

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 et 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).

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

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

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).

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, Triennial 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.

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