SOUTENANCE DE THÈSE

M^me Manel Brini

Soutiendra sa thèse de **Doctorat** sur le sujet :

Safety-bag pour les systèmes complexes

Dans l'Unité de Recherche :

HEUDIASYC UMR CNRS 7253

Vendredi 23 novembre 2018 à 9h30
à l'UTC, bâtiment du génie informatique, salle GI 042

devant le jury composé de :

M. Simon Collart-Dutilleul, directeur de recherche, IFSTTAR/ESTAS, Villeneuve d'Ascq
M. Jérémie Guiochet, maître de conférences, université de Toulouse III
M^me Julie Beugin, chargée de recherche, IFSTTAR/ESTAS, Villeneuve d'Ascq
M^me Véronique Cherfaoui, professeur, université de technologie de Compiègne, Heudiasyc, UMR CNRS 7253
M. Benjamin Lussier, université de technologie de Compiègne, Heudiasyc, UMR CNRS 7253
M. Walter Schön, professeur, université de technologie de Compiègne, Heudiasyc, UMR CNRS 7253

Résumé :

Les véhicules automobiles autonomes sont des systèmes critiques. En effet, suite à leurs défaillances, ils peuvent provoquer des dégâts catastrophiques sur l'humain et sur l'environnement dans lequel ils opèrent. Le contrôle des véhicules autonomes robotisés est une fonction complexe, qui comporte de très nombreux modes de défaillances potentiels. Dans le cas de plateformes expérimentales qui n'ont suivi ni les méthodes de développement ni le cycle de certification requis pour les systèmes industriels, les probabilités de défaillances sont beaucoup plus importantes.

En effet, ces véhicules expérimentaux se heurtent à deux problèmes qui entravent leur sûreté de fonctionnement, c'est-à-dire la confiance justifiée que l'on peut avoir dans leur comportement correct.

Tout d'abord, ils sont utilisés dans des environnements ouverts, au contexte d'exécution très large. Ceci rend leur validation très complexe, puisque de nombreuses heures de test seraient nécessaires, sans garantie que toutes les fautes du système soient détectées puis corrigées. De plus, leur comportement est souvent très difficile à prédire ou à modéliser. Cela peut être dû à l'utilisation des logiciels d'intelligence artificielle pour résoudre des problèmes complexes comme la navigation ou la perception, mais aussi à la multiplicité de systèmes ou composants interagissant et compliquant le comportement du système final, par exemple en générant des comportements émergents.

Une technique permettant d'augmenter la sécurité-innocuité (safety) de ces systèmes autonomes est la mise en place d'un composant indépendant de sécurité, appelé « Safety-Bag ». Ce système est intégré entre l'application de contrôle-commande et les actionneurs du véhicule, ce qui lui permet de vérifier en ligne un ensemble de nécessités de sécurité, qui sont des propriétés nécessaires pour assurer la sécurité-innocuité du système. Chaque nécessité de sécurité est composée d'une condition de déclenchement et d'une intervention de sécurité appliquée quand la condition de déclenchement est violée. Cette intervention consiste soit en une inhibition de sécurité qui empêche le système d'évoluer vers un état à risques, soit en une action de sécurité afin de remettre le véhicule autonome dans un état sûr.

La définition des nécessités de sécurité doit suivre une méthode rigoureuse pour être systématique.

Pour ce faire, nous avons réalisé dans nos travaux une étude de sûreté de fonctionnement basée sur deux méthodes de prévision des fautes : AMDEC (Analyse des Modes de Défaillances, leurs Effets et leur Criticité) et HazOp-UML (Etude de dangers et d'opérabilité) qui mettent l'accent respectivement sur les composants internes matériels et logiciels du système et sur l'environnement routier et le processus de conduite. Le résultat de ces analyses de risques est un ensemble d'exigences de sécurité. Une partie de ces exigences de sécurité peut être traduite en nécessités de sécurité implémentables et vérifiables par le Safety-Bag. D'autres ne le peuvent pas pour que le système Safety-Bag reste un composant relativement simple et validable.

Ensuite, nous avons effectué des expérimentations basées sur l'injection de fautes afin de valider certaines nécessités de sécurité et évaluer le comportement de notre Safety-Bag. Ces expériences ont été faites sur notre véhicule robotisé de type Fluence dans notre laboratoire dans deux cadres différents, sur la piste réelle SEVILLE dans un premier temps et ensuite sur la piste virtuelle simulée par le logiciel Scanner Studio sur le banc VILAD.

Le Safety-Bag reste une solution prometteuse mais partielle pour des véhicules autonomes industriels. Par contre, il répond à l'essentiel des besoins pour assurer la sécurité-innocuité des véhicules autonomes expérimentaux.

Mots clés : Safety-Bag, sûreté de fonctionnement, tolérance aux fautes, véhicules autonomes, AMDEC, HazOp-UML