Contribution to the safety analysis of the latest generation of railway control-command and signalling systems based on "moving block"

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. The research work that will be carried out within the framework of this position aims to contribute to the challenge of verifying the safety of the future ERTMS / ETCS (*European Rail Traffic Management System* / *European Train Control System*) level 3 system. It is a rail control-command and signalling system that integrates new location and communication technologies. Taking part in this challenge will greatly facilitate the implementation of this system that can allow mobilities to progress in an efficient and sustainable manner. This work will be based on our existing formal models of behaviour [Himrane 2022] [Saddem et al. 2022] [Ghazel 2014], some of which have been developed in the framework of European Shift2Rail projects. Moreover, a group of railway experts, members of the grouping and constituted around this theme, offers a privileged environment of exchanges on technical knowledge, which confers a very enriching context to rigorously model a set of functions intervening in the complete cycle of train control (from route control to movement authorities granted to trains).

Candidate profile
Master's or engineering degree in dependability, systems engineering or automation/computing

Location
ESTAS laboratory
Lille Campus

Starting date
ASAP

Duration
3 years

Contacts
julie.beugin@univ-eiffel.fr
mohamed.ghazel@univ-eiffel.fr
rim.saddem@lis-lab.fr

Work description

ERTMS level 3 aims to operate trains in an optimal and safe way by using moving blocks. This operating mode requires transferring certain train protection functionalities from trackside equipment to on-board train equipment. In particular, track occupancy information (the position of the front and rear of the train with their margins related to inaccuracy) will stem from the trains and not from the infrastructure. On-board/trackside communication will then enable the infrastructure to get this information in order to manage all train routes and track occupancies in safety on the railway network.

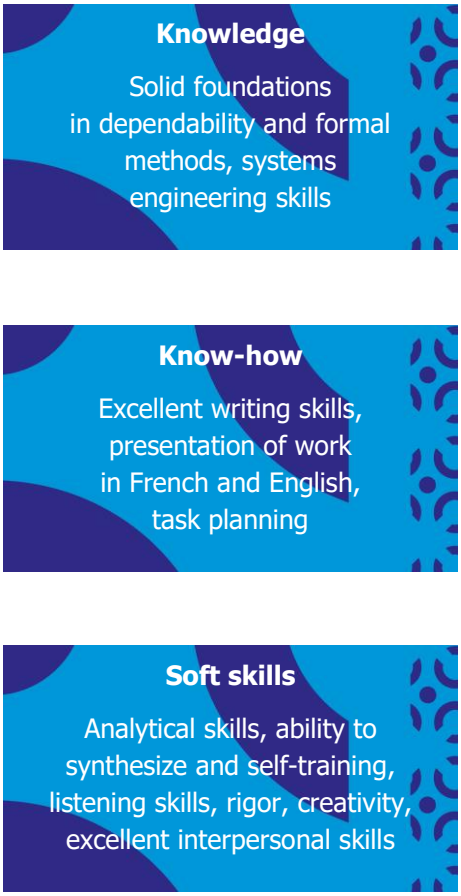
The use of advanced technologies for train integrity monitoring (no broken couplings) and positioning, makes it possible to determine the precise track occupancy of a vehicle, in particular with satellite localisation technologies (GNSS, Global Navigation Satellite Systems) in conjunction with various sensors and processing. However, the current work on ERTMS level 3 and its variants (with virtual blocks or hybrid variants) is hampered by the lack of safety assessment methods that allow the complex interactions between the different parts of the control-command system to be understood during its operation, additionally to the fact that the railway environment has a highly variable and disturbing impact on the on-board equipment incorporating GNSS.

To contribute to the safety analysis of mobile block operations, the proposed work aims at developing a process based on the modelling of complex functional interactions within ERTMS level 3 to assess operational safety properties and evaluate different hazard situations. The performance pertaining to integrity monitoring, communications and positioning equipment (in particular, related to satellite localisation) will be considered in the process as parameters to show their impact on safety properties.

The first step will be to understand and analyse the complex functional interactions in a control-command system using moving blocks and including the inaccuracies specific to satellite localisation. Since the train movement is

subject not only to temporal constraints, but also to spatial constraints (e.g., specific points to be passed with a given speed) and speed constraints (static and dynamic speed profile, temporary speed restriction) along the railway track, a difficult challenge is to take into account, in adapted models, position and speed inaccuracies in the context of moving block operation. This information, measured by the train, is transmitted to the trackside subsystem with a time delay. Despite this delay, the subsystem uses this information to identify occupied track sections and thus manage the different train itineraries.

Recent work includes interesting modelling elements linked to existing or planned control-command systems, the principles of which are adaptable to ERTMS/ETCS level 3 [Basile 2021, 2022] [Berger 2018]. The second phase aims to develop and come up with a process using advanced techniques for modelling complex behaviours for the verification of safety properties linked to ERTMS/ETCS level 3. Behavioural models may be based, for example, on timed automata (of probabilistic, stochastic, hybrid types) or Petri nets (timed, coloured, stochastic, interpreted), with approaches to failure analysis or reachability of feared events based on model checking (of classical, statistical, probabilistic type).



References :

- 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.
- Saddem-Yagoubi R., Beugin J., Ghazel M. (2022). Verification Framework for Moving Block System Safety: application on the Loss of Train Integrity Use Case. 11th TRISTAN conference, Triennal Symposium on Transportation Analysis, 19-25 June, Mauritius Island.
- 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.
- Ghazel M. (2014). Formalizing a Subset of ERTMS/ETCS Specifications for Verification Purposes. Transportation Research Part C - Emerging Technologies, vol. 42, pp. 60-75.
- 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.

Université Gustave Eiffel

OFFRE DE THÈSE

Chaire « Sécurité des Systèmes Ferroviaires »

Contribution à l'analyse de sécurité liée aux systèmes de contrôle-commande ferroviaires de dernière génération dits « à cantons mobiles »

Contexte

Cette thèse 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.

Les travaux de recherche qui seront menés dans le cadre de cette thèse visent à contribuer au défi de la vérification de la sécurité du futur système de contrôle-commande ERTMS / ETCS (European Rail Traffic Management System / *European Train Control System*) niveau 3 intégrant de nouvelles technologies de localisation de de communication. Prendre part à ce défi favorisera grandement la mise en service d'un tel système capable de faire évoluer l'exploitation ferroviaire de manière efficace et durable.

Ces travaux s'appuieront sur des modèles formels de comportements existants issus de travaux de l'équipe [Himrane 2022] [Saddem et al. 2022] [Ghazel 2014], dont certains ont été développés dans le cadre de projets européens de Shift2Rail. De plus, un groupe d'experts ferroviaires membres du groupement et constitué autour de cette thématique, permet d'offrir un environnement privilégié d'échanges sur des connaissances métier, ce qui confère un contexte très enrichissant pour modéliser rigoureusement un ensemble de fonctions intervenant dans le cycle de contrôle des trains (de la commande d'itinéraire aux autorisations de mouvement octroyées aux trains).

Profil du(de la) candidat(e)

Master ou diplôme d'ingénieur en sûreté de fonctionnement, ingénierie des systèmes ou automatique/informatique

Affectation

Laboratoire ESTAS
Campus de Lille

Date de début

Au plus tôt

Durée

3 ans

Contacts

julie.beugin@univ-eiffel.fr
mohamed.ghazel@univ-eiffel.fr
rim.saddem@lis-lab.fr

Description du travail

Le niveau 3 d'implémentation d'ERTMS vise à exploiter les trains de manière optimale et sûre en s'appuyant sur le concept de « canton mobile ». Ce mode d'exploitation requiert le transfert de certaines fonctionnalités de protection des trains depuis les équipements de voie vers les équipements embarqués à bord des trains. En particulier, les informations d'occupation de la voie (la position de l'avant et de l'arrière du train avec leurs marges d'imprécision) pourront être issues des trains et non plus de l'infrastructure. La communication bord/sol permettra alors à l'infrastructure de connaître ces informations pour gérer en sécurité sur le réseau ferré, l'ensemble des itinéraires et emplacements des trains.

L'emploi de technologies avancées de surveillance d'intégrité des trains (absence de rupture d'attelage), et de positionnement, rend possible la détermination fine de l'occupation de la voie par un véhicule, en particulier avec les technologies de localisation satellitaire (GNSS, Global Navigation Satellite Systems) en lien avec différents capteurs et traitements. Toutefois, les travaux actuels sur l'ERTMS niveau 3 et ses variants (à cantons virtuels ou les variants hybrides) sont freinés par le manque de méthodes d'évaluation de sécurité permettant d'appréhender les interactions complexes entre les différentes parties du système de contrôle-commande lors de son exploitation, ajouté à cela le fait que l'environnement ferroviaire a un impact très variable et perturbant sur les équipements embarqués intégrant les GNSS.

Pour contribuer à la problématique de l'analyse de sécurité des opérations à base de cantons mobiles, les travaux envisagés visent à développer un processus s'appuyant sur la modélisation des interactions fonctionnelles complexes au sein de l'ERTMS niveau 3 pour évaluer des propriétés de sécurité opérationnelles et évaluer différentes situations de danger. Les performances propres aux équipements de contrôle d'intégrité, de communications et de positionnement (en particulier, liés à la localisation satellitaire) seront considérées dans le processus en tant que

paramètres pour montrer leur impact sur ces évaluations. Il s'agira dans un premier temps de comprendre et analyser les interactions fonctionnelles complexes dans le système de contrôle-commande utilisant les cantons mobiles et incluant les imprécisions propres à la localisation satellitaire. Étant donné que le mouvement d'un train est sujet non seulement à des contraintes temporelles mais aussi à des contraintes spatiales (ex. points spécifiques à franchir avec une vitesse donnée) et de vitesse (profil de vitesse statique et dynamique, restriction temporaire de vitesse) le long de la voie ferroviaire, un défi délicat à relever est la prise en compte, dans des modèles adaptés, des imprécisions de position et de vitesse dans le contexte de l'exploitation en cantons mobiles. Ces informations mesurées par le train sont transmises au sous-système sol avec un temps de latence. Malgré ce décalage temporel, ce sous-système les utilise pour recenser les portions de voie occupées et ainsi gérer les différents itinéraires des trains.

Des travaux récents comportent des éléments de modélisation intéressants liés à des systèmes de contrôle-commande existants ou prévus, dont les principes sont adaptables à ERTMS/ETCS niveau 3 [Basile 2021, 2022] [Berger 2018]. Dans un deuxième temps, il s'agira donc de concevoir et développer un processus utilisant des techniques avancées de modélisation de comportements complexes pour la vérification de propriétés de sécurité liés à ERTMS/ETCS niveau 3. Des plans de voie proposés en tant que « benchmarks » pourront être utilisés [Berger 2018] et les modèles de comportement pourront s'appuyer par exemple sur les automates temporisés (probabilistes, stochastiques, hybrides) ou les réseaux de Petri (temporisés, colorés, stochastiques, interprétés), avec des approches d'analyse pouvant être fondées sur le "model checking" (classique, statistique, probabiliste).

Savoir

Bases solides en sûreté de fonctionnement et méthodes formelles, compétences en ingénierie des systèmes

Savoir faire

Excellentes capacités rédactionnelles, présentation de travaux en français et en anglais, planification de tâches

Savoir être

Capacités d'analyse, de synthèse d'auto-formation et d'écoute, rigueur, créativité, excellent relationnel

Références :

- 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.
- Saddem-Yagoubi R., Beugin J., Ghazel M. (2022). Verification Framework for Moving Block System Safety: application on the Loss of Train Integrity Use Case. 11th TRISTAN conference, Triennal Symposium on Transportation Analysis, 19-25 June, Mauritius Island.
- 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.
- Ghazel M. (2014). Formalizing a Subset of ERTMS/ETCS Specifications for Verification Purposes. Transportation Research Part C - Emerging Technologies, vol. 42, pp. 60-75.
- 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.