path to the automated road or highway. One example consists in building convoys, or platoons of vehicles that can evolve autonomously. The development of automated highways is aimed at improving the flow of traffic and road safety (by reducing accidents), while reducing fuel consumption and pollution. In this paper, we address the problem of the evaluation of quantitative measures characterizing dependability in the context of an automated highway system, based on the use of platoons of vehicles driven by more or less autonomous agents, interacting in a multiagent system environment.

1. Introduction

Le domaine de l'automobile a fait l'objet de nombreux travaux de recherche durant les dernières décennies pour développer de nouvelles solutions permettant de faire face à l'augmentation croissante du trafic, d'améliorer la sécurité routière et également de répondre à de nouveaux besoins écologiques et sociétaux. Un intérêt particulier a porté sur l'utilisation des technologies de l'informatique embarquée et de la communication pour répondre à ces besoins [4]. Dans ce contexte, nombreux travaux ont été focalisés sur le développement de systèmes d'assistance à la conduite automobile, pouvant aller jusqu'à une automatisation complète se traduisant par une évolution autonome des véhicules sur des autoroutes équipées des infrastructures nécessaires [6, 14]. L'automatisation de la conduite (ou la conduite automobile collaborative) utilise les communications (inter-véhicules, ou véhicules-infrastructure fixe) pour l'échange d'informations nécessaires pour assurer la sécurité dans de tels systèmes.

Le développement d'autoroutes automatisées a fait l'objet de plusieurs projets de recherche, principalement aux Etats-Unis [2, 3, 18] et au Japon [5, 12, 17]. Les recherches ont porté en particulier sur la conception et la réalisation d'architectures de contrôle et de communication permettant l'automatisation de la conduite et l'évaluation des performances du système en termes de capacité et de débit de trafic.

Dans cet article, nous abordons le problème de l'évaluation de mesures quantitatives caractérisant la sûreté de fonctionnement dans le contexte d'un système d'autoroute automatisée, basé sur l'utilisation de pelotons de véhicules conduits par des agents plus ou moins autonomes, interagissant dans un même environnement multiagent ([10], voir chapitre 1). Notre travail porte sur le développement de méthodes et de modèles permettant d'évaluer la sécurité de pelotons mis en œuvre dans un contexte mobile avec des réseaux ad-hoc. Dans cet article, "sécurité" désigne sécurité-innocuité (par rapport aux défaillances accidentelles).

La sécurité caractérise la confiance que l'on peut accorder au système vis-à-vis de l'absence de défaillances pouvant engendrer des conséquences catastrophiques sur l'environnement, par exemple en termes de pertes de vies humaines [13]. Plusieurs phénomènes, tels que l'occurrence de fautes accidentelles, la mobilité des véhicules, les déconnexions fréquentes des communications, sont à prendre en compte. Cette problématique est nouvelle dans le contexte d'applications et de systèmes d'autoroute automatisée mis en œuvre sur des réseaux ad-hoc, et il n'existe pas encore à notre connaissance de méthodes d'évaluation de la sûreté de fonctionnement dans ce domaine. Les gains attendus de l'automatisation de la conduite font l'objet de nombreux travaux de recherche. Cependant, à notre connaissance, il n'y a pas eu d'études concernant l'évaluation de leur sûreté de fonctionnement. Nous évaluons des mesures quantifiant le risque d'accident dans un contexte de conduite coopérative, afin d'estimer l'impact des nouvelles technologies sur la conduite automobile automatisée.

Nous considérons comme cas d'étude les architectures développées dans le cadre d'un projet de systèmes de transport intelligents du programme PATH (*Partners for Advanced Transit and Highways* « PATH » [18]) à l'Université de Californie à Berkeley aux Etats-Unis. Ce projet porte sur le développement d'un système d'autoroute automatisée basée sur des pelotons de voitures autonomes utilisant des communications inter-véhicules et véhicules-infrastructures pour se coordonner mutuellement. Les architectures proposées s'appuient sur la mise en œuvre de manœuvres automatiques permettant d'assurer la sécurité des véhicules en présence d'évolutions de la configuration des pelotons résultant d'arrivées ou de départs de véhicules au sein d'un peloton. Des manœuvres sont aussi prévues pour assurer le bon fonctionnement du système suite à l'occurrence de défaillances affectant les véhicules, leur environnement ou la communication inter-véhicules.

Dans cet article nous présentons une approche de modélisation basée sur les chaînes de Markov et les réseaux de Petri stochastiques permettant d'évaluer la probabilité d'échec des manœuvres mises en œuvre pour assurer la sécurité d'un peloton. La section 2 présente le système étudié. La section 3 décrit l'approche de modélisation proposée. Dans la section 4, nous présentons des exemples de résultats et des études de sensibilité. Enfin la section 5 conclut l'article et présente les extensions envisagées.

[1] Ce travail a été partiellement financé par la Commission Européenne dans le cadre du projet HIDENETS (IST-FP6-26979, http://www.hidenets.aau.dk) et du réseau d'excellence ReSIST (IST-FP6-26764, http://www.resist-noe.org)

2. Description du système

Un *peloton p* est composé d'un ensemble de véhicules qui se suivent de façon autonome par accrochage virtuel [16]. Le véhicule de tête est appelé *leader* et les autres membres sont appelés *suiveurs*. Un peloton qui contient un seul véhicule est un leader appelé *agent libre*. La Figure 1 montre trois pelotons : *p1* contient trois véhicules, un *leader* et deux *suiveurs* ; *p2* est un peloton *voisin* ; et *p3* est un *agent libre*. La distance *intra-peloton* (Δx) est de un à trois mètres. La distance *inter-peloton* (Δp) entre deux pelotons qui roulent dans la même direction varie entre trente et soixante mètres.

Les travaux du projet PATH [18] se sont concrétisés par le développement d'une architecture hiérarchique tolérante aux fautes permettant de contrôler le peloton de véhicules en fonctionnement normal et en mode dégradé. Dans ces travaux, les véhicules utilisent à la fois des contrôleurs de position au niveau latéral et longitudinal afin de leur permettre de se suivre les uns les autres sur une route équipée de plots magnétiques. Plusieurs manœuvres automatiques ont été définies pour permettre le fonctionnement du système dans des conditions de sécurité, en fonctionnement normal et en présence de défaillances. Les manœuvres principales consistent à diviser ou fusionner des pelotons, à faire sortir ou à insérer un véhicule dans un peloton. En particulier, en cas de défaillance affectant un véhicule du peloton, des manœuvres doivent être réalisées afin de lui permettre de quitter le peloton sans danger et de continuer à rouler sans problème [8].

Dans la suite, nous décrivons brièvement l'architecture de PATH en nous focalisant sur les modes de défaillance pris en compte et les stratégies de recouvrement et manœuvres permettant d'assurer le fonctionnement du système dans des conditions de sécurité.

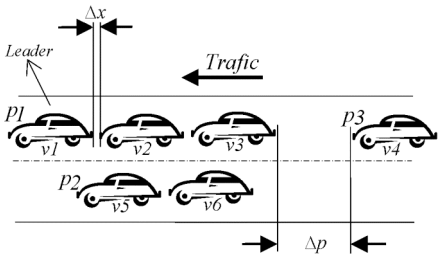

Figure 1 : Contexte d'un peloton

2.1 Architecture de contrôle de PATH

Le contrôle est organisé de façon hiérarchique, selon quatre couches qui sont représentées sur la Figure 2 [11]. Les deux couches hautes (*réseau* et *liaison*) sont mises en œuvre au niveau de l'infrastructure fixe (c'est-à-dire du côté de l'autoroute). Elles sont principalement dédiées à la planification et la gestion du trafic pour maximiser la capacité de l'autoroute. Les décisions concernent les vitesses, la taille et la disposition des véhicules et des pelotons, localement au niveau des sections de l'autoroute (couche liaison), ou bien globalement au niveau de l'ensemble du réseau routier (couche réseau). Les deux couches basses (*coordination* et *régulation*) sont mises en œuvre au niveau des véhicules. Elles sont principalement dédiées à assurer la sécurité. La couche coordination permet de coordonner les opérations de pelotons voisins. Elle reçoit des requêtes de la couche liaison et détermine les manœuvres appropriées qui doivent être mises en œuvre par la couche régulation au niveau des véhicules concernés [8]. Ces manœuvres sont conçues pour assurer le bon fonctionnement du système en mode nominal et garantir la sécurité en cas d'occurrence de défaillances affectant les véhicules ou en présence de conditions dangereuses imprévues issues de l'environnement. Elles consistent par exemple à fusionner deux pelotons, séparer un peloton en deux, effectuer un changement de voie, ou bien faire entrer ou sortir un véhicule du peloton. La couche *physique* ne fait pas partie du contrôleur. Elle fournit à ce dernier les données brutes issues des capteurs installés dans les véhicules et sur l'autoroute et reçoit les commandes calculées par le contrôleur qui doivent être mises en œuvre au niveau des actionneurs des véhicules.

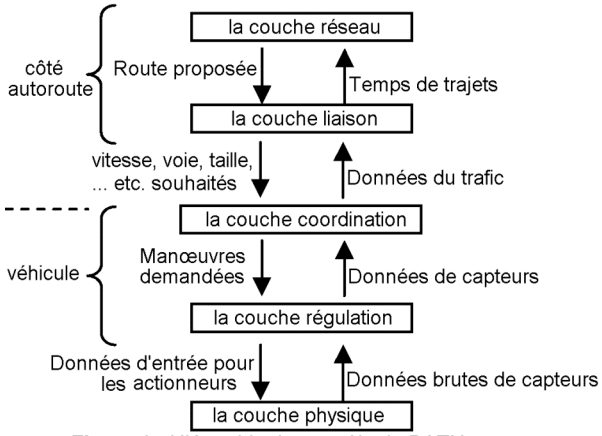

Figure 2 : Hiérarchie de contrôle de PATH

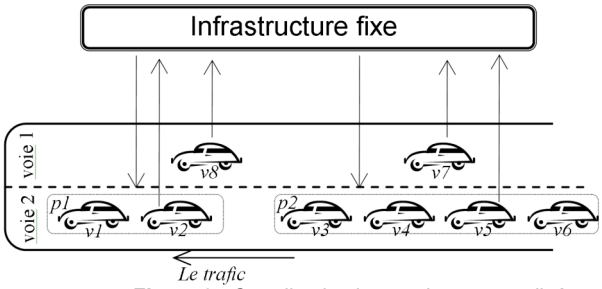

Figure 3 : Coordination inter-peloton centralisée

2.2 Coordination des véhicules

La mise en œuvre de l'architecture de contrôle et des manœuvres nécessite la coordination des véhicules au sein des pelotons et entre pelotons voisins. Différentes méthodes ont été proposées pour la coordination *inter-peloton* et *intra-peloton* ([10], voir chapitre 5). Pour chacune de ces dernières, un modèle de coordination est réalisé, de façon centralisée, ou de façon décentralisée. Dans ce qui suit, nous présentons brièvement les principes de fonctionnement de ces différents modèles de coordination.

2.2.1 Coordination inter-peloton

La coordination inter-peloton centralisée prend en compte l'existence d'une entité de contrôle de trafic installée au niveau de l'infrastructure fixe du côté de l'autoroute [1, 9, ([10], voir chapitre 5)]. Le principe de la coordination inter-peloton centralisée est illustré par la Figure 3 qui

montre un exemple d'autoroute constituée de deux voies et deux pelotons, *p2* suivant *p1* sur la *voie2*, et deux véhicules sur la *voie1*. L'échange entre véhicules est illustré à travers le scénario de fonctionnement en l'absence de fautes suivant :

1. les deux véhicules *v8* et *v7,* venant d'entrer sur l'autoroute (*voie1*), veulent s'insérer sur la *voie2* au sein des pelotons *p1* et *p2* respectivement.
2. simultanément, les véhicules *v2* et *v5* qui font respectivement partie des pelotons *p1* et *p2*, essayent de coordonner des manœuvres pour leur permettre de quitter leurs pelotons, parce qu'ils doivent rejoindre la *voie1* pour sortir de l'autoroute.

Dans cette situation, plusieurs informations sont échangées entre la couche *liaison* et la couche *coordination* des véhicules, afin de coordonner les changements des voies de ces véhicules. À l'étape finale de cette coordination, les décisions sont communiquées aux véhicules voisins, et les manœuvres peuvent être exécutées sans risque. Plus en détail, les quatre véhicules *v7*, *v8*, *v2*, et *v5* proposent des manœuvres *inter-peloton* à l'infrastructure fixe. A partir de ces propositions de manœuvre, la couche *liaison* détermine que *v7* et *v8* sont prioritaires, parce qu'il est plus important de libérer la *voie1* aussi rapidement que possible pour que *v2* et *v5* puissent quitter l'autoroute. Les propositions de *v2* et *v5* seront prises en compte après que les manœuvres de *v7* et *v8* soient finies.

Dans le cas où *la coordination inter-peloton est décentralisée*, la mise en œuvre des manœuvres repose directement sur les leaders des pelotons concernés [11].

2.2.2 Coordination intra-peloton

Dans le cas où *la coordination intra-peloton est centralisée*, les manœuvres impliquant les véhicules d'un peloton sont coordonnées par le *leader* du peloton. Pour maintenir la formation de peloton, le *leader* est la seule entité qui peut donner des ordres. Dans ce cas, les suiveurs appliquent seulement les changements demandés. Prenons comme exemple le cas d'une manœuvre qui consiste à « *faire diviser »* un peloton afin de permettre la sortie d'un véhicule défectueux dans des conditions de sécurité. La réalisation de cette manœuvre implique principalement trois véhicules : le *leader*, le véhicule défectueux, et le véhicule qui le suit (s'il existe). Le véhicule défectueux doit annoncer le besoin d'engager cette manœuvre au leader de son peloton. Le *leader* donne alors les changements de distance inter-véhicules, changement de voie, et calcule le point ou la vitesse à respecter aux véhicules impliqués dans la manœuvre.

Dans le cas où *la coordination intra-peloton est décentralisée*, chaque membre de peloton a la connaissance de la formation de peloton et peut réagir de façon autonome, par la communication directement avec d'autres véhicules. Le *leader* est toujours le représentant du peloton [18], mais uniquement pour la coordination inter-peloton.

2.3 Modes de défaillance et manœuvres en mode dégradé

Plusieurs modes de défaillance ayant différents niveaux de gravité sur la sécurité d'un système d'autoroute automatisée peuvent affecter les véhicules impliqués dans les pelotons [11]. Selon la gravité des défaillances, différentes manœuvres peuvent être envisagées pour garantir la sécurité. Certaines manœuvres peuvent nécessiter de stopper le véhicule défaillant ou l'aider à sortir le plus vite possible de l'autoroute grâce à l'assistance apportée par les véhicules avoisinants. Dans le cas où les défaillances ont un effet mineur vis-à-vis de la sécurité, la sortie du véhicule défectueux de l'autoroute peut être envisagée sans l'assistance d'autres véhicules.

En s'appuyant sur l'étude présentée dans [6, 7], le Tableau 1 présente des exemples de modes de défaillance, leur niveau de gravité, et les manœuvres permettant d'assurer la continuité de service dans des conditions sûres, malgré la présence de ces défaillances. Le niveau de gravité « A » est le plus élevé, correspondant aux défaillances les plus critiques. Les manœuvres considérées pour pallier aux défaillances sont respectivement : *Arrêt Assisté* (AA), *Arrêt d'Urgence* (AU), *Arrêt en Douceur* (AD), *Sortie Immédiate-Escortée* (SI-E), *Sortie Immédiate* (SI) et *Sortie Immédiate-Normale* (SI-N). Ces manœuvres sont décrites en détail dans [15]. Les modes de défaillance et les manœuvres présentées dans le Tableau 1 sont la base des modèles que nous présentons dans la section 4 pour quantifier la sécurité d'un système d'autoroute automatisée.

Tableau 1 : Modes de défaillance, gravité et manœuvres

Mode de défaillance	niveau de gravité		Manœuvre (Stratégie de recouvrement)
MD1 : défaillance des freins	A	A3	Arrêt Assisté (AA)
MD2 : perte de contrôle du papillon des gaz, transmission de puissance en panne.		A2	Arrêt d'Urgence (AU)
MD3 : incapacité de détecter des véhicules dans les voies adjacentes, blocage du moteur.		A1	Arrêt en Douceur (AD)
MD4 : transmission défaillante, pneu à plat	B	B/B2	Sortie Immédiate-Escortée (SI-E)
MD5 : contrôleur d'accélération défaillant, tableau de bord défaillant		B2	Sortie Immédiate (SI)
MD6 : capteurs redondants ou veilleuses défaillantes.	C		Sortie Immédiate – Normale (SI-N)

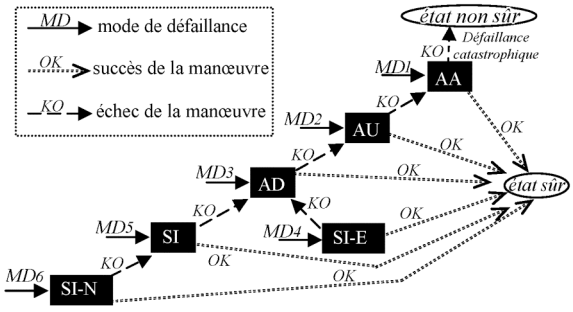

Figure 4 : Manœuvres successives et leur impact sur la sécurité

Généralement, le choix de la stratégie la plus appropriée dépend de deux facteurs [11]: (i) la sévérité de la défaillance et les capacités du véhicule défectueux ; et (ii) les capacités des véhicules voisins. En cas d'occurrence de plusieurs modes de défaillance dans le même véhicule, la stratégie correspondant à la priorité la plus élevée est appliquée. La même logique est aussi suivie quand des modes de défaillance multiples affectent différents véhicules dans le même peloton ou dans des pelotons différents. Les manœuvres associées aux modes de défaillance du niveau de gravité « A » ont la priorité la plus élevée; elles sont suivies des manœuvres associées au niveau « B », puis « C ». Le niveau « A » est scindé en trois sous-classes, A3 ayant la priorité la plus élevée. Une décomposition en deux niveaux est également considérée pour la classe « B ». Cependant, les manœuvres associées aux niveaux B/B2 et B2 ont la même priorité.

Quand une manœuvre échoue, le système évolue vers un état plus dégradé et une manœuvre correspondant au niveau supérieur de priorité doit être tentée pour ramener le système dans un état sûr. Le succès d'une manœuvre dépend de plusieurs facteurs, par exemple, les états des véhicules impliqués dans le peloton, l'état des véhicules du peloton avoisinant (en particulier celui du leader), et la densité du

trafic. L'échec de plusieurs manœuvres successives peut finalement conduire à un état catastrophique. Ceci est illustré sur la Figure 4. Considérons à nouveau l'exemple de la Figure 3 où *v1* est défectueux et doit effectuer la manœuvre SI. Si un autre véhicule effectue déjà une manœuvre plus prioritaire, la demande de manœuvre de *v1* sera refusée. Le véhicule *v1* devra demander des manœuvres de priorité plus élevée (AD, AU et ainsi de suite) jusqu'à ce que sa manœuvre soit acceptée.

En théorie, le nombre de défaillances pouvant affecter un système d'autoroute automatisée peut être élevé. Cependant, plus ce nombre est important, plus la probabilité correspondante sera faible. En considérant la définition introduite dans [7], un système d'autoroute automatisée est jugé sûr s'il ne provoque pas de *catastrophe* suite à l'occurrence d'au plus trois défaillances successives proches dans le temps et l'espace. Une *catastrophe* correspond à une collision à grande vitesse.

En fait, il n'y a pas de garantie absolue qu'il n'y aura pas d'accident ; il peut y avoir des situations où il est impossible de trouver une stratégie de recouvrement adaptée. C'est le cas par exemple quand un véhicule est affecté par la combinaison des trois défaillances suivantes : freins en panne, blocage du moteur, et transmission de puissance en panne. Si le véhicule ne peut ni freiner, ni se diriger, ni demander l'aide, il peut être impliqué dans une collision à grande vitesse. Un accident peut aussi survenir avec moins de trois défaillances. C'est le cas par exemple du scénario suivant où on considère deux agents libres qui se suivent sur la même voie. Si les deux véhicules ont des freins en panne, alors un accident peut survenir.

Il faudrait que la probabilité que de telles situations se produisent soit la plus faible possible. L'approche de modélisation présentée dans la section suivante a pour objectif de permettre la quantification de la sécurité en prenant en compte différentes combinaisons possibles de défaillances affectant les véhicules. En prenant en compte la classification des modes de défaillance mentionnée dans le Tableau 1 en terme de gravité, nous considérons les scénarios de défaillances catastrophiques incluant jusqu'à trois défaillances dans un voisinage, et pas plus d'une défaillance de niveau de gravité « A ». Le terme "*voisins"* indique les véhicules pouvant apporter une assistance au véhicule défectueux, par exemple pour l'aider à sortir de l'autoroute.

3. Description de l'approche de modélisation

Rappelons que notre objectif est de faire un modèle qui nous permettra d'obtenir des mesures quantitatives caractérisant la sécurité du système d'autoroute automatisée et d'analyser l'impact de différents paramètres du système vis-à-vis de la sûreté de fonctionnement. La modélisation doit prendre en compte les modes de défaillance affectant chaque véhicule impliqué dans les scénarios considérés mais aussi les dépendances entre véhicules résultant des manœuvres utilisées pour ramener le système dans un état sûr. Comme nous l'avons expliqué dans la section 2, les conditions de réussite de ces manœuvres dépendent de l'état des véhicules impliqués. L'identification de ces derniers dépend de la configuration des pelotons et du mode de coordination considéré au sein des pelotons et entre les pelotons voisins (centralisée ou décentralisée). Il est important de noter que les configurations des pelotons évoluent dans le temps, par exemple suite à la sortie ou l'entrée de véhicules au niveau de l'autoroute, la fusion ou la division de pelotons.

Les techniques de modélisation analytique basées sur les réseaux de Petri stochastiques généralisées (RdPSG) et les chaînes de Markov sont bien appropriées pour effectuer des évaluations de sûreté de fonctionnement. En employant ces techniques, le système est d'abord décrit à un niveau élevé d'abstraction. Des hypothèses simplificatrices sont généralement nécessaires pour obtenir des modèles utilisables. Un des aspects critiques qui doivent être abordés pendant la modélisation est la maîtriser de la complexité des modèles pendant la construction et le traitement des modèles. Dans la suite nous présentons une vue globale de l'approche que nous avons développée et des exemples de modèles élaborés dans le cadre de cette approche. Nous présentons ensuite quelques exemples de résultats issus du traitement des modèles et des études de sensibilité permettant de comparer en particulier différentes stratégies de coordination intra-peloton (voir section 2.2).

3.1 Présentation de l'approche

L'approche que nous avons développée suit une démarche compositionnelle. Elle se déroule en trois étapes :

1. identifier les différentes configurations de pelotons à prendre en compte et modéliser l'évolution dynamique du système entre ces configurations. L'objectif de cette étape est d'évaluer la probabilité de séjour du système dans ces différentes configurations.
2. construire pour chaque configuration un modèle de sûreté de fonctionnement en RdPSG qui décrit les modes de défaillance affectant les véhicules concernés, les manœuvres associées ainsi que leur impact sur la sécurité. Cette étape se termine par l'évaluation d'une mesure quantitative caractérisant la sécurité du système quand ce dernier évolue dans cette configuration.
3. évaluer une mesure globale de la sécurité du système par composition des résultats obtenus aux deux premières étapes.

Soit *NC* le nombre de configurations considérées et π_i la probabilité en régime stationnaire que le système soit dans la configuration C_i. On note *S(t)* la mesure caractérisant la sécurité globale du système d'autoroute automatisée et $S_{Ci}(t)$ la sécurité de la configuration C_i.

S(t) peut être évaluée à partir de la combinaison des mesures $S_{Ci}(t)$ pondérée par les probabilités π_i comme indiqué par l'équation (1).

$$S(t) = \sum_{i=1}^{NC} \pi_i S_{C_i}(t) \qquad (1)$$

$\overline{S}(t)$, la probabilité que le système atteigne un état non sûr suite à l'occurrence d'une défaillance catastrophique, est donnée par :

$$\overline{S}(t) = 1 - S(t) = \sum_{i=1}^{NC} \pi_i \overline{S}_{C_i}(t) \qquad (2)$$

Dans la suite, nous décrivons plus en détail les deux premières étapes de notre approche. Des exemples illustrant l'approche de modélisation et les mesures évaluées sont présentées dans la section 4.

3.2 Modélisation des configurations du système

Nous supposons un nombre maximum, fixe, de véhicules traversant l'autoroute et nous identifions les configurations qui sont pertinentes pour modéliser la sécurité du système. Une configuration est déterminée par le nombre de pelotons, leurs positions relatives et le nombre de véhicules par peloton. Le passage d'une configuration à une autre résulte de l'entrée ou de la sortie d'un véhicule dans un peloton.

La Figure 5 donne un exemple simple en considérant une autoroute constituée de deux voies et deux pelotons constitués de deux véhicules au maximum chacun. Nous obtenons six configurations différentes possibles. Le séjour du système dans les différentes configurations et la

transition entre ces configurations peuvent être modélisés par un graphe d'états comme c'est illustré sur la Figure 5-b. Chacune des configurations identifie un état de l'autoroute automatisée à un instant donné. Les transitions entre les configurations sont provoquées par l'occurrence des événements « rejoindre » ou « quitter » un peloton.

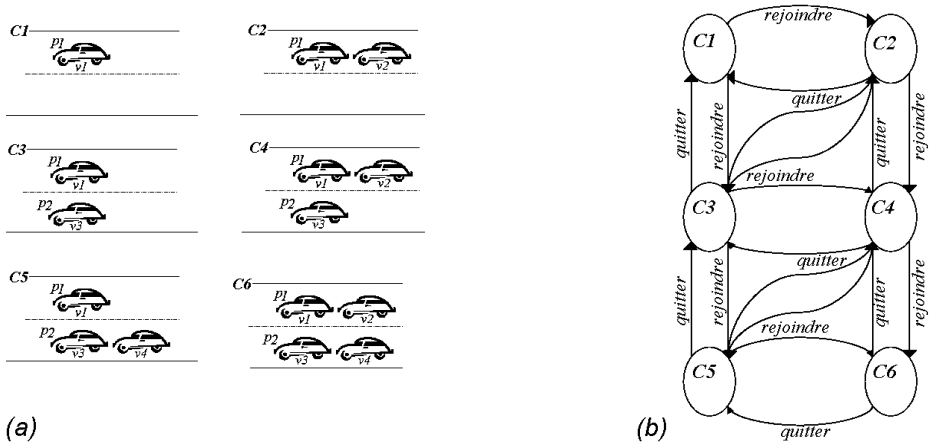

Figure 5 : Configurations pour une autoroute automatisée constituée de deux pelotons et deux véhicules maximum par peloton

Le type de modèle associé à la Figure 5-b dépend des hypothèses relatives aux distributions de probabilité caractérisant l'occurrence des transitions entre les configurations. La caractérisation de ces distributions peut s'appuyer sur la simulation de différents scénarios de trafic sur une autoroute automatisée. Dans le cas où ces distributions sont exponentielles, nous obtenons une chaîne de Markov. Nous pouvons alors évaluer les probabilités de séjour du système dans les différentes configurations correspondant aux paramètres π_i de l'équation (1) à partir du traitement de ce modèle.

3.3 Modèles RdPSG pour chaque configuration

Dans cette section, nous présentons l'approche proposée pour élaborer les modèles RdPSG caractérisant la sécurité du système d'autoroute automatisée quand ce dernier est dans une configuration donnée. Nous commençons d'abord par décrire le modèle d'un véhicule et nous détaillerons ensuite l'élaboration du modèle pour le système entier.

3.3.1 Modèle RdPSG pour un véhicule

Le modèle RdPSG décrivant le comportement d'un véhicule a pour objectif de modéliser l'impact sur la sécurité des modes de défaillance du véhicule et des manœuvres associées, présentés dans le Tableau 1. Au stade actuel de nos travaux, nous n'avons pas pris en compte la défaillance de l'infrastructure fixe. Le modèle que nous avons développé est constitué de six RdPSG élémentaires interconnectés. Chaque RdPSG élémentaire modélise l'occurrence d'un mode de défaillance correspondant à une classe de gravité donnée et la manœuvre associée. Comme illustré sur la Figure 6, chaque réseau élémentaire est constitué de cinq places, deux transitions temporisées, et deux transitions immédiates.

Les deux transitions temporisées sont caractérisées par des distributions exponentielles à taux constant :

- La première transition temporisée décrit l'occurrence du mode de défaillance considéré ; nous noterons par λi le taux correspondant ;
- La deuxième transition temporisée décrit le déroulement de la manœuvre associée au mode de défaillance ; nous noterons par γ_i le taux correspondant ($1/\gamma_i$ correspond à la durée moyenne de l'exécution de la manœuvre).

La place CC_i avec un jeton identifie un état initial à partir duquel le mode de défaillance décrit par le taux λ_i peut être activé. Le franchissement de cette transition conduit au marquage de la place LM_i correspondant au lancement de la manœuvre associée. Quand la manœuvre arrive à son terme (la transition est franchie), un jeton est placé dans la place FM_i. Si la manœuvre réussit, la transition instantanée t_{ok} est immédiatement tirée conduisant au marquage de la place *OK*. L'échec de la manœuvre est modélisé par la transition instantanée t_{ko} et le marquage de la place *KO*. Des prédicats sont associés aux transitions t_{ok} et t_{ko} pour indiquer les conditions permettant le franchissement de ces transitions en fonction de l'état des autres véhicules impliqués dans la manœuvre (voir Section 2.3).

La Figure 7 présente le modèle RdPSG d'un véhicule qui prend en compte l'ensemble des modes de défaillance et des manœuvres associées identifiées dans le Tableau 1. Les niveaux de gravité correspondant aux modes de défaillance sont explicitement identifiés. Les RdPSG élémentaires associés aux différentes manœuvres sont interconnectés par l'intermédiaire des transitions immédiates t_{12}, t_{24}, t_{34}, et t_{56}. Ces transitions sont franchies quand la manœuvre associée échoue, conduisant ainsi au lancement de la manœuvre de priorité immédiatement supérieure pour ramener le système dans un état sûr. En bout de chaîne, c'est la manœuvre 'AA' qui doit être exécutée. L'échec de cette manœuvre entraîne une défaillance catastrophique du véhicule.

En cas d'occurrence de défaillances multiples au sein d'un véhicule, la manœuvre correspondant au mode de défaillance le plus grave est lancée. Par conséquent, la manœuvre de priorité inférieure qui était en cours sera avortée. Ces priorités sont gérées par le biais de prédicats associés aux transitions temporisés γ_i et aux transitions immédiates en sortie des places t_{ok} et t_{ko}. Ces prédicats consistent à définir les conditions de sensibilisation de ces transitions en fonction du marquage des places FM_i.

3.3.2 Modèle RdPSG pour le système global

Le modèle RdPSG décrivant le comportement du système d'autoroute pour la configuration considérée est obtenu en associant un modèle RdPSG à chaque véhicule. Les dépendances entre les modèles des différents véhicules sont exprimées par des prédicats qui déterminent les priorités pour l'exécution des manœuvres et les conditions du succès ou d'échec des manœuvres en fonction des états des véhicules concernés. Dans le cas où une manœuvre de priorité supérieure a besoin d'être réalisée par un véhicule voisin, toutes les manœuvres en cours sont suspendues jusqu'à la fin de la réalisation de cette manœuvre. Les manœuvres suspendues reprennent ensuite leurs exécutions.

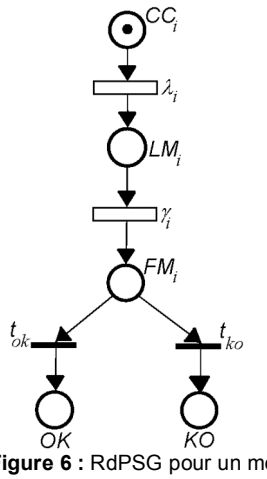

Figure 6 : RdPSG pour un mode de défaillance

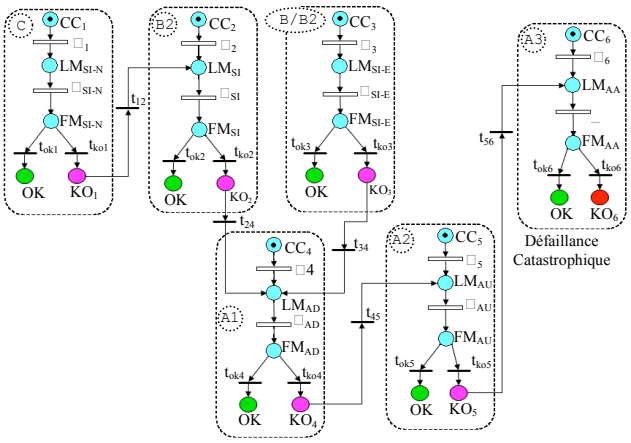

Figure 7 : RdPSG d'un véhicule

Le Tableau 2 montre les manœuvres et les véhicules *voisins* concernés pour chaque classe de mode de défaillance, selon la méthode de coordination intra-peloton considérée (centralisée ou décentralisée), en distinguant si le véhicule défectueux est un leader (*L*) ou un suiveur. Les prédicats associés aux transitions t_{ok} et t_{ko} sont définis en fonction des états des véhicules contribuant à la manœuvre.

Tableau 2: Modes de défaillance et manœuvres associées

Classe de gravité de la défaillance		Manœuvre	Véhicules contribuant à la manœuvre			
			Intra-peloton centralisé		Intra-peloton décentralisé	
			VD = leader ou agent libre	VD ≠ {leader, *AL*}	VD = leader ou agent libre	VD ≠ {leader, *AL*}
A	A3	AA	*VD, v.PV, s.VD*	*VD, L, v.PV, s.VD*	*VD, v.PV, s.VD*	*VD, v.PV, s.VD*
	A2	AU	*VD, v.PV, s.VD, d.VD*	*VD, L, v.PV, s.VD, d.VD*	*VD, v.PV, s.VD, d.VD*	*VD, v.PV, s.VD, d.VD*
	A1	AD	*VD, v.PV, s.VD, d.VD*	*VD, L, v.PV, s.VD, d.VD*	*VD, v.PV, s.VD, d.VD*	*VD, v.PV, s.VD, d.VD*
B	B/B2	SI-E	*VD, v.PV, s.VD, d.VD*	*VD, L, v.PV, s.VD, d.VD*	*VD, v.PV, s.VD, d.VD*	*VD, v.PV, s.VD, d.VD*
	B2	SI	*VD, v.PV, s.VD*	*VD, L, v.PV, s.VD*	*VD, v.PV, s.VD*	*VD, v.PV, s.VD, d.VD*
C		SI-N	*VD, v.PV, s.VD*	*VD, L, v.PV, s.VD*	*VD, v.PV, s.VD*	*VD, v.PV, s.VD*

L : Leader d'un peloton
AL : Agent libre
VD : Véhicule défectueux
v.PV : Véhicule du peloton voisin
s.VD : Suiveur du véhicule défectueux
d.VD : Véhicule devant le véhicule défectueux

Considérons un exemple simple d'une configuration d'autoroute automatisée qui contient deux pelotons *p1* et *p2* et trois véhicules (voir Figure 8) : (*v1*, *v2*) constituent le peloton *p1* et *v3* est un agent libre (*p2*). Nous faisons l'hypothèse que les coordinations intra-peloton et inter-peloton sont centralisées. Considérons le cas où le véhicule *v2* est affecté par une défaillance du contrôleur d'accélération qui correspond à un niveau de gravité B2 nécessitant de lancer la manœuvre *SI « Sortie-Immédiate »*. Dans ce cas, le véhicule *v2* doit contacter son leader *v1* pour l'informer de son besoin d'effectuer cette manœuvre qui nécessite la contribution de *v3*. Cette manœuvre sera couronnée de succès si les deux véhicules *v1* et *v3* sont dans un état de bon fonctionnement et que la communication est fiable.

Le modèle RdPSG complet correspondant à cet exemple est illustré sur la Figure 9 où chaque RdPSG représente un véhicule de cette configuration. Les flèches représentent schématiquement les interconnections entre les RdPSG des trois véhicules pour la gestion des priorités entre les manœuvres qui sont exprimées par des prédicats au niveau des transitions temporisées γ_i.

Il est à noter que pour calculer la mesure de sécurité du système correspondant à cette configuration, il suffit d'évaluer à partir du modèle RdPSG complet la probabilité que l'une des places correspondant à l'occurrence de la défaillance catastrophique suite à l'échec d'une manœuvre « AA » soit marquée. Nous utilisons l'outil SURF-2[2], développé au LAAS-CNRS, pour le traitement des modèles RdPSG.

4. Résultats et études de sensibilité

Cette section montre des exemples de résultats issus du traitement des modèles présentés dans les sections précédentes ainsi que des études de sensibilité permettant d'observer l'influence de différents paramètres sur la sécurité d'un système d'autoroute automatisée. L'analyse porte essentiellement sur l'influence du taux λ associé aux modes de défaillance des véhicules, le nombre de véhicules *n,* et les méthodes de coordination intra-peloton (centralisée ou décentralisée). Dans ce qui suit, les résultats concernent le cas où la coordination inter-peloton est centralisée. L'objectif est d'illustrer le type de résultats qu'on peut obtenir avec l'approche de modélisation proposée et d'analyser des tendances plutôt que d'obtenir des estimations réalistes de la sécurité dans l'absolu.

Les configurations du système d'autoroute considérées dans les exemples sont celles décrites dans la Figure 5. Nous faisons l'hypothèse que les événements « rejoindre un peloton » et « quitter un peloton » sont décrits par des distributions exponentielles (à taux constant). Nous avons considéré la même valeur numérique égale à 6.7 10^{-2}/hr correspondant à un événement toutes les 4 minutes. Dans ce cas, le modèle décrivant les configurations est une chaîne de Markov. Il est facile d'obtenir les probabilités stationnaires π_i correspondant à chaque configuration. Le nombre de configurations à prendre en compte dépend du nombre de véhicules *n* considéré.

Les résultats sont basés sur les valeurs suivantes pour les taux de défaillance relatifs aux modes de défaillance identifiés dans le Tableau 2, en considérant différentes valeurs pour le paramètre λ correspondant au taux d'activation associé à une source de défaillance élémentaire : $\lambda_1 = 2\lambda$; $\lambda_2 = 3\lambda$; $\lambda_3 = 2\lambda$; $\lambda_4 = 2\lambda$; $\lambda_5 = 2\lambda$; $\lambda_6 = \lambda$.

[2] Outil d'évaluation de la sûreté de fonctionnement par chaînes de Markov et réseaux de Petri Stochastiques http://www.laas.fr/surf/what-fr.html.

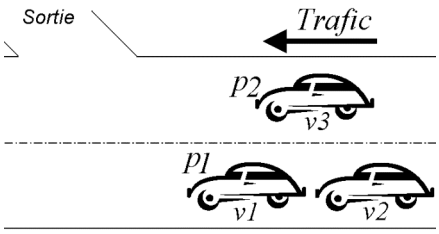

Figure 8 : Exemple de configuration

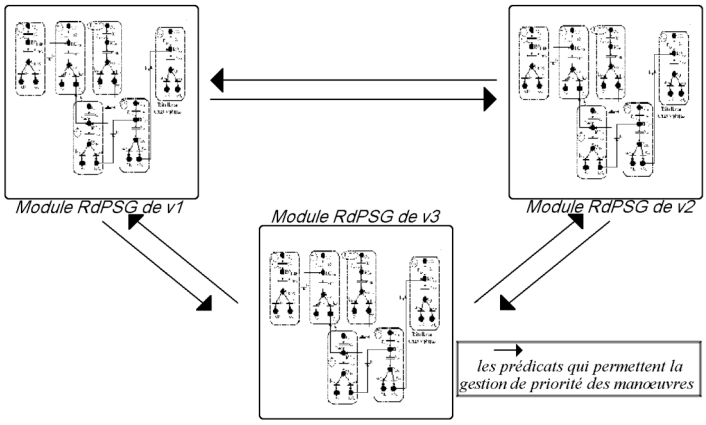

Figure 9 : Modèle RdPSG associé

4.1 Influence du nombre de véhicules *n* et du taux de défaillance λ

Les courbes de la Figure 10 donnent l'évolution de $\overline{S}(t)$ (voir équation 2) en fonction du temps, pour une durée de trajet variant de 6 minutes à 10 heures, et en considérant trois valeurs différentes de *n*, le nombre maximal de véhicules impliqués dans les configurations de système d'autoroute considérées, pour une coordination intra-peloton centralisée. Pour une valeur donnée *n*, on peut observer que le risque de défaillances catastrophiques augmente avec la durée du trajet, ce qui est prévisible. Par exemple, pour une durée de trajet courte (6 minutes), l'insécurité est de l'ordre de 10^{-7} alors qu'elle est de deux ordres de grandeur plus élevée pour des trajets de 10 heures.

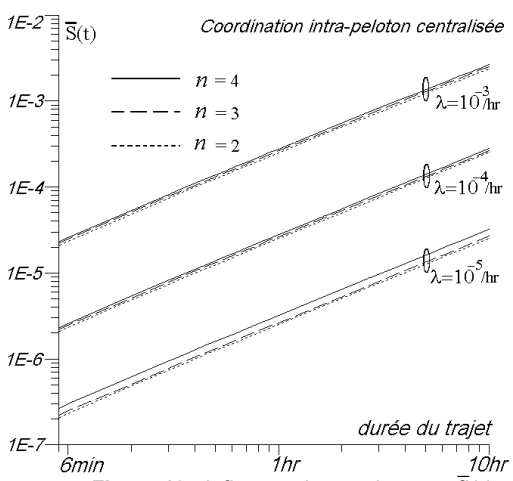

Figure 10 : Influence de *n* et de λ sur $\overline{S}(t)$

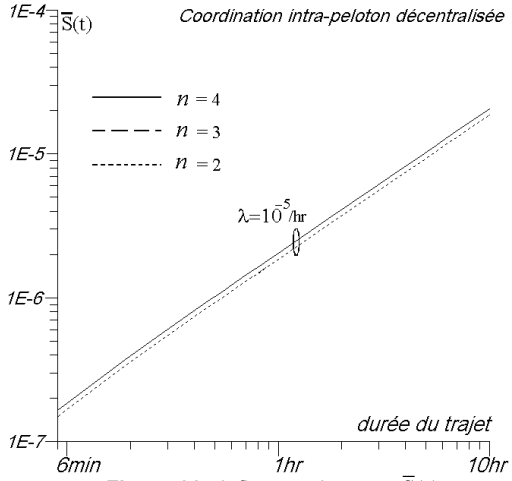

Figure 11 : Influence de *n* sur $\overline{S}(t)$

Par ailleurs, l'augmentation du nombre de véhicules diminue la sécurité du système, car le nombre de sources de défaillance susceptibles d'affecter la sécurité augmente en conséquence. Cette augmentation reste faible pour les valeurs que nous avons considérées. Par exemple, pour des trajets de 10 heures et un taux de défaillance $\lambda = 10^{-3}$/hr, l'insécurité est de 2.66 10^{-3}/hr pour $n = 4$ et 2.38 10^{-3}/hr pour $n = 2$.

Comme illustré sur la Figure 10, nous observons des tendances similaires pour des taux de défaillance λ plus élevés. La probabilité d'atteindre un état non sûr augmente avec la valeur du taux de défaillance. Par exemple, pour des trajets de 10 heures, une augmentation du taux de défaillance d'un ordre de grandeur conduit à une dégradation de la sécurité du même ordre de grandeur.

4.2 Influence de la méthode de coordination intra-peloton

Les résultats précédents correspondent au cas où les coordinations inter-peloton et intra-peloton sont centralisées. Dans cette section, nous analysons de façon comparative l'impact sur la sécurité du choix d'une stratégie de coordination intra-peloton décentralisée.

La Figure 11 présente l'évolution de $\overline{S}(t)$ en fonction de la durée du trajet. Cette figure montre que *n* a moins d'impact sur la sécurité dans le cas d'une communication intra-peloton décentralisée que centralisée pour $\lambda = 10^{-5}$/hr. Pour des valeurs plus grandes de λ,*n* n'a pas d'impact significatif. Le choix d'une coordination décentralisée se traduit par une amélioration de la sécurité. Ce résultat est illustré sur la Figure 12 pour $n = 4$ et trois valeurs de λ. L'amélioration varie entre 16% et 20% selon la valeur du taux λ, et la durée du trajet.

5. Conclusion

Certes, l'évolution vers une conduite automobile automatisée sur autoroute améliore la sécurité globale puisqu'elle fait intervenir les véhicules voisins d'un véhicule défectueux pour ramener l'ensemble vers un état sûr. Cependant, le risque d'accident n'est pas nul pour autant. Cet article propose une approche d'évaluation du risque d'accident dans un environnement de conduite coopérative sur autoroute, faisant intervenir des communications entre véhicules voisins de façon centralisée ou décentralisée. Nos modèles prennent en compte les modes de défaillance affectant les véhicules, leur niveau de gravité et les manœuvres permettant de ramener le système dans un état sûr. L'approche est conçue pour prendre en compte l'évolution des configurations des pelotons durant le trajet. Elle est basée sur les RdSPG.

Elle est modulaire et compositionnelle, en développant des modèles génériques caractérisant le comportement des véhicules qu'on peut interconnecter facilement quand une nouvelle configuration ou un nombre de véhicules plus important doit être pris en compte.

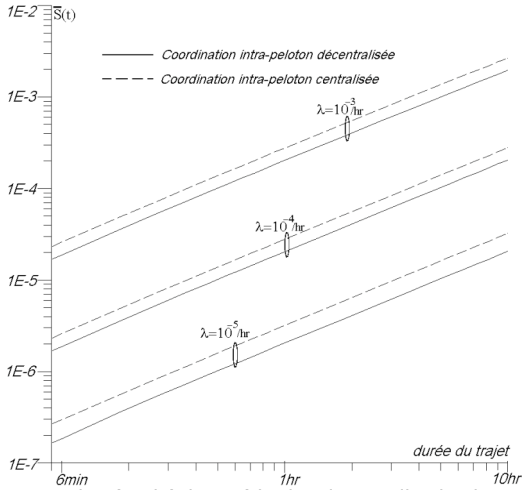

Figure 12 : Impact sur la sécurité des méthodes de coordination intra-peloton (n = 4)

Pour illustrer l'approche et le type de résultats que l'on peut obtenir, nous avons considéré des exemples simples. Nous avons effectué des études de sensibilité permettant d'analyser l'impact de quelques paramètres sur la sécurité d'un système d'autoroute automatisée : les taux associés aux modes de défaillance affectant les véhicules, le nombre de véhicules, et les méthodes de coordination intra-peloton. En particulier, les analyses que nous avons effectuées nous ont permis de quantifier et d'analyser de façon comparative le gain en terme de sécurité que l'on peut espérer avec le système étudié.

Nous avons considéré un cadre de modélisation RdPSG en supposant que les processus intervenant dans le modèle suivent des distributions exponentielles. Ces hypothèses peuvent s'avérer discutables dans certains contextes, en particulier pour ce qui concerne le processus de *sortie* ou d'*entrée* dans un peloton qui dépend fortement des caractéristiques de mobilité des utilisateurs. Les extensions envisagées pour nos travaux ont pour objectif d'étendre les modèles actuels pour prendre en compte d'autres types de coordination caractérisant les méthodes d'interaction entre les véhicules. D'autres extensions envisageables concernent la prise en compte de comportements de l'environnement du domaine ad-hoc.

Nous envisageons également la prise en compte de scénarios impliquant un nombre significatif de véhicules et de pelotons, et ensuite la généralisation de l'approche à des scénarios plus complexes. Une attention particulière sera également consacrée à une meilleure prise en compte de la mobilité des véhicules dans les modèles, en nous appuyant par exemple sur la simulation.

6. Références

[1] S. V. Bana, "Coordinating Automated Vehicles via Communication," Institute of Transportation Studies, University of California, Berkeley, Rapport No UCB-ITS-PRR-2001-20 2001.

[2] R. E. Fenton, G. C. Melocik, and K. W. Olson, "On the Steering of Automated Vehicles: Theory and Experiment," IEEE Transaction on Automatic Control, vol. AC-21, pp. 306-315, Juin 1976.

[3] R. E. Fenton and R. J. Mayhan, "Automated Highway Studies," in IEEE Trans. on Vehicular Technology, vol. 40., 1991, pp. 306-315.

[4] T. Fraichard, "Cybercar: l'alternative à la voiture particulière," Navigation (Paris), vol. 53, n° 209, pp. 53-74, Janvier 2005.

[5] Y. Furukawa, "Status and Future Direction of Intelligent Drive Assist Technology," IEEE Intelligent Trans. Systems, pp. 113-118, 2000.

[6] D. N. Godbole, J. Lygeros, E. Singh, A. Deshpande, and A. E. Lindsey, "Towards a Fault Tolerant AHS Design Part II: Design and Verification of Communication Protocols," Institute of Transportation Studies, University of California, Berkeley, Rapport No UCB-ITS-PRR-96-15 1996.

[7] A. Hitchcock, "A Specification Of An Automated Freeway With Vehicle-borne Intelligence," Institute of Transportation Studies, University of California, Berkeley, Rapport UCP-ITS-PRR-92-18 1992.

[8] R. Horowitz, C.-W. Tan, and X. Sun, "An Efficient Lane Change Maneuver for Platoons of Vehicles in an Automated Highway System," Institute of Transportation Studies, University of California, Berkeley, UCB-ITS-PRR-2004-16 4239, May 2004.

[9] R. W. Hall, "Longitudinal and lateral throughput on an idealized highway," Transport Science, vol. 29, pp. 118-127, 1995.

[10] S. Hallé, "Automated Highway Systems: Platoons of Vehicles Viewed as a Multiagent System," Mémoire de Maître ès Sciences, Faculté des études supérieures de l'Université Laval. Québec, 2005.

[11] S. Hallé, B. Chaib-draa, and J. Laumonier, "Car Platoons Simulated as a Multiagent System," Agent Based Simulation, vol. 4, pp. 57-63, Mars 2003.

[12] S. Masayasu, S. Shigeki, U. Ken'ya, and M. Hiroshi, "Design of Lane-Keeping Control with Steering Torque Input," Transaction of Society of Automotive Engineers of Japan, pp. 163-168, vol. 53, n° 1, 2003.

[13] J.-C. Laprie, Guide de la Sûreté de Fonctionnement. Édition Cépaduès, Mai 1995.

[14] S. Mammar, "Contrôle latéral assisté et automatisé des véhicules : approches par commandes robustes," in Mémoire d'Habilitation à diriger les recherches. Évry, France: Université d'Évry, 2001.

[15] S. Sastry, R. Horowitz, and J. K. Hedrick, "Design Of Fault Tolerant Control Systems For AHS," Institute of Transportation Studies, University of California, Berkeley, Rapport No UCB-ITS-PRR-98-16 1998.

[16] T. Sakaguchi, A. Uno, S. Kato, and S. Tsugawa, "Cooperative Driving of Automated Vehicles with Inter-Vehicle Communications," In Proceedings of IEEE Intelligent Vehicles Symposium 2000, Dearbsorn, MI, USA 2000.

[17] M. Tsuji, R. Shirato, H. Furusho, and K. Akutagawa, "Estimation of Road Configuration and Vehicle Attitude by Lane Detection for Lane Keeping system," Society of Automotive Engineers, pp. 45-51, 2001.

[18] P. Varaiya, "Smart Cars on Smart Roads: Problems of Control," IEEE Trans. on Automatic Control, vol. 38, pp. 195-207, février 1993.