REF : DSR-2022-16-3SA
Pour postuler[1] : paolo.crisafulli@irt-systemx.fr , stages@irt-systemx.fr

Génération de simulations automobile à partir d'un modèle formel

CONTEXTE DU STAGE

Au sein de l'Institut de Recherche Technologique SystemX, situé au cœur du campus scientifique d'excellence mondiale de Paris-Saclay, vous prendrez une part active au développement d'un centre de recherche technologique de niveau international dans le domaine de l'ingénierie numérique des systèmes. Adossé aux meilleurs organismes de recherche français du domaine et constitué par des équipes mixtes d'industriels et d'académiques, ce centre a pour mission de générer de nouvelles connaissances et solutions technologiques en s'appuyant sur les percées de l'ingénierie numérique et de diffuser ses compétences dans tous les secteurs économiques.

Vous serez encadré par un ingénieur chercheur SystemX du domaine Sûreté de Fonctionnement, et vous aurez des échanges avec des chercheurs du Laboratoire Méthodes Formelles (LMF) de l'Université Paris-Saclay.

Vous travaillerez au sein du projet de recherche SystemX 3SA – Simulation pour la Sécurité des systèmes du véhicule Autonome (https://www.irt-systemx.fr/projets/3sa/) – dont les partenaires industriels sont Apsys, AVsimulation, Expleo, Stellantis, Oktal-SE, Renault, SECTOR Group, Valeo et les partenaires académiques le CEA (Commissariat à l'Energie Atomique), le LNE (Laboratoire national de métrologie et d'essais) et le LMF (Laboratoire Méthodes Formelles).

Le poste est basé à l'IRT SystemX – 2, Boulevard Thomas Gobert 91120 Palaiseau

DUREE ET DATE DE DEMARRAGE

Durée du stage : 6 mois
Date de démarrage envisagée : février 2022

PRESENTATION DETAILLEE DU SUJET

Objectifs du stage

L'utilisation de la simulation pour la démonstration de la sécurité du véhicule autonome est un complément incontournable aux validations physiques (essais sur bancs, pistes et routes), ceci afin d'assurer un comportement sûr du véhicule dans la multitude de situations auxquelles il pourra être confronté. Le projet 3SA ambitionne l'étude des méthodes et des outils de simulation des systèmes de conduite autonome, la modélisation des capteurs, la mise à disposition d'une bibliothèque de scénarios de roulage, le développement d'une méthode d'analyse des modèles décrivant des scénarios des véhicules autonomes avec plusieurs acteurs.

[1] Merci d'indiquer la référence du stage dans l'objet de votre mail de candidature

Le stage se situe dans le contexte de la tâche de création de la base de scénarios de roulage. Cette base sert à valider la sûreté de fonctionnement des véhicules autonomes, qui sont des systèmes critiques, en tant qu'ils doivent garantir la sécurité des passagers aussi bien que celle des usagers de la route plus généralement. Il s'agit donc de contribuer à répondre à la question cruciale de l'exhaustivité de la couverture de la base de scénarios, au regard des situations dangereuses que le véhicule autonome devra être capable d'affronter.

L'une des approches étudiées mobilise les méthodes de preuve formelle réalisées dans un assistant de preuve semi-interactive (Isabelle/HOL). Dans un travail antérieur, il a été démontré que des scénarios de véhicules autonomes peuvent être spécifiés avec Isabelle/HOL-CSP (une combinaison de la logique d'ordre supérieur et du formalisme CSP – « Concurrent Sequential Processes » – une théorie de référence pour étudier les modèles comportementaux, introduite par Tony Hoare [2].

À partir de ces spécifications, on a pu démontrer des propriétés de « safety » pour les scénarios où tous les véhicules appliquent une « driving strategy » bien connue, dite RSS [3], et générer un ensemble de scénarios paramétrés (dits « scénarios logiques »). L'objectif de ce stage est de concevoir une méthode outillée de génération d'une base de scénarios exécutables, qui soit couvrante dans un sens à étudier et à concevoir. On aura notamment recours aux bibliothèques de génération de tests existant dans Isabelle/HOL (cf. [4] et [5]).

Missions

- Prendre connaissance de l'état de l'art et le compléter quant aux aspects de génération de scénarios concrets à partir des modèles en Isabelle/HOL-CSP (https://www.isa-afp.org/entries/HOL-CSP.html).
- Concevoir et développer un composant de génération de scénarios concrets, à partir à la fois du modèle, de la preuve formelle, et de critères de couverture à élaborer.
- Intégrer l'exécution de ces scénarios concrets dans un environnement de simulation.
- Présenter les résultats aux chercheurs de l'équipe projet ainsi qu'aux partenaires industriels.

Références bibliographiques

[1] Technical Committee ISO/TC 22 and Subcommittee SC 32. Road vehicles — safety of the intended functionality. techreport ISO/PAS 21448:2019, International Organization for Standardization, 2019.
[2] C. A. R. Hoare. Communicating Sequential Processes. Prentice-Hall, Inc., Upper Saddle River. 1985.
[3] S. Taha, B. Wolff: Modelling and Proving Safety in Autonomous Cars Scenarios in HOL-CSP. SystemX Technical Report, Oct 2021.[4] Brucker, A.D., Wolff, B. On theorem prover-based testing. Form Asp Comp 25, 683–721 (2013). https://doi.org/10.1007/s00165-012-0222-y
[5] Achim D. Brucker, Lukas Brügger, and Burkhart Wolff. Formal Firewall Conformance Testing: An Application of Test and Proof Techniques. In Software Testing, Verification & Reliability (STVR), 25 (1), pages 34-71, 2015.

PROFIL ET COMPETENCES

De formation : BAC +5 Master Informatique/école d'ingénieur en informatique

Compétences :

- Programmation Fonctionnelle
- Développement Compilateurs
- Méthodes Formelles en général
- Bases en systèmes cyber-physiques.

Aptitudes personnelles :

- créativité,
- curiosité intellectuelle.