Nom : Siegfried SOLDANI

Directeur de thèse : Michel COMBACAU
Encadrant industriel : Jérôme THOMAS
Encadrant : Audine SUBIAS

Problématique :

Au cours de la dernière décennie, les systèmes automobiles se sont de plus en plus complexifiés. Les systèmes électroniques se sont développés et sont devenus des éléments indispensables aux véhicules. Mais cette avancée technologique ne s'est pas accompagnée de sa maîtrise. Ainsi de nombreux problèmes liés à l'électronique sont apparus, et notamment les problèmes liés aux défauts fugitifs et intermittents. A l'heure actuelle, ces problèmes ne sont pas résolus dans la mesure où les outils de diagnostic que l'on retrouve dans les différents garages sont des outils débarqués et par conséquent ils ne peuvent diagnostiquer un défaut, une panne que si elle est persistante. L'idée est donc d'embarquer un module dans la voiture dans le but de détecter ces défauts fugitifs et intermittents, voir de les localiser si possible ou d'apporter le maximum d'informations sur le contexte d'apparition de ces défauts.
Le système que nous considérons est constitué de différents composants reliés entre eux par l'intermédiaire d'un réseau. Notre idée est d'établir un modèle de bon fonctionnement, donc sans prendre en compte les états de défaillance possibles, d'une fonction (ou d'une tâche) à réaliser par ce système. Nous pouvons suivre l'évolution de l'état d'une fonction au travers des échanges de messages qui circulent entre les composants sur le réseau de communication. Nous considérerons donc les messages comme des événements observables. Nous connaissons l'état du système, les événements reçus, les événements attendus, et les états suivants liés à ces événements. Il y a détection si l'événement observé est incohérent avec ceux attendus. Dans un contexte perturbé, on peut considérer que l'événement circulant sur le réseau n'est pas intègre. Il faut alors supposer que l'événement perçu n'est pas reconnu tant qu'il n'est pas confirmé par des événements suivants. Nous pouvons ainsi définir une fenêtre comportant un certain nombre d'événements dont l'occurrence n'est pas encore confirmée. Ces événements seront remis en cause lors de la détection d'une incohérence. Nous pourrons ainsi prendre en compte l'absence d'événements (ce sont des événements ``potentiellement inobservables'') ou bien le fait qu'un message se soit inséré de façon inopinée entre deux autres messages ou une combinaison des deux. Une autre approche pourra consister à obtenir un modèle représentant ce genre de fautes et ainsi pouvoir suivre en ligne l'évolution du comportement.

Objectif des travaux (dans quel cadre)

Le sujet de cette thèse s'intègre dans le cadre d'une convention CIFRE entre le LAAS et la société ACTIA, qui se sont regroupés avec l'IRIT, au sein du laboratoire commun Autodiag. Ce laboratoire a pour but de définir de nouvelles approches et de nouveaux outils pour le diagnostic automobile. L'objectif de cette thèse est d'établir une nouvelle méthode de détection et de diagnostic pour les systèmes à événements discrets dans le cadre des systèmes embarqués.

Contexte et positionnement :

Ainsi l'apparition de messages erronés sur le bus peut provoquer une défaillance du système et de son fonctionnement. On retrouve par exemple ce genre de réseaux sur le nouvel airbus A380 (réseau AFDX) ou encore sur toutes les automobiles (réseau CAN,VAN), ou autres moyen de transports,…
C'est pourquoi les trois acteurs que sont le LAAS, l'IRIT et ACTIA se sont réunis pour résoudre certains problèmes que le domaine du diagnostic automobile rencontre à l'heure actuelle. En effet, la préoccupation des constructeurs automobiles est d'accroître le confort et la sécurité dans les véhicules. Ainsi de nouvelles fonctionnalités telles que le système antiblocage des roues ou bien des sièges chauffants sont apparues pour les systèmes automobiles, ou encore la gestion de rampe d'accès pour handicapés dans les autobus. Cette augmentation des nouvelles fonctionnalités s'accompagne d'une explosion de l'électronique embarquée dans les systèmes de transport. Pour une raison évidente de

coût, il a été développé un réseau standard, appelé réseau CAN sur lequel sont reliés les différents composants électroniques du véhicule. Certains de ces composants, appelé calculateurs, dialoguent entre eux pour accomplir une « fonction » du véhicule (e. g. la gestion de rampe d'accès pour handicapés).
Les défauts fugitifs et intermittents peuvent être la cause de messages erronés. Un modèle comportemental de ces fonctions peut être obtenu à partir des données de conceptions du constructeur. Ainsi, on peut décrire le comportement d'une fonction comme les états successifs dans lesquels elle se trouve. Ce comportement pourra être modélisé par un système à événements discrets du type réseau de Petri. Nous nous dirigerons donc vers un modèle comportemental plutôt qu'un modèle structurel qui serait basé sur l'architecture du véhicule, le but étant d'être indépendant de l'architecture matérielle en raison de son évolution constante. En outre, l'évolution de la technologie dans le domaine automobile croit fortement depuis ces dernières années, et par conséquent elle s'accompagne de l'apparition continuelle de nouvelles fautes. C'est pourquoi il est évident que la modélisation de fautes fugitives et intermittentes est impossible, de même que la modélisation de l'ensemble des fautes dues à l'électronique qui donnerait un ensemble non-exhaustif et donc non intéressant du point de vue application. Néanmoins, si un tel modèle de faute existe, il faudra le prendre en compte.
Beaucoup de travaux ont été menés sur le diagnostic à base de modèles pour des systèmes à événements discrets. Nous retrouvons les modèles à base de réseaux de Petri ([1],[2],[4],[6]), les corrélations d'alarmes ([3],[7]), l'approche diagnostiqueur ([5],[8],[9]),… mais dans l'ensemble de ces méthodes, le système modélisé prend en compte les fautes (i.e. que le modèle intègre des états de défaillances). Généralement, cette défaillance est détectée par un capteur et l'événement associé est une alarme qui est considérée comme un événement observable.

Etat d'avancement des travaux :

L'objectif est donc de surveiller les messages circulant sur le bus et de les comparer à un modèle de bon fonctionnement de la fonction à surveiller.
Le modèle du comportement de la fonction décrit ses différents états. Il est dérivé des modèles utilisés lors de la conception du véhicule. Les réseaux de Petri ont été choisis car ils décrivent bien les synchronisations et les parallélismes et possèdent un formalisme rigoureux. Leur formalisme est également bien adapté pour décrire les mécanismes de détection et de diagnostic. Ensuite, pour qu'une fonction soit réalisée, elle a besoin de nombreuses informations provenant des capteurs, des calculateurs, d'autres fonctions,… informations qui ne sont pas toutes observables. A priori, seules les informations circulant sur le bus de données seront disponibles. Nous projetons donc notre modèle sur l'ensemble des observables c'est-à-dire des messages circulant sur le bus de communication. Cette projection rend difficile la discrimination des différents états de la fonction. Nous pouvons donc discerner un état ou un groupement d'état. À partir de ce modèle et des informations reçues, nous pourrons déterminer un état (voire un ensemble d'états), et par conséquent connaître les événements précédents et les événements que l'on est supposé attendre.
La deuxième étape consiste à formaliser le mécanisme de détection. Ce mécanisme explicite la détection d'un événement incohérent avec l'ensemble des événements attendus par le modèle L'événement ainsi détecté ne correspond pas nécessairement à l'événement issu d'une défaillance. En effet, l'événement issu de la défaillance est susceptible de faire évoluer le modèle dans une autre trajectoire avant de détecter une incohérence. Ainsi, la détection d'une incohérence ne se produira qu'après avoir reçu un certain nombre d'événements. Nous supposons donc que l'événement reçu n'est pas vrai tant qu'il n'y a pas eu confirmation de la part des événements suivants.
L'application de notre sujet se fait dans un contexte embarqué. Il a fallu trouver des approches qui nous permettent de réduire au minimum les calculs en ligne. C'est pourquoi, actuellement nous avons travaillé sur une approche qui consiste à prendre en considération l'ensemble des insertions et des absences d'événements possibles et à les représenter dans un modèle. Il nous suffit de suivre en ligne l'évolution de ce ou ces modèle(s) pour avoir de façon immédiate, lors de la détection, l'ensemble des explications possibles à l'incohérence observée. Pour ce travail, nous nous sommes dirigés vers les approches diagnostiqueurs qui utilisent des modèles de fautes. Ces modèles de fautes sont la représentation d'une ou des défaillance(s) **connue(s)** à travers les observations qui peuvent en découler. En d'autres termes, un diagnostiqueur est une compilation de l'information de diagnostic

dans une structure de données (appelée diagnostiqueur) qui relie efficacement les observations aux fautes lors du diagnostic en ligne. Ces modèles utilisent les automates comme représentation. Comme le passage de nos modèles vers les automates ne nous posait pas de problèmes particuliers car il n'existait pas de synchronisation, nous avons décidé d'utiliser ce formalisme pour étudier cette approche. Nous avons donc établit des modèles de « classe de fautes » i.e. des modèles génériques qui représentent l'insertion ou l'absence d'événement mais contrairement aux diagnostiqueurs, ces fautes ne sont pas « connues ». À partir de ces modèles de classes de fautes et du modèle de bon fonctionnement, par une règle simple, en l'occurrence ici un produit synchronisé des automates, et par une transformation simple par la suite, nous obtenons un diagnostiqueur pour chaque classe de faute qui nous permet d'avoir en temps réel, l'ensemble des explications possibles des observations que l'on a reçues. L'avantage de cette approche est d'avoir tous les calculs faits hors-ligne. La seule contrainte est de faire évoluer nos modèles au fur et à mesure que l'on reçoit des événements. Cet inconvénient vient du fait que le produit synchronisé génère un grand nombre d'états ce qui pour un système un peu complexe peut rapidement devenir difficile à maîtriser. Pour résoudre ce problème, nous avons développé une approche diagnostiqueur utilisant des réseaux de Petri (RdP). Les RdP nous permettent de représenter le mélange des connaissances entre le modèle de bon fonctionnement et les modèles de classe de fautes par une synchronisation des modèles au lieu d'un produit synchronisé. Au lieu d'avoir un produit de modèle, nous avons une simple somme de modèle. Ce qui nous permet de réduire drastiquement la taille de celui-ci. Pour obtenir le diagnostiqueur, nous avons modifié l'algorithme de Karp et Miller, couramment utilisé pour l'analyse des réseaux de Petri afin de prendre en compte nos différentes contraintes. La représentation de cet algorithme est sous forme d'un arbre. Pour plus de lisibilité, nous transformons cet arbre en un nouveau RdP qui représente notre diagnostiqueur. Trouver une explication possible, c'est mettre en cause l'intégrité d'un événement et implicitement l'intégrité du composant ou d'un ensemble de composants qui a émis ou pas cet événement. C'est là que se situe notre localisation ou plutôt notre « pré-localisation ».
Actuellement nous mettons en œuvre le développement de nos approches sur un banc de test qui nous permettra de les valider ou de les infirmer.

Publications

[1] S. Soldani, M. Combacau, A. Subias, and J. Thomas. "On-board diagnosis system for intermittent fault: application in automotive industry."
In 7th IFAC Conference on Fieldbuses and Networks in Industrial and Embedded Systems, FET'07, Toulouse (France), Novembre 2007.

[2] S. Soldani, M. Combacau, A. Subias, and J. Thomas. "Intermittent fault diagnosis: a diagnoser derived from the normal behavior."

- In 1st IFAC Workshop on Dependable Control of Discrete Systems, DCDS'07, pages 261-266, Cachan, Paris (France), June 2007.
- In 18th International Workshop on Principles of Diagnosis, DX'07, pages 391-398, Nashville, Tenessee (USA), Mai 2007.

[3] S. Soldani, M. Combacau, J. Thomas, and A. Subias. "Intermittent fault detection through message exchanges: a coherence based approach."

- In 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SAFEPROCESS'2006, pages 1549–1554, Beijing (China), August 2006.
- In 17th International Workshop on Principles of Diagnosis, DX'06, pages 251–256, Burgos (Spain), Juin 2006.

[4] S. Soldani "Détection et localisation de défauts intermittents dans les systèmes à événements discrets. Application au domaine automobile."
In 7ème Congrès des Doctorants de l'Ecole Doctorale Systèmes (EDSYS), Tarbes (France), 11 Mai 2006, 6p.

Références

[1] S. GENC et S. LAFORTUNE. “Distributed Diagnosis of Discrete-Event Systems Using Petri Nets”. Dans *ICATPN’03*, pages 316–336, 2003.
[2] C.N. HADJICOSTIS et G.C. VERGHESE. “Monitoring Discrete Event Systems Using Petri Net Embeddings”. Dans *ICATPN’99*, pages 188–207, 1999.
[3] G. JAKOBSON et M.D. WEISSMAN. “Alarm Correlation”. *IEEE Network*, 7(6) :52–59, 1993.
[4] G. JIROVEANU et R.K. BOEL. “Petri Net Model-based Distributed Diagnosis for Large Interacting Systems”. Dans *Proceedings of the 16th International Workshop on Principles of Diagnosis, DX’05*, Monterey, California (USA), June 2005.
[5] G. LAMPERTI et M. ZANELLA. “Continuous Diagnosis of Discrete-Event Systems”. Dans *Proceedings of the 14th International Workshop on Principles of Diagnosis, DX’03*, pages 105–112, Washington D.C. (USA), 2003.
[6] D. LEFEBVRE et C. DELHERM. “Diagnosis with Causality Relationships and Directed Paths in Petri Net Models”. Dans *IFAC World Congress’05*, Pragues (Czech Republic), July 2005.
[7] Y. A. NYGATE. “Event Correlation using Rule and Object Based Techniques”. Dans *Proceedings of 4th Symposium on Integrated Network Management*, pages 290–301, Santa Barbara (USA), 1995.
[8] Y. PENCOLE. “Diagnosability Analysis of Distributed Discrete Event Systems”. Dans *Proceedings of the 16th European Conference on Artificial Intelligence -ECAI’2004*, pages 43–47, Valencia (Spain), 2004.
[9] M. SAMPATH, S. LAFORTUNE, et D. TENEKETZIS. “Active Diagnosis of Discrete-Event Systems”. *IEEE Transactions on Automatic Control*, 43(7) :908–929, 1998.