Proposition d'une approche orientée modèles pour évaluer la sécurité des systèmes de signalisation ferroviaire utilisant les GNSS

Ouail Himrane, Julie Beugin, Mohamed Ghazel

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Proposition d'une approche orientée modèles pour évaluer la sécurité des systèmes de signalisation ferroviaire utilisant les GNSS

Proposal for a model-oriented approach to evaluate the safety of railway signalling systems using GNSS

Ouail Himrane
COSYS-ESTAS, Univ Gustave Eiffel
IFSTTAR, Univ Lille
Villeneuve d'Ascq, France
ouail.himrane@univ-eiffel. fr

Julie Beugin
COSYS-ESTAS, Univ Gustave Eiffel
IFSTTAR, Univ Lille
Villeneuve d'Ascq, France
julie.beugin@univ-eiffel. fr

Mohamed Ghazel
COSYS-ESTAS, Univ Gustave Eiffel
IFSTTAR, Univ Lille
Villeneuve d'Ascq, France
mohamed.ghazel@univ-eiffel. fr

Résumé — **Ce papier présente une approche modulaire et paramétrique pour évaluer la sécurité des systèmes avec GNSS dans la signalisation ferroviaire. Le système complexe est décomposé en modules puis modélisé de façon formelle. Ce travail s'inscrit dans le cadre d'une méthode de sécurité générique.**

Abstract — **A modular and parametric approach to evaluate the safety of GNSS-based systems in railway signalling is presented in this paper. The complex system is broken down into modules that are formally modelled. This work is part of a generic safety method**.

Mots-Clés — Localisation ferroviaire, GNSS, Sécurité ferroviaire, Méthodes de vérification formelle, Approche orientée modèles, ERTMS.

I. INTRODUCTION ET CONTEXTE DE L'ETUDE

L'introduction des technologies GNSS (Global Navigation Satellite Systems) pour la localisation des trains est aujourd'hui envisagée dans le but d'améliorer la compétitivité des services de transport ferroviaire. En effet les performances permises par ces technologies favorisent l'augmentation de la capacité des circulations. Par ailleurs, leur déploiement à bord des trains permet de réduire les coûts d'installation et de maintenance ; la localisation étant actuellement assurée par des équipements déployés en nombre sur la voie. Toutefois, cela implique une percée technique importante en termes de contrôle et de commande des trains. En effet, l'utilisation des signaux GNSS permettrait aux trains de se géolocaliser de manière continue et autonome sur l'ensemble des zones couvertes par les satellites GNSS. Des principes d'exploitation plus souples sont donc envisageables. En outre, l'usage des GNSS ouvre la voie à la conduite ferroviaire autonome [1]. Afin d'explorer et de promouvoir l'utilisation de solutions de localisation intégrant les GNSS dans les systèmes de contrôle-commande ferroviaires, la Commission européenne a financé plusieurs projets de recherche sur ce sujet. Les premiers grands projets étaient APOLO, GADEROS et LOCOPROL. Pour renforcer les travaux menés sur les questions de performances et de sécurité de ces systèmes, d'autres projets ont été financés au cours de la dernière décennie, tels que les projets Satloc, GaloROI et 3InSat. Le concept de "balise virtuelle" utile à la signalisation ferroviaire a vu le jour dès le projet RUNE, sa définition et sa mise en œuvre ayant été précisées plus récemment dans 3InSat, NGTC, ou ERSAT-GGC. Pour maîtriser les dégradations susceptibles d'affecter les signaux GNSS, des projets récents tels que STARS et Rhinos ont porté respectivement sur la caractérisation de la réception de ces signaux dans les environnements ferroviaires et sur le contrôle du risque d'intégrité associés à ces signaux. Actuellement, le projet européen X2Rail-2[1], financé par l'entreprise commune Shift2Rail dans le cadre de son deuxième programme d'innovation (IP2) sur la signalisation, se concentre sur les questions de certification de ces solutions avec GNSS prévues pour le positionnement des trains dans les systèmes avancés de gestion et de contrôle du trafic. Bien que ces projets de recherche n'aient pas encore débouché sur des produits commerciaux opérationnels, ils ont contribué à l'introduction du GNSS dans les mentalités ferroviaires [2]. En outre, ces projets ont soulevé plusieurs questions nouvelles portant d'une part sur la normalisation des interfaces et des spécifications pour atteindre l'interopérabilité ferroviaire sur le réseau européen. D'autre part, les travaux menés ont mis en avant des pistes sur les preuves de sécurité à apporter pour pouvoir certifier ces solutions au regard des exigences nationales et européennes en matière de sécurité ferroviaire, telles que celles des spécifications techniques d'interopérabilité (STI) relatives aux sous-systèmes de contrôle-commande et de signalisation [3].

[1] https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-2

L'apport de suffisamment de preuves de sécurité est essentiel pour garantir que tous les nouveaux risques possibles sont identifiés et contrôlés. Ces preuves permettent de répondre conformément à la réglementation et par conséquent conditionnent la mise en service de ces nouveaux systèmes. À l'heure actuelle, les questions suivantes demeurent : est-ce que les différents choix d'architecture avec leurs dispositifs de détection de fautes et leur implémentation opérationnelle mènent à un risque acceptable ? comment évaluer le risque intrinsèque au système et le risque émanant du système lorsqu'il sera en exploitation ? Quels critères de sécurité utiliser sachant que les GNSS possèdent leurs propres critères définis dans des MOPS (*Minimum Operational Performances Standards*) ? Des travaux passés [4] ont porté sur des méthodes d'évaluation de critères de performances opérationnelles liées à la sécurité et ont montré des liens possibles entre critères issus de l'aéronautique et ceux utilisés dans le domaine ferroviaire. Des travaux récents [5] ont décrit les étapes et outils permettant d'employer les méthodes de vérification formelles de propriétés de sécurité associées à une implémentation opérationnelle des GNSS dans l'ERTMS (*European rail Traffic Management System*). L'intérêt pour ce type de méthodes apparait dans le fait qu'elles reposent sur une vérification systématique et exhaustive de différentes propriétés par l'analyse automatique de toutes les situations dans lesquelles un système peut se trouver. Cette analyse s'appuie sur des modèles rigoureusement structurés afin de mettre en évidence les séquences temporelles d'événements susceptibles de conduire à un événement dangereux. Cependant, dans le contexte lié à la localisation avec GNSS, la difficulté réside dans l'obtention de modèles adéquats tenant compte des incertitudes sur l'erreur de position et des défaillances dues à la dégradation des signaux satellitaires reçus provoquées par les phénomènes de propagation locaux liés à l'environnement d'exploitation ferroviaire [6]. De plus, deux aspects dynamiques interviennent : les trains se déplacent et les phénomènes de propagation locaux dépendent de la configuration des satellites à un instant et à un endroit donné. Le problème est alors de structurer un modèle qui prend correctement en compte les aspects dynamiques et incertains [7].

Par conséquent, ce papier propose une démarche visant à établir un modèle structuré dédié à la démonstration de sécurité des systèmes de signalisation ferroviaire impliquant la technologie satellitaire dans la fonction de localisation des trains. Cette approche consiste à représenter, en parallèle et en utilisant des notations formelles, le comportement nominal du système de signalisation, l'aspect dysfonctionnel lié aux défaillances des composants, et les perturbations résultant de l'environnement d'exploitation ferroviaire. L'article s'intéresse plus particulièrement à la modélisation du comportement du système en mode nominal. Ce travail est réalisé en vue d'élaborer une méthode générique et modulaire pour évaluer le respect ou non de conditions de sécurité lors de l'utilisation des technologies GNSS pour la localisation ferroviaire.

Ce papier est organisé comme suit : la section II introduit les principes de fonctionnement des systèmes de contrôle-commande et de signalisation ferroviaire. Elle décrit en particulier la manière selon laquelle les systèmes de localisation utilisant les GNSS peuvent améliorer les performances et réduire les coûts. Les principes généraux de l'approche proposée visant à établir un modèle dédié à la démonstration de sécurité des systèmes de signalisation ferroviaire sont présentés en section III. Ensuite, la section IV est dédiée à l'application de l'approche de modélisation. Les modules permettant l'étude des caractéristiques de sécurité sont décrits en section V, la section VI se concentrant sur l'analyse de propriétés de sécurité selon deux cas d'étude. Une discussion sur la méthodologie présentée et les perspectives de ce travail seront enfin abordées dans la section VII.

II. VERS UN SYSTEME DE SIGNALISATION FERROVIAIRE AVANCE INTEGRANT LES GNSS

Pour garantir la sécurité de la circulation des trains, les systèmes de signalisation ont pour rôle principal d'orchestrer les mouvements des trains en sécurité sur le réseau. Ces systèmes permettent ainsi d'alerter le conducteur, afin qu'il puisse adapter la vitesse du train ou freiner si nécessaire. Les principales fonctions de contrôle-commande d'un système de signalisation consistent à gérer les itinéraires des trains et à les espacer suffisamment afin de prévenir les collisions et les déraillements. Pour que cela fonctionne, il faut connaître l'emplacement, la vitesse et la direction de chaque train. Les technologies utilisées jusqu'à présent ne permettant pas de connaître directement et à tout moment ces informations, les systèmes de signalisation classiques s'appuient sur la décomposition de la voie en cantons et sur des marqueurs visuels délimitant les différentes zones (signaux, panneaux, etc.) afin de fournir au conducteur du train les indications nécessaires pour faire avancer son train en sécurité. Le principe de base repose sur le fait qu'un canton ne peut pas être occupé par plus d'un train en même temps. Aujourd'hui des évolutions technologiques sont possibles en vue d'assurer une localisation précise et continue du train, notamment en lien avec le standard ERTMS. Cette section montre en particulier comment les technologies de localisation satellitaire peuvent faire évoluer ce système.

A. Le standard ERTMS

Historiquement, chaque pays de l'UE a mis en place son propre système de contrôle-commande et de signalisation ferroviaire sans harmonisation technique et opérationnelle. Afin d'assurer l'interopérabilité ferroviaire au niveau européen, la norme ERTMS a été définie. Elle décrit les spécifications fonctionnelles ainsi que l'architecture de l'ETCS (European Train Control System), le système de protection des trains prévu pour remplacer les différents systèmes nationaux.

La fonction principale de l'ETCS est de surveiller la vitesse du train en fonction des informations reçues du sous-système sol. L'ETCS amène le train à ralentir automatiquement si sa limite de vitesse autorisée est dépassée. Les modules ETCS sont répartis entre le sous-système embarqué à bord des trains et les équipements d'infrastructure au sol. En fonction des différentes configurations des équipements sol, des équipements embarqués et des conditions d'exploitation (figure 1), la norme ERTMS/ETCS définit trois niveaux d'exploitation distincts et de nombreux modes de fonctionnement. Dans la sous-section suivante, nous présenterons le niveau 2 ainsi que ses limites d'utilisation actuelles amenant à envisager les technologies GNSS pour le niveau 3. Cela est possible dans la mesure où le niveau 3 est seulement défini comme un

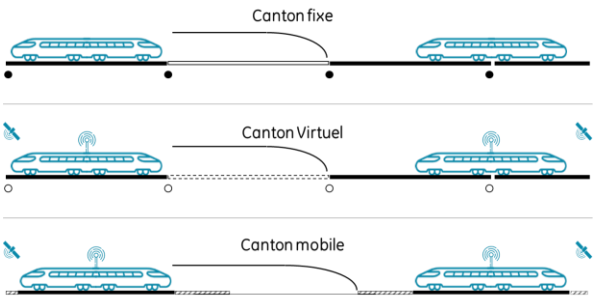

Figure 1: Principes de signalisation ferroviaire

concept à la différence du niveau 2 qui fonctionne aujourd'hui sur plusieurs lignes ferroviaires.

B. ERTMS niveau 2

Dans ce niveau d'opération, la position des trains est déterminée sur la base de la détection de l'occupation des sections de voie. Des dispositifs installés le long des rails, tels que les circuits de voie, les compteurs d'essieux et les balises, permettent de détecter les sections occupées. Faisant partie intégrante du sous-système sol des niveaux 1 et 2 d'ERTMS, les Eurobalises installées le long des voies sont utilisées pour le positionnement exact du train tandis que le RBC (Radio Block Centers), en interface avec l'enclenchement (interlocking), fournit les informations de signalisation (zones de circulation autorisées, restriction temporaire de vitesse, changement de mode opérationnel, etc.) au sous-système bord par la transmission continue de données via le GSM-R. Les équipements de voie en supplément des balises sont nécessaires pour la détection de l'intégrité du train (vérification de l'absence de rupture d'attelage). Comme évoqué précédemment, les systèmes de signalisation ferroviaire actuels s'appuient sur l'occupation de cantons de longueur fixe, i.e., chaque canton est un segment de voie entre deux points fixes. La longueur des cantons est choisie en fonction de divers paramètres tels que la limite de vitesse de la ligne, les caractéristiques de freinage des trains exploités et la densité de trafic envisagée. De plus, afin de répondre aux exigences de sécurité de l'exploitation ferroviaire. En réalité, la longueur des cantons est fixée en fonction de la distance de freinage la plus grande, indépendamment de la vitesse effective des trains. Par conséquent, plus les trains sont autorisés à circuler rapidement, plus leur distance de freinage doit être longue. Il en est alors de même pour la taille des cantons, ce qui réduit la densité de trafic de la ligne. Pour gagner en capacité, des principes d'exploitation plus souples sont étudiés, leur mise en œuvre marquera le passage du niveau 2 vers le niveau 3 de l'ERTMS.

C. ERTMS niveau 3

La définition de l'ERTMS niveau 3 telle qu'attendue dans le règlement européen sur l'interopérabilité des systèmes de contrôle-commande et de signalisation ferroviaire de l'UE [3] devra couvrir toute implémentation capable de fournir régulièrement au RBC la position du train sans nécessiter d'équipements au sol (ou à défaut, un nombre limité d'équipements). En d'autres termes, les fonctionnalités au sol dédiées à la localisation d'un train et la surveillance de son intégrité sont déportées à bord. Le train devra alors être seul responsable de la surveillance de sa position et de sa vitesse. À cette fin, les systèmes de localisation embarqués qui associent plusieurs composants de localisation performants, dont les récepteurs GNSS, et qui s'appuient sur des algorithmes d'hybridation de données innovants, sont examinés. Leur utilisation est envisagée de deux manières, comme détaillé ci-dessous.

1) Concept de balise virtuelle

La première solution proposée s'appuie sur le concept de balise virtuelle [8] pour implémenter l'ERTMS niveau 3 hybride [9]. Le principe de base consiste à remplacer un grand nombre de balises physiques (PB) délimitant des sections de voie, par des entités abstraites connues sous le nom de balises virtuelles (VB). L'objectif est d'améliorer les performances d'ERTMS niveau 2 avec un minimum de modifications des exigences actuelles et de l'architecture de référence. Pour cela, les données telles qu'elles auraient été codées dans les PB si elles avaient été installées au sol, sont à la place enregistrées dans une base de données à bord du train. Il n'y a alors plus d'activation des PB par un rayonnement électromagnétique au passage du train, mais une détection des VB. Il s'agit pour le système bord d'utiliser les informations contenues dans une VB dès lors que la position estimée du train coïncide avec celle de cette balise (VB). Ce principe conduira à une division logique plutôt que physique de la ligne en sections de longueur connue. La longueur des cantons virtuels ainsi obtenus peut alors être ajustée en fonction des conditions d'exploitation. Plus précisément, comme les balises virtuelles restent affectées à un endroit fixe, il s'agit d'augmenter leur nombre (sans coût supplémentaire) pour pouvoir diviser la ligne en cantons plus petits, ce qui laisse plus de souplesse à l'exploitation. Par conséquent, l'espacement entre trains peut être réduit et chaque train peut rouler à sa vitesse maximale autorisée tout en gardant une distance de freinage sûre.

2) Le concept de canton mobile

L'autre solution proposée pour permettre une localisation autonome des trains à partir de technologies GNSS, s'appuie sur le concept de canton mobile, concept à l'origine d'ERTMS niveau 3. Il s'agit pour un RBC de calculer une zone de sécurité autour d'un train en mouvement à partir de la position de l'arrière du train précédant. Cette zone de sécurité est prise en compte par le RBC pour déterminer et fournir l'autorisation de mouvement au train (MA), i.e., le point cible à ne pas franchir ainsi que la vitesse limite cible à ce point. Par conséquent, les distances entre trains qui se suivent peuvent être considérablement réduites, en s'appuyant principalement sur la distance de freinage (augmentée des temps de latence des messages radio transitant entre le RBC et le train, et d'une certaine marge de sécurité pour les incertitudes liées à l'estimation de position).

Le principe de signalisation à l'aide de cantons mobiles repose donc sur la communication continue entre sous-systèmes sol et bord et sur le calcul de MA. Ce principe est actuellement implémenté dans certaines lignes de métro automatique, dans le cadre des systèmes de 'contrôle des trains basés sur la communication' (CBTC).

Cette section a permis de montrer les évolutions de rupture technologiques qui sont envisagées pour les systèmes de localisation dans le contexte de l'ERTMS, notamment avec l'emploi de systèmes satellitaires. Les deux pistes présentées n'impliquent pas seulement de redéfinir certaines règles d'exploitation ferroviaire, mais rend également nécessaire de reconsidérer, voire de réinventer, les démonstrations de sécurité attestant que le risque d'accidents lié à l'utilisation du GNSS est maîtrisé [10]. À cette fin, la section suivante définit les principes d'une nouvelle méthode

d'évaluation de la sécurité fondée sur un modèle dans lequel l'exploitation ferroviaire est considérée ainsi que l'incertitude et les erreurs des systèmes de positionnement avec GNSS.

III. PRINCIPES DE BASE DE L'APPROCHE DE MODELISATION POUR L'EVALUATION DE LA SECURITE PROPOSEE

Dans cette section, nous décrivons le cadre permettant de mettre en place une méthodologie d'évaluation de la sécurité fondée sur des modèles et utilisant des notations formelles pour évaluer la sécurité des opérations ferroviaires lorsque des systèmes de localisation avec GNSS sont utilisés.

A. Configurabilité et modularité

Le service de localisation fourni par un GNSS ne peut pas être garanti sur l'ensemble du réseau ferroviaire en raison de l'indisponibilité des signaux dans les tunnels et des phénomènes de masquages dans les environnements contraints (zones urbaines denses, forêts, tranchées ferroviaires, etc.). C'est pourquoi il est nécessaire de coupler tout récepteur GNSS à d'autres moyens de localisation embarqués (capteurs inertiels, odomètre, etc.). Cela donne lieu à différentes propositions de solutions d'architectures, à la fois au niveau du couplage physique des composants qu'au niveau de la fusion de leurs données (hybridation), sans oublier les fonctions de détection d'erreur associées. Nous sommes donc dans un contexte de systèmes complexes pour lesquels aucune preuve de sécurité adéquate n'a encore été fournie [11].

Dans l'optique de développer une méthodologie d'évaluation de la sécurité adaptée aux différentes architectures possibles (certaines étant connues, d'autres étant en cours de proposition), il est crucial de réfléchir à une modélisation flexible et adaptable aux différentes solutions. Ainsi, nous optons pour une approche paramétrique et modulable permettant d'examiner plusieurs configurations avec un minimum d'effort de paramétrage.

Afin d'adapter la modélisation à la complexité de ces systèmes, nous adoptons une approche modulaire en décomposant le système en sous-systèmes suivant une logique structurelle. Ces sous-systèmes sont ensuite divisés en composants pouvant être caractérisés individuellement (ordinateur de bord, récepteur GNSS, odomètre…). Enfin, chaque élément ainsi obtenu est modélisé par une représentation formelle qui reflète ses paramètres, ses états et son évolution. De plus, ces modules peuvent communiquer et échanger des données afin de représenter l'état du système global.

En effet, la modularité implique de nombreux avantages en termes de la réutilisabilité et de flexibilité des modules du système. De plus, cette méthode de modélisation, fondée sur des modules paramétriques et hautement configurables, facilite également la considération de multiples architectures possibles.

B. Utilisation de méthodes formelles

La fonction de localisation est une fonction critique pour le contrôle/commande ferroviaire. Dès lors, l'utilisation de méthodes de vérification formelles est fortement recommandée pour fournir des preuves de sécurité [12]. En effet, contrairement aux méthodes de test sur site, les techniques formelles s'appuient sur des bases logiques et mathématiques rigoureuses et permettent une analyse exhaustive du comportement du système modélisé au moyen de notations formelles [13]. À ce propos, une enquête récente réalisée dans le cadre du projet européen ASTRail démontre l'applicabilité et les avantages des méthodes formelles dans le domaine ferroviaire [5].

L'approche proposée dans le présent document s'inscrit dans ce contexte. En particulier, le comportement du système est décrit dans un formalisme de type automates à états. D'autre part, les propriétés à vérifier sont décrites dans une logique temporelle. Finalement, un algorithme de vérification automatique, de type « model checking », explore les états possibles du système afin de prouver si le modèle satisfait ou non la propriété. Un contre-exemple est notamment présenté, en exploitant les interdépendances temporelles, quand la propriété n'est pas vérifiée. En outre, nous adoptons différents points de vue de modélisation comme détaillé dans ce qui suit.

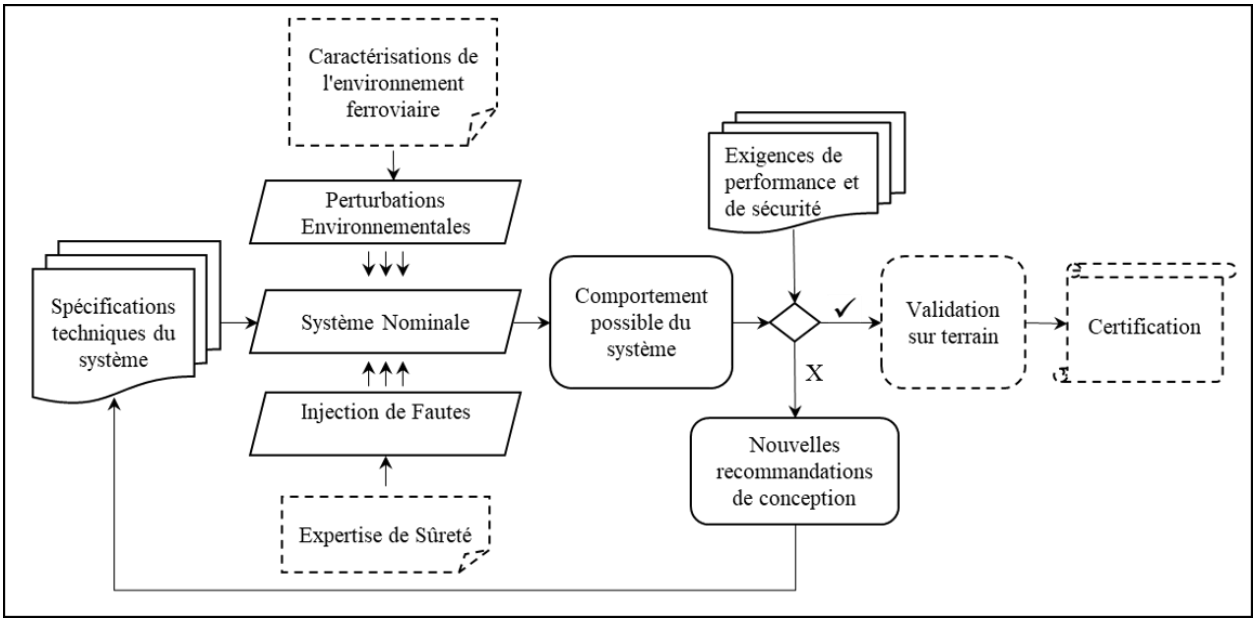

Figure 2: Schéma de l'approche proposée

C. Les points de vue de modélisation

Pour fournir une représentation fidèle du système, nous choisissons de construire nos modèles selon trois points de vue (Figure 2): fonctionnel, dysfonctionnel et retraçant les interactions avec l'environnement opérationnel.

1) Point de vue fonctionnel

Ce premier aspect de modélisation a pour objectif de traduire le comportement nominal du système. Le comportement nominal du système est représenté par l'ensemble de ses évolutions et ses fonctionnalités telles que prévues lors de la conception du système. Ceci repose sur les performances que les constructeurs garantissent pour leur composant en l'absence de faute. Ces exigences de performance sont définies dans les spécifications techniques. Les fournisseurs des composants considérés sont tenus de garantir leur respect.

Comme vu précédemment, l'architecture du système est préalablement décomposée en modules. Compte tenu de ces modules et des spécifications techniques du système, les différentes fonctionnalités internes du système sont formellement traduites et modélisées. Ceci passe par la détermination de l'ensemble des informations et données en entrée et en sortie de chaque module, ainsi que ses interactions et ses échanges de données avec les autres modules.

Finalement, l'état du système global à un moment donné est représenté par l'ensemble des états actifs de tous les modules constituant le système.

Cet aspect de comportement nominal du système sera particulièrement développé et détaillé dans la section V de ce papier.

2) Point de vue dysfonctionnemel

Ce point de vue de modélisation est motivé par la nécessité de prendre en considération les aspects dysfonctionnels ou de fonctionnement dégradé suite à l'occurrence de faute dans le système.

Cet aspect vise particulièrement à étudier les paramètres FMDS (Fiabilité – Maintenabilité – Disponibilité – Sécurité) du système. Cela est rendu possible suite à l'introduction de paramètres probabilistes liés aux caractéristiques des éléments du système en leur associant des taux de défaillance et des taux de réparation.

De plus, cet aspect de fonctionnement dégradé permettra d'analyser différentes variantes d'architectures en examinant l'introduction de redondances.

Il est à noter que cette approche basée sur des modèles formels ne vise pas à remplacer ou éliminer le rôle des experts métiers dont les connaissances techniques et opérationnels sont indispensables. Elle cherche plutôt à les accompagner en mettant à leur disposition des outils d'aide à la décision établis sur des fondements mathématiques venant en support des analyses de sûreté de fonctionnement (SdF). En effet, l'ensemble des paramètres liés aux occurrences de fautes sont des données d'entrées pour les modèles pouvant provenir de bases de données ou d'expertises de SdF. De plus, des fautes peuvent être volontairement et facilement injectées dans le modèle selon les cas de test étudiés [14].

3) Point de vue retraçant les interactions avec l'environnement

Figure 3: Exemple des différents types d'environnement ferroviaire

L'objectif de ce dernier point de vue de modélisation est de représenter les dégradations liées à l'interaction du système avec son environnement d'exploitation.

Cet aspect découle des perturbations des signaux GNSS avec des éléments environnementaux tels que la végétation ou les bâtiments. Ces perturbations peuvent entraîner le blocage, l'atténuation, la réflexion et la diffraction de chaque signal. Les signaux bloqués peuvent être facilement détectés puisqu'ils ne sont pas reçus par le système. Dans les autres cas, les temps de propagation d'un signal entre les satellites et le récepteur peuvent être retardés. Étant donné que ces temps de propagation sont les paramètres les plus importants pour l'estimation de la position par GNSS, les informations de positionnement peuvent être biaisées sans que le système ne détecte ces perturbations.

De ce fait, et dans le but de caractériser l'environnement ferroviaire, plusieurs projets reposant principalement sur des campagnes de mesures tentent d'étudier et de modéliser les performances liées au système de localisation par GNSS dans différents contextes d'exploitation (Figure 3).

Un ensemble d'exigences minimales devrait alors être associé à chaque type d'environnement. Dans l'approche proposée dans ce papier, les informations résultats de ces projets sont considérées comme des données d'entrée paramétrables dans nos modèles.

La section suivante présente l'application de cette approche d'évaluation de la sécurité dans le cas de l'ERTMS niveau 3 hybride fondée sur le concept de balise virtuelle présenté en section II.

IV. APPLICATION DE L'APPROCHE A L'ERTMS NIVEAU 3 HYBRIDE

Ce chapitre illustre l'application de la méthode précédemment décrite sur un système de signalisation ferroviaire de type ERTMS niveau 3 hybride. Comme ce système s'appuie sur les spécifications d'ERTMS niveau 2 en y introduisant le concept de balise virtuelle, nous nous appuierons sur les spécifications techniques d'ERTMS niveau 2 [15], en particulier celles dans lesquelles interviennent les aspects liés à la localisation des trains. Dans un premier temps, le système de signalisation est modélisé selon le point de vue fonctionnel. Le modèle résultant pourra être enrichi par la suite en introduisant les aspects de fonctionnement dégradé ainsi que les perturbations liées à l'environnement.

Pour répondre à l'objectif de modularité de l'approche, la première étape consiste à décomposer le système global.

A. Décomposition du système

Le système de signalisation étudié est divisé en deux sous-systèmes : système embarqué, système au sol.

Le sous-systèmes sol (Trackside) comporte :

- *Interlocking* ***(ITX):*** responsable sur la gestion de l'itinéraire des trains et de l'acquisition du statut d'occupation des voies.
- *Radio Block Centers* ***(RBCs):*** recueillent l'état des voies (cantons occupés / libres) et fournissent aux trains les autorisations de mouvement, les profils de vitesse statiques et d'éventuelles alertes d'urgence.
- *Physical Balises* ***(PB):*** transmettent des télégrammes de position au train lorsque celui-ci les croise.

Dans le sous-système embarqué à bord du train, nous considérons les modules suivants.

- *Radio Transmission Module* ***(RTM)****:* fournit une interface bidirectionnelle avec le système au sol.
- *Balise Transmission Module* ***(BTM)****:* interface utilisée pour alimenter les balises en énergie et recevoir les télégrammes de ces balises.
- *European Vital Computer* ***(EVC)****:* un système informatique embarqué essentiel pour la sécurité
- *Balises Virtuelles* ***(VB)****:* entité abstraite non physique qui a un rôle équivalent aux balises physiques.
- *Virtual Balise Reader* ***(VBR):*** Module d'interface entre l'unité de localisation située à bord du train et les balises virtuelles.
- *Localisation Unit* ***(LU):*** a pour rôle de fusionner les données afin d'assurer le couplage entre les capteurs de position.
- *Train Interface Unit* ***(TIU):*** fournit une interface pour l'exécution des instructions du système de protection automatique des trains (ATP).
- *Driver Machine Interface* ***(DMI):*** interface bidirectionnelle avec le conducteur du train.

Dans la suite de la démarche, chaque module devra être formellement modélisé. Les modules représentant PB, VB, BTM, VBR et LU sont développés dans la section V. L'outil adopté pour cette étape de modélisation est présenté ci-dessous.

B. Motivations du choix de l'outil UPPAAL

Afin d'implémenter l'approche proposée, nous choisissons d'utiliser l'outil UPPAAL SMC (Statistical Model Checking). Les modèles UPPAAL sont basés sur des automates temporisés stochastiques très expressifs. Cet outil formel de modélisation et de vérification permet la représentation en temps-réel du système et permet de considérer les aspects probabilistes [16]. De plus, l'utilisation d'UPPAAL permet une représentation selon une approche modulaire. Ces modules, qui évoluent en parallèle dans le temps, peuvent être synchronisés et communiquer via des "canaux de diffusion" et des variables partagées. D'autre part, chaque module est considéré comme un *"template"* qui peut être instancié en fonction du besoin de modélisation par le biais de paramètres de configuration. Cela permet notamment la généralisation à plusieurs trains sans avoir à modifier le modèle global. On peut ainsi effectuer des simulations et des analyses pour un certain nombre de trains non fixé au préalable dans le modèle. L'ensemble de ces fonctionnalités peuvent être conjointement utilisées. Ceci répond aux besoins et aux objectifs visés par l'approche de modélisation proposée dans ce papier (modularité, prise en compte des aspects probabilistes, flexibilité et paramétrabilité). Ceci explique le choix de l'outil Uppaal.

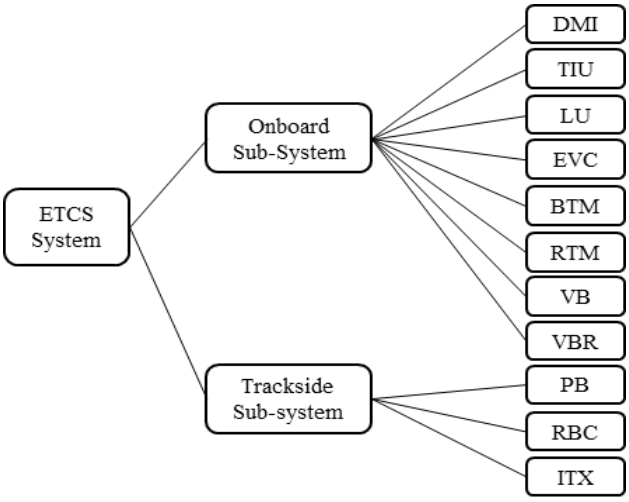

Figure 4: Décomposition du système ETCS

Les hypothèses et principes adoptés pour la modélisation sont présentées dans la sous-section suivante.

C. Hypothèses du système considéré

Le système de signalisation modélisé est un système ERTMS niveau 3 hybride adoptant le principe de balise virtuelle et sans changement de niveau pendant le trajet.

Dans ce papier, on s'intéresse uniquement à l'aspect de localisation des trains et les incertitudes introduites suite à l'utilisation des systèmes GNSS. De ce fait, les aspects liés aux pertes de paquets lors de la communication Radio, aux erreurs de calculs et de transmission des MA, et au problèmes de '*handover*' lors du changement de zone radio gérée par un RBC, ne sont pas considérés dans cette contribution. Les erreurs humaines n'étant pas prises en compte dans cette contribution, nous supposons que les procédures d'accélération et de freinage sont automatiquement déclenchées par l'EVC sans passer par le module DMI qui pourrait traduire les retards et erreurs liés aux réactions du conducteur.

Le modèle d'automate liés aux modules qui concernent directement la localisation des trains sont décrits dans la section suivante.

V. PRESENTATION DES MODULES LIES A LA LOCALISATION AVEC GNSS

Cette section décrit les modules développés dédiés à la localisation. Les modules ont pour but de traduire le comportement global de chaque composant du système en fonctionnement nominal. Ils peuvent naturellement interagir entre eux.

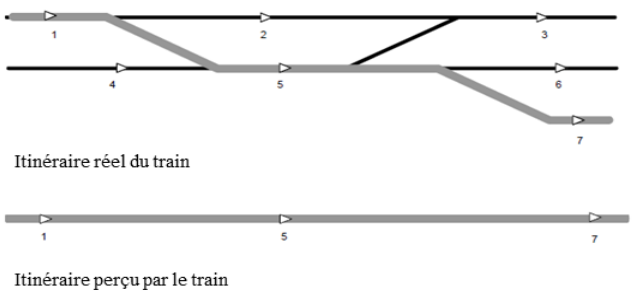

Figure 5: Itinéraires perçu par le train [3]

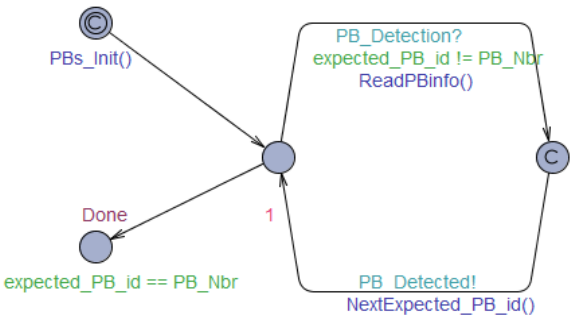

Figure 6: Module représentant l'enchaînement des balises physiques franchies par un train

A. *Module représentant les balises PB et –VB*

Ces modules (PB et VB) ont pour objectif de modéliser l'enchaînement des balises physiques ou virtuelles franchies par un train. La Figure 6 illustre uniquement le module PB sachant que le module VB se calque sur ce modèle en remplaçant PB par VB. Ces modules représentent finalement les itinéraires empruntés par un train. Ces itinéraires peuvent être complexes du fait des différents changements de voie possibles. Cependant, l'itinéraire est perçu par le train d'une manière linéaire puisque le sous-système bord a uniquement connaissance des balises qu'il doit franchir, comme le montre la Figure 5. L'ensemble des balises que va rencontrer le train sur son itinéraire forme alors une liste modélisée par une variable de type tableau. Chaque colonne du tableau regroupe les informations contenues dans le télégramme que transmets chaque balise : identifiant, position de référence….

Les modèles d'automate PB et VB traduisent le comportement d'une balise dont la fonction est de transmettre des informations au système bord. Cette action s'effectue lorsque le train franchit la balise physique ou virtuelle, i.e. la position de référence de la balise. Ces modèles sont des modules passifs dont l'évolution dépend des sollicitations émanant du train via une interface appropriée. Cette interface représente l'opération d'activation des balises.

Afin de distinguer les balises physiques placées sur la voie des balises virtuelles qui elles sont des entités logiques, deux modules sont développés (PB et VB respectivement). Le module VB est associé au module d'interface VBR, tandis que le module PB dépend du module d'interface BTM.

B. *Modules d'interfaces BTM et VBR*

Comme mentionné précédemment, les balises ne transmettent les informations que si elles sont activées par le train via une interface appropriée. Les modules BTM et VBR sont les modules d'interface entre l'unité de localisation située à bord du train et les balises. Le rôle de ces modules est de représenter l'opération d'activation des balises. Pour les PB cette activation se fait via un champs électromagnétique émis en permanence par le BTM. Dans le cas des VB, le module VBR calcule périodiquement la position de l'antenne du récepteur GNSS et la compare avec les emplacements associés aux balises virtuelles.

L'opération d'activation est modélisée dans le modèle d'automate Figure 7 par la fonction '*testVB_Activation*' ('*testPB_Activation*' dans le cas de la PB, cf. Figure 8). Cette fonction prend comme donnée d'entrée la position estimée de l'antenne GNSS pour le VBR (la position réelle du train pour le BTM) afin de la comparer aux positions de VB enregistrées dans la base de donnée du train (à la position de référence de la balise prévue dans l'itinéraire du train).

Si la position du train correspond à l'emplacement d'une balise, la fonction retourne une valeur 'vrai'. Elle modifie également la variable booléenne utilisée comme garde sur la transition '*VBActivation*' ('*PBActivation*') permettant la communication entre le train et la balise activée. La synchronisation entre les modules VB et VBR (ou bien PB et BTM) est alors possible et les informations de la balise sont transmises au train.

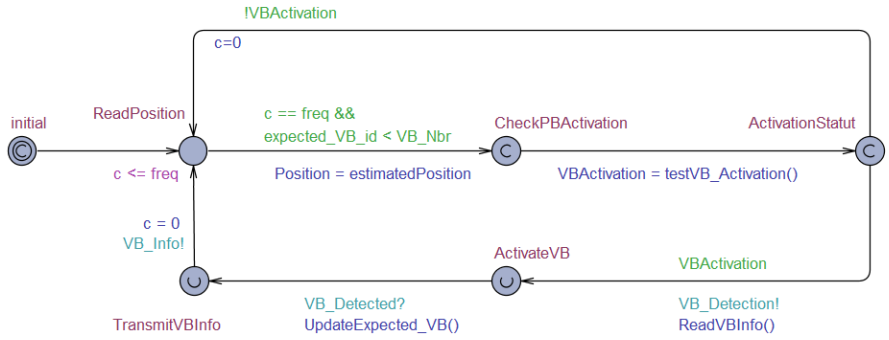

Figure 7: Modules d'interfaces VBR

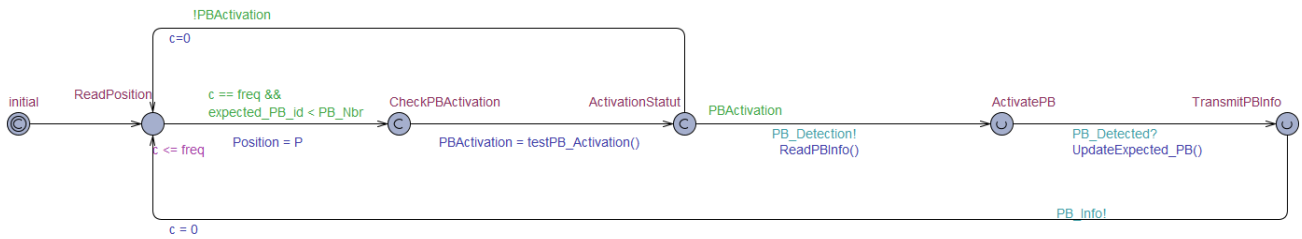

Figure 8: Modules d'interfaces BTM

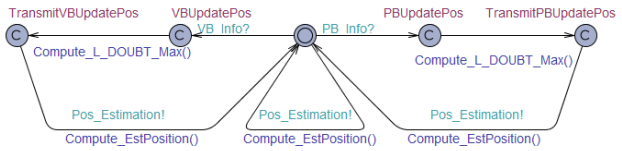

Figure 9: module de l'unité de localisation

Dans le cas où la position du train ne correspond pas à un emplacement de balise, la fonction '*test_activation()*' retourne une valeur 'faux', la transition de synchronisation n'est alors pas valide et le module retourne à l'état initial sans activer la balise. Ce processus est répété cycliquement jusqu'à ce que toutes les balises prévues sur l'itinéraire soient détectées.

C. Module de l'unité de localisation LU

Le module de localisation (Figure 9) traite les informations issues d'une balise détectée. Ces informations sont alors considérées couplées à d'autres capteurs de position (ex. l'odomètre) afin d'estimer la position du train, sa vitesse, ainsi que les bornes de l'erreur de position et l'intervalle de confiance de l'estimation de position. Le module LU communique avec les modules d'interface (VBR – BTM) via des transitions de synchronisation permettant au LU de récupérer les informations des balises.

Les performances intrinsèques des différents capteurs doivent être garanties par les constructeurs et spécifiées dans les exigences techniques du système (ex. la précision). Le module de localisation s'appuie alors sur ces paramètres en les considérant comme des données d'entrées afin de pouvoir calculer et estimer toutes les valeurs liées au positionnement du train. Dans le cas applicatif de cette section, l'ERTMS niveau 3 hybride, les erreurs d'estimation de la position de la VB (i.e. écart par rapport à la position de référence) sont calculées sur la base des spécifications définies dans le cadre du projet européen X2Rail-2 [17]. Ces spécifications s'appuient sur une règle qui dépend actuellement des paramètres suivants (Figure 10) :

- Imprécision sur la position de référence des balises (erreur calculée dynamiquement par le VBR) : *'VbdDynAcc'*
- Imprécision sur la détection des balises (valeur statique d'erreur liée aux imprécisions pouvant être introduites lors de la préparation des données constituant la base de données enregistrée à bord) : '*EVbdAcc*'
- Imprécision liée à l'odomètre (erreur qui dépend de la distance parcourue depuis la dernière balise) *'OdoAcc'*

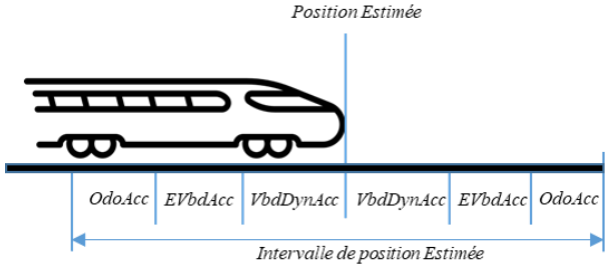

Figure 10: Intervalle de confiance lié à l'estimation de la position

Ces paramètres sont combinés selon l'inégalité suivante :

$$L_{Doubt} \leq Max(0,(VbdDynAcc-EVbdAcc)) + EVbdAcc + Q\_LOCACC + OdoAcc$$

Cette inégalité est implémentée dans notre modèle à travers les fonctions : *Compute_L_DOUBT_Max()* et *Compute_EstPosition()*. La deuxième fonction calcule la position estimée à bord du train juste au moment où elle est appelée. La première fonction calcule l'intervalle de confiance associé à cette estimation.

Dans le cas où la balise détectée est une balise physique, seule une erreur statique liée à l'incertitude du positionnement de la balise sur le rail Q_LOCACC est prise en compte.

Dans le modèle, les paramètres statiques (constants) sont définis lors de la déclaration des variables. Les paramètres dynamiques évalués à bord du train sont quant à eux calculés et mis à jour par l'automate en utilisant la fonction '*Random()*'. Cette fonction génère une valeur aléatoire comprise dans l'intervalle spécifié par les exigences. Différentes lois de calcul de position et exigence de performance du système pourront être considérées par la suite grâce à l'adaptation des paramètres de configuration de nos modèles.

Finalement, le module LU synthétise les résultats pour composer un 'rapport de position' (il s'agit du message PR envoyé depuis le sous-système bord vers le RBC). Ce rapport comporte l'ensemble des informations (position estimée, borne maximum sur l'erreur, sens de circulation du train, vitesse instantanée…) et sera transmis au module EVC. Le module EVC s'appuiera d'une part sur ce rapport de position ainsi que sur les autorisations de mouvement MA communiquées depuis le RBC via RTM, et d'autre part sur les caractéristiques de freinage du train afin de calculer la "courbe de freinage" garantissant la supervision sur la conduite du train.

D. Dynamique

Ce module (cf. Figure 11) ne représente pas un composant physique du système ERTMS, mais a pour objectif de modéliser les aspects dynamiques liés aux mouvements du train sur la voie, à savoir la position et la vitesse instantanée. Ces paramètres jouent un rôle important pour deux raisons : 1) pour permettre de modéliser les déplacements et l'espacement entre les trains 2) étudier la sécurité des opérations ferroviaires en fonction des caractéristiques de freinage.

L'utilisation de l'outil de modélisation UPPAAL avec l'extension SMC permet de traduire de manière fiable cet aspect. L'utilisation des variables de type « *horloges hybrides* » permet de modéliser les grandeurs physiques dont la variation suit une évolution pouvant être modélisée en système d'équations différentielles.

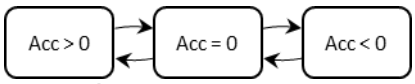

Figure 11: les trois états de la dynamique du train

La déclaration d'une variable de ce type représente la vitesse du train. Sa variation dépend de la valeur de l'accélération instantanée du train. « *V'==Acc* » est défini comme invariant d'un nœud état dans le module dynamique du train. Ainsi, la vitesse du train est automatiquement calculée de manière dynamique et continue. De même, la variable représentant la position du train est définie en fonction de la vitesse instantanée du train « *P'==V* ».

Le modèle à la figure 11 distingue 3 états dépendant de la valeur de l'accélération :

- Acc > 0 : représentant les phases d'accélération.
- Acc < 0 : représentant les phases de freinage.
- Acc=0 : cet état représente la circulation du train à vitesse constante.

Le module résultat est un module passif, dont l'évolution et le passage d'un état à un autre dépend des instructions émises par l'EVC.

La modélisation de la structure globale du système et de son évolution possible dans le temps font l'objet de la section suivante dédiée à l'étude de caractéristiques de sécurité.

VI. MODULES DES CARACTERISTIQUES DE SECURITE

Dans cette section, nous montrons comment étudier des caractéristiques de sécurité à partir du modèle formel du système présenté précédemment. Pour cela, deux cas d'étude sont décrits. La vérification du modèle et la simulation par UPPAAL sont utilisées.

A. *Cas d'étude 1 : « dépassement d'un point de danger »*

Figure 13: Cas d'étude dépassement d'un point de danger

Ce point de danger peut représenter : une jonction, un passage à niveau ou bien le début d'un canton occupé (Figure 13). Il est associé à la fin de l'autorisation de mouvement. Afin que la propriété de sécurité soit vérifiée, on doit garantir que la position du train ne dépasse en aucun cas ce point.

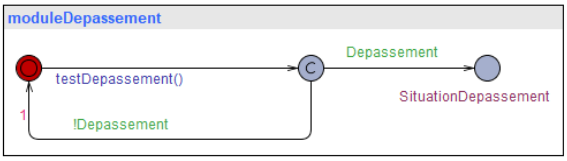

Figure 14: Module dépassement d'un point de danger

Pour cela, on propose de combiner le modèle du comportement du système à un module dédié à la vérification de cette propriété (Figure 14). La fonction principale de ce module est une fonction de test '*testDépassement()'*. Cette fonction, récupère la position du train de façon continue et la compare à la position du point de danger préalablement déterminée. Si le point n'est pas dépassé, la fonction test retourne '*faux'* et le module retourne à l'état initial. Dans le cas où la condition de sécurité n'est plus respectée, cette fonction '*testDépassement()'* retourne '*vrai'* et la transition vers l'état '*SituationDepassement*' est alors validée. L'algorithme du model-checking intégré à UPPAAL est finalement utilisé pour vérifier l'atteignabilité de cet état '*dépassement'*.

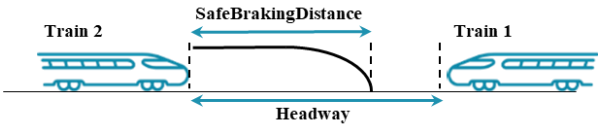

Figure 15: Cas d'étude espacement entre deux trains

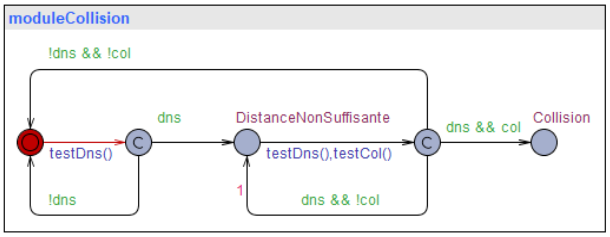

Figure 12: Module espacement entre deux trains

B. *Cas d'étude 2 : « collision »*

Le modèle d'automates présentés dans ce papier traduit la dynamique d'un seul train sur la voie. Cependant, les modules implémentés en utilisant l'outil UPPAAL sont considérés comme des classes (*Templates*). On peut alors facilement généraliser le modèle à plusieurs trains juste par l'utilisation des paramètres.

Il est à noter que les auteurs de [18] ont montré qu'il suffit de prouver qu'un système de signalisation est exempté de collision entre deux trains quelconques pour garantir la sécurité d'un nombre indéterminé de trains. De ce fait, une modélisation de la circulation de deux train successifs est alors suffisante.

Dans ce cas, il faut que l'espacement entre les deux trains soit étudié. Cet espace doit être :

- Supérieur à la distance de freinage du deuxième train afin de garantir que ce train peut s'arrêter en toute sécurité en cas de besoin.
- Supérieur à zéro pour traduire l'absence de collision

Le module développé pour ce cas de test (Figure 12) évalue la probabilité d'être dans la situation critique '*Distance de freinage Non Suffisante'* ainsi que l'atteignabilité de l'état d'accident *'Collision'*

Les modules présentés dans cette contribution ont pour objectif d'illustrer les principes pouvant être exprimés en adoptant l'approche que nous proposons. Ces modules

peuvent être enrichis graduellement et adaptés aux spécificités des cas d'études.

VII. CONCLUSION ET PERSPECTIVES

L'introduction de la localisation par GNSS comme fonction de sécurité dans le secteur ferroviaire représente une rupture technologique. Outre les défis techniques liés à la conception et au développement de ces systèmes, l'acceptation et l'autorisation de cette solution ne peut être envisagée que si sa sécurité est prouvée. La preuve par des approches d'expérimentation sur site nécessite des ressources importantes (temps et coûts). Par conséquent, il convient d'envisager des méthodes de démonstration de la sécurité sans test sur site.

L'approche proposée dans ce papier peut être considérée comme un premier pas vers d'adoption de techniques basées sur des modèles formels pour l'évaluation des systèmes de localisation fondés sur le GNSS dans l'exploitation ferroviaire. L'objectif global de l'approche de modélisation est de fournir les moyens de vérifier la cohérence des comportements attendus du système lui-même (fonctionnalités internes), et du système dans son environnement d'exploitation (interactions externes)

Afin d'atteindre ces objectifs, la méthode proposée est basée sur une représentation modulaire du système. Cela permet de prendre en compte la complexité du système de manière progressive, de tester l'impact de chaque sous-système sur la performance du système global et de fournir la base d'une méthode évolutive qui peut être enrichie de manière itérative. De plus, chaque module présenté est considéré comme une classe configurable et peut être instancié via des paramètres. Ce choix de modélisation permet de considérer plusieurs trains dans différents contextes d'exploitation et différentes configurations de système avec peu de changements dans le modèle global.

Le déploiement de ces modules est réalisé selon trois angles de modélisation complémentaires. L'aspect du fonctionnement nominal est exposé dans ce papier afin de traduire formellement le comportement et la dynamique du système à partir des spécifications techniques.

Les travaux futurs envisagés dans la continuité de cette approche ont pour objectif d'implémenter les aspects complémentaires au fonctionnement nominal, en injectant des fautes dans le modèle. La vérification de propriétés de sécurité plus précises est également prévue.

Finalement, l'objectif visé par la proposition de cette méthode ne se limite pas à la vérification de la sécurité du système mais vise à contribuer à la conception de cette nouvelle génération de systèmes de signalisation ferroviaire.

REFERENCES

[1] J. Yin, T. Tang, L. Yang, J. Xun, Y. Huang, and Z. Gao, "Research and development of automatic train operation for railway transportation systems: A survey," *Transportation Research Part C: Emerging Technologies*, vol. 85, pp. 548–572, Dec. 2017, doi: 10.1016/j.trc.2017.09.009.

[2] J. Marais, J. Beugin, and M. Berbineau, "A Survey of GNSS-Based Research and Developments for the European Railway Signaling," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2602–2618, Oct. 2017, doi: 10.1109/TITS.2017.2658179.

[3] Commission Regulation (EU) 2016/919, "Technical Specification for Interoperability relating to the Control-Command and Signalling subsystems of the rail system in the European Union," May 2016.

[4] J. Beugin and J. Marais, "Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization," *Transportation Research Part C: Emerging Technologies*, vol. 22, pp. 42–57, Jun. 2012, doi: 10.1016/j.trc.2011.12.002.

[5] A. Ferrari *et al.*, "Survey on Formal Methods and Tools in Railways: The ASTRail Approach," in *Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification*, Cham, 2019, vol. 11495, pp. 226–241, doi: DOI: 10.1007/978-3-030-18744-6_15.

[6] J. Beugin, C. Legrand, J. Marais, M. Berbineau, and E. El-Koursi, "Safety Appraisal of GNSS-Based Localization Systems Used in Train Spacing Control," *IEEE Access*, vol. 6, pp. 9898–9916, 2018, doi: 10.1109/ACCESS.2018.2807127.

[7] D. Lu and E. Schnieder, "Performance evaluation of GNSS for train localization," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 1054–1059, 2015.

[8] C. Wullems, F. Sperandio, M. Basso, S. Sturaro, and S. Sabina, "A Preliminary Apportionment of Safety Targets for Virtual Balise Detection using GNSS in Future Evolutions of ERTMS," in *2018 16th International Conference on Intelligent Transportation Systems Telecommunications (ITST)*, Oct. 2018, pp. 1–8, doi: 10.1109/ITST.2018.8566952.

[9] EEIG ERTMS Users Group, "Hybrid ERTMS/ETCS Level 3," 2018.

[10] D. Basile, M. H. ter Beek, A. Ferrari, and A. Legay, "Modelling and Analysing ERTMS L3 Moving Block Railway Signalling with Simulink and Uppaal SMC," in *Formal Methods for Industrial Critical Systems*, Cham, 2019, vol. 11687, pp. 1–21, Accessed: Aug. 27, 2019. [Online]. Available: http://link.springer.com/10.1007/978-3-030-27008-7_1.

[11] A. Filip, S. Sabina, and F. Rispoli, "A framework for certification of train location determination system based on gnss for ertms/etcs," *International Journal of Transport Development and Integration*, vol. 2, no. 3, pp. 284–297, Jan. 2017, doi: 10.2495/TDI-V2-N3-284-297.

[12] CENELEC, *EN 50128 : Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems*. 2011.

[13] M. Ghazel, "Formalizing a subset of ERTMS/ETCS specifications for verification purposes," *Transportation Research Part C: Emerging Technologies*, vol. 42, pp. 60–75, May 2014, doi: 10.1016/j.trc.2014.02.002.

[14] D. Basile, M. H. ter Beek, and V. Ciancia, "Statistical Model Checking of a Moving Block Railway Signalling Scenario with Uppaal SMC," in *Leveraging Applications of Formal Methods, Verification and Validation. Verification*, 2018, pp. 372–391.

[15] ERTMS Users Group, "System Requirements Specification v3.6.0 - SUBSET-026," ERA UNISIG EEIG, Jun. 2016.

[16] A. David, K. G. Larsen, A. Legay, M. Mikučionis, and D. B. Poulsen, "Uppaal SMC tutorial," *International Journal on Software Tools for Technology Transfer*, vol. 17, no. 4, pp. 397–415, Aug. 2015, doi: 10.1007/s10009-014-0361-y.

[17] Alfio Beccaria *et al.*, "Deliverable D3.2: System Architecture Specification and System Functional Hazard Analysis of the Fail-Safe Train Positioning subsystem," Mar. 2019.

[18] P. James *et al.*, "Verification of Solid State Interlocking Programs," in *Software Engineering and Formal Methods*, Cham, 2014, pp. 253–268, doi: 10.1007/978-3-319-05032-4_19.