Offre de post-doctorat OU Ingénieur de recherche – 12 mois extensibles à 24 mois

Université Gustave Eiffel

Titre : *Étude comparative des apports et limites des méthodes formelles au regard de l'évaluation des fonctions sécuritaires dans les systèmes ferroviaires.*

Lieu de travail : Univ-Eiffel – Campus de Lille – COSYS/ESTAS, France

Laboratoire d'accueil

Créée le 1er janvier 2020, l'Université Gustave Eiffel est un établissement pluridisciplinaire français issu de la fusion de l'Université Paris-Est-Marne-la-Vallée (UPEM) avec l'Institut français des sciences et technologies des transports, de l'aménagement et des réseaux (IFSTTAR), et de l'intégration de l'École d'architecture de la ville & des territoires Paris-Est (Éav&t), et de trois écoles d'ingénieurs (EIVP, ENSG et l'ESIEE Paris).

Le laboratoire ESTAS (Évaluation des Systèmes de Transport Automatisés et de leur Sécurité) du département COSYS (Composants et Systèmes) développe des méthodes, techniques et outils destinés à faciliter et à améliorer l'analyse et l'évaluation des fonctions de sécurité des systèmes de transports guidés. La recherche finalisée, qui est l'une des caractéristiques fortes à ESTAS, trouve ses fondements dans la synergie entre la recherche appliquée et le retour d'expérience des activités d'expertises et d'assistance technique dans le domaine des systèmes de transport guidés.

Détails

Contexte

Ce poste s'inscrit dans le cadre du volet "Évaluation de la sécurité des systèmes ferroviaires" de la chaire "Sécurité des Systèmes Ferroviaires". Cette dernière est soutenue par CERTIFER Association et GAPAVE, groupement qui inclut plusieurs acteurs du domaine ferroviaire : opérateurs, constructeurs et évaluateurs indépendants de sécurité.

Aujourd'hui les systèmes de contrôle/commande et de signalisation ferroviaire ne cessent de se complexifier en vue de répondre aux exigences croissantes en termes de sécurité, de performance et de confort, et de manière générale pour faire gagner en compétitivité le mode de transport ferroviaire qui engendre une emprunte carbone moindre par rapport aux autres modes de transport. Les évolutions qui voient le jour dans le secteur ferroviaire s'accompagnent par une digitalisation accrue, par l'introduction de nouvelles technologies (localisation à base des GNSS, gestion embarquée de l'intégrité des trains, etc.), notamment en vue d'introduire de nouveaux modes opératoires plus performants, en particulier l'exploitation en « canton mobile ».

Ces évolutions doivent s'accompagner par des méthodes d'évaluation de la sécurité à même de prendre en compte la complexité induite, tout en répondant aux exigences des normes en vigueur.

Au sein d'ESTAS, nous menons des travaux autour de l'usage de modèles semi-formels et formels et des méthodes formelles, qui sont fortement recommandées par les normes ferroviaires, pour l'analyse et l'évaluation de questions relatives à la sécurité et l'interopérabilité dans les systèmes ferroviaires. Ces travaux serviront d'entrées à l'étude à mener dans le cadre de ce poste, en plus des différents résultats de l'état de l'art.

Description du travail

Comme précisé plus haut, les méthodes formelles (MF) sont aujourd'hui fortement recommandées par les normes ferroviaires pour les applications sécuritaires, en particulier la

CENELEC 50128. Ces méthodes ont déjà fait leur preuve sur des applications sécuritaires dans le transport guidé (ex. méthode B sur la ligne 14 du métro parisien). Cependant, aujourd’hui les MF ne cessent de se diversifier pour prendre en compte une multitude de variantes de comportements (aspects temporels, aspects probabilistes, etc.), et de spécifications (types de propriétés à vérifier, etc.). Des outils sont également proposés pour supporter ces techniques et sont de plus en plus matures. Or, l’adoption des MF dans le transport guidé reste relativement cantonné à quelques méthodes. Dans le cadre de cette étude, nous proposons de mener une étude comparative de différentes techniques formelles pour en mesurer les avantages et limites relatifs. Bien que certains travaux se sont déjà penchés sur la comparaison de quelques MF, les résultats de ces travaux sont assez généraux, et ne prennent pas en compte les exigences des normes ferroviaires en vigueur. Nous envisageons par ailleurs de faire usage d’un cas d’étude ferroviaire réel dans le cadre de ce travail, et d’investiguer de manière comparative à quel point les exigences des normes ferroviaires sont remplies par les différentes MF étudiées.

Le travail à mener donnera lieu à des rapports intermédiaires, ainsi qu’à un livrable final qui synthétise l’ensemble des résultats issus de l’étude comparatives des différentes MFs.

Références :

- EN 50126-1:2017 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process. CENELEC CLC/TC 9X standard, 2017-10.

- EN 50128:2011 Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems. CENELEC CLC/TC 9X standard, 2011-06.

- EN 50129:2003 Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling. CENELEC CLC/TC 9X standard, 2003-02.

- Ghazel M., Formalizing a Subset of ERTMS/ETCS Specifications for Verification Purposes, Transportation Research Part C - Emerging Technologies, Elsevier, vol. 42, pp. 60-75.

- Technical Note, X2Rail-2 WP5, Task 5.2.1: Questionnaires related to Formal Methods, January 23, 2018.

- Deliverable D4.1: Report on Analysis and on Ranking of Formal Methods (2019), ASTRail european project, SAtellite-based Signalling and Automation SysTems on Railways along with formal Method and Moving Block validation, 126p.

- Jean-Raymond Abrial. 2006. Formal methods in industry: achievements, problems, future. In Proceedings of the 28th international conference on Software engineering (ICSE '06). ACM, New York, NY, USA, 761-768.

- Saddem-Yagoubi R., Sanwal M.-U., Libutti S., Benerecetti M., Beugin J., Flammini F., Ghazel M., Janssen B., Marrone S., Mogavero F., Nardone R., Peron A., Seceleanu C., Vittorini V. (2022). Toward Usable Formal Models for Safety and Performance Evaluation of ERTMS/ETCS Level 3: The PERFORMINGRAIL Project. ESREL 2022 - 32nd European Safety and Reliability Conference, 28 August-1st September, Dublin, Ireland.

- Himrane, O. (2022) Contribution to Safety and Operational Performance Evaluation of GNSS-based Railway Localization Systems Using a Formal Model-based Approach. PhD thesis, Lille University, ESTAS laboratory.

- Basile D., ter Beek M.H., Ferrari A., Legay A. (2022). Exploring the ERTMS/ETCS full moving block specification: an experience with formal methods, International Journal on Software Tools for Technology Transfer, vol. 24(3), pp. 351370.

- Basile D., Fantechi A., Rucher L., Mandò G. (2021). Analysing an autonomous tramway positioning system with the UPPAAL Statistical Model Checker, Formal Aspects on Computing, Formal Aspects of Computing, vol. 33(6), pp 957-987.

- Berger U., James P., Lawrence A., Roggenbach M., Seisenberger M. (2018). Verification of the European Rail Traffic Management System in Real-Time Maude, Science of Computer

Programming, vol. 154, pp. 61-88.

- Patrick Behm, Paul Benoit, Alain Faivre, and Jean-Marc Meynadier. 1999. Météor: A Successful Application of B in a Large Project. In Proceedings of the Wold Congress on Formal Methods in the Development of Computing Systems-Volume I - Volume I (FM '99), Jeannette M. Wing, Jim Woodcock, and Jim Davies (Eds.), Vol. I. Springer-Verlag, London, UK, UK, 369-387.

- Frédéric Badeau and Arnaud Amelot. 2005. Using b as a high level programming language in an industrial project: roissy VAL. In Proceedings of the 4th international conference on Formal Specification and Development in Z and B (ZB'05), Helen Treharne, Steve King, Martin Henson, and Steve Schneider (Eds.). Springer-Verlag, Berlin, Heidelberg, 334-354.

- Sabatier D., Burdy L., Requet A., Guéry J. (2012) Formal Proofs for the NYCT Line 7 (Flushing) Modernization Project. In: Derrick J. et al. (eds) Abstract State Machines, Alloy, B, VDM, and Z. ABZ 2012. Lecture Notes in Computer Science, vol 7316. Springer, Berlin, Heidelberg.

- D. H. Garavel and D. S. Graf. Formal Methods for Safe and Secure Computers Systems. Tech. Rep., Federal Office for Information Security, 2013.

Profil du(de la) candidat(e) :

- Doctorat en automatique, informatique ou mathématiques appliquées (**ou** Master + expérience en recherche sur les sujets du poste)
- Connaissance en méthodes formelles, sûreté de fonctionnement, analyse des systèmes,
- Une expérience dans les systèmes de contrôle-commande et de signalisation ferroviaires serait appréciée.
- Esprit de synthèse, capacité d'auto-formation, sens de l'initiative, rigueur, pédagogie
- Excellentes capacités rédactionnelles, aisance en anglais (oral et écrit)

Information :

- La candidature (cv, lettre de motivation, lettre(s) de recommandations) doit être adressée par e-mail **dès que possible** à : mohamed.ghazel@univ-eiffel.fr
- Type de contrat : CDD de 12 mois extensible à 24 mois
- Salaire brut : ~2 500 € / mois
- Recrutement **dès que possible**

Post-doctoral OR Research Engineer position – 12 months extendable to 24 months

Université Gustave Eiffel

Title: *Comparative study of formal methods with regard to the evaluation of safety functions in railway systems.*

Location: Univ-Eiffel – Lille Campus – COSYS/ESTAS, France

Host laboratory

Université Gustave Eiffel is a French multidisciplinary university of national importance. Since the 1st of January 2020 this new institution has brought together a university (UPEM), a research institute (Ifsttar), a school of architecture (Éav&t) and three engineering schools (EIVP, ENSG and ESIEE Paris).

The ESTAS laboratory (Evaluation and Safety of Automated Transport Systems) of the COSYS department (Components and Systems) develops methods, techniques and tools intended to help analysing the safety of guided transport systems. The finalized research, which is one of the main features of ESTAS, finds its foundations in the synergy between applied research and feedback from expertise and technical assistance activities in the field of guided transport systems.

Details

Context

This position is part of the "Safety Assessment of Railway Systems" axis of the "Safety of Railway Systems" Chair. The latter is supported by CERTIFER Association and GAPAVE, a grouping that includes several actors in the railway field: operators, manufacturers and independent safety assessors.

Today, railway control/command and signalling systems are constantly becoming more complex in order to meet growing requirements in terms of safety, performance and comfort, and in general to make the railway mode which generates a lower carbon footprint compared to other modes of transport, more competitive. The developments that are emerging in the railway sector are accompanied by increased digitalisation, as well as by the introduction of new technologies (GNSS-based localization, on-board monitoring of train integrity, etc.), in particular with a view to introduce new more efficient operating methods. Besides, a specific effort is made today by the major railway actors in Europe to implement the "moving block" operation.
These developments must be accompanied by the deployment of some safety assessment methods which are able of handling the resulting complexity, while meeting the requirements of the railway standards in force.

Within ESTAS, we conduct various research actions around the use of semi-formal and formal models and formal methods, which are strongly recommended by railway standards, for the analysis and evaluation of safety and interoperability issues in railway systems. These works will serve as inputs for the study to be carried out within the framework of this post, in addition to the various results of the state of the art.

Work description

As mentioned above, formal methods (FMs) are today strongly recommended by railway standards for safety applications, in particular the CENELEC 50128 standard. These methods have already proven to be very relevant on safety applications in guided transport (e.g. method B on line 14 of the Paris metro). However, today FMs are constantly diversifying to take into account a variety of behavioural features (temporal aspects, probabilistic aspects, etc.), and specifications (types of properties to be verified, etc.). Some tools are also proposed to support these techniques, while showing to be more and more mature. However, the adoption of FMs in guided transport applications remains relatively confined to a few methods. As part of this study, we propose to conduct a comparative analysis of different formal techniques to measure their respective advantages and limitations. Although some work has already focused on the comparison of some FMs, the results of this work are quite general, and do not take into account the requirements of the railway standards in force. Besides, we also plan to use a real railway case study as part of this work, and to investigate in a comparative way to what extent the requirements of railway standards are met by the different FMs investigated.

The work to be carried out will give rise to intermediate technical reports, as well as to a final deliverable which synthesizes all the results resulting from the comparative study of the different FMs.

References:

- EN 50126-1:2017 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process. CENELEC CLC/TC 9X standard, 2017-10.

- EN 50128:2011 Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems. CENELEC CLC/TC 9X standard, 2011-06.

- EN 50129:2003 Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling. CENELEC CLC/TC 9X standard, 2003-02.

- Ghazel M., Formalizing a Subset of ERTMS/ETCS Specifications for Verification Purposes, Transportation Research Part C - Emerging Technologies, Elsevier, vol. 42, pp. 60-75.

- Technical Note, X2Rail-2 WP5, Task 5.2.1: Questionnaires related to Formal Methods, January 23, 2018.

- Deliverable D4.1: Report on Analysis and on Ranking of Formal Methods (2019), ASTRail european project, SAtellite-based Signalling and Automation SysTems on Railways along with formal Method and Moving Block validation, 126p.

- Jean-Raymond Abrial. 2006. Formal methods in industry: achievements, problems, future. In Proceedings of the 28th international conference on Software engineering (ICSE '06). ACM, New York, NY, USA, 761-768.

- Saddem-Yagoubi R., Sanwal M.-U., Libutti S., Benerecetti M., Beugin J., Flammini F., Ghazel M., Janssen B., Marrone S., Mogavero F., Nardone R., Peron A., Seceleanu C., Vittorini V. (2022). Toward Usable Formal Models for Safety and Performance Evaluation of ERTMS/ETCS Level 3: The PERFORMINGRAIL Project. ESREL 2022 - 32nd European Safety and Reliability Conference, 28 August-1st September, Dublin, Ireland.

- Himrane, O. (2022) Contribution to Safety and Operational Performance Evaluation of GNSS-based Railway Localization Systems Using a Formal Model-based Approach. PhD thesis, Lille University, ESTAS laboratory.

- Basile D., ter Beek M.H., Ferrari A., Legay A. (2022). Exploring the ERTMS/ETCS full moving block specification: an experience with formal methods, International Journal on Software Tools for Technology Transfer, vol. 24(3), pp. 351370.

- Basile D., Fantechi A., Rucher L., Mandò G. (2021). Analysing an autonomous tramway positioning system with the UPPAAL Statistical Model Checker, Formal Aspects on Computing, Formal Aspects of Computing, vol. 33(6), pp 957-987.

- Berger U., James P., Lawrence A., Roggenbach M., Seisenberger M. (2018). Verification of the European Rail Traffic Management System in Real-Time Maude, Science of Computer Programming, vol. 154, pp. 61-88.

- Patrick Behm, Paul Benoit, Alain Faivre, and Jean-Marc Meynadier. 1999. Météor: A Successful Application of B in a Large Project. In Proceedings of the Wold Congress on Formal Methods in the Development of Computing Systems-Volume I - Volume I (FM '99), Jeannette M. Wing, Jim Woodcock, and Jim Davies (Eds.), Vol. I. Springer-Verlag, London, UK, UK, 369-387.

- Frédéric Badeau and Arnaud Amelot. 2005. Using b as a high level programming language in an industrial project: roissy VAL. In Proceedings of the 4th international conference on Formal Specification and Development in Z and B (ZB'05), Helen Treharne, Steve King, Martin Henson, and Steve Schneider (Eds.). Springer-Verlag, Berlin, Heidelberg, 334-354.

- Sabatier D., Burdy L., Requet A., Guéry J. (2012) Formal Proofs for the NYCT Line 7 (Flushing) Modernization Project. In: Derrick J. et al. (eds) Abstract State Machines, Alloy, B, VDM, and Z. ABZ 2012. Lecture Notes in Computer Science, vol 7316. Springer, Berlin, Heidelberg.

- D. H. Garavel and D. S. Graf. Formal Methods for Safe and Secure Computers Systems. Tech. Rep., Federal Office for Information Security, 2013.

Candidate profile:

- PhD. degree in automation engineering, computer science or applied mathematics (**OR** Master degree + Experience on the position topics)
- Knowledge in formal methods, dependability/safety analysis, system engineering
- Experience in railway control-command and signalling systems will be appreciated.
- Ability to synthesise, capacity for self-training, sense of initiative, rigour, pedagogy
- Excellent writing skills, proficient in French or in English (spoken and written)

Information:

- The application (resume, cover letter, and reference letter(s) if possible) has to be addressed by e-mail **as soon as possible** to: mohamed.ghazel@univ-eiffel.fr
- Type of contract: fixed-term contract of 12 months extendable to 24 months
- Gross salary: ~2 500 € / months
- Starting date: **as soon as possible**