Topic: Formal methods in Railway applications
Starting date: as soon as possible
Deadline for application: 22th of March 2019

10 months (+possible extension) Post-doc position at IFSTTAR Lille
www.ifsttar.fr

Context

IFSTTAR/ESTAS laboratory "Evaluation of Automated Transport Systems and their Safety" develops methods, techniques and tools to facilitate and improve the analysis and evaluation of the safety functions of guided transport systems.

The finalized research, which is one of the strongest features of ESTAS, is based on the synergy between research, applications, and the feedback of expertise and technical assistance activities in the field of guided transport systems.

This type of applied research is based on a particular mode relying heavily on the needs generated by expertise and technical assistance to respond to concerns on the ground.

In collaboration with academic and industria partners, ESTAS is currently involved in various national and European projects that strive to promote the use of formal methods for the design and development of railway systems, including autonomous trains. Such methods are highly recommended for the engineering of safety critical systems. The activities to be carried out in the framework of this post-doc position is related to the aformentioned activities.

Mission

Even in systems with low complexity, it is a challenge to ensure correct behaviour, interoperability, safety and reliability. This challenge is very real for modern rail control and signalling, such as the ERTMS interoperability standard. Schedules to deliver such systems are long and hardly predictable, and systems are costly to procure, develop and maintain. One of the main root causes for these problems is that tender requirements often tend to be vague and imprecise:
- Significant effort and know-how is needed to interpret and detail requirements, leading to critical design choices and interfaces whose impact is not understood until late phases.
- Design choices may lead to systems being based on proprietary solutions (“vendor lock-in”).
- Vague and imprecise requirements complicate the process to verify that systems comply with their requirements, and assessment of their safety.
- The need to implement changes is discovered late, when changes are expensive to perform.
Another main root cause, in part a consequence of vague and imprecise tender requirements, is that verification is mainly based on traditional methods such as review and test:

- These methods are time-consuming and error-prone, and verification coverage for critical system properties is poor; they can only detect issues, not prove absence.

- Traditional verification methods applied using imprecise requirements necessitates senior staff to manage such verification work, and to judge quality and safety.
- It becomes complex to grasp on what basis systems are assessed to be safe and in compliance with requirements, affecting system delivery schedules, maintenance and life-cycle costs.

Requirements on safety, security, and reliability in railway signalling are complex since they cover a vast state space, and because they use many concepts from multiple domains. To ensure that such requirements are satisfied is only possible by using Formal Methods in specification, development and verification. Formal methods provide techniques and tools to define and precisely analyse such concepts and relationships, and to verify requirements exhaustively. In addition to improved verification of critical system properties to reduce time-to-market and cost, formal methods can also improve requirement quality and reliability. Successful applications in the railway domain demonstrate these benefits, and that the number of defects becomes reduced.
A related topic that will be investigated within this mission is pertaining to the evaluation of artificial intelligence-based functions. The introduction of AI in some critical functions in railway command and control must, indeed, be undertaken while ensuring high safety levels.

The selected candidate will be in charge of and/or participate to the followings:
- Making a state of the art on the application of formal methods in railways;
- Development of semi-formal and formal models for some selected use case systems;
- Application of formal methods on the use cases selected;
- Specification and V&V for standard interfaces;
- Safety analysis of AI-based functions (Artificial intelligence)
- Participation in various coordination meetings (possible travels in France and abroad);
- Participation to project meetings with all European partners;
- Participation to the management of other possible involved persons (students, etc.).
- Contribution to the achievement of deliverables and scientific publications.

Requirements
- PhD related to some or all of the following topics: Formal methods (Model-checking, etc.), modelling, Safety analysis, discrete event systems, artificial intelligence.
- Knowledge of railway applications would be appreciated
- Semi-formal and formal modelling
- Good skills in software engineering
- Good skills in scientific writing
- Good English skills

Application
If interested, please send a detailed CV, the two most representative publications of your work, and if possible some recommandation letters to **mohamed.ghazel@ifsttar.fr**

Deadline for application: March 22th 2019

Work location
IFSTTAR Lille
COSYS/ESTAS

Gross salary (Brut)
~ 2700 euros/month