FORUM MÉTHODES FORMELLES

Cycle de conférences

Groupe de Travail

" VÉHICULES AUTONOMES ET MÉTHODES FORMELLES "

Mardi 10 Octobre 2017 Toulouse

Grenoble **Informations & Inscription**

LAAS CNRS

Salle de Conférences à Inscription par mail

Retransmis en direct **Saclay** **Informations & Inscription**

Rennes **Informations & Inscription**

PROGRAMME

Accueil

- 08h45 -08H55 Accueil des participants
- 08h55-09h00 **« Courte introduction à la journée »** Slides /Vidéo
  Agusti Canals (CS Communication & Systèmes, Toulouse, France)

Exposé Introductif

- 09h00-10h00 **« La voiture autonome : développements en cours, problématiques »**
  Serge Boverie (Continental Automotive, Toulouse, France) Slides /Vidéo

résumé : *Tous les constructeurs automobiles mondiaux et les grands équipementiers automobiles travaillent sur le véhicule autonome. Mais avant qu'on puisse confier son petit dernier à sa seule voiture pour l'emmener à l'école, la route est encore longue et les problèmes à résoudre nombreux …*
Cet exposé va donc présenter la road-map du véhicule autonome telle qu'elle est envisagée aujourd'hui, et les différentes problématiques majeures qu'il faudra résoudre pour y arriver, par exemple : interaction humain-voiture dans les premières étapes «partiellement autonomes», validation des systèmes ,«simulation in the loop», démonstration de sûreté de fonctionnement, etc.
L'exposé posera enfin la question : saura-t-on passer avec succès ces étapes et arriver jusqu'à la mise en service de véhicules autonomes sans utilisation intensive de méthodes formelles ?

Analyse formelle des concepts opérationnels

- 10h00-10h30 **« Formal methods will not prevent self-driving cars from having accidents »**
  Thierry Fraichard (INRIA, Grenoble, France) Slides/Vidéo

  résumé : *Autonomous navigation technologies have matured and improved to the point that self-driving cars have been able to safely drive an impressive number of kilometers. Does it mean that car accidents will soon be history? Well, things are not that simple... The primary purpose of this seminar is to raise the audience's awareness of the strong impact that the presence of moving objects in the environment of an autonomous system has on its decision-making process when it comes to collision avoidance. The difficulties that a system has to solve as soon as it tries to navigate in dynamic environments will be explored. The concept of Inevitable Collisions States (i.e. states for which no matter what the system does next, a collision eventually occurs) will be called upon, it will be shown that even when complete information is available (i.e. full knowledge of the environment and its future evolution), safe navigation can sometimes be impossible to guarantee. In real situations where such a complete information is simply not available, things get worse. The seminar will also explore how the models used to represent the environment and its future evolution (e.g. conservative vs. probabilistic) can affect the safety of the navigational decisions that are made. Possible solutions to the safe navigation problem will be presented.*

- 10h30-11h00 **« Analyse fonctionnelle des systèmes cyber-physiques avec incertitudes »**
  Goran Frehse (Verimag, Grenoble, France) Slides /Vidéo

  résumé : *Les systèmes cyber-physiques posent de nouveaux défis de conception : L'interaction avec le monde physique produit des situations difficiles à prédire et tester. Par exemple, la conduite autonome doit faire face à une infinité de situations*

de trafic différentes. Nous utilisons la simulation par un modèle mathématique pour soit détecter, soit formellement exclure des erreurs fonctionnelles. Cette simulation est exhaustive grâce à un calcul ensembliste, qui produit une enveloppe de tous les comportements du système. Cette enveloppe peut souvent être calculée même avec des incertitudes considérables, comme la position d'une voiture voisine sur l'autoroute, dont on ignore les intentions.
La simulation ensembliste s'applique dans trois domaines d'analyse :

- *la vérification : pour garantir le bon fonctionnement d'un système en phase de conception,*
- *le monitoring : pour mesurer si le fonctionnement d'un système existant est bon et conforme au modèle,*
- *la prédiction : pour enclencher des mesures d'urgence bien en avance.*

Nous illustrons les principes sur des exemples issus de la conduite autonome et de la collaboration homme-robot.

11h00-11h30 : **Pause Café**

Sûreté et sécurité formelle des systèmes

- 11h30-12h00 **« Apport d'Altarica pour la sécurité du binage autonome »** (projet en collaboration avec Naïo)
  Jean-Loup Farges (ONERA, Toulouse, France) & Pascal Schmidt (Naïo Technologies, Toulouse, France) Slides /Vidéo

  résumé : *Dans un contexte où les robots mobiles sont de plus en plus présents dans notre environnement, il est nécessaire que les méthodes d'analyse de sécurité soient adoptés par les fabricants de ces robots. A titre expérimental, une analyse de sécurité basée sur un modèle est conduite pour le robot Oz produit par Naio Technologies et dont la fonction est de biner des rangées de cultures. Des arbres de fautes pour les cas de panne, qui sont ici la collision et la sortie du champ à biner, sont générés automatiquement à partir d'un modèle Altarica proposé après concertation avec les concepteurs du robot.*

- 12h00-12h30 **« FORCES3 : Formal engineering for certified control-command embedded systems »**
  Claire Pagetti (ONERA, Toulouse, France) Slides/Vidéo

  résumé : *Le projet de recherche Forces 3 (Formal engineering of critical control-command embedded systems) a pour objectif de définir une approche complète de développement et de vérification de systèmes de contrôle-commande embarqués. Lors de cette présentation, nous décrirons :*
  1. la phase de génération de code à partir d'une spécification Simulink jusqu'à du C en passant par du Lustre/Prelude
  2. la phase de vérification de propriétés de conservation d'invariants entre la

spécification et le code C.
L'étude de cas ROSACE (Research Open-Source Avionics and Control Engineering) servira de support illustratif au cours de l'exposé.

12h30-14h00 : **Pause Repas**

Modélisation pour la vérification formelle

- 14h00-14h30 **« Deadlock free dispatching for fleets of vehicles »**
  Franco Mazzanti, Alessio Ferrari and Giorgio O. Spagnolo (ISTI-CNR, Pisa, Italy) Slides /Vidéo

  résumé *An intuitive approach in avoiding gridlocks during the dispatching of a fleet of vehicles is the one of constraining the number of vehicles which can concurrently be present in certain "most critical regions". Given a layout and a set of vehicle missions, model checking allows to precisely identify all the "critical regions" present in the network and the maximum number of vehicles allowed to enter them. This approach has been originally investigated for the design of a prototype of Automatic Train Supervision System (ATS) in the context of a CBTC (Communication Based Train Control) System, but can be generalised to the dispatching of generic fleets of vehicles.*

- 14h30-15h00 **« Validation and verification of time properties of the functional level of autonomous vehicles »**
  Félix Ingrand (LAAS-CNRS, Toulouse, France) Slides /Vidéo

  résumé : *GenoM is an approach to develop robotic software components, which can be controlled, and assembled to build complex applications. Its latest version GenoM3 provides a template mechanism which is versatile enough to deploy components for different middleware without any change in the specification and user code. But this same template mechanism also enables us to automatically synthesize formal models for various Validation and Verification frameworks (BIP, Fiacre/TINA, UPPAAL) of the final components. These formals models can be used offline to verify properties, but also online to perform run time verification. We illustrate our approach on real deployed examples (an autonomous shuttle and a drone) for which we prove offline real-time properties, and for which we synthesize a controller to perform runtime verification.*

Vérification formelle du code embarqué

- 15h00-15h30 **« Development and Formal Verification of a Micro-Glider Flight Stack with SPARK »**
  Emanuel Regnath (Technical University of Munich, Munich, Germany) Slides /Vidéo

résumé : *In contrast to classical testing and simulation, formal methods are able to prove the absence of errors but are often considered to be complicated. In this presentation, we illustrate the main features of the SPARK toolsuite from Adacore, evaluate how SPARK can be used in practice, and which constraints need to be considered. For this purpose, we developed and verified a flight stack for a high-altitude micro glider from ground up. During implementation, we added code annotations on demand and verified the absence of run-time errors in parallel. This parallel verification process helped to identify faults early but also revealed limitations and pitfalls of software design and verification, which will be discussed.*

- 15h30-16h00 **« Méthodes formelles au service de la voiture autonome »**
  Vassil Todorov (PSA, Paris, France) Slides /Vidéo

  résumé : *La part croissante des fonctions d'assistance à la conduite, leur criticité, ainsi que la perspective d'une certification de ces fonctions, rendent nécessaire leur vérification et leur validation avec un niveau d'exigence que le test seul ne peut assurer. Depuis quelques années déjà d'autres domaines comme l'aéronautique ou le ferroviaire sont soumis à des contextes équivalents. Pour répondre à certaines contraintes ils ont localement mis en place des méthodes formelles.*
  Le groupe PSA expérimente différentes techniques formelles afin de déterminer celles qui seraient pertinentes, pour quel type de développement, ainsi que l'impact de leur déploiement sur le processus.
  Cette présentation fait un tour d'horizon des techniques formelles expérimentées sur du code embarqué réellement utilisé en production, donne une synthèse des résultats obtenus et propose quelques perspectives pour l'avenir.

Retour d'expérience

- 16h00-16h30 **« Sur la pratique des méthodes formelles par de non praticiens : Autopsie d'un robot »**
  Eric Jenn (IRT Saint Exupéry, Toulouse, France) Slides /Vidéo

  résumé : *Dans le cadre du projet de recherche "INGEQUIP" conduit à l'IRT Saint Exupéry entre 2014 et 2017, plusieurs méthodes de développement et de vérification formelles --- model-checking, développement par raffinement formel, etc. --- ont été expérimentées et mises en œuvre lors du développement d'un petit robot mobile, TwIRTee. Dans cette présentation, nous nous proposons de vous présenter les aspects techniques et non techniques de cette expérience, sa portée, ses limites.*

- 16h30-17h00 **« SynC Contest: an Automatic Driving Challenge using Model-based Design and Synchronous Programming »**
  Mihaela Sighireanu (LIAFA/Université Paris Diderot, Paris, France) Slides /Vidéo

  résumé : *The SynC Contest is a new academic competition for designing embedded*

software using formal methods. The first edition of this competition took place in January 2017 and involved five teams from French and German universities.
The challenge consists in programming an automatic driver that is able to circulate into a city with traffic lights, obstacles, and other vehicles. Two cities were given as environment: a fully virtual city programmed in SCADE, and a real city on a robotic platform using Lego Mindstorms.
The main aim was to give an opportunity to students following the model-based design course to prove their technical skills in synchronous programming with SCADE. This talk will present the competition, the SCADE environment programmed for it, the results obtained, and the lessons learnt.
The SynC Contest has been sponsored by ANSYS, Expectra, the Engineering School of Denis Diderot EIDD and the University Paris- Diderot.