Contributions aux activités de sécurité des systèmes complexes critiques ferroviaires – Cadre des systèmes de contrôle-commande avancés

Julie Beugin

École Doctorale MADIS : Mathématiques, sciences du numérique et de leurs interactions

Mémoire pour l'obtention de l'Habilitation à Diriger des Recherches

Spécialité : Génie informatique, automatique et traitement du signal

Contributions aux activités de sécurité des systèmes complexes critiques ferroviaires

Cadre des systèmes de contrôle-commande avancés

Julie BEUGIN

Chargée de recherche – Université Gustave Eiffel, COSYS, ESTAS

Soutenu publiquement le 14 novembre 2024 devant le jury composé de :

Garant	Mohamed GHAZEL	Directeur de Recherche, Université Gustave Eiffel
Rapporteurs	Walter SCHÖN	Professeur des Universités, Université de Technologie de Compiègne
	Zineb SIMEU-ABAZI	Professeure des Universités, Université Grenoble Alpes
	Philippe WEBER	Professeur des Universités, Université de Lorraine
Examinateur	Stefano RICCI	Professor, Sapienza Università di Roma
Invité	Laurent CEBULSKI	Directeur de l'Établissement Public de Sécurité Ferroviaire

Laboratoire d'Évaluation des Systèmes de Transports Automatisés et de leur Sécurité

Université Gustave Eiffel, COSYS, ESTAS,

20 rue Élisée Reclus 59650 Villeneuve d'Ascq

REMERCIEMENTS

Je tiens à exprimer toute ma reconnaissance envers Zineb Simeu-Abazi, Professeure des Universités au laboratoire G-SCOP de l'Université Grenoble Alpes, Walter Schön, Professeur des Universités au laboratoire HEUDIASYC de l'Université de Technologie de Compiègne, et Philippe Weber, Professeur des Universités au CRAN de l'Université de Lorraine. Je les remercie sincèrement pour l'honneur qu'ils m'ont fait en acceptant de rapporter ce mémoire ainsi que pour leur présence au sein de mon jury d'HDR.

J'adresse également mes plus vifs remerciements à Stefano Ricci, Professeur et Doyen de la section transport de l'Université la Sapienza de Rome, ainsi qu'à Laurent Cébulski, Directeur de l'Établissement Public de Sécurité Ferroviaire, pour l'intérêt qu'ils portent à nos travaux et pour l'honneur qu'ils m'ont fait en intégrant mon jury d'HDR.

Je remercie chaleureusement Mohamed Ghazel, garant de ce mémoire, pour ses précieux conseils pour ce projet d'HDR, pour la confiance qu'il m'accorde dans notre travail commun et pour les missions partagées au sein du laboratoire ESTAS, qu'il dirige aujourd'hui.

J'ai eu le plaisir de collaborer avec de nombreuses personnes — doctorants, post-doctorant·e·s, ingénieur·e·s, stagiaires, collègues du campus de Lille-Villeneuve d'Ascq, ainsi que nos partenaires issus de l'industrie et du milieu académique. Chacun a contribué, à sa manière, au développement des recherches présentées dans ce mémoire, et je tiens à leur adresser mes sincères remerciements. Contribuer ensemble à des transports durables, en particulier dans le secteur ferroviaire, est pour moi une source de motivation constante. Je n'oublie pas les équipes administratives, techniques et d'appui à la recherche, dont le travail essentiel assure le bon déroulement des activités quotidiennes : un grand merci à elles.

Enfin, je remercie mes collègues de tous les jours, dont le soutien et la bienveillance ont enrichi mon expérience professionnelle et humaine. À chacun·e d'entre vous, je suis profondément reconnaissante pour votre aide, vos encouragements et votre amitié. Un merci particulier à Marielle et Sonia pour le temps qu'elles ont consacré à relire mon mémoire.

Je dédie ce mémoire à Aurélien et nos deux fils, et leur témoigne toute mon affection et ma gratitude pour leur soutien permanent dans ce projet.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

– INTRODUCTION GÉNÉRALE –

L'amélioration et la croissance des transports ferroviaires, et des transports guidés en général, sont aujourd'hui fortement encouragées par les acteurs décisionnels nationaux et européens. En effet, ce mode de transport collectif répond pleinement à l'enjeu central de décarbonation de nos mobilités. Un levier important d'amélioration réside dans l'évolution des systèmes de contrôle-commande et de signalisation, conçus pour gérer les circulations de manière optimisée et en sécurité. Les mutations technologiques liées à ces systèmes critiques permettent d'aboutir à une exploitation plus performante des trains. Cependant, elles soulèvent également des questions sur les mesures et conditions de sécurité à adapter face aux changements envisagés. Pour guider les réponses à apporter, la sûreté de fonctionnement, discipline spécifique tirant partie des techniques et méthodes issues de l'automatique et de l'informatique, vise à analyser le niveau de confiance accordé à tout service délivré par un système. Son analyse représente un enjeu crucial pour les systèmes critiques en général, car les pannes et les dysfonctionnements de ces systèmes peuvent entraîner des conséquences graves, telles que des décès, des blessures graves, d'importants dégâts matériels, voire des impacts sérieux sur l'environnement. De plus, les défaillances de ces systèmes peuvent réduire ou interrompre le service fourni pour une période prolongée, perturbant ainsi la mobilité des personnes et des biens et impactant l'activité économique. Afin de prévenir les dysfonctionnements résultant de défauts introduits lors du développement des systèmes critiques, ou pour remédier aux défaillances potentielles en exploitation ou aux conditions de fonctionnement problématiques, différentes techniques d'analyse de la sûreté de fonctionnement existent. Elles permettent d'identifier les erreurs, les défaillances et les liens de causalité entre événements, afin de caractériser les différents problèmes possibles, puis soit de les éliminer, les prévenir ou les tolérer, et dans tous les cas, les contrôler.

Les techniques d'analyse de sûreté de fonctionnement se confrontent à la problématique de la complexité croissante des systèmes, une réalité à laquelle ne peuvent échapper les systèmes critiques de contrôle-commande ferroviaires. Cette accentuation de la complexité est liée à différents facteurs : le nombre croissant d'éléments interconnectés et interdépendants engendrant de multiples interactions internes et externes, l'hétérogénéité des composants, qu'ils soient logiciels ou matériels, provenant de différentes technologies, ainsi que le besoin d'optimisations technologiques ou structurelles des architectures pour répondre aux exigences de performances et de sécurité. Le premier besoin d'optimisation évoqué amène principalement à intégrer des technologies issues de l'ère de la "digitalisation" qui permettent de représenter des informations par des codages binaires, de transmettre ces données entre dispositifs et de procéder à des traitements pour agir sur le système. Le second besoin est lié à la robustesse face aux pannes, et des solutions structurelles pour y répondre consistent, par exemple, à utiliser des techniques de fusion de données sophistiquées ou des stratégies de redondance de composants. En complément, il est important de noter que la gestion de la complexité elle-même constitue un facteur de complexité supplémentaire dans les processus de gestion de projet, d'assurance qualité et de sécurité. L'intervention humaine est également plus délicate

car elle peut être à la fois une source d'erreurs dans ces processus et dans le fonctionnement des systèmes eux-mêmes, ainsi qu'une barrière pour empêcher un événement redouté ou en atténuer les effets. L'utilisation d'analyses structurées, assistées de traitements automatisés, apparaît donc comme une aide indispensable aux démarches d'évaluation de sûreté de fonctionnement dans le contexte des systèmes complexes critiques.

Ce défi d'analyse de sûreté de fonctionnement face à la complexité des systèmes, je l'ai découvert en 2002 lors de mon projet de fin d'études au laboratoire en transports Fraunhofer-IVI de Dresde. Un tel défi demeure plus que jamais d'actualité dans le domaine ferroviaire avec l'utilisation actuelle et future de nouvelles technologies et de concepts opérationnels avancés visant à augmenter la capacité des réseaux ferrés. C'est suite à ce projet que je me suis pleinement investie dans l'univers ferroviaire, plus généralement dans celui des transports guidés, en me concentrant sur l'évaluation de leur sécurité lors de ma thèse de doctorat à l'Université de Valenciennes en 2006. Mon parcours m'a permis de poursuivre et d'explorer cette voie sous différents angles et dans des contextes plus spécifiques en rejoignant d'abord l'INRETS en tant que post-doctorante en 2007, puis en tant que chercheure en 2011 au sein du laboratoire ESTAS, intégré entre-temps à l'IFSTTAR, et finalement à l'Université Gustave Eiffel. Ce mémoire présente une synthèse de mes travaux de recherche et activités associées, menées initialement sur les quatre années de post-doctorat que j'ai passées à l'INRETS/IFSTTAR au sein du LEOST puis, sur les treize années que j'ai passées au sein du laboratoire ESTAS de l'Université Gustave Eiffel.

Pour garantir que le niveau de confiance d'un système corresponde aux attentes de l'utilisateur, la sûreté de fonctionnement s'appuie sur des évaluations et des moyens liés aux critères spécifiques de *fiabilité*, *disponibilité*, *maintenabilité* et *sécurité*, regroupés sous l'acronyme FDMS. La réglementation de sécurité ferroviaire se réfère à ces critères dans ses principales normes, à savoir l'EN 50126 (parties 1 et 2), l'EN 50128, l'EN 50129 et l'EN 50159 [30, 31, 32, 33, 34], et s'appuie sur les phases du cycle de vie d'un système pour définir les activités attendues en termes de FDMS. Ces normes décrivent ainsi les différents processus, analyses, et moyens à mettre en œuvre, à chaque phase. La *sécurité* est un critère essentiel dans le fonctionnement des systèmes ferroviaires, en atteste l'existence des 28 autorités de sécurité ferroviaire en Europe (l'EPSF en France, *Établissement Public de Sécurité Ferroviaire*) issues de la directive européenne de sécurité ferroviaire de 2004 [26, 25], qui s'assurent du respect des règles de sécurité lors de l'exploitation ferroviaire. Toutefois, même si la sécurité est une priorité dans le domaine ferroviaire, il faut souligner que les critères FDM et S sont interdépendants. En effet, les exigences en matière de qualité de service opérationnel, exprimées en termes de FDM, sont définies de manière à préserver les conditions de sécurité. Ces dernières sont décrites avec des exigences visant à gérer les risques, et elles peuvent limiter les performances en termes FDM, par exemple en imposant un fonctionnement du système en mode dégradé. Ainsi, il est nécessaire de trouver un compromis entre les critères opérationnels (FDM) et de sécurité pour, par exemple, ne pas systématiquement arrêter un train par mesure de précaution.

Dans ce contexte, mes axes de recherche se concentrent principalement sur les activités liées à la sécurité menées en parallèle et en interrelation avec celles dédiées à l'ingénierie système pour la conception et le développement d'un système. L'objectif est de développer des méthodes et des

approches utiles à différentes phases du cycle de vie des systèmes complexes critiques, contribuant ainsi à l'établissement de leur démonstration de sécurité avant leur mise en service. Avec les résultats et conclusions documentés issus des différentes étapes de cette démonstration, communément appelés "preuves de sécurité", ces travaux ont également vocation à assister l'apport d'entrées nécessaires à la certification de ces systèmes. À savoir que dans le domaine ferroviaire, comme dans d'autres secteurs réglementés faisant intervenir des systèmes critiques, la certification représente la dernière étape avant la demande d'accord de mise en service d'un système auprès de l'autorité nationale. Bien que les travaux menés se situent dans un cadre ferroviaire, et plus spécifiquement en lien avec les nouvelles technologies sans fil de localisation satellitaire (les GNSS, *Global Navigation Satellite Systems*) et de communication, en raison de leur nombreux atouts pour l'évolution des systèmes de contrôle-commande, j'ai voulu orienter le développement des approches proposées afin qu'elles puissent être utilisées quel que soit le domaine.

Ce mémoire d'habilitation à diriger des recherches est organisé en deux parties :

— La partie I présente mes activités sur la période 2007-2024. Elle débute par un curriculum vitæ-synthétique mettant en lumière mon parcours académique et professionnel, suivi d'un résumé de mes travaux de recherche et mes enseignements. Ensuite, mes activités d'encadrement, ma participation à des jurys et comités scientifiques, ainsi que mes contributions à des projets et expertises sont exposées. Cette section se clôture par un bilan de mes publications.

— La partie II constitue mon mémoire de recherche et comporte quatres sections :
  - La section II.1 est dédiée à la présentation des activités de sécurité dans le cycle de vie d'un système critique, débutant par la définition des concepts liés à la sûreté de fonctionnement et à la sécurité. L'objectif est de mettre en lumière chaque étape clé prévue pour contrôler, démontrer et assurer les conditions de sécurité et les méthodes qui leur sont communément rattachées. Après avoir introduit le contexte ferroviaire des travaux, les points problématiques qui émergent lors de la mise en œuvre des étapes clés seront dégagés, en particulier dans le cas des systèmes de contrôle-commande ferroviaires avancés intégrant des technologies sans fil de localisation satellitaire et de communication.
  - La section II.2 s'intéresse à l'étape d'"*appréciation des risques*" regroupant les activités qui aboutissent aux exigences de sécurité. Ces dernières impliquent l'allocation d'objectifs de sécurité aux situations dangereuses d'une part, et l'allocations de SIL (niveaux d'intégrité de sécurité) aux fonctions de sécurité d'autre part. Fondée sur ces concepts clés, une méthodologie générique d'allocations d'exigences de sécurité est proposée afin de tenir compte de la multiplicité des fonctions de sécurité en interaction. Cette méthodologie est proposée dans le cadre général des systèmes complexes ferroviaires. Ces principes sont ensuite déclinés dans le cadre de l'utilisation des GNSS pour la localisation ferroviaire en tenant compte des imprécisions dans les allocations inhérentes à ces systèmes.

- La section II.3 se rapporte à l'étape de "*démonstration de la conformité aux exigences de sécurité*", ou étape de démonstration de sécurité, pour les systèmes de contrôle-commande ferroviaires avancés intégrant des technologies sans fil. De manière générale, une telle démonstration s'appuie sur des méthodes d'évaluation de la sécurité dédiées à l'analyse des risques d'un système et vise à montrer que tous les risques identifiés sont couverts par des mesures de sécurité adéquates. Cette section se concentre en particulier sur l'analyse des risques techniques. Deux approches d'évaluation, développées et appliquées aux systèmes ferroviaires embarqués utilisant les GNSS, sont présentées : l'une à partir d'arbres de défaillance étendus, l'autre concentrée sur l'évaluation de propriétés d'intégrité.
- La section II.4 se rapporte quant à elle à l'analyse de risques opérationnels effectuée lors de cette même étape de démonstration de sécurité. Une approche de modélisation et de vérification formelle est proposée pour l'analyse de scénarios dangereux liés à l'utilisation de systèmes complexes critiques, ainsi qu'une version évoluée adaptée aux conditions opérationnelles. Cette approche prend en considération un ensemble de spécifications qui, dans le contexte de ce mémoire, se rapportent au système ferroviaire de contrôle-commande avancé ETCS niveau 3 intégrant l'utilisation des GNSS dans sa fonction de localisation.

Enfin, des conclusions et perspectives sont détaillées à la fin du mémoire de recherche.

I – CV ÉTENDU

Cette première partie constitue une synthèse des différentes activités que j'ai menées entre les années 2007 et 2024. Dans un premier temps, elle présente un CV synthétique résumant mon parcours en tant que chercheure et ma formation académique, accompagné d'éléments marquant ce parcours. Ces éléments sont ensuite détaillés, précédés d'un résumé de mes travaux de recherche réalisés durant cette période et d'une description des enseignements que j'ai dispensés au début de ma carrière. Mes activités d'encadrement sont alors exposées, suivies de ma participation à des jurys, comités et évaluations, qui témoignent du rayonnement scientifique de mes travaux. Enfin, sont décrits les projets, groupes et expertises auxquels j'ai contribué. Un bilan de mes publications conclut cette partie.

I.1 CV synthétique

PERSONAL INFORMATION

Julie BEUGIN, researcher

Université Gustave Eiffel - Campus de Lille
COSYS/ESTAS, 20 rue Elisée Reclus, 59650, Villeneuve d'Ascq, France

julie.beugin@univ-eiffel.fr

https://www.researchgate.net/profile/Julie-Beugin

https://www.linkedin.com/in/julie-beugin-phd-03382029/

ORCID 0000-0003-1981-1906

Nationality French – born on 15/06/1979, 2 children

WORK EXPERIENCE

March 2007 – present

Since 2011

Researcher – **Université Gustave Eiffel**

Permanent researcher at **ESTAS** since 01/09/2011, Laboratory of Evaluation of Automated Transport Systems and their Safety, Villeneuve d'Ascq, France

Research interest: dependability and safety evaluation of complex guided transportation systems; specific issues related to wireless solutions embedded in train control applications

- Involved in PERFORMINGRAIL project (2020-2023) – PERformance-based Formal modelling and Optimal tRaffic Management for movING-block RAILway signalling, H2020 EU Research and Innovation programme, open call of Shift2Rail
- Involved in ERSAT-GGC project (2017-2019) – ERTMS on Satellite Galileo Game Changer, H2020 EU Research and Innovation programme
- Involved in STARS project (2016-2018) – Satellite Technology for Advanced Railway Signalling, H2020 EU Research and Innovation programme
- Coordinator of the SIL project (2013-2015) – funded by EPSF (French National Safety Authority), proposal for a guide defining an allocation method for 'Safety Integrity Level' to railway safety functions
- Involved in Systuf project (2012-2015) – Telecommunication System for Future Urban Transport, French government programme 'Investments for the Future'
- Involved in GaLoROI project (2012-2014) – Galileo Localisation for Railway Operation Innovation, 7th European framework programme
- Involved in QualiSar project (2012-2013) – Qualification procedure for Galileo receivers in safety applications, 7th European framework programme

2007-2011 Post-doctoral researcher at **LEOST** from 03/2007 to 08/2011, Laboratory on Electronics, Waves and Signal Processing for Transport, Villeneuve d'Ascq, France

Topic: RAMS demonstration issues of satellite-based solutions embedded in train control applications

- 2 studies realized for DGITM (French General Directorate of Infrastructures, Transport and the Sea) on railway applications of satellite navigation, approach development for quantifying dependability performance indicators with GPS data analysis, and modelling of signal behaviour with Petri nets
- Involved in Tr@in-MD project (2007-2009) – Intelligent transport of dangerous goods by rail, French research programme in experimentation and innovation in land transport (ANR-PREDIT)

Jan. 2017 – present

Secondment agreement with **Certifer**

- Recognised as an assessor to realise ISA missions (Independent Safety Assessment)
- Involved in Grand Paris Express control-command system assessment

Sept. 2012 – present

Secondment agreement with **Railenium**

- Involved in FLEXY project coordinated by SNCF (Starting year: 2022)
- Involved in Shift2Rail-funded projects X2Rail-2 (2017-2020) and X2Rail-4 (2020-2023)
- Involved in TC-Rail project (2017-2021) and 'Train-Autonome Voyageurs' project (2018-2023), French innovative and research programme
- Involved in SATRAIL feasibility study (2016): navigation and communication satellites for railway CCS

Oct. 2002 – Feb. 2007

ATER, Temporary Research and Teaching Attaché – **UPHF**

Université Polytechnique Hauts-de-France, Valenciennes, concurrently with the preparation of my doctoral thesis

- Training of IUT (A-Level+2 years) and engineering students to dependability methods and tools, workflow management and algorithmic programming
- Research works in railway safety according to railway safety standards, applying these works in UGTMS / MODUrban European projects (urban guided transports)

March 2002 – Aug. 2002

Engineer – critical applications – **Fraunhofer IVI**

Fraunhofer Institute for Transportation and Infrastructure Systems, Dresden, Germany, to underline weaknesses and risk level of video surveillance equipment installed on station platforms. System functional modelling using UML, FMEA, and Fault Tree. Work within the KOMPAS project funded by the German Federal Ministry of Research

EDUCATION AND QUALIFICATION

2008 **Qualification to the function of 'Maître de conférence'**, *Section 61* - Computer science engineering, automatic and signal treatment, France

Oct. 2002 – Dec. 2006

PhD. Thesis — **UPHF**

Université Polytechnique Hauts-de-France, Valenciennes, France

PhD in Automation and Computing Sciences

Thesis title: Contribution to safety evaluation of complex guided transportation systems

Sept. 2001 – Sept. 2002

Master Degree — **LAMIH**

Laboratory of Industrial and Human Automation Control, Mechanical engineering and Computer Science), Valenciennes, France

Master thesis title: Fault tree modelling by neural networks for the safety evaluation of complex systems

Speciality: Industrial and Human Automation Control

Sept. 1999 – Aug. 2002

Engineering Degree — **INSA Hauts-de-France**

National Institutes of Science and Technology (ex-ENSIAME), Valenciennes, France

Speciality: automation and computing

INVITED TALKS / LECTURES

2018 **Satellite positioning in the transport domain: applications and challenges**, Workshop 4: Navigation Technologies and Geographic Information System for a better traffic management, Data Science and Mobility Conference supported by SBB/CFF/FFS, Lausanne, Switzerland

2012 **RAMS terminology in standardization**, tutorial session at the 9th FORMS-FORMAT symposium, Braunschweig, Germany

2009 **INRETS activities on Galileo, results of recent scientific research**, session panel "GNSS on tracks: railroad", the 7th Munich Satellite Navigation Summit, Germany

2008 **A dependability approach for integrating a satellite positioning system in a railway application**, invited lecture for Braunschweiger Verkehrskolloquium, DLR -Deutsches Zentrum für Luft- und Raumfahrt (German Center for Air- and Space-flight), Braunschweig, Germany

CONFERENCE ORGANISATION

2024, 2022, 2020, 2018, 2016 Member of the program committee of the Lambda-Mu conference, French reference conference on risk, safety, and reliability topics

2021 Member of the program committee of the 16th IFAC–CTS'2021 conference

2012 Member of the program committee of the 9th FORMS-FORMAT symposium

2009 Member of the program committee of the 9th ITS-T conference

REFEREE ACTIVITY

Referee activity for scientific and research institutions

2018 Assessment committee member of the risk research axis of the CETU - Tunnel Study Centre, French Ministry of Ecological Transition

2013 Research project reviewer, French National Agency for Research Expertise

Referee activity for journals

Journal of Traffic and Transportation Engineering – International Journal of Rail Transportation – Computing – Reliability Engineering & System Safety – IEEE Intelligent Transportation Systems Magazine – Journal of Rail and Rapid Transit – Simulation Modelling Practice and Theory

Participation in doctoral committees

2024 Doctoral com. member: Mohammed CHELOUATI, Railenium & ESTAS Lab of Université Gustave Eiffel

2022 Doctoral com. member: Ouail HIMRANE, ESTAS Lab, Université Gustave Eiffel

2021 Doctoral com. member: Ayyoub IMAKHLAF, Heudiasyc Lab, University of Technology of Compiègne

2018 Doctoral com. member: Manel BRINI, Heudiasyc Lab, University of Technology of Compiègne

2017 Doctoral com. member: Subeer RANGRA, Heudiasyc Lab, University of Technology of Compiègne

2016 Doctoral com. member: Cyril LEGRAND, ESTAS Lab, Université Gustave Eiffel

Participation in selection boards

2023 Selection board member: research engineer position in computer science, COSYS department, Université Gustave Eiffel

2022 Selection board member: lecturer-researcher position (ECC) in computer science, University of Technology of Compiègne

RESEARCH SUPERVISION

Contractual researcher supervision

2021-2022 Supervision of Mohammed Chelouati, Université Gustave Eiffel, "Safety of Railway Systems" Chair, post-doctoral researcher, *Contribution to safety assurance activities for autonomous trains*

2021-2022 Supervision of Rim Saddem-Yagoubi, Université Gustave Eiffel, post-doctoral researcher, *Formal approach for the safety of railway moving block systems*

2020-2022 Supervision of Insaf Sassi, Railenium, research engineer, *Safety assessment of train integrity monitoring and satellite-based localisation systems*

2020 Supervision of Nourdine Aït Tmazirte, Railenium, research engineer, *Safety behaviour of satellite-based localisation systems*

2013-2015 Supervision of Thi Phuong Khanh Nguyen, Université Gustave Eiffel, post-doctoral researcher, *Dynamic reliability and availability assessment of satellite-based localisation and communication systems in railways*

2013-2016 Kiswendsida Abel Ouedraogo, Université Gustave Eiffel, post-doctoral researcher, *Allocation of safety integrity levels in railway systems*

PhD student supervision

2020-2024 Supervision of Mohammed Chelouati, Railenium & Université Gustave Eiffel / COSYS / ESTAS, *Contributions to safety assurance of autonomous trains*

2018-2022 Supervision of Ouail Himrane, Université Gustave Eiffel / COSYS / ESTAS, *Formal approach for the safety of satellite-based localisation systems in railways*

2012-2016 Supervision of Cyril Legrand, Railenium & Université Gustave Eiffel / COSYS / ESTAS, *Safety appraisal of satellite-based localisation systems in railways*

Master student supervision

2016 Supervision of the specialised master internship of Gaël Ouensavi, Polytech'Lille, *Statistical evaluation of performance indicators for a GNSS system embedded in train*

2012 Supervision of the Master thesis of Nacer Boumeis, Université de Lorraine, *Preliminary safety and reliability study for an LTE-based wireless system*

2012 Supervision of the Master thesis of Olimpia Hoinaru, Université de Lille, *Formalisation of performance criteria using the Iglos terminology management tool*

2009 Supervision of the Master thesis of Djily Diaw, Polytech'Lille, *Performance evaluation of a satellite tracking system for freight wagons*

2008 Supervision of the Master thesis of Mathias Ruiz-Huidobro, INSA Hauts-de-France, *Development of RAIM algorithms - Receiver Autonomous Integrity Monitoring*

PERSONAL SKILLS

Language skills

French — Mother tongue

English — Understanding (listening B2, reading C1), speaking (production C1, interaction B2), writing (C2)

German — Understanding (listening B1, reading B2), speaking (production B1, interaction B1), writing (B1)

Levels: A1 and A2: Basic user – B1 and B2: Independent user – C1 and C2: Proficient user
Common European Framework of Reference for Languages

Areas of expertise

RAMS analysis — Reliability, Availability, Maintainability, and Safety methods: PHA, FME(C)A, Fault tree, Markov chain

Railway systems — Control-command and signalling: ERTMS-ETCS / CBTC / moving block principles, recognised expertise in satellite-based railway applications

Normative and regulatory framework
- Railway standards: EN50126 (RAMS), EN50128 (software safety), EN50129 (safety systems for signalling), EN50159 (Safety-related communication) – CERTIFER training certificate
- European regulation: CSM-RA – Common Safety Method on risk evaluation and assessment

Complex system engineering
- Modelling languages: UML, SysML (Eclipse Papyrus SysML 1.6)
- Modelling tools: Petri Nets, configurable timed and probabilistic automata

Programming languages — C, C++

Simulation tools — Matlab / Simulink, GRIF, UPPAAL, UPPAAL-SMC

I.2 Activités de recherche

I.2.1 Contexte général

Les travaux de thèse que j'ai entrepris entre 2002 et 2006 au LAMIH de l'UPHF, sous la supervision de Laurent Cauffriez et Dominique Renaux, m'ont donné l'opportunité d'approfondir des travaux de recherche dans le domaine de la sécurité des transports guidés. Cette expérience, combinée aux connaissances acquises sur les systèmes de signalisation dédiés à la sécurité des circulations des trains lors des projets UGTMS et MODUrban, m'a conduite à être recrutée en tant que post-doctorante à l'INRETS au sein du LEOST entre 2007 et 2011. J'y ai mené des travaux sur l'évaluation de performances de sûreté de fonctionnement de solutions GNSS (*Global Navigation Satellite Systems*) prévues pour être utilisées dans des applications ferroviaires sécuritaires. Mon parcours de chercheure à l'Université Gustave Eiffel, d'abord au sein de l'INRETS puis de l'IFSTTAR et aujourd'hui dans la composante de recherche COSYS de l'université, a donc débuté en tant que chercheure contractuelle. En 2011, j'ai intégré en tant que chercheure permanente, le laboratoire ESTAS, rejoignant l'équipe "Approche Système de la Sécurité" alors animée par El-Miloudi El-Koursi, dont j'assure la relève depuis 2023.

Lors de mon post-doctorat au LEOST (2007-2011), sous la responsabilité de Juliette Marais, j'ai mené des recherches en collaboration avec elle et Aleš Filip, à cette époque directeur du LIS (*Laboratory of Intelligent Systems*) de l'Université de Pardubice en République Tchèque. Cette collaboration avait pour but de démontrer comment les caractéristiques du service "sûreté de la vie" fourni par le système européen de navigation par satellite Galileo peuvent répondre aux exigences de sécurité ferroviaire. Cette période de post-doctorat a été, pour moi, très formatrice scientifiquement grâce à Juliette Marais qui m'a fait découvrir les GNSS et l'écosystème de recherche associé. L'intérêt des acteurs ferroviaires pour ces systèmes se manifeste par les avantages qu'ils peuvent offrir aux systèmes de contrôle-commande ferroviaire. Malgré ces avantages, ces systèmes sont confrontés à des besoins de démonstration de sécurité pour évaluer le niveau de confiance qui peut leur être accordé et ainsi pouvoir être autorisés sur le réseau ferroviaire.

Ainsi, lors de mon recrutement à ESTAS en 2011 suite au concours de chargé de recherche sur le profil de poste intitulé "Modélisation et gestion des risques du système ferroviaire", j'ai proposé à l'équipe Sécurité d'ESTAS de continuer une partie de mes activités sur les travaux précédents afin de renforcer la collaboration entre les laboratoires ESTAS et LEOST, et d'étendre mes recherches à l'usage sécuritaire des systèmes sans fil dans le domaine ferroviaire. Les systèmes sans fil implémentent de nouvelles technologies qui permettent d'intégrer à bord d'un train ce qui est aujourd'hui réalisé à l'aide d'équipements installés le long des voies, offrant ainsi des perspectives très intéressantes pour les dernières générations de systèmes de contrôle-commande ferroviaires, tel que l'ETCS niveau 3 (développé en détail dans le mémoire de recherche). En témoignent les demandes exprimées dans les projets de recherche européens et nationaux. Cependant, leur utilisation suscite des préoccupations en matière de sécurité et de disponibilité dès lors que le service qu'ils fournissent est envisagé pour contribuer à la gestion des circulations ferroviaires et se substituer à des équipements sécuritaires au sol.

Par ailleurs, le fait de faire partie d'une équipe de recherche axée sur la thématique générale de la sécurité ferroviaire et d'avoir des liens étroits, au sein du laboratoire, avec l'équipe spécialisée dans les expertises de dossiers techniques dans ce domaine a été, et demeure pour moi, un atout pour mener mes recherches. Cela m'a également permis de mieux appréhender l'écosystème réglementaire qui encadre la sécurité ferroviaire, notamment grâce à la vue d'ensemble maîtrisée par El-Miloudi El-Koursi, tout en contribuant au renforcement des réseaux de recherche historiques du laboratoire.

I.2.2 Axes de recherche

Compte tenu de ce contexte applicatif ferroviaire en lien avec la question générale de la démonstration de sécurité de systèmes complexes, les orientations que j'ai prises se sont concentrées sur deux aspects principaux. D'une part, mes travaux se sont penchés sur l'approfondissement des conditions d'utilisation de ces systèmes sans fil dans les systèmes de contrôle-commande et signalisation ferroviaire (abrégés CCS par la suite). D'autre part, ils se sont concentrés sur l'analyse de ces systèmes, aussi bien à l'aide d'indicateurs de performance de sûreté de fonctionnement qu'à travers l'évaluation de propriétés liées aux risques issus de scénarios opérationnels dangereux. Ces orientations, suivies tout au long de mon parcours peuvent se décliner selon les trois axes qui suivent :

— Allocation d'exigences de sécurité aux fonctions d'un système critique ferroviaire : Les travaux dans cet axe ont mené au développement d'une méthodologie générique pour l'allocation de SIL (*Safety Integrity Level*) aux fonctions de sécurité par le biais d'allocation d'objectifs de sécurité aux situations dangereuses, et au développement de deux approches se concentrant sur les fonctions de systèmes intégrant la localisation satellitaire. Ces travaux s'appuient sur les contributions post-doctorales de Kiswendsida Abel Ouedraogo pour la méthodologie générique dans le cadre du projet SIL (2013-2016) en collaboration avec Frédéric Lisiecki de l'EPSF, Joffrey Clarhaut et Dominique Renaux, enseignants-chercheurs du LAMIH de l'UPHF, et El-Miloudi El-Koursi directeur de recherche à ESTAS. Les principes de la méthodologie ont été adaptés pour les fonctions de surveillance d'intégrité d'un train dans les projets européens X2Rail-2-WP4 (2017-2020) et X2Rail-4-WP7 (2021-2023) avec les contributions d'Insaf Sassi de l'IRT Railenium et d'El-Miloudi El-Koursi. Ces mêmes principes ont également été adaptés en tenant compte de l'imprécision dans les allocations, en raison de la variabilité d'utilisation des GNSS pour les fonctions de localisation considérées. Ces travaux ont été effectués dans le cadre des projets européens ERSAT-GGC (2017-2019) et X2Rail-2-WP3 (2020) avec le concours de Mohamed Sallak, enseignant-chercheur de l'Université de Technologie de Compiègne, Insaf Sassi et Nourdine Aït Tmazirte de l'IRT Railenium. Une méthode alternative a été proposée dans les travaux de post-doctorat de Thi Phuong Khanh Nguyen pour décliner des objectifs de sûreté de fonctionnement au niveau composants, et a été valorisée dans le projet régional Smarties (2018-2019).
— Analyse des risques techniques de CCS avancés : Évaluations liées à l'occurrence d'états risqués d'un système technique au comportement dynamique. Cet axe s'appuie sur le socle de recherche en analyse de sûreté de fonctionnement des GNSS que j'ai construit lors de mes travaux de post-doctorat au LEOST. Les travaux dans cet axe ont pour objectif de contribuer à

l'analyse quantitative des risques liés à des systèmes techniques ayant des états de fonctionnement dépendant du temps et dont les états de défaillance sont non directement observables. Les approches d'évaluation développées, l'une à partir d'arbres de défaillances étendus, l'autre concentrée sur l'évaluation de propriétés d'intégrité, ont été appliquées aux systèmes de localisation utilisant les GNSS, ceux-ci étant particulièrement intéressants pour la mise en œuvre des concepts opérationnels ferroviaires avancés de contrôle-commande envisagés pour l'ERTMS niveau 3. Les recherches dans cet axe se rapportent aux contributions de Thi Phuong Khanh Nguyen dans le cadre du projet européen GaLoROI (2013-2014) et aux travaux effectués durant la thèse de Cyril Legrand (2012-2016) valorisés dans le projet européen STARS (2016-2018) en collaboration avec Juliette Marais du LEOST.

— Analyse des risques opérationnels de CCS avancés : lignes directrices pour aboutir à des modèles de systèmes complexes vérifiables. Les travaux dans cet axe portent sur la proposition d'une approche de modélisation et de vérification formelle pour l'analyse de scénarios dangereux liés à l'utilisation de systèmes complexes critiques, ainsi que sur une adaptation de cette approche aux conditions opérationnelles. L'approche proposée repose sur un processus générique de modélisation visant à développer des modèles formels qui sont à la fois paramétrables, modulaires et réutilisables selon différentes configurations. La nature formelle de ces modèles permet l'utilisation de techniques de vérification automatique, en particulier les techniques de *Model-Checking* statistique capables de fournir des résultats quantitatifs liés à la sécurité de systèmes dynamiques complexes. Le processus développé prend en considération un ensemble de spécifications qui, dans le contexte de ce mémoire, se rapportent à l'ETCS niveau 3. Ensuite, cette approche est adaptée pour tenir compte de l'influence des conditions opérationnelles ferroviaires changeantes. Cette adaptation est orientée vers la vérification de propriétés liées à l'une des fonctions clés des CCS ayant des impacts en termes de sécurité : la localisation, en particulier réalisée à l'aide de GNSS. Les recherches dans cet axe se rapportent aux travaux effectués durant la thèse de Ouail Himrane (2018-2022) valorisés dans le projet PERFORMINGRAIL (2020-2023), en lien avec les travaux de post-doctorat de Rim Saddem (2021-2022) en collaboration avec Mohamed Ghazel, directeur de recherche à ESTAS.

Les travaux liés à ces trois axes seront détaillés dans mon mémoire de recherche en partie II. Ces axes incarnent le fil directeur adopté dans mon mémoire de recherche sur le déroulement des activités de sécurité le long du cycle de développement d'un système critique ferroviaire. Par conséquent, les contributions et leurs résultats seront présentés, non pas selon leur ordre chronologique de réalisation, mais selon la succession des macro-phases caractérisant les activités de sécurité. Ce choix d'organisation du mémoire a pour but de mettre en lumière les activités formant la démonstration de sécurité d'un système, appelée plus simplement *démarche sécurité*, et fournissant les preuves sur lesquelles les experts peuvent former un jugement pour la certification du système. Nous montrerons alors dans cette partie comment s'articulent nos travaux et, aussi, comment ils ont été intégrés et valorisés dans le cadre des projets de recherche européens et nationaux présentés à la section I.6. Leur positionnement dans le contexte scientifique international y sera également souligné.

Il est important de noter que ces dernières années, la recherche sur la mobilité autonome a pris beaucoup d'ampleur dans la communauté scientifique des transports. Pour élargir mes recherches, je me suis récemment intéressée à la question de l'appréciation des risques incluant l'analyse et l'évaluation des nouveaux risques opérationnels liés aux trains autonomes. Ces risques ne découlent pas uniquement de l'introduction de nouvelles technologies, mais aussi, de manière générale, du fait que le système "bord" doit être capable de réagir et de prendre des décisions seul dans les situations dangereuses tout en gérant les risques de manière dynamique, à l'instar d'un conducteur humain. Les perspectives à court terme bénéficient d'ores et déjà des travaux développés dans le projet national TC-Rail (2017-2021) et dans le cadre de la thèse de Mohammed Chelouati (2020-2024) en collaboration avec Abderraouf Boussif, chercheur à ESTAS. Ces derniers sont valorisés dans le projet national Train-Autonome – Service voyageurs (2018-2023). Ces travaux récents ne sont pas décrits en détails dans ce mémoire, car ils se rattachent de manière différente aux axes présentés précédemment, même s'il est toujours possible d'établir un lien. Néanmoins, ils sont discutés à la fin du mémoire pour mettre en lumière des perspectives à moyen et à long termes.

I.3 Activités d'enseignement

Les enseignements que j'ai dispensés pendant mes années de thèse et mon poste d'ATER (Attachée Temporaire d'Enseignement et de Recherche) sont résumés dans cette section. J'y indique le nombre d'heures effectuées, les niveaux de formation concernés ainsi que les détails de ces enseignements, en lien avec mes domaines de compétences. De plus, je répertorie les cours, tables rondes et tutoriels que j'ai donnés suite à des invitations d'organismes de recherche.

Résumé des heures d'enseignement :

Période 2002-2006	Disciplines	Cours	TD	TP	Heures effectives
ATER (1 an sur un ½ poste et 6 mois sur un poste complet)	- Sûreté de fonctionnement - Gestion de flux	15 h 12 h	27 h 48 h	24 h 145 h	228,2 h
Vacations (durant les 3 années de thèse)	- Sûreté de fonctionnement - Programmation informatique	45 h 0 h	45 h 17,5 h	36 h 90 h	214 h

Établissements d'enseignement :

- IUT GEII (Génie Électrique et Informatique Industrielle)
- ENSIAME (École Nationale Supérieure d'Ingénieurs en Informatique, Automatique, Mécanique, Énergétique et Électronique), maintenant INSA Hauts-de-France
- ISIV (Institut Supérieur Industriel de Valenciennes), constituant maintenant le département alternance de l'INSA Hauts-de-France

Niveaux :

- Enseignements en **IUT** 1ère et 2ème années (formations **universitaire** et par **apprentissage**)

— Enseignements en **école d'ingénieurs** 2ème et 3ème année (formations **universitaire**, par **apprentissage** et **continue**)

Détails des enseignements :

— Les enseignements en sûreté de fonctionnement visaient à présenter les concepts et méthodes dédiés. Réalisés en collaboration avec l'équipe enseignante de l'ENSIAME, ils étaient dispensés sous la forme d'apprentissage par problèmes. Cinq études de cas faisaient intervenir les méthodes d'arbres de défaillances et d'espace des états, en mettant particulièrement l'accent sur cette dernière pour la construction et l'évaluation de graphes de Markov. Les travaux pratiques portaient sur la construction de modèles de systèmes sous le logiciel SIMFIA (Airbus), permettant l'évaluation des paramètres de sûreté de ces modèles.

— Pour les enseignements en gestion des flux de production, j'ai pu monter un cours complet reprenant les notions de base, problématique et approches de la gestion des flux (approche par les stocks et en flux tirés, méthode MRP-*Material Requirement Planning*). Les TD et TP, en collaboration avec l'équipe enseignante, visaient à modéliser la fabrication d'un produit sur une cellule flexible (celle du groupement d'intérêt scientifique de l'AIP-Primeca, aujourd'hui dénommé GIS S.mart – *Systems Manufacturing Academics Resources Technologies* – à l'UPFH) à l'aide du logiciel de simulation Arena (Rockwell Automation). L'exécution du modèle du système de production obtenu, en lien avec un rendu visuel des tâches et parcours relatifs aux produits, permettait de vérifier la conformité du modèle avec la réalité. L'analyse des résultats de simulation permettait de tester des stratégies pour optimiser la production.

— Les enseignements en programmation regroupaient les TD et TP sur la programmation en langage C et l'encadrement d'étudiants en BETR (Bureau d'Étude et Travaux de Recherche) sur le thème de l'informatique répartie et le système d'exploitation Unix.

Conférences "invitées" : Suite à l'invitation d'organismes de recherche, j'ai participé aux cours, tables rondes et tutoriels suivants :

— **2018 :** J. BEUGIN et P.-Y. GILLIERON, *Satellite positioning in the transport domain : applications and challenges*, Workshop 4 : Navigation Technologies and Geographic Information System for a better traffic management, Data Science and Mobility Conference supported by SBB/CFF/FFS, January 31, Lausanne, Switzerland, 2018

— **2012 :** J. BEUGIN et C. STEIN, *RAMS Terminology in Standardization*, Tutorial session at the 9th FORMS-FORMAT symposium (Formal Methods for Automation and Safety in Railway and Automotive Systems), December 11-13, Braunschweig, Germany, 2012

— **2009 :** J. BEUGIN et J. MARAIS, *INRETS activities on GALILEO, results of recent scientific research*, the 7th Munich Satellite Navigation Summit 2009, session panel "GNSS on tracks : railroad", 3-5 March, Germany, 2009

— **2008 :** J. BEUGIN et al., *A dependability approach for integrating a satellite positioning system in a railway application*, invited lecture for Braunschweiger Verkehrskolloquium, DLR -Deutsches Zentrum für Luft und Raumfahrt- (centre aérospatial allemand), Braunschweig, Allemagne, 7 Février, 2008

— **2008 :** A. FILIP et al., *Galileo Safety of Life Service for Railway Signalling*, invited lecture for Braunschweiger Verkehrskolloquium, DLR -Deutsches Zentrum für Luft und Raumfahrt- (centre aérospatial allemand), Braunschweig, Allemagne, 7 Février, 2008

I.4 Encadrements doctoral et scientifique

I.4.1 Encadrements de thèses de doctorat (3)

Cette sous-section indique les doctorants avec qui j'ai mené des travaux de recherche, notamment dans le cadre de collaborations avec le LEOST de l'Université Gustave Eiffel, le laboratoire CRIStaL de l'Université de Lille et l'IRT Railenium. Trois thèses ont été soutenues en 2016, 2022 et 2024. Une future thèse dans le cadre de la chaire "Sécurité des Systèmes Ferroviaires" (cf. §I.6.3) débutera à l'automne 2024, en collaboration avec le LIS de l'Université d'Aix-Marseille.

Encadrement de travaux de thèse	
fin 2024 – fin 2027	**Araaf Dinullah RECTA** (Master 2 Master Automatique et Robotique, parcours "*Control Systems*" de l'École Centrale de Nantes) sur la "*Contribution à l'analyse de sécurité liée aux systèmes de contrôle-commande ferroviaires de dernière génération dits –à cantons mobiles–*" *Financement :* chaire "Sécurité des Systèmes Ferroviaires" *Encadrement :* R. Saddem, J. Beugin (co-directrice de thèse) et M. Ghazel (co-directeur de thèse)
10/2020 – 06/2024	**Mohammed CHELOUATI** (Master 2 Ingénierie des Systèmes Complexes de la Faculté des Sciences et Technologies de Nancy) sur la "*Contributions à l'assurance sécurité des trains autonomes*" *Financement :* Railenium au travers du projet Train Autonome – Service voyageurs *Encadrement :* A. Boussif (50%), J. Beugin (30%) et E.-M. El-Koursi (directeur de thèse) *Publication :* auteur de 2 ACL, auteur d'1 ACTI, co-auteur d'1 ACTI, auteur de 2 ACTN *Parcours ultérieur* : post-doctorant à ESTAS
10/2018 – 12/2022	**Ouail HIMRANE** (Master 2 Ingénierie des Systèmes Complexes de l'École Normale Supérieure Paris-Saclay) sur le sujet de "*l'évaluation de la sécurité et des performances opérationnelles des systèmes de localisation ferroviaire utilisant le GNSS par une approche fondée sur les modèles formels*" *Financement :* Université Gustave Eiffel (50%) et région Hauts-de-France (50%) *Encadrement :* J. Beugin (70%) et M. Ghazel (directeur de thèse, 30%) *Publication :* auteur d'1 ACL, co-auteur d'1 ACLN, auteur de 2 ACTI, co-auteur d'1 ACTI, auteur d'1 ACTN *Parcours ultérieur* : ingénieur de recherche à Railenium

Encadrement de travaux de thèse	
12/2012 – 12/2016	**Cyril LEGRAND** (Master 2 Automatisation Intégrée et Systèmes Homme-Machine, UPHF Valenciennes) sur le sujet de "*l'évaluation de la sécurité de systèmes de localisation ferroviaires basés sur les GNSS par la formalisation des concepts d'intégrité étendue*" *Financement :* Railenium *Encadrement :* J. Beugin (50%), J. Marais (30%), E.-M. El-Koursi et M. Berbineau (direc·teur·trice de thèse) avec la collaboration de B. Conrard (CRIStAL) *Publication :* auteur d'1 ACL, co-auteur d'1 ACL, auteur de 3 ACTI *Parcours ultérieur* : post-doc en collaboration avec l'EPSF et Railenium sur la modélisation opérationnelle des SGS (Systèmes de Gestion de la Sécurité), puis chargé de mission à l'EPSF ; aujourd'hui : "*Safety Assurance engineer*" chez Alstom.

I.4.2 Encadrements de post-doctorant·e·s (4)

Cette sous-section indique les chercheur·e·s post-doctoraux avec qui j'ai mené des travaux de recherche dans le cadre des projets décrits dans la section I.6.

Encadrement de travaux post-doctoraux	
06/2024-03/2025	**Mohammed CHELOUATI** (docteur de l'Université Gustave Eiffel) sur la chaire "Sécurité des systèmes ferroviaires" pour contribuer aux activités d'assurance sécurité des trains autonomes. *Encadrement* : J. Beugin (50%) et E.-M. El-Koursi (50%)
04/2021-08/2022	**Rim SADDEM-YAGOUBI** (docteur de l'Université de Montpellier) sur le projet européen PERFORMINGRAIL pour développer un processus de vérification formelle de propriétés de sécurité du système de signalisation ferroviaire ETCS niveau 3 implémentant les principes des cantons mobiles. *Encadrement* : J. Beugin (50%) et M. Ghazel (50%) *Parcours ultérieur* : maître de conférences à l'Université d'Aix-Marseille
03/2013-12/2015	**Thi Phuong Khanh NGUYEN** (docteur de l'École Centrale de Nantes) contribuant aux approches d'évaluation de disponibilité et fiabilité du système de localisation développé dans le projet européen GaLoROI (03/2013 à 01/2014). Elle a ensuite travaillé sur le projet Systuf sur la modélisation par réseaux de Petri de comportements dynamiques de défaillances/perturbations du lien radio LTE utilisé au sein de métros/tramways pour ainsi proposer des approches d'évaluation de critères de disponibilité et de sécurité. *Encadrement* : J. Beugin (90%) et J. Marais (10%), puis J. Beugin (90%) et M. Berbineau (10%) *Parcours ultérieur* : maître de conférences à l'Université de Technologie Tarbes Occitanie Pyrénées (UTTOP)

Encadrement de travaux post-doctoraux	
12/2013-09/2016	**Kiswendsida Abel OUEDRAOGO** (docteur de l'UPHF, Valenciennes) sur le projet SIL (12/2013-05/2015). Il a partagé son temps (10/2015-09/2016) entre la suite du projet SIL (pour répondre ensemble aux nouveaux besoins exprimés par l'EPSF) et le projet Use-It (dans lequel je n'étais pas impliquée). Il a travaillé sur le développement d'une méthodologie d'allocation des niveaux d'intégrité de la sécurité dans le domaine ferroviaire en tenant compte des problématiques rencontrées par les constructeurs et exploitants. *Encadrement* : J. Beugin (90%) et E.-M. El-Koursi (10%) *Parcours ultérieur* : post-doc à Railenium puis montage d'une société de consulting

I.4.3 Encadrements d'ingénieur·e·s (3)

Cette sous-section indique les ingénieur·e·s de recherche et d'étude avec qui j'ai mené des travaux de recherche dans le cadre des projets décrits dans la section I.6.

Encadrement de travaux d'ingénieur de recherche	
2020-2022	**Insaf SASSI** (docteur de la Commmunauté Université Grenoble Alpes) — sur les projets européens X2Rail-2 (WP4) et X2Rail-4 (WP6 et WP7) pour contribuer à la mise en place d'une démarche permettant d'obtenir la certification des trois classes de systèmes de surveillance de l'intégrité d'un train. — sur le projet européen X2Rail-2 (WP3) pour contribuer à la proposition d'une méthodologie d'allocation d'objectifs quantitatifs de sécurité aux fonctions du système de localisation satellitaire embarqué. *Encadrement :* J. Beugin (90%) et E.-M. El-Koursi (10%), puis J. Beugin (100%) *Parcours ultérieur* : ingénieure de recherche à Railenium
2020	**Nourdine AÏT TMAZIRTE** (diplôme d'ingénieur à l'Institut de Génie Informatique et Industriel, et Master Automatique, Génie Informatique et Image de l'École Centrale de Lille) sur le projet européen X2Rail-2 (WP3) pour contribuer à la proposition d'une méthodologie d'allocation d'objectifs quantitatifs de sécurité aux fonctions du système de localisation satellitaire embarqué. *Encadrement :* J. Marais (90%) et J. Beugin (10%) *Parcours ultérieur* : ingénieur de recherche à l'Université Gustave Eiffel

Encadrement de travaux d'ingénieur d'étude	
2021	**Abhimanyu TONK** (diplômé du Mastère spécialisé – Safety Engineering Management de l'INSA de Toulouse) sur le projet TC-RAIL pour contribuer à la démonstration de la sécurité opérationnelle de la téléconduite des trains. *Encadrement :* A. Boussif (80%), J. Beugin (10%) et S. Collart-Dutilleul (10%) *Parcours ultérieur* : ingénieur à Railenium

I.4.4 Encadrements de stages de Master (5)

Cette sous-section indique les étudiant·e·s de Master que j'ai encadré·e·s sur les sujets de stage que j'ai proposés.

Encadrement de stages	
2016 (6 mois)	**Gaël OUENSAVI** sur l'évaluation statistique d'indicateurs de SdF d'un système GNSS embarqué dans un train ⇒ validation de la formation MEs2M (mastère spécialisé Mécatronique et Management) de l'école d'ingénieurs Polytech'Lille. *Encadrement :* J. Beugin (100%)
2012 (5 mois)	**Nacer BOUMEIS** sur une étude qualitative de la sûreté de fonctionnement d'un système sans fil basé sur le LTE ⇒ validation de la formation de Master 2 - Ingénierie de systèmes complexes, spécialité automatique et traitement de l'information embarqués, Université de Lorraine, Nancy *Encadrement :* J. Beugin (60%), M. Kassab (30%), M. Berbineau (10%)
2012 (5 mois)	**Olimpia HOINARU**, stage dans le cadre du projet QualiSaR, sur la formalisation de critères de performances caractérisant un récepteur GNSS à l'aide de l'outil de gestion terminologique Iglos ⇒ validation de la formation Master 2 - Lexicographie, Terminographie et Traitement Automatique des Corpus, Université de Lille *Encadrement :* J. Beugin (70%), J. Marais (30%)
2009 (4 mois)	**Djily DIAW**, stage dans le cadre du projet Tr@in-MD, sur l'évaluation des performances d'un système de localisation par satellites de wagons de fret ⇒ validation de la dernière année du cycle ingénieur Polytech'Lill, Université de Lille *Encadrement :* J. Beugin (70%), J. Marais (30%)
2008 (6 mois)	**Mathias RUIZ-HUIDOBRO** sur le développement d'algorithmes RAIM - *Receiver Autonomous Integrity Monitoring* ⇒ validation de la dernière année du cycle ingénieur ENSIAME, Valenciennes *Encadrement :* J. Beugin (70%), J. Marais (30%)

I.5 Rayonnement scientifique

I.5.1 Participation à des jurys

Cette sous-section répertorie mes participations à des jurys de thèse, de comité de sélection et de concours.

Examinatrice dans des jurys de thèse	
5 juin 2024	**Mohammed CHELOUATI** (Laboratoire ESTAS de l'Université Gustave Eiffel) : *Contribution to safety assurance of autonomous trains*
16 déc. 2022	**Ouail HIMRANE** (Laboratoire ESTAS de l'Université Gustave Eiffel) : *Contribution to safety and operational performance evaluation of GNSS-based railway localization systems using a formal model-based approach*
11 mars 2021	**Ayyoub IMAKHLAF** (Laboratoire Heudiasyc de l'UTC) : Application des diagrammes de décision binaire pour l'analyse des arbres de défaillance cohérents et non cohérents en présence d'incertitudes
23 nov. 2018	**Manel BRINI** (Laboratoire Heudiasyc de l'UTC) : *Safety-Bag* pour les systèmes complexes

Examinatrice dans des jurys de thèse	
3 oct. 2017	**Subeer RANGRA** (Laboratoire Heudiasyc de l'UTC) : *Performance shaping factor based human reliability assessment using valuation-based systems – application to railway operations*
16 déc. 2016	**Cyril LEGRAND** (Laboratoire ESTAS de l'Université Gustave Eiffel) : *Contribution à l'évaluation de la sécurité de systèmes de localisation ferroviaires basés sur les GNSS par la formalisation des concepts d'intégrité étendue*

Comité de sélection d'enseignant-chercheur contractuel	
Oct. 2022	**Corps :** ECC de l'Université de Technologie de Compiègne **Section CNU :** 27ème, 61ème **Profil recherche :** sûreté de fonctionnement / cyber-sécurité **Laboratoire :** Heudiasyc, équipe SCOP (sûreté, communication, optimisation) **Département :** ingénierie informatique (formation par la voie de l'apprentissage)

Jury de concours externe d'ingénieur·e de recherche	
Juillet 2023	**Spécialité :** informatique scientifique **Affectation :** Département COSYS (Composants & Systèmes) de l'Université Gustave Eiffel

I.5.2 Comités de programme de conférences et présidence de sessions

Cette sous-section répertorie mes participations en tant que membre du comité de programme de diverses conférences, ainsi que mon rôle de co-présidente de session lors de certaines de ces conférences.

Membre de comités de programme	
2021	**CTS-2021** (16th *IFAC Symposium on Control in Transportation Systems*), organisé par Univ. Eiffel/COSYS/ESTAS , 8-10 Juin, Lille — Relecture d'articles — **Présidence** de la session TuA1 '*Optimisation and Control of Transportation Systems*'
2024, 2022, 2020, 2018, 2016	**Lambda-Mu** (Maîtrise des risques et sûreté de fonctionnement) — Relecture de résumés et d'articles — 2024 : **présidence** de la session interactive 1C 'Sûreté de fonctionnement appliquée à un système de formation en ligne' — 2016 : **co-présidence** de la session 4E 'fiabilité des systèmes' — 2022 : **co-présidence** de la session 1C 'Méthodes de sûreté de fonctionnement'
2012	**Forms-Format** (9th *Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems*), 11-13 décembre, Braunschweig, Allemagne — **co-présidence** de la session '*Safety Modeling and Risk Assessment*', — **présentation d'un tutoriel** en binôme avec un chercheur du laboratoire iVA de Braunschweig (Institut en transports) [INV2]

Membre de comités de programme	
2009	**ITS-T** (9th *International Conference on Telecommunications for Intelligent Transport Systems*), 20-22 octobre, Lille ⇒ relecture d'article, support au comité d'organisation
2003	**JDA/JNA** (Journées Doctorales/Journées Nationales d'Automatique), organisé par le LAMIH et le GDR MACS, 25-27 juin, Valenciennes ⇒ support au comité d'organisation
2003	**PENTOM** (Performances et Nouvelles Technologies en Maintenance), organisé par le LAMIH, 26-28 mars, Valenciennes ⇒ support au comité d'organisation

I.5.3 Évaluations pour des revues et conférences

Cette sous-section répertorie les revues internationales et les conférences pour lesquelles j'ai accepté la relecture d'articles.

Articles de revue	
2024	**JTTE** (*Journal of Traffic and Transportation Engineering*)
2023	**JRT** (*International Journal of Rail Transportation*)
2022	**COMP** (*Computing*)
2019, 2014	**RESS** (*Reliability Engineering & System Safety*)
2018, 2017	**IEEE ITS Magazine** (*Intelligent Transportation Systems*)
2016	**JRRT** (*Journal of Rail and Rapid Transit*)
2014	**SIMPAT** (*Simulation Modelling Practice and Theory*)

Articles de conférence	
2024	**CPHS 2024** (5th *Workshop on Cyber-Physical Human Systems*)
2024, 2021	**CTS** (*IFAC Symposium on Control in Transportation Systems*)
2021	**ESREL** (31st *European Safety and Reliability conference*)
2016-2024 (bisannuel)	**Lambda-Mu** (Maîtrise des risques et sûreté de fonctionnement)
2014	**TRA 2014** (*Transportation Research Arena*)
2012	**Forms-Format** (*Formal Methods for Automation and Safety in Railway and Automotive Systems*)
2018, 2009	**ITS-T** (*International Conference on Telecommunications for Intelligent Transport Systems*)
2010, 2009, 2008, 2007	**Journées des doctorants IFSTTAR** (INRETS)

I.5.4 Participation à des commissions d'évaluation et d'expertise de projets

Cette sous-section indique les commissions d'évaluation et d'expertise de projets scientifiques auxquelles j'ai participé.

Évaluatrice	
2018	**Participation à la commission d'évaluation de l'axe stratégique n° 6 du CETU** "Analyser et maîtriser les risques en exploitation" sur la période 2010-2018. CETU - Centre d'Études des Tunnels [RPEX4]
2013	**Expertise d'un projet ANR pour l'appel à projet JCJC** (programme blanc Jeunes Chercheuses et Jeunes Chercheurs), du comité SIMI 3 (Matériels et logiciels pour les systèmes et les communications) [RPEX6]

I.5.5 Participation à des groupes de recherche

Je suis membre du comité technique TC 9.2 (*Systems and Control for Societal Impact)* de l'IFAC (*International Federation of Automatic Control)* depuis 2023.

J'ai par ailleurs participé aux groupes de recherche suivants où les travaux mentionnés ont été présentés :

- **Groupe SED du GdR MACS :** R. SADDEM-YAGOUBI et al., *Moving Block System : Verification Framework*, journée commune du comité techniques SED du GDR-MACS (Systèmes à Événements Discrets) et du comité technique AFSEC (Approches Formelles des Systèmes Embarqués Communicants) du GDR-GPL, Paris, 11 Avril, 2023
- **Groupe Transfiab :** J. BEUGIN, *Approches d'évaluation de sûreté de fonctionnement de systèmes sans fil dans le domaine ferroviaire*, 1ère journée d'échanges réseau thématique de l'IFSTTAR "Transfiab", outils probabilistes pour l'analyse de la fiabilité, Marne-la-Vallée, 7 Déc. 2016
- **GERI GNSS :** J. BEUGIN et J. MARAIS, *Méthodes de sûreté de fonctionnement appliquées aux GNSS*, séminaire du GERI GNSS - Groupes d'Echanges et de recherches Ifsttar sur la Géolocalisation et la Navigation par un Système de Satellites, Villeneuve d'Ascq, 17 Nov. 2011
- **PFI GNSS :** J. BEUGIN et J. MARAIS, *L'intégrité dans les applications de localisation ferroviaire*, séminaire de la PFI GNSS - Plateformes Intégratrices sur la Géolocalisation et la Navigation par un Système de Satellites, Villeneuve d'Ascq, 4 Mai, 2010
- **Groupe ConecsSdF du GdR MACS :** J. BEUGIN et al., *Approches de sûreté de fonctionnement pour des systèmes sans fil : le cas de Galileo*, journée ConecsSdF – Co-design de systèmes commandés en réseaux Sûrs de Fonctionnement, GdR MACS, Paris, 24 Sept. 2009

I.6 Responsabilités scientifiques

Pour une partie de mes activités, je suis impliquée scientifiquement dans des projets de recherche européens et nationaux, et dernièrement, dans la chaire "Sécurité des Systèmes Ferroviaires". J'ai été sollicitée ou j'ai contribué au montage de ces projets en raison de mon expertise sur des sujets impliquant notamment les techniques d'allocations d'objectifs de sécurité et d'analyses de sûreté de fonctionnement de systèmes complexes ferroviaires, en particulier ceux intégrant les GNSS. J'ai représenté l'Université Gustave Eiffel soit directement, soit par le biais de mises à disposition dans l'Institut de Recherche Technologique Railenium.

Les ressources humaines et financières obtenues grâce à ces projets permettent d'approfondir mes orientations de recherche malgré les contraintes temporelles, notamment en fournissant des cas applicatifs et en adaptant ou en faisant évoluer les approches de manière collaborative. Les

activités sont menées en partenariat, selon le projet, avec des entités académiques (universités ou centres de recherche), industrielles ou institutionnelles, dont les membres possèdent des expertises variées.

Dans cette section, je détaille brièvement les objectifs pour chaque projet auquel j'ai participé, les contributions, les rôles et responsabilités que j'ai assumés, ainsi que les partenaires impliqués, les types de financement et les montants octroyés.

I.6.1 Projets européens (9)

1) PERFORMINGRAIL (2020-2023) – programme H2020 et 'open call' de Shift2Rail[1]

Le projet PERFORMINGRAIL (*PERformance-based Formal modelling and Optimal tRaffic Management for movING-block RAILway signaling*) a permis la participation des équipes "*Approche Système de la Sécurité*" et "*Exploitation et Intermodalité*" de notre laboratoire ESTAS.

Le projet a pour objectif de définir les spécifications et les principes d'exploitation sûrs d'ERTMS/ETCS niveau 3 fondé sur les cantons mobiles. Le projet repose sur la mise en œuvre d'une approche système qui s'appuie sur l'emploi de technologies fiables et avancées de contrôle d'intégrité et de positionnement des trains, ainsi que sur l'utilisation de modèles et techniques de vérification formels et d'algorithmes optimisés de gestion du trafic.

⇒ J'ai **contribué au montage** du projet et j'ai **coordonné le groupe de travail WP1** (*'Specifications for minimum Moving Block performance standards'*) et la tâche T1.1 (*'Review of Moving Block systems including ETCS-L3 and virtual coupling'*). J'ai contribué également aux travaux du WP2 (*'Modelling and analysis of Moving Block specifications'*) et du WP3 (*'Fail Safe Train Locationing'*).

Rim Saddem-Yagoubi (post-doctorante), Mohamed Ghazel et moi-même avons été fortement impliqués dans les travaux de recherche du WP2 qui ont mené à **4 articles de conférence** [ACTI3, ACTI4, ACTI5, ACTI6] sur la définition du 'workflow' de modélisation et d'analyse formelles, et à **3 livrables** : D2.1 (*Modelling guidelines and Moving Block Use Cases characterization*) [RPRE7], D2.2 (*Moving Block Specification Development*) [RPRE1], et D2.3 (*Moving Block Verification and Validation*) [RPRE3].

Nous avons pu fournir dans le cadre du livrable D1.1 (*Baseline System Specification and Definition for Moving Block Systems*), un état de l'art sur les systèmes utilisant les principes des cantons mobiles (*Moving Blocks*) et un état de l'art sur les systèmes de localisation utilisant les GNSS avec une description des dangers liés aux systèmes de Balise Virtuelle [RPRE5]. Nous avons pu intégrer une revue des métriques ferroviaires (FDMS) et GNSS dans le livrable D1.2 (*Best Practices, Recommendations and Standardisation to Definition of the Railway Minimum Operations Performance Standards*) [RPRE2]. Dans le livrable D3.1 (*Design document of the location algorithms*), j'ai pu apporter une synthèse des travaux de recherche liés à la localisation satellitaire pour les systèmes de contrôle-commande ferroviaire [RPRE6].

1. Shift2Rail est une initiative européenne sous la forme d'une entreprise commune (EC) ayant pour objectif de coordonner et gérer les investissements de recherche et d'innovation dans le domaine ferroviaire. Ses 9 membres fondateurs sont : Alstom, Ansaldo STS, Bombardier, CAF, NetworkRail, Siemens, Thales, Trafikverkert, et l'UE. L'EC compte 19 membres associés dont plusieurs consortia comme SmartRaCon. Ce dernier est le seul membre venant du monde académique et inclut Railenium. Europe's Rail est l'initiative successeur de Shift2Rail depuis 2023.

8 partenaires : The University of Birmingham (coordinateur), TU DELFT, Université Gustave Eiffel, CINI, Mälardalen University, CERTIFER, ROKUBUN, Eulynx

Montant : 1 335 358 € dont 157 483 € pour Univ. Eiffel/COSYS/ESTAS

2) X2Rail-4 (2020-2023) – programme H2020 ouvert aux membres de Shift2Rail

X2RAIL-4 est le projet sélectionné suite au 4ème appel à projet de Shift2Rail sur l'IP2 et l'IP5 (*innovation programmes*). Son titre mentionne les thématiques de recherche sur lesquelles des travaux sont menés : *'Advanced signalling and automation system - Completion of activities for enhanced automation systems, train integrity, traffic management evolution and smart object controllers'*. Les groupes de travail WP6 et WP7 visent à tester et démontrer la sécurité de systèmes de surveillance de l'intégrité des trains (absence de rupture d'attelage d'un train) pour permettre à l'ETCS de gérer les circulations ferroviaires en sécurité.

⇒ J'ai participé aux WP6 et au WP7, au travers d'une mise à disposition auprès de Railenium, avec l'objectif de contribuer à la mise en place d'une démarche permettant d'obtenir la certification des trois classes de systèmes de surveillance de l'intégrité. Cette démarche implique en premier lieu de fournir les **prérequis nécessaires à l'évaluation indépendante de sécurité** d'un produit (cf. mon rôle d'ISA pour CERTIFER, §I.7). J'ai pu présenter ces prérequis aux partenaires du projet et je les ai synthétisés dans le livrable **D7.1** [RPRE4]. J'ai contribué aussi au processus d'allocation de niveaux d'intégrité de sécurité aux fonctions du système en faisant bénéficier l'équipe "sécurité" de Railenium des résultats du projet SIL (cf. §I.6.2). Cela a mené à 1 **communication** [COM2] et 1 article **soumis à la revue** *IEEE-Access* [Sub1].

20 partenaires : Railenium, Alstom (coordinateur), Hitachi Rail STS (ex Ansaldo STS), AZD, Bombardier Tranportation, CAF, CEIT, DLR, Hacon, Indra, Mermec, Siemens, Thales, SNCF, Trafikverket, OBB, SBB, Slovenske Železnice, DB, Network Rail

Montant : 41 109 700 € (coût total pour tous les WP de X2RAIL-4) dont 581 630 € pour Railenium

3) X2Rail-2 (2017-2020) – programme H2020 ouvert aux membres de Shift2Rail

X2RAIL-2 est le projet sélectionné suite au 2nd appel à projet de Shift2Rail sur l'IP2 (*innovation programme*). Son titre mentionne les thématiques de recherche sur lesquelles des travaux sont menés : *'Enhancing railway signalling systems based on train satellite positioning, on-board safe train integrity, formal methods approach and standard interfaces, enhancing Traffic Management System functions'*. Le groupe de travail WP3 vise à développer un système de positionnement embarqué sûr incluant des technologies de localisation par satellite pour permettre à l'ETCS de gérer les circulations ferroviaires en sécurité. Les technologies GNSS associées à des techniques d'odométrie existantes sont prévues pour permettre à un train de se localiser à partir d'équipements embarqués plutôt qu'à partir d'équipements au sol coûteux à déployer et à entretenir (ex. balises).

⇒ J'ai participé au WP3, au travers d'une mise à disposition auprès de Railenium, avec l'objectif de contribuer aux méthodes de certification à mettre en place pour le système de positionnement prévu. J'ai proposé et rédigé, initialement pour Railenium, un sujet de post-doctorat intitulé "méthode

d'évaluation de sécurité pour une localisation avec GNSS sûre et certifiée dans le domaine ferroviaire". Le travail que j'ai ensuite mené avec deux ingénieurs de recherche de Railenium, Insaf Sassi et Nourdine Aït Tmazirte, et la poursuite de collaboration avec un collègue du laboratoire Heudiasyc de l'Université de Technologie de Compiègne, Mohamed Sallak, ont permis au final de bénéficier des compétences complémentaires de chacun pour répondre à ce sujet (compétences de sécurité ferroviaire et de sûreté de fonctionnement, de traitement de signaux GNSS au sein de systèmes multi-capteurs, de calculs probabilistes intégrant des incertitudes).

Les activités se sont appuyées sur les résultats du projet ERSAT-GGC. Nos travaux se sont concentrés sur la proposition d'une méthodologie d'allocation d'objectifs quantitatifs de sécurité, celle-ci venant en amont des activités V&V (Vérification & Validation). Pour cela, une méthodologie d'allocation de THR imprécis (*Tolerable Hazard Rates*) a été proposée. Celle-ci tient compte des incertitudes sur l'apparition des dangers liés au GNSS. Cette méthodologie a été appliquée dans le cas du VBTS (système avec balise virtuelle) et peut être déclinée à tout autre système dès lors que l'arbre de défaillances du système cible est construit. Ces travaux ont été **publiés** [ACTI12, COM3] et font partie du **livrable** D3.7 (*V&V Process Definition, Functional and Non-Functional Test Specification for the Fail-Safe Train Positioning Subsystem*) [RPRE8].

15 partenaires pour le WP3 : Railenium, Hitachi Rail STS (ex Ansaldo STS, coordinateur), CAF, AZD, NSL, MERMEC, Siemens, Thales Transportation Systems, CEIT, Bombardier Transportation, Alstom, SNCF, Trafikverkert, DB, SBB

Montant : 30 152 828 € (coût total pour tous les WP de X2RAIL-2) dont 329 805 € pour Railenium

4) ERSAT-GGC (2017-2019) – programme européen H2020 – appel Galileo-GSA-2017

Le but du projet ERSAT-GGC (*ERTMS on Satellite Galileo Game Changer*) est de définir et de développer des moyens pour la validation de l'utilisation d'un système de localisation aidé du GNSS au sein d'ERTMS en utilisant le concept de balise virtuelle. L'objectif final est de guider la certification de la solution issue du projet passé ERSAT (architecture développée depuis plusieurs années par Hitachi (ex-Ansaldo) et installée sur une ligne test en Sardaigne).

⇒ Mes activités dans le projet ERSAT-GGC se sont concentrées, avec la contribution d'un collègue de l'Université de Technologie de Compiègne, Mohamed Sallak, sur la définition et l'utilisation de THR (*Tolerable Hazard Rate*) imprécis pouvant traduire la variabilité des erreurs liées aux signaux GNSS, ceci à l'aide de l'arithmétique des intervalles. J'ai participé au **livrable** D3.2 (*GNSS Quantitative Analysis for ERSAT-GGC Project*) qui intègre cette contribution [RPRE9]. Nous avons continué notre collaboration dans le projet X2Rail-2.

14 partenaires : RFI, Hitachi Rail STS (ex Ansaldo STS), RINA Consulting, IFSTTAR, CEDEX, INECO, Italcertifer, ADIF, DLR, Bureau Veritas, Trenitalia, RadioLabs, UNIFE (coordinateur), SNCF

Montant : 3 107 286 € (coût total du projet) dont 250 696 € pour IFSTTAR-LEOST / ESTAS

5) Projet STARS (2016-2017) – programme européen H2020

Le projet STARS (*Satellite Technology for Advanced Railway Signalling*), auquel les laboratoires ESTAS et LEOST ont participé, vise à répondre à la problématique de l'emploi de l'EGNSS (*European GNSS*) pour des applications de contrôle-commande ferroviaire. En particulier, il vise à fournir une approche permettant de garantir les performances minimales atteignables par ce système de localisation pour pouvoir être utilisé dans l'ETCS. Deux axes sont approfondis : (1) caractériser l'environnement de propagation ferroviaire pour développer une approche de prédiction des performances de l'EGNSS et (2) quantifier les bénéfices économiques d'une solution ETCS intégrant ce système.

⇒ Mes activités, en collaboration avec Juliette Marais (LEOST), s'inscrivent dans le WP5 (*EGNOS Technology Feasability Study*) au sein duquel j'ai contribué au **livrable** D5.1 (*State of the art of EGNSS projects for the rail application*) [RPRE10] et à une conférence [ACTI13]. J'ai également apporté des propositions de modifications au livrable D5.3 (*EGNSS Target Performances to meet railway safety requirements*). J'ai rédigé un article en premier auteur lié au projet dans la **revue** *IEEE Access* [ACL5].

17 partenaires : Alstom, Hitachi Rail STS (ex Ansaldo STS), Bombardier, Siemens, CAF, AŽD Praha, UNIFE (coordinateur), IFSTTAR, RadioLabs, Thales Alenia Space, Telespazio, Università Bocconi, University of West Bohemia, Ineco, Thales Transportation Systems, D'Appolonia, TU Braunschweig

Montant : 4 458 831 € (coût total du projet) dont 135 750 € pour IFSTTAR-LEOST / ESTAS

6) Projet GaLoROI (2012-2014) – 7ème programme cadre européen)

Le projet GaLoROI (*Galileo Localisation for Railway Operation Innovation*), auquel les laboratoires ESTAS et LEOST ont participé, visait à développer un système embarqué de localisation utilisant les signaux des satellites Galileo. Ce système est dédié aux trains circulant sur des lignes ferroviaires à faible trafic et est développé pour répondre aux exigences normatives de sécurité associées.

⇒ Mes activités en collaboration avec Thi Phuong Khanh Nguyen (post-doctorante) et Juliette Marais (LEOST), se sont focalisées sur l'analyse et l'évaluation des propriétés de sûreté de fonctionnement du système conçu et développé dans le cadre du projet. La méthodologie présentée dans le §II.3 a donné lieu à **3 articles de conférence** [ACTI16, ACTI21, ACTI25], un article dans la **revue** RESS [ACL10], et au **livrable** D6.1 (*RAMS parameter analysis*) [RPRE13].

6 partenaires : BBR Verkehrstchnik, IFSTTAR LEOST et ESTAS, iQST (coordinateur, Institute for Quality, Safety and Transportation), iVA (Institute for Traffic Safety and Automation Engineering), KIT-MRT, Septentrio

Montant : 1 539 220 €

7) Projet QualiSaR (2012-2014) – 7ème programme cadre européen

Le projet QualiSaR (*Development of a Qualification Procedure for the Usage of Galileo Satellite Receivers for Safety Relevant Applications*), auquel le laboratoire ESTAS et le LEOST ont participé, visait à définir un processus normatif pour la qualification d'équipements de localisation embarqués dédiés aux applications de sécurité ferroviaire et routière et basés sur des signaux satellitaires (GPS, Galileo). Ce processus nécessite le développement d'un système de référence capable de vérifier la qualité de mesures de position.

⇒ Mes activités se sont focalisées sur la définition d'une terminologie unifiée en collaboration avec Olimpia Hoinaru (stage de master) et Juliette Marais (LEOST). Cette terminologie tient compte des propriétés liées aux domaines d'application (dont les propriétés de sûreté de fonctionnement de type FDMS - Fiabilité, Disponibilité, Maintenabilité, Sécurité). L'objectif est de définir à partir de la structure terminologique obtenue et des techniques de mesures proposées, une procédure de standardisation capable de s'insérer dans un standard global IEC ou ISO. Ces travaux ont donné lieu à un article de **conférence** [ACTI23] et au **livrable** D1.1 (*Structuring of terms describing the quality of GNSS*) [RPRE17].

5 partenaires : ABATEC, DLR, IFSTTAR LEOST et ESTAS, iVA (coordinateur), Technical University of Denmark (division of geodesy)

8) et 9) Projets UGTMS / MODUrban (2002-2008) – 5ème et 6ème programmes cadres européens

Les projets de recherche UGTMS (*Urban Guided Transport Management System*) et MODUrban (*MODular Urban Guided Rail Systems*) se sont succédés sur la même thématique (périodes 2002-2004, 2005-2008) et ont regroupé les mêmes partenaires dont les principaux étaient UNIFE, Alstom, Alcatel, CSEE, Bombardier, Siemens et la RATP.

Ils se sont concentrés sur la conception, le développement et le test d'une architecture de système de transport guidé ouvert et innovant. Les travaux liés à la sécurité ont mené, d'une part, à l'élaboration d'un modèle fonctionnel de la sécurité du système de transport guidé, d'autre part à l'intégration des facteurs humains dans la conception du système. Ces deux tâches ont été réalisées par le LAMIH et j'y ai participé durant ma thèse au travers de présentations et en contribuant à un livrable [RPRE21]. Une démarche d'harmonisation des procédures d'acceptation et de certification du système au regard de la sécurité faisait également partie des activités liées à la sécurité.

I.6.2 Projets nationaux (9)

1) FLEXY (début en 2022)

Ce projet vise à concevoir un système de véhicule léger innovant et économe en énergie, capable de circuler à la fois sur rail et sur route. L'objectif est de permettre la ré-utilisation de certaines petites lignes ferroviaires inexploitées et d'améliorer la desserte des zones rurales en proposant une solution de transport plus flexible et adaptable. En effet, le véhicule Flexy est imaginé pour quitter les rails et emprunter la route afin de desservir au plus près et de manière plus régulière les usagers de ces zones.

⇒ Je suis mise à disposition de Railenium pour contribuer à la proposition d'une approche dédiée à l'analyse des risques au niveau des plateformes de manœuvre dans la zone de transition rail-route, en collaboration avec Insaf Sassi et Ouail Himrane. Mon expertise en matière de démarche de sécurité est requise pour aborder les problématiques posées par la prise en compte conjointe des aspects de sécurité (criticité, allocations, mesures) relatifs aux domaines ferroviaire et automobile.

Partenaires : SNCF (coordinateur, SNCF-DTIPG, SNF-CIM, SFERIS), Railenium, Michelin, Milla

Montant : Dossier déposé à l'appel à projet 2023 de Corifer [1] pour une demande de financement, actuellement assumé par la SNCF

2) Train autonome–service voyageurs (fin 2018-2023) – PIA au travers de l'IRT Railenium

Ce projet se situe dans le cadre du programme d'Innovation et Recherche de la SNCF : Tech4Rail. Il a pour objectif la mise en œuvre d'un démonstrateur de train autonome voyageurs (TER) à horizon 5 ans, apte à circuler autant sur une ligne équipée d'ERTMS niveaux 1 et 2 que sur une ligne de classe B (i.e., système de signalisation national).

⇒ Je suis mise à disposition de Railenium pour contribuer à l'harmonisation des diverses activités de démonstration de sécurité du train autonome. Dans ce contexte **j'encadre les travaux de thèse** de Mohammed Chelouati en trinôme avec El-Miloudi El-Koursi (directeur) et Abderraouf Boussif de Railenium, sur le " **développement d'une démarche d'aide à l'assurance sécurité des trains autonomes**". Ces travaux ont pour but de vérifier la cohérence, la complétude, l'intégrabilité et la traçabilité de l'ensemble des activités de sécurité pour le train autonome. **3 articles de conférence** [ACTN1, ACTI2, ACTN2] et **2 articles de revue** [ACL1, ACL2] présentent ces recherches.

Partenaires : Railenium (partenaires académiques mis à disposition : Université Gustave Eiffel, UPHF, Université de Lille), SNCF (coordinateur), Bombardier Transport France, Bosch, SpirOps, Thales Communications & Security SAS

Montant : 57 millions d'€ à la fois pour les projets 'TA–service fret' et 'TA–service voyageurs'

3) Projet TC-Rail (fin 2017-2021) – PIA au travers de l'IRT Railenium

Ce projet se situe dans le cadre du projet chapeau "Train Autonome" du programme d'innovation et recherche de la SNCF : Tech4Rail. En effet, TC-Rail a pour but de développer un système de télécommande d'une motrice de fret qui permettra de reprendre la main à distance sur un train de fret autonome en cas de fonctionnement dégradé. Pour cela, il est nécessaire de :

- démontrer la possibilité de conduire manuellement une locomotive depuis un site à distance en toute sécurité, sans conducteur dans la cabine du train, avec un niveau de sécurité Globalement Au Moins Équivalent (GAME) à celui obtenu en présence d'un conducteur en cabine,
- lever tous les obstacles techniques qui pourraient s'opposer à une telle exploitation.

1. CORIFER signifie Conseil d'Orientation de la Recherche et de l'Innovation de la filière ferroviaire. Il s'agit d'une instance nationale définissant les plans d'action pour la filière en termes d'innovations et de pilotage.

⇒ J'ai participé au lot 11 (sécurité de la téléconduite) au travers d'une mise à disposition auprès de Railenium. J'ai **contribué à l'analyse préliminaire de risques de l'architecture** développée dans le projet. Celle-ci s'appuie sur une méthodologie d'évaluation de la non-régression de sécurité pour la téléconduite d'un train par rapport à un référentiel SNCF existant : le Référentiel Conducteur de Ligne. En collaboration avec Simon Collart-Dutilleul d'ESTAS, Abderraouf Boussif et Abhimanyu Tonk (de l'équipe "sécurité" de Railenium), nous avons travaillé sur les **scénarios de risques opérationnels de la téléconduite**. L'idée est d'adapter des concepts utilisés pour les véhicules routiers autonomes (notamment l'ODD – *Operational Design Domain*) aux véhicules autonomes ferroviaires, en particulier aux véhicules téléconduits. Ces travaux ont donné lieu à **3 articles de conférence** [ACTI7, ACTI9, ACTN3] et un article dans la **revue** *Safety and Reliability* [ACLN1].

Partenaires : Railenium (partenaires académiques mis à disposition : Université Gustave Eiffel, UPHF, Université de Lille, Université de Technologie de Compiègne) (co-coordinateur), SNCF (co-coordinateur), Thales Communications & Security, Actia Telecom, CNES

Montant : 7 227 730 €

4) Projet Smarties (2015-2020) – Contrats de Plan État-Région Hauts-de-France

J'ai été impliquée dans le projet Smarties (*Smart, Fail-Safe Communication and Positioning Systems*) de l'OS4 (Objectif Stratégique) "Dimensionnement et performances des fonctions véhicule" du projet ELSAT 2020 (Écomobilité, Logistique, Sécurité et Adaptabilité des Transports à l'horizon 2020). ELSAT 2020 est le projet fédérateur retenu dans le cadre du contrat de plan État-Région 2015-2020 (région Hauts-de-France) pour le domaine des transports. Il est porté par le CISIT (Campus International de Sécurité et d'Intermodalité des Transports), collectif régional de la recherche académique dans les transports.

⇒ Je me suis positionnée dans le groupe WP2 "Localisation sûre et intègre pour tous les modes ferroviaires" sur la tâche 1 "Système GNSS et multicapteurs pour le ferroviaire" en lien avec les travaux de thèse que j'ai encadrés sur 2013-2016. J'ai obtenu en 2017 un **demi-financement de thèse** par la région mais le candidat a fait défaut. Je l'ai obtenu de nouveau pour la thèse de Ouail HIMRANE en 2018. Un article écrit suite à des travaux commencés en 2016 en collaboration avec Thi Phuong Khanh NGUYEN a été publié en 2019 dans la **revue** *'Journal of ITS'* et a été valorisé dans ce cadre [ACL4].

Partenaires : Université Gustave Eiffel, CRIStAL, IEMN

Montant : 245 000 € (sur 2016) pour COSYS-LEOST

5) Projet SatRail (sur 2016) – contrat SNCF par l'intermédiaire de l'IRT Railenium

Le projet SatRail est une étude qui vise à investiguer l'utilisation des satellites de navigation et de communication pour le contrôle-commande ferroviaire. Ce projet est coordonné par Railenium et répond au besoin de SNCF-Réseau de documenter un certain nombre de points sur ce sujet comme :

- l'état de l'art sur *i)* l'utilisation des satellites de communication pour le contrôle-commande ferroviaire, *ii)* les développements passés et projetés du GNSS pour le ferroviaire,

– le contexte et les problématiques de démonstrations de sécurité des systèmes de localisation ferroviaires utilisant les GNSS.

⇒ Mes activités dans ce projet, dans le cadre d'une mise à disposition pour Railenium, ont mené à la rédaction du **livrable** sur le contexte et les problématiques de démonstration de sécurité des systèmes de localisation ferroviaires utilisant les GNSS [RPED1]. J'ai pu également présenter le contenu de ce livrable à la SNCF lors d'une réunion du **COPIL Rail&GNSS** fin décembre 2016 (ce COPIL regroupe des membres de la SNCF, du CNES –un accord a été signé entre la SNCF et le CNES en 2016–, de Railenium, du ministère, de Fer de France, et de l'EPSF). Un autre livrable sur les développements passés et futurs du GNSS pour le ferroviaire a débouché sur un article dans la **revue** IEEE-ITS (*Intelligent Transportation Systems*), article auquel j'ai contribué et qui a été publié en 2017 [ACL7].

Partenaires : IFSTTAR, Railenium (coordinateur), SNCF

Montant : 20 000 € HT (coût total du projet) dont 3 257 € de mise à disposition IFSTTAR-ESTAS pour Railenium

6) Projet Systuf (2012-2015) – programme Investissement d'Avenir

Le projet Systuf (*Système de télécommunication pour les transports urbains du futur*), auquel les laboratoires ESTAS et LEOST ont participé, vise à démontrer la faisabilité de l'utilisation d'un réseau de télécommunications unique (LTE - *Long Term Evolution* ou 4G) partagé entre différents acteurs et répondant simultanément aux exigences des applications sécuritaires ou non d'un exploitant de transports guidés (tramway et métro). L'objectif est d'avoir un seul système ouvert et normalisé de communication par le biais d'une unique infrastructure.

⇒ Mes activités dans ce projet étaient en collaboration avec Thi Phuong Khanh NGUYEN (post-doctorante), Marion Berbineau (COSYS) et Mohamed Kassab (LEOST puis ENSI Tunis/HANA research group). Les travaux ont donné lieu à un article de **conférence** [ACTI20], au **livrable** 6.5.1 (*Recommandations pour la mise en œuvre des études de sûreté de fonctionnement des fonctions CBTC sur un lien LTE*) [RPRE11] et à un **article** paru dans la **revue** *IEEE Transactions on ITS* [ACL9].

Partenaires : Nokia (coordinateur), Alstom Transport, IFSTTAR (LEOST et ESTAS), EURECOM, MERCE, RATP, TELECOM BRETAGNE, SIMPULSE

Montant : 4 506 915 € (coût total du projet) dont 181 663 € pour IFSTTAR-LEOST / ESTAS

7) Projet SIL (2013-2015) et extension du projet (sur début 2016, nommé SIL2) – Contrat forfaitaire de recherche financé par l'EPSF

Le projet SIL vise à élaborer une méthodologie générique pour l'allocation des SIL (*Safety Integrity Level* – niveau d'intégrité de sécurité) aux fonctions relatives à la sécurité d'un matériel roulant ferroviaire.

L'EPSF, en tant qu'autorité française de sécurité ferroviaire, a souhaité éclaircir les diverses pratiques et problèmes liés à ce type d'allocation. Nous avons alors proposé de fournir une démarche homogène et cohérente par rapport aux textes réglementaires et normatifs existants de sécurité ferroviaire.

⇒ J'ai effectué le **montage et la coordination** du projet. Je suis co-auteure de **4 livrables** avec Kiswendsida Abel Ouedraogo (post-doctorant), El-Miloudi El-Koursi, Joffrey Clarhaut et Dominique Renaux (maîtres de conférences à Valenciennes et membres du LAMIH) [RPRE12, RPRE14, RPRE15, RPRE16]. **2 articles de conférence** ont été publiés lors de la phase principale du projet [ACTI18, ACTI22].

L'extension du projet SIL a consisté à faire évoluer la méthodologie et le livrable associé en tenant compte des retours écrits formulés suite à la consultation de nombreux acteurs ferroviaires, notamment par le biais de courriers adressés à la FIF (Fédération des Industries Ferroviaires) et à l'UTP (Union des Transports Publics et ferroviaires). Six organismes ferroviaires ont répondu (RATP / TÜV / Belgorail / Bureau Veritas / Alstom / SNCF) et nous avons pu rencontrer leurs représentants (une nouvelle fois pour certains) lors d'une réunion qui a pu soulever des divergences de pratiques. Ces divergences ont été publiées dans **2 articles de conférence** [ACTI14, ACTN6]. La publication du guide méthodologique proposé dans le projet ne s'est pas faite directement sur la base documentaire de l'EPSF, certains acteurs français préférant que seules les exigences et détails concernant les SIL de la nouvelle version de la norme EN50126 (2017) soient visibles au niveau national. Toutefois, l'EPSF a souhaité mettre en avant la méthodologie auprès de l'ERA (Agence ferroviaire européenne) et de ses interlocuteurs afin d'apporter une contribution au niveau européen. Ainsi, nous avons publié un article synthétisant les problématiques et les résultats du projet dans la **revue** *Risk Analysis* [ACL6].

Partenaires : EPSF (Établissement Public de Sécurité Ferroviaire), IFSTTAR-ESTAS (coordinateur), LAMIH

Montant : 122 230 € (phase principale du projet) + 26 418 € (poursuite dans le projet SIL 2)

8) Contrats forfaitaires de recherche financés par la DGITM (2009 puis 2010)

⇒ J'ai contribué à la rédaction d'une étude de veille technologique pour la DGITM (DG des Infrastructures, des Transports et de la Mer) [RPRE20]. Une deuxième étude (2010) complétant la première – le projet GARA (*Galileo for Railways*) – a permis d'apporter des méthodologies de traitement des mesures pour l'évaluation des performances GNSS en environnement ferroviaire, et de présenter des résultats issus de données expérimentales [RPRE18]. Ce travail a été valorisé dans un article pour la revue *'Journal of Transportation Research, part C'* [ACL11].

Partenaires : DGITM, IFSTTAR-LEOST

9) Projet Tr@in-MD (2007-2009) – financement PREDIT

Le projet Tr@in-MD (*Transport intelligent par fer des Marchandises Dangereuses*) est un projet financé par l'ADEME dans le cadre du PREDIT (Programme de Recherche et d'Innovation dans les Transports Terrestres). Il avait pour objectif la mise en place d'un système dédié à la surveillance et au suivi en temps réel de wagons transportant des matières dangereuses sur le réseau ferroviaire. Le but est d'assurer une meilleure traçabilité de ces convois à risque et la sécurité de leur transport. Pour cela, un système embarqué utilise un moyen de localisation par satellites (balise GPS/GSM), celui-ci étant associé à différents moyens techniques de communication et de détection d'anomalies comme les fuites, les émanations de gaz, etc.

⇒ Les résultats, que j'ai obtenus avec la contribution de Djily Diaw (en stage de master), ont permis de quantifier l'impact de différents environnements ferroviaires types sur la fonction de localisation. Ils ont permis également d'apporter des recommandations au projet sur l'emplacement à privilégier de la balise en considérant le gabarit standard d'un wagon transportant des marchandises dangereuses. Ces travaux ont donné lieu à **5 articles de conférence** [ACTI26, ACTI27, ACTI28, ACTI29, ACTI30], un article dans la **revue** *Navigation* [ASCL1], et un **livrable** [RPRE19].

Partenaires : SNCF (coordinateur), IFSTTAR-LEOST, SENSEOR, CEA-LIST, MARTEC, Sonovision / Ligeron, SOLVAY, ERMEWA, SAPHYMO

Montant : 4,34 millions d'€

I.6.3 Participation à une chaire de recherche

En 2022, l'Université Gustave Eiffel s'est associée à l'Association CERTIFER (organisme de certification ferroviaire international) et au GAPAVE (groupement des associations APAVE) pour renforcer son action dédiée à la réduction significative de l'"empreinte carbone" de nos déplacements, en encourageant l'évolution d'un levier reconnu : le transport ferroviaire. Toutefois, quel que soit le changement apporté dans le système ferroviaire global, technologique, organisationnel, etc., celui-ci nécessite la mise en place de mesures garantissant que le niveau de sécurité est maintenu.

Ainsi, pour développer des travaux innovants sur différents enjeux de sécurité ferroviaire et construire un partenariat public-privé de long-terme soutenant les activités de recherche pouvant alimenter les activités de certification et de formation, la **chaire "Sécurité des Systèmes Ferroviaires"** a été créée en juin 2022 sous la coordination de Paola Pellegrini du laboratoire ESTAS. La thématique de cette chaire est au cœur de nos activités et permet de mobiliser les compétences et partager les connaissances des chercheurs/chercheuses du laboratoire.

Les activités sont prévues dans le cadre de cette chaire pour une durée de 5 ans (mi 2022-mi 2027). Elles sont adossées à trois thèmes :

- Évaluation de la sécurité des systèmes ferroviaires,
- Enjeux de cybersécurité et impacts sur l'évaluation de la sécurité des systèmes ferroviaires,
- Optimisation de l'infrastructure ferroviaire.

⇒ J'interviens, en collaboration avec les membres de l'équipe Sécurité Système d'ESTAS, sur le premier thème dans les deux sujets suivants :

- *Démarche d'aide à l'assurance de sécurité pour le train autonome*. Ces travaux font suite au travaux de thèse avec Mohammed Chelouati et sont en collaboration avec El-Miloudi El-Koursi (responsable scientifique) et Pierre-Jean Meyer de l'équipe Sécurité d'ESTAS.
- *Démarche d'analyse de sécurité liées aux systèmes de contrôle-commande ferroviaires de dernière génération dits 'à cantons mobiles'*. Je suis responsable scientifique de cette thématique sur laquelle j'interviens en collaboration avec Mohamed Ghazel. Dans ce contexte, j'ai proposé un sujet de thèse dans la continuité des travaux de Ouail Himrane, en lien avec les projets européens sur l'ETCS niveau 3, notamment le projet PERFORMINGRAIL sur lequel nous sommes intervenus. Cette thèse débutera à l'automne 2024, en collaboration avec Rim Saddem du LIS (Laboratoire d'Informatique et Systèmes) de l'Université Aix-Marseille. Des discussions ont déjà eu lieu avec des experts membres du comité technique de la chaire, en particulier des exploitants, constructeurs, évaluateurs de sécurité, pour présenter les travaux initiés sur cette thématique à l'Université Gustave Eiffel et détailler le périmètre visé pour la recherche.

Montant : 900 000 €

I.7 Activités d'expertise

Je suis reconnue en qualité d'**Évaluateur Certifer depuis le 30 janvier 2017** sur les aspects suivants :

- Techniques : généraliste ferroviaire et localisation satellitaire
- Norme-processus : sûreté de fonctionnement
- Règlementation : méthode CSM-RA (*Common Safety Method on risk evaluation and assessment*) et normes CENELEC EN 50126 - EN 50129.

Suite à cette reconnaissance, Certifer m'a contactée en avril 2017 pour effectuer une première évaluation. Celle-ci portait sur l'utilisation et la pertinence de la méthodologie issue du projet européen MODSafe dans la démonstration de niveaux de SIL, en particulier sur l'utilisation et la justification des facteurs de réduction du risque E, P & C dans des scénarios de dangers liés à la future exploitation du tramway de Doha (Qatar) [RPEX5].

Certifer a obtenu en août 2019 le **contrat d'évaluation du système de contrôle-commande du projet de métro Grand Paris Express**. Ce contrat intègre la mise à disposition de l'équipe expertise d'ESTAS pour assurer le rôle d'ISA (*Independent Safety Assessor*) au sens des normes de sécurité ferroviaire. Au sein de cette équipe, j'interviens à hauteur de 10% de mon temps pour contribuer aux activités d'analyse des documents et preuves de sécurité du projet. L'envergure de ce projet nous engage sur un travail de plusieurs années. Nous avons fourni jusqu'à présent 3 rapports d'évaluation intermédiaire [RPEX1, RPEX2, RPEX3].

Depuis août 2015, je fais partie du groupe de travail BNF/100E "Applications ferroviaires – Localisation par satellite" du **Bureau de Normalisation Ferroviaire** en tant qu'**experte** sur cette thématique.

I.8 Bilan des publications

Le tableau ci-dessous présente le bilan de mes publications. Celles-ci sont listées à la fin du document en Annexe 1.

	Code	Nb Total
Mémoire de thèse	TH	1
Article dans une revue à comité de lecture répertoriée dans les BDI	ACL	13 +1 soumis
Article dans une revue à comité de lecture non répertoriée dans les BDI	ACLN	4
Article dans une revue sans comité de lecture	ASCL	1
Conférence invitée dans un congrès international ou national	INV	5
Communication avec actes dans un congrès international	ACTI	36
Communication avec actes dans un congrès national	ACTN	8
Communication orale sans actes dans un congrès international ou national	COM	6
Séminaires	SEM	7
Rapport de recherche	RPRE	21
Rapport d'étude	RPED	1
Rapport d'expertise	RPEX	6
Ouvrage de vulgarisation ou chapitre	OV	1

II – MÉMOIRE DE RECHERCHE

Contenu

Dans ce mémoire de recherche, quelques lignes de "focus" en vert apparaissent pour chaque approche ou méthodologie détaillée. Elles mettent en évidence l'implication des doctorants et post-doctorant·e·s qui ont contribué aux travaux de recherche présentés, ainsi que les collaborations avec différents organismes partenaires aux compétences complémentaires. Les références aux publications associées sont également fournies. Le concours de l'ensemble des personnes avec qui j'ai eu la chance de mener mes recherches apparaît au cours des sections "activités de recherche", "encadrement" et "projets" de la partie I de ce document.

II.1 Contrôler, démontrer et assurer la sécurité d'un système ferroviaire

Pour distinguer les aspects fondamentaux liés au contrôle, à la démonstration et à l'assurance de la sécurité d'un système critique ferroviaire, cette section passe en revue, dans les sous-sections II.1.1 et II.1.2, les concepts de sûreté de fonctionnement et de gestion des risques sur lesquels reposent les travaux présentés dans ce mémoire. Ces concepts sont des points clés non seulement dans le secteur ferroviaire, mais également dans tous les secteurs confrontés à des problématiques de sécurité comme les secteurs automobile, aéronautique, nucléaire, spatial, de l'énergie, de la santé, etc. Ils sont employés lors des activités relatives à la sécurité qui sont liées aux différentes phases du cycle de vie d'un système, comme le montrera la sous-section II.1.3. Par la suite, les questions de recherche relatives à la sécurité des systèmes complexes critiques, tels que les systèmes de contrôle-commande ferroviaires, seront abordées dans la sous-section II.1.4.

II.1.1 Concepts et méthodes liés à la sûreté de fonctionnement (SdF)

1) Concepts

La sûreté de fonctionnement (SdF) d'un système se réfère à des exigences spécifiques associées au système. Celles-ci interviennent en relation étroite avec d'autres types d'exigences qu'il convient de présenter au préalable. En effet, les exigences de SdF s'y réfèrent, voire même nécessitent de les modifier ou de les compléter (exemple ajout d'exigences fonctionnelles en lien avec la sécurité). La norme EN 50126-partie-1 classe les autres types d'exigences évoquées ci-dessus selon trois catégories principales [30] :

— Les **exigences fonctionnelles** font référence à ce qu'un utilisateur attend du système, c'est-à-dire comment le système doit se comporter. Elles peuvent être "*complétées par des propriétés qui qualifient le comportement* [du système] *(par ex., fiabilité, sécurité, exactitude, synchronisation, etc.) et par des exigences de performance exprimées en termes de valeurs limites des paramètres fonctionnels (par ex., vitesse maximale, durée du service, temps de réponse, précision, etc)*". Par conséquent, lors de l'établissement des exigences fonctionnelles, des **propriétés** et des **exigences de performance** quantitatives peuvent être nécessaires.

— Les **exigences contextuelles** se réfèrent à la relation entre le système et son environnement en termes de profil de mission, de logistique, de facteurs humains, de coûts, etc.

— Les **exigences techniques** sont des exigences qui ne découlent pas des fonctions du système mais de sa mise en œuvre technique (par ex., les menaces potentielles créées par la technologie indépendamment de leurs fonctions prévues).

Les exigences de SdF sont quant à elles, décrites par des concepts fondamentaux regroupés dans le sigle **FDMS**. Chaque lettre de ce sigle renvoie aux concepts suivants dont la définition est la même quel que soit le secteur technique :

— La **fiabilité** est "*l'aptitude à fonctionner tel que requis sans défaillance, pendant un intervalle de temps donné et dans des conditions données*" [45].

— La **disponibilité** est "*l'aptitude à être en état de fonctionner tel que requis*" [45], i.e. "*d'accomplir une fonction requise dans des conditions données à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens nécessaires est assurée*" [30].

— La **maintenabilité** est "*l'aptitude à être maintenu ou rétabli dans un état permettant de fonctionner tel que requis, dans des conditions données d'utilisation et de maintenance*" [45].
— La **sécurité** est "*l'absence de risque inacceptable [de dommage]*" [46]. Le dommage fait référence à la blessure physique ou à l'atteinte à la santé des personnes, aux biens ou à l'environnement.

Les concepts FDM regroupent des exigences décrites en termes opérationnels et sont liées à la qualité de service du système. Concernant le critère S, il est dépendant d'un ensemble de concepts spécifiques liés à la gestion des risques (cf. sous-section II.1.2). Les exigences peuvent être définies à la fois de manière qualitative et quantitative. Les **exigences qualitatives de FDMS** se réfèrent aux processus et aux conditions associées pour :

— maintenir le système dans un état tel qu'il puisse fournir un service opérationnel requis, ceci malgré l'apparition possible de défaillances ou l'occurrence d'erreurs humaines au cours de la mission du système. Cela renvoie à la maîtrise des exigences FDM (avec, par exemple, l'utilisation de redondances ou de modes dégradés).
— éviter les risques inacceptables et gérer les risques résiduels tolérables. Cela renvoie à la maîtrise des exigences de sécurité (avec, par exemple, l'utilisation de processus de contrôle, et de mesures techniques de sécurité intrinsèque ou contrôlée introduites en conception pour passer d'un état dangereux à un état sécuritaire).

Les **exigences quantitatives de FDMS** sont associés à des propriétés et paramètres dont un certain nombre sont présentés à la figure II.1. Ceux-ci sont définies dans le Vocabulaire Électrotechnique International [1], en particulier dans les parties IEC 60050-192 [45] et IEC 60050-903 [46], ainsi que dans la norme de sécurité fonctionnelle générique IEC 61508 [48]. Une branche spécifique à la norme de sécurité ferroviaire EN 50126 [30] a été ajoutée en bas de la figure avec des concepts utilisés par la suite dans ce mémoire. Dans la version numérique de ce document, les concepts inscrits en bleu dans la figure sont associés à un lien menant à leur définition internationale. De plus, la plupart d'entre-eux sont détaillés par Signoret & Leroy [92] et dans la norme IEC 61703 [49]. Il peut être constaté dans la figure II.1, qu'une distinction est faite entre les concepts **probabilistes** et **opérationnels**. Les concepts probabilistes sont consacrés à la caractérisation de l'occurrence des défaillances du système au cours des phases de développement du système ; elles font appel à des **analyses prévisionnelles de FDMS**. Les concepts opérationnels sont des indicateurs de performances opérationnels mesurés lors d'**analyses opérationnelles de FDMS**. La sous-section II.1.1.2 ci-dessous mentionnent les principales méthodes d'analyse de SdF existantes.

Les exigences FDMS sont interdépendantes et leur spécification dépend du niveau de détails considéré pour le système. Un exemple de granularité qui peut être observé pour un système de contrôle-commande ferroviaire est illustré à la figure II.2. Dans cette figure se distinguent les niveaux système, sous-système et équipement. Au niveau de l'équipement, voire des composants, d'autres critères de performance peuvent exister, en particulier certains critères propres aux technologies spécifiques dont l'usage pourra permettre d'atteindre les caractéristiques prévues du système. C'est

1. https://www.electropedia.org, IEC 60050 – *International Electrotechnical Vocabulary*

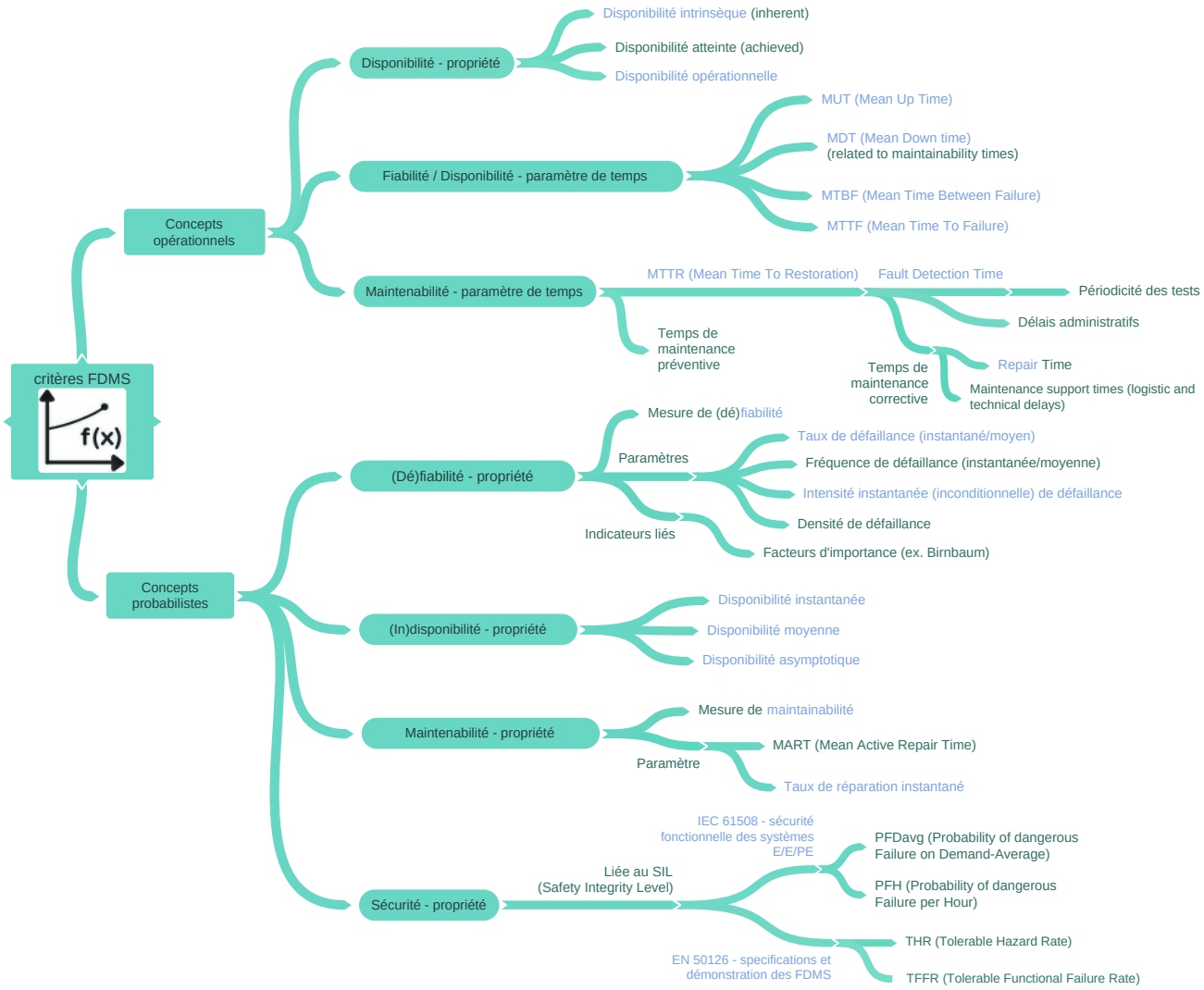


FIGURE II.1 – Critères FDMS – exemple de propriétés et de paramètres temporels associés

Niveau 'Système'	Niveau 'Sous-système'	Niveau 'Équipement'
• Infrastructure + trains	• Sous-système 'bord' • Sous-système 'sol' • Sous-système de communication	• Lié à la position du train • Lié à l'intégrité du train • Détecteurs de trains sur la voie • Contrôleurs d'objets aux aiguillages • …

FIGURE II.2 – Différents niveaux pour quantifier les propriétés FDMS d'un système de contrôle-commande ferroviaire

notamment le cas des technologies basées sur les GNSS et les technologies de télécommunication qui sont envisagées pour réaliser les fonctions de localisation, de contrôle de l'intégrité et de communication dans les systèmes de contrôle-commande ferroviaires avancés.

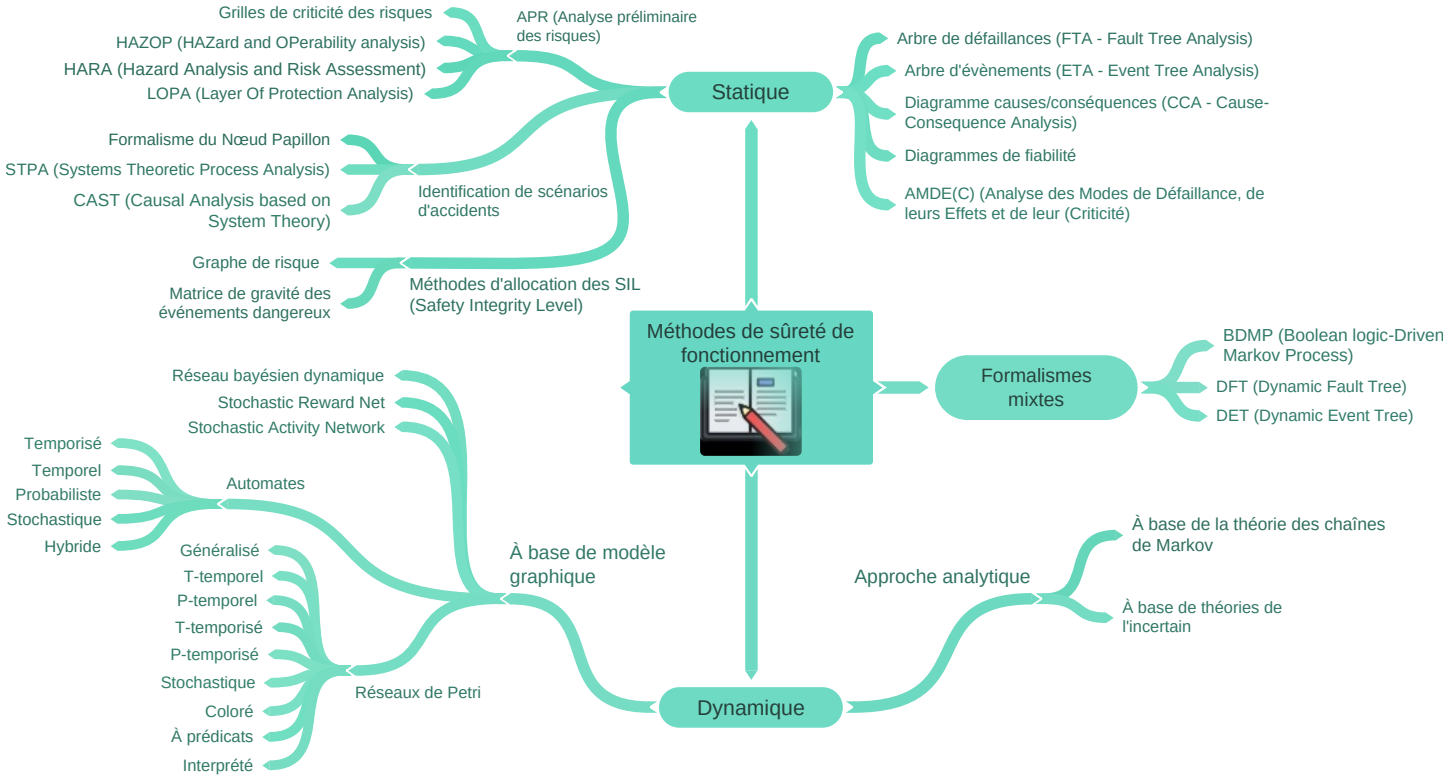


FIGURE II.3 – Méthodes d'analyse de SdF

2) Méthodes

Les principales méthodes d'analyses prévisionnelles de SdF sont citées dans la norme [47]. Elles sont classées en deux catégories :

- Les méthodes spécifiques à la SdF [99, 92], citons les méthodes traditionnelles de :
  - l'arbre de défaillances : pour l'analyse de combinaisons de défaillances dans un système,
  - l'arbre de conséquences : pour l'analyse de séquences de défaillances et/ou d'événements extérieurs au système,
  - Le diagramme de fiabilité : pour l'analyse des chemins de succès dans l'architecture du système,
  - l'AMDE(C) : pour l'Analyse des Modes de Défaillance, et de leurs Effets (et de leur Criticité),
  - l'APR (Analyse Préliminaire des Risques) : classe de méthodes pour l'identification de situations dangereuses, l'évaluation et le management des risques associés.
- Les méthodes d'ingénierie générale venant en appui de l'analyse de la SdF, comme l'ingénierie de la fiabilité logicielle (exemple de l'utilisation de méthodes de vérification formelle) et l'ingénierie système (exemple de l'utilisation de formalismes comme celui des réseaux de Petri, des automates et des réseaux bayésiens) [6, 7, 101, 99, 92].

Certaines méthodes tirent partie de théories de calculs analytiques, comme la théorie liée aux processus de Markov permettant de tenir compte des dépendances entre états de panne, ou aussi, les théories de l'incertain offrant les moyens de représenter les incertitudes dans les modèles probabilistes de panne (exemple des sous-ensembles flous ou des fonctions de croyance). D'autres méthodes ont vu le jour pour investiguer plus en détails des points précis d'analyse comme l'identification de scénarios d'accidents (exemple des méthodes STPA et du nœud papillon). Des éléments supplémentaires sur les méthodes employées plus particulièrement pour les *études de sécurité* seront donnés en sous-section II.1.2.2. La figure II.3 répertorie les différents types de méthodes en donnant des exemples.

À noter que des groupes de travaux nationaux opèrent au sein de l'association SAGIP[2] (*Société d'Automatique, de Génie Industriel et de Productique*) créée en 2020 par les communautés du GDR MACS (Groupement de Recherche *Modélisation, Analyse et Conduite des Systèmes Dynamiques*). Parmi ceux-ci, les GT SED et S3 se concentrent respectivement sur les thématiques des *Systèmes à Évènements Discrets* et de la *Sûreté / Surveillance / Supervision*. Le groupe AFSEC[3] (*Approches Formelles des Systèmes Embarqués Communicants*) du GDR GPL (*Génie de la Programmation et du Logiciel*) collabore avec le GT SED pour les applications de sûreté de fonctionnement. L'IMdR (*Institut pour la Maîtrise des Risques*) est une association regroupant entreprises et organismes publics autour des questions de maîtrise des risques ; elle soutient la conférence Lambda-Mu, réputée sur ces questions et possède différents groupes de travaux dont le GT Recherche Méthodologique. Au niveau européen, des associations telles que l'ESRA[4] (*European Safety and Reliability Association*) qui soutient la conférence renommée ESREL (*European Safety and Reliability Conference*), facilitent les échanges autour des questions de recherche en sûreté de fonctionnement. Certains travaux exposés dans ce mémoire ont été présentés dans ces différents réseaux.

II.1.2 Concepts et méthodes spécifiques liés à la sécurité

1) Concepts

Le concept de sécurité ayant été défini précédemment, cette sous-section présente les principaux éléments entrant en jeu dans la démonstration de sécurité d'un système à concevoir. Il sera alors souligné comment les résultats de cette démonstration et la mise en œuvre de moyens pour les obtenir (i.e., processus d'organisation et de suivi, méthodologies d'analyses) mènent à l'assurance sécurité.

La **démonstration de sécurité** utilise des méthodes d'évaluation de la sécurité pour analyser les risques associés au système. À partir de ces analyses, la démonstration de sécurité a pour but de montrer que tous les risques associés au système sont couverts par des mesures de réduction du risque et que la combinaison de ces mesures aboutit à un risque résiduel acceptable et maîtrisé. Cela va de pair d'une part avec le fait que l'implémentation technique de ces mesures doit être *sûre de fonctionnement*, ceci malgré les fautes / erreurs / défaillances possibles dans les éléments matériels / logiciels et les erreurs pouvant être engendrées par l'action humaine. D'autre part, cela implique

2. http://sagip.org
3. http://gdr-gpl.cnrs.fr/Groupes/AFSEC
4. http://esra.website

la conception additionnelle au sein du système de *mesures de contrôle*. Le processus mis en place pour analyser, démontrer et effectuer le suivi des mesures de réduction des risques, est souvent qualifié de "démarche sécurité".

L'**appréciation des risques** apparaît comme étant une étape préalable essentielle à la démonstration de sécurité, car elle permet d'identifier, en amont du développement d'un système, les principaux risques et les mesures de réduction associées (parfois appelées avec l'anglicisme "*mitigations*"). Dans la plupart des cas, ces mesures de réduction agissent comme des barrières de sécurité *préventives*, visant à éviter la survenue d'un accident. Les barrières de *protection contre le risque* n'interviennent qu'en dernier recours, lorsque le risque identifié est associé à un accident inévitable et nécessite l'atténuation des conséquences de cet accident. Le caractère préalable à la démarche de sécurité n'est pas à considérer au sens strict, car cette étape d'appréciation des risques se poursuit en symbiose avec les activités de démonstration de sécurité. En effet, l'affinement, voire l'ajout de mesures de réduction des risques, s'effectue au cours de ces activités de démonstration, au fur et à mesure que la conception du système se précise.

L'**assurance sécurité** est au final le résultat combiné des différents résultats des analyses de sécurité fonctionnelles / techniques / opérationnelles, ainsi que de la justification de la mise en œuvre d'un processus rigoureux pour les obtenir. Ce processus se réfère à l'établissement et au suivi d'un plan d'activités à mener, c'est-à-dire un document décrivant une méthode d'organisation des activités d'analyse et d'évaluation de la sécurité, appelé **plan de sécurité**. Dans ce document y figurent les objectifs de chaque activité prévue, leurs liens et, pour chacune d'entre-elles, une liste explicite d'éléments d'entrée et de sortie. Ce plan indique nécessairement les ressources servant à l'élaboration des activités de sécurité ainsi que les responsabilités des intervenants et relations entre parties prenantes. La synthèse des résultats de démonstration issues des activités de sécurité, et des justifications sur la manière dont ils ont été obtenus en se référant au plan de sécurité, sont rédigées dans un **dossier de sécurité** (appelé aussi dossier d'assurance sécurité). Ajouté à cela, les moyens de suivi pour maintenir, en conditions opérationnelles, le bon fonctionnement des mesures de sécurité mises en place, font également partie intégrante de l'assurance sécurité.

Le tableau II.1 synthétise les définitions des termes en lien avec la sécurité et les risques, et qui seront utilisés dans ce mémoire. Les références indiquées dans la colonne "*source*" renvoient aux normes ou règlements de sécurité du domaine ferroviaire. Toutefois, ces définitions sont issues de normes internationales utilisées dans tout domaine, dont la norme IEC 60050-903 pour les définitions liées à l'*appréciation des risques* [46], et la norme de sécurité fonctionnelle générique IEC 61508 pour les systèmes électriques / électroniques / électroniques programmables (E/E/PE) relatifs à la sécurité [48].

Ajouté à ces définitions, il convient de définir un concept pivot intervenant dans les analyses liées à la démonstration de la sécurité : l'**intégrité de la sécurité**. Il s'agit de "*l'aptitude d'un système relatif à la sécurité à remplir ses fonctions de sécurité requises dans toutes les conditions spécifiées, au sein d'un environnement opérationnel spécifié et pendant une durée donnée*" [30]. Ce concept caractérise la manière dont sont contrôlées les défaillances dangereuses fonctionnelles et se réfère à des **niveaux d'intégrité de sécurité ou SIL** (*Safety Integrity Levels)*. Ce sont des niveaux définis sur une échelle de 1 à 4 ; le SIL 4 désigne le niveau de sécurité le plus contraignant du fait d'exigences fortes de sécurité associées, et le SIL 1 désigne au contraire le niveau le moins contraignant. Les SIL

TABLE II.1 – Définitions des concepts liés à la sécurité et aux risques

Concept	Définition	Source
Analyse des risques	Utilisation systématique de toutes les informations disponibles pour identifier les dangers et estimer le risque.	[4]
Appréciation des risques	Processus global comprenant une analyse de risque et une évaluation des risques.	[4]
Critères d'acceptation des risques	Éléments au regard desquels l'acceptabilité d'un risque particulier est évaluée ; ces critères sont utilisés pour déterminer si le niveau d'un risque est suffisamment bas pour qu'il ne soit pas nécessaire de prendre des mesures immédiates pour le réduire davantage.	[4]
Danger	Condition pouvant conduire à un accident (éq. situation dangereuse).	[4][30]
Estimation des risques	Processus utilisé pour aboutir à une mesure du niveau des risques analysés par l'estimation de la fréquence, l'analyse des conséquences et l'intégration des informations y afférent.	[4]
Évaluation (des risques)	Procédure fondée sur l'analyse de risque pour déterminer si un niveau de risque acceptable a été atteint.	[4]
Exigences de sécurité	Caractéristiques de sécurité (qualitatives ou quantitatives, ou, au besoin, qualitatives et quantitatives) devant être observées dans la conception, l'exploitation (y compris les règles d'exploitation) et l'entretien d'un système pour que les objectifs de sécurité établis par la législation ou l'entreprise soient atteints.	[1]
Mesures de sécurité	Série de mesures réduisant le taux d'occurrence d'un danger ou atténuant ses conséquences afin d'atteindre et/ou de maintenir un niveau de risque acceptable.	[4]
Organisme d'évaluation	Personne, organisation ou entité indépendante et compétente, externe ou interne, qui procède à des investigations pour formuler un jugement fondé sur des preuves au sujet de l'aptitude d'un système à respecter les exigences de sécurité qu'il doit satisfaire.	[4]
Principe d'acceptation des risques	Règles utilisées pour déterminer si le risque lié à un ou plusieurs dangers particuliers est acceptable ou non.	[4]
Risque	Fréquence d'occurrence d'accidents et d'incidents F causant un dommage (dû à un danger) et le degré de gravité de ce dommage G (R = F, G).	[4]
Situation dangereuse	Équivalent à danger (*hazard*).	[4]

sont employés uniquement pour spécifier les exigences de sécurité des fonctions réalisées par des systèmes techniques E/E/PE relatifs à la sécurité [48], ce qui est le cas de la plupart des fonctions d'un système de contrôle-commande ferroviaire. L'utilisation des SIL permet de prendre en compte les défaillances dangereuses rares mais possibles des constituants de sécurité dans un système critique. En résumé, les exigences qui découlent de l'utilisation des SIL sont principalement des exigences de sécurité fonctionnelle.

La fiabilité humaine est un aspect critique de la sécurité de nombreux systèmes complexes. La conception, l'installation et la maintenance des systèmes sont des tâches confiées à des personnes et sont donc soumises au facteur humain. Il en est de même pour certaines tâches opérationnelles, même si la plupart des systèmes techniques actuels sont conçus pour parer aux erreurs humaines

en situations nominales, ce qui est particulièrement le cas pour les systèmes de contrôle-commande ferroviaire. L'intervention de l'opérateur humain est toutefois essentielle en situations perturbées, en particulier lorsque le système doit fonctionner en mode dégradé. Les méthodes d'analyse de la fiabilité humaine n'étant pas utilisées dans ce mémoire, elles ne seront pas détaillées. Une revue de la littérature sur la fiabilité humaine dans l'ingénierie ferroviaire effectuée sur les deux dernières décennies est néanmoins consultable dans [19].

TABLE II.2 – Méthodes d'analyse de sécurité

	APD/APR Analyse Préliminaire des Dangers / Risques	**FTA** Analyse par arbre de défaillances	**ETA** Analyse par arbre d'événements	**CCA** Analyse de Cause-Conséquence	**AMDE/ AMDEC** Analyse des Modes de Défaillance, de leurs Effets / et de leur Criticité	**STPA** System-Theoretic Process Analysis
Type d'analyse	Qualitative / semi-quantitative	Qualitative / quantitative	Qualitative / quantitative	Qualitative / quantitative	Qualitative / semi-quantitative	Qualitative
Avantages	Analyse systématique des dangers et évaluation du risque associé.	La chaîne causale des défaillances peut être facilement visualisée.	La chaîne d'événements peut être facilement visualisée.	Aide à identifier les scénarios car les séquences d'événements sont visibles.	Exigences de sécurité structurées.	Permet d'analyser plusieurs facteurs : problèmes de sécurité liés aux erreurs de conception, défauts des logiciels, interaction entre composants et erreurs de décision humaine.
Inconvénients	L'appréciation des ingénieurs chargés de l'analyse est déterminante, les causes de danger peuvent être omises.	Méthode binaire qui rend difficile la gestion des composants multi-états et de leurs dépendances.	Analyse d'un seul événement déclencheur à la fois et difficultés à gérer les dépendances.	Difficile à utiliser pour les systèmes complexes.	Fastidieux et coûteux si elle est appliquée à toutes les parties d'un système complexe.	Il est difficile d'identifier les risques de base pour les nouveaux composants et de définir la structure de contrôle.
Automatisation	Non	Oui	Oui	Non	Oui	Non
Langage ou artefacts utilisés		Structure logique obtenue manuellement ou à partir de diagrammes de fiabilité, ou de décision binaires pour la quantification.	Structure arborescente.	Structure logique et structure arborescente.		

2) Méthodes

Plusieurs méthodes traditionnelles d'analyses prévisionnelles de SdF des systèmes évoquées à la sous-section II.1.1.2, sont spécifiquement utilisées pour l'analyse et l'évaluation de la sécurité. Celles qui prédominent sont présentées dans le tableau II.2. Dans ce tableau, les avantages et inconvénients de ces méthodes sont mentionnés, ainsi que leur possibilité d'automatisation pour appréhender les systèmes de grande taille, et les langages ou artefacts associés permettant leur mise en œuvre [41], [85].

L'utilisation d'approches d'analyse et d'évaluation de la sécurité basées sur des modèles (MBSA, *Model-Based Safety Assessment*) est l'un des principaux axes de recherche de la communauté de l'ingénierie de la sécurité des systèmes depuis plus de deux décennies, comme le souligne l'article de Sun *et al.* de 2024 [97]. Leurs avantages par rapport aux méthodes d'analyse traditionnelles résident dans leur capacité à prendre en compte la complexité des systèmes en considérant différentes vues (fonctionnelle, structurelle, comportementale) et en réutilisant des artefacts de modélisation développés lors de la conception du système (*design model*). De plus, l'utilisation possible de notations formelles permet d'éliminer les ambiguïtés des analyses de sécurité traditionnelles, de détecter rapidement des défauts de conception, et de supporter les méthodes de traitement automatique associées. L'investigation de ces méthodes sera développée dans les perspectives de ce mémoire.

Ainsi les analyses de sécurité effectuées par diverses méthodes présentent plusieurs avantages :

- Garantir le fonctionnement des systèmes en maîtrisant les risques,
- Apporter une réponse argumentée aux exigences contractuelles et réglementaires pour donner confiance et satisfaction aux utilisateurs du système,
- Capitaliser sur les bonnes pratiques grâce à la documentation des preuves de sécurité issues des résultats des analyses,
- Bien que ce ne soit pas l'objectif premier, aider à optimiser le système en identifiant des points faibles et en proposant des améliorations, contribuant ainsi à atteindre des objectifs de performances spécifiques.

Les concepts et méthodes principaux liés au cadre de la démonstration de sécurité d'un système ayant été abordés ci-dessus, la sous-section suivante se concentre sur l'ensemble des activités en support à cette démonstration et qui ont lieu lors des phases de développement d'un système, en particulier d'un système ferroviaire. Il est à noter que même si un ensemble de mesures ont été mises en place durant son développement, des processus sont tout de même requis en exploitation pour assurer sa sécurité. Il s'agit alors de : mesurer des indicateurs, intervenir lorsqu'il y a diagnostic de défaut, maintenir le système ou malheureusement, enquêter lorsqu'un événement plus grave s'est produit. En effet, la surveillance du système est continue partant du principe que le risque "zéro" n'existe pas.

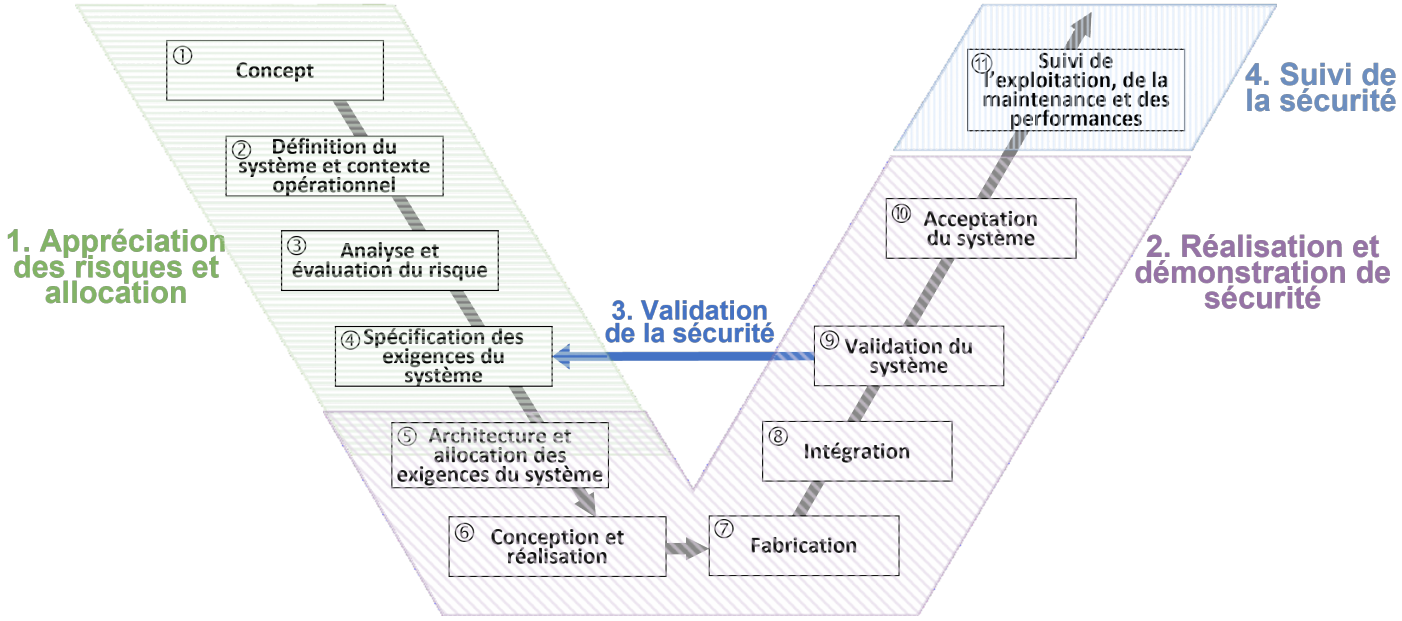


FIGURE II.4 – Activités de sécurité dans le cycle de développement d'un système ferroviaire critique (adapté de la norme EN 50126 [30])

II.1.3 Activités de sécurité dans le cycle de vie et méthodes associées

Les pratiques d'ingénierie de la sécurité pour les systèmes ont été établies à partir des années 1970 par le biais de standards du DoD (*United States Department of Defense*), notamment le MIL-STD-882D et ses évolutions [73]. Tout comme dans ces pratiques, les activités de sécurité dans le domaine ferroviaire sont fondées sur les principes de l'"*approche système*" pour faire face à la complexité évoquée en introduction de ce mémoire. Il s'agit de considérer un système dans sa globalité et de comprendre son comportement en considérant les actions (des fonctions ou processus) du système qui, selon des contraintes environnementales, évoluent dans le temps pour atteindre une finalité. L'"*approche système*" se concentre alors sur les interactions au sein du système (échanges de matières, énergie ou informations) selon des interfaces d'échange, ainsi que sur l'organisation du système en parties pouvant être structurées de manière fonctionnelle ou organique [TH1].

Les activités de sécurité fondées sur les cadres méthodologiques de l'ingénierie système et de la SdF, sont regroupées selon les quatre macro-phases suivantes représentées à la figure II.4 (cette figure est issue des normes ferroviaires mais est généralisable) :

1) L'appréciation des risques pour l'allocation d'exigences de sécurité,
2) La réalisation et la démonstration de la conformité aux exigences de sécurité,
3) La vérification et la validation du respect des exigences de sécurité,
4) Le suivi des performances de sécurité en exploitation.

Les paragraphes qui suivent synthétisent ces activités et les méthodes classiquement employées quelle que soit la technologie. Ils soulignent les particularités ferroviaires [31] et mentionnent aussi, pour éviter toute confusion, les principaux termes anglais retrouvés dans la littérature car ils sont non nécessairement liés par une traduction littérale.

1) Appréciation des risques pour l'allocation d'exigences de sécurité

L'appréciation des risques (*Risk assessment*) est effectuée dans la majorité des projets par les méthodes de type APR (cf. sous-sections II.1.1 et II.1.2). À partir d'une liste générique d'accidents, l'APR se concentre en premier lieu sur l'identification des situations dangereuses liées à un système et pouvant mener à un accident. Elle comporte une étape d'évaluation des risques durant laquelle les risques associés à chaque danger peuvent être jugés comme étant acceptables ou inacceptables (éventuellement : intolérables, tolérables, négligeables) d'après un principe d'acceptation du risque donné. Selon le résultat de l'évaluation, l'analyse mène à la définition de **mesures permettant de couvrir les risques** évalués comme étant inacceptables / intolérables.

L'identification des situations dangereuses et de leurs effets incite l'analyste à se concentrer sur les **scénarios d'accident**. En effet, une telle situation se caractérise par un évènement déclencheur, un contexte, et une (des) séquence(s) potentielle(s) d'évènements qui peuvent conduire à un accident, avec des conséquences diverses telles que des dommages matériels ou des décès. La conjonction de l'ensemble danger/effet constitue un profil de risque. Le contexte se rapporte à l'environnement, au lieu (par exemple, dans le domaine ferroviaire : station, inter-station, garage) et aux conditions de fonctionnement (par exemple, dans le domaine ferroviaire : arrêt, démarrage, vitesse spécifique du train) et d'exploitation (ex. automatique, manuel). Pour une analyse complémentaire à l'analyse ascendante danger-conséquences, l'APR peut inclure une liste de causes possibles des situations dangereuses relatives à l'architecture fonctionnelle, jusqu'à indiquer l'enchaînement d'événements menant au danger qualifié de **scénario dangereux**. Dans ce cas, il est fait référence aux défaillances et insuffisances fonctionnelles susceptibles de se produire au sein de l'architecture. Cette dernière est toutefois considérée à un haut niveau structurel en raison du caractère préliminaire de l'analyse. Les mesures identifiées ont alors pour but d'empêcher le déroulement d'un scénario d'accident pour réduire le risque.

Cette étape précoce d'analyse des risques sert de base pour spécifier des **exigences de sécurité de haut niveau** pour le système à concevoir par rapport aux mesures identifiées. Ce sont des exigences de sécurité *liées à des fonctions* et, dans le cadre spécifique ferroviaire, des règles d'exploitation. Dans le cadre de système de grande taille, ces exigences sont attribuées, à des fins de mise en œuvre, à différents groupes de travail dédiés aux parties spécifiques du système. À noter que des exigences peuvent être exportées vers d'autres entités, ou définies pour les interfaces aux frontières du système.

Suite à cette étape préliminaire incarnée par les méthodes de type APR, l'analyse des risques (AR) se poursuit simultanément aux phases ultérieures du cycle de vie (classiquement non illustrée sur le schéma du cycle de vie) lorsque la conception du système se précise. Dans ce cadre, l'application de méthodes comme l'AMDEC, FTA, HAZOP (etc.) aux sous-systèmes puis aux composants logiciels et matériels est utile. De manière générale, l'emploi d'un **modèle de risque** est utile pour identifier les relations de causes à effets, c'est-à-dire l'identification de successions ou coïncidences de défaillances, d'événements, d'états de fonctionnement, de conditions opérationnelles et d'environnement (etc.) du système et de ses composants qui peuvent conduire aux dangers. Cela rejoint la macro-phase de démonstration de sécurité, détaillée ci-dessous, qui a pour but d'**affiner** / **préciser** / **compléter les exigences de sécurité** par rapport aux différents niveaux de décomposition du

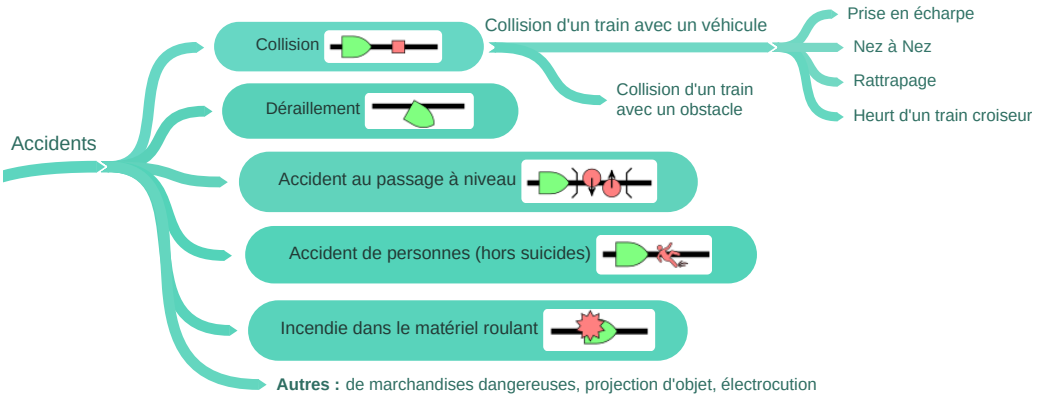


FIGURE II.5 – Accidents génériques ferroviaires

système (exemple de la figure II.2 pour le domaine ferroviaire). À cette fin, le registre des situations dangereuses (*Hazard log*) est un outil de recueil des dangers à tout niveau, ainsi que des mesures associées pour les éviter.

Des preuves documentaires viennent alimenter, dès cette macro-phase d'appréciation des risques, le **processus d'assurance sécurité** évoqué précédemment, i.e. la constitution du corpus documentaire d'assurance sécurité démarre ainsi. Comme avec toutes les preuves à venir, il requiert la mention des méthodologies, hypothèses, données, jugements et interprétations utilisés. Quelques spécificités ferroviaires sont données ci-dessous.

Liste générique d'accidents ferroviaires : La figure II.5 illustre la liste d'accidents génériques ferroviaires mentionnés dans l'arrêté français du 4 janvier 2016 [5].

Principes ferroviaires d'acceptation du risque :

Pour l'évaluation du risque, il existe trois principes d'acceptation du risque dans le domaine ferroviaire. Ils sont harmonisés à l'échelle européenne dans le règlement CSM-RA (*Common Safety Method for Risk Assessment*) [4]. Ce sont les suivants :

— "*L'application de règles de l'art*", appelées aussi codes de bonne pratique : ce principe consiste à appliquer des référentiels tels que des normes, des règles nationales, pour parer un ou plusieurs dangers spécifiques.

— "*La comparaison avec un système similaire*", appelé aussi système de référence : ce principe consiste en la comparaison du nouveau système avec un système similaire. Les deux systèmes satisferont au final aux mêmes types d'exigences de sécurité permettant d'obtenir un risque acceptable. Dès lors que l'objectif d'application de ce principe est la non-régression du "niveau de sécurité global" du système examiné par rapport à celui du système existant assurant une mission équivalente, l'approche est qualifiée de GAMÉ (Globalement Au Moins Équivalent).

— "*L'estimation explicite des risques*" : dans le cas où les dangers ne sont pas couverts par l'un des deux principes précédents (système entièrement nouveau ou écarts importants avec les codes de pratique ou systèmes similaires), une estimation des risques dans le contexte opéra-

5. Annexe I de l'arrêté relatif à la nomenclature de classification des événements de sécurité ferroviaire : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031824520

tionnel particulier dans lequel survient le danger, peut être utilisée. L'estimation de l'occurrence d'accident suite au danger et du niveau de gravité associé peut s'effectuer selon une échelle quantitative ou qualitative.

Allocation d'objectifs de sécurité ferroviaire :

Les exigences de sécurité de plus haut niveau, en lien avec les *fonctions de sécurité*[6] à intégrer au système ou en lien avec les *fonctions relatives à la sécurité*[7] déjà présentes dans le système, peuvent être spécifiées de manière qualitative et/ou quantitative. À noter que par souci de simplicité, par la suite 'fonction de sécurité' sera employé pour englober les deux types de fonctions évoquées.

Les exigences qualitatives décrivent les mesures associées et les exigences quantitatives font référence à des **objectifs de sécurité**. Dans le domaine ferroviaire, les objectifs de sécurité sont fixés par différents taux, à des niveaux de considération divers :

— au niveau d'un type d'accident à l'échelle d'un état. Le risque "zéro" n'existant pas, des taux, les plus minimes soient-ils, sont toujours utilisés et vérifiés par les autorités de sécurité nationale. Ils sont établis en fonction du retour d'expérience sur le nombre d'accidents ferroviaires et font l'objet de deux règlements européens : l'un sur les **objectifs de sécurité communs – CST** (*Common Safety Target*) [24] et l'autre sur la méthode de calcul pour les obtenir fondée sur la notion de VNR (Valeur Nationale de Référence) [23].

— au niveau d'un type de danger lié à un système technique. L'objectif de sécurité se réfère dans ce cas à un **taux d'occurrence maximal acceptable de danger – THR** (*Tolerable Hazard Rate*). Il s'obtient sur la base des principes d'acceptation du risque évoqués précédemment qui utilisent des aspects quantitatifs.

— au niveau de la ou des fonctions de sécurité mises en place pour couvrir un danger, i.e. pour que le système technique puisse respecter le THR alloué à ce danger. L'objectif se réfère dans ce cas à un **taux de défaillance fonctionnelle acceptable – TFFR** (*Tolerable Functional Failure Rate*). À noter que des objectifs qualifiés "de conception" (CSM-DT, *Common Safety Method-Design Target*) ont été définis de manière harmonisée à l'échelle européenne pour les défaillances fonctionnelles menant "directement" à des accidents, ceci avec des **taux de défaillance par heure d'exploitation** (10^{-9} et 10^{-7} respectivement pour les accidents "catastrophiques" avec multiples décès, et "critiques" avec un décès) [1].

Dans le cadre d'un système à concevoir, les objectifs de sécurité sont alloués aux dangers à l'aide des THR dans le cadre de l'*appréciation des risques*. Ces THR sont ensuite déclinés sur (voire, partagés entre) les différentes fonctions en TFFR puis, sur les éléments techniques de plus bas niveaux qui sont prévus pour assurer un fonctionnement en sécurité. Ceci explique le chevauchement sur la figure II.4 entre les macro-phases d'*appréciation des risques* et de *réalisation et démonstration des exigences de sécurité*.

6. Les *fonctions de sécurité* sont les fonctions dont le seul objectif est d'assurer la sécurité du système (ex., contrôler la vitesse, verrouiller les portes).

7. Les *fonctions relatives à la sécurité* sont les fonctions dont la défaillance affecte la sécurité du système et n'ont pas pour rôle premier de réduire le risque mais leur défaillance génère néanmoins des risques (ex., maintenir la vitesse, ouvrir les portes).

À noter que les exigences de sécurité qualitatives/quantitatives sont établies à un haut niveau d'un point de vue opérationnel sous la responsabilité d'une société d'exploitation ferroviaire. La déclinaison de ces exigences sur les sous-systèmes et composants sont ensuite à la charge des constructeurs.

2) Réalisation et démonstration de la conformité aux exigences de sécurité

Cette macro-phase s'appuie sur la définition d'une architecture pour le système à développer, c'est-à-dire une *décomposition structurée* du système en sous-systèmes et composants. Celle-ci est associée à des interfaces marquant les limites du système à l'étude.

Par rapport aux activités de sécurité de cette macro-phase, elles se réfèrent aux activités concomitantes suivantes :

1. l'analyse des causes des dangers déjà identifiés, couplée à l'identification des nouveaux dangers issus des solutions techniques ou induits par le système. Il s'agit de l'**analyse des dangers** (*Hazard Analysis*).
2. la **maîtrise des situations dangereuses** (*Hazard Control*).

Pour le premier point, comprendre comment un système peut être source de danger nécessite d'analyser les interactions internes et externes entre les sous-systèmes, ainsi que celles entre les composants. Comme évoqué précédemment, un **modèle de risque** est utile à ce niveau pour soutenir les deux types de raisonnement suivants. D'un côté, il s'agit d'un **raisonnement fonctionnel**, c'est-à-dire sur le comportement du système dans son environnement, ceci afin d'identifier tout comportement fonctionnel potentiellement dangereux. Ce raisonnement fait appel aux méthodes d'ingénierie système évoquées en sous-section II.1.1.2. D'un autre côté, il s'agit d'un **raisonnement sur les défaillances** des équipements et leur causalité. Un danger peut être issu d'une défaillance unique, de défaillances multiples, ou de défaillances de causes communes dans le système, qu'il convient d'identifier. Les méthodes de SdF pour l'analyse de causes avec quantification probabilistes de défaillances en termes FDMS sont utilisées.

Pour le second point, il s'agit de montrer que les sous-systèmes accomplissent les fonctions prévues, qu'ils interagissent en sécurité entre eux, c'est-à-dire en se prémunissant des sources d'erreurs par des mécanismes et procédures qui prennent en compte les défaillances aléatoires et systématiques *à caractère dangereux*. Les **défaillances aléatoires** sont liées à des mécanismes de dégradations du matériel qui peuvent être contrôlés statistiquement. Les caractéristiques physiques sont dès lors caractérisées par des modèles probabilistes dont la plupart sont décrits dans des bases de référence de fiabilité prévisionnelle (ex. MIL-HDBK-217F, EN 61709, UTE C80-811) ou alors proviennent de données constructeurs. Les **défaillances systématiques** sont des défaillances latentes qui se révèlent durant la phase d'exploitation du système opérant sous certaines conditions déterministes (ex. défauts de conception d'un logiciel, erreurs de fabrication ou d'installation). Elles peuvent uniquement être corrigées par des processus et méthodes d'organisation adaptées. Elles ne sont pas quantifiables du fait de leurs causes difficilement prévisibles [48]. Afin de les limiter ou de les éliminer, les activités d'assurance qualité tiennent une place importante dans la gestion de ces défaillances. De même, de nombreuses exigences normatives existent, notamment les exigences d'intégrité de sécurité par rapport aux défaillances systématiques, à savoir des exigences sur les

mesures qualitatives à mettre en œuvre. Ces mesures qualitatives dépendent du SIL et sont de plus en plus contraignantes du SIL 1 au SIL 4. Les exigences d'intégrité de sécurité concernent à la fois les défaillances aléatoires et systématiques et sont des exigences de sécurité fonctionnelle. Pour se prémunir des sources d'erreurs dans les sous-systèmes et composants, des exigences de sécurité technique et contextuelle sont également définies. Les premières contiennent les contraintes techniques de conception / installation / utilisation, les secondes couvrent les exigences d'exploitation et de maintenance.

Au final, d'un point de vue **assurance sécurité** dans le cadre de cette macro-phase de réalisation et démonstration de la sécurité, il s'agit d'apporter les preuves dans la documentation que : *i)* les scénarios fonctionnels faisant interagir les sous-systèmes et son environnement comportent l'action de fonctions de sécurité couvrant les dangers, *ii)* que les modes de défaillances des sous-systèmes et composants ont été analysés et sont dotés d'un contrôle adapté, enfin *iii)* que l'atteinte d'objectifs de sécurité a été démontrée. De plus, compte tenu d'exigences de sécurité allouées aux sous-systèmes et composants à partir d'exigences de haut niveau, les exigences sont nécessairement traçables à partir d'un lien explicite entre les informations d'une phase donnée vers celles des phases qui suivent.

Spécificités ferroviaires :

Les activités de réalisation et de démonstration des exigences de sécurité ferroviaire dépendent du type de principe d'acceptation du risque utilisé :

- lors de l'utilisation des *règles de l'art*, il n'y a pas de méthode d'analyse à proprement parler. Les preuves de sécurité sont des preuves de conformité de la réalisation par rapport aux codes de bonne pratique utilisés.
- lors de l'utilisation de *la comparaison avec un système similaire*, l'analyse des dangers issus du système examiné est effectuée par écarts avec un système de référence. Les preuves de sécurité se réfèrent à la manière dont les écarts ont été contrôlés.
- lors de l'utilisation de l'*estimation explicite des risques*, les activités reposent sur l'allocation de THR/TFFR/SIL et sur la vérification que les équipements développés pour réaliser les fonctions de sécurité prévues, permettent d'atteindre les objectifs de sécurité fixés. Les preuves de sécurité sont la description et les résultats de ces activités. À noter que dans le domaine ferroviaire, une exigence d'intégrité de sécurité relative à la défaillance aléatoire d'une fonction est aujourd'hui exprimée par un TFFR. De ce fait, les exigences quantitatives liées aux SIL sont liées à des plages de valeurs sur les TFFR.

Les activités de maîtrise des situations dangereuses pour les systèmes critiques ferroviaires (cf. second point ci-dessus), tels que les systèmes de contrôle-commande et de signalisation (CCS), le matériel roulant, les installations fixes sur voie et l'alimentation électrique, font face à de nombreuses défaillances systématiques représentées à la figure II.6. Aux actions entreprises pour résoudre ces problèmes de défaillance, s'ajoutent aussi les problèmes d'incompatibilité et de migration à gérer entre les nouveaux et anciens systèmes. En effet, ces derniers restent en place des années, à savoir qu'une infrastructure ferroviaire a une durée de vie de plus de 100 ans et celle d'un train est d'en

moyenne 40 ans. L'intégration des sous-systèmes en sécurité, avec notamment des tests et essais de terrain (au travers d'outils, d'équipements de soutien technique utilisés, de modèles de simulation utilisés), prend donc aussi une part importante dans les activités de sécurité.

FIGURE II.6 – Type de défaillances systématiques pour les systèmes critiques ferroviaires

3) Vérification et validation du respect des exigences de sécurité

La vérification et la validation sont des concepts utilisés, d'une part, dans le cadre général du développement d'un système pour s'assurer que le besoin client est exhaustivement pris en compte et satisfait tout au long du cycle de vie du système [50, 52]. D'autre part, ces concepts interviennent aussi dans un cadre plus spécifique lié au développement de modèles de comportement, ces modèles cherchant à représenter, comprendre et analyser le fonctionnement d'un système. Quel que soit le cadre, les analystes associent classiquement ces concepts aux questions suivantes :

— Pour la vérification : "est-ce que nous développons le système/modèle correctement ?"
— Pour la validation : "est-ce que nous construisons le bon système/modèle ?"

Dans le contexte d'un modèle, la vérification se concentre sur la conformité aux spécifications, c'est-à-dire d'une part, que le modèle a été construit en s'assurant que le processus de modélisation a été effectué de manière robuste, et d'autre part, qu'il mène à des résultats cohérents et précis lors de son utilisation pour effectuer des analyses (= le modèle est "correct"). La vérification peut être formelle ou informelle. Lorsqu'elle est **formelle**, elle implique l'utilisation de méthodes mathématiques ou d'outils d'analyse formelle pour garantir que le modèle satisfait certaines propriétés spécifiées. Lorsqu'elle est **informelle**, elle peut inclure des examens par des experts, des simulations et des tests. La validation se concentre sur la conformité au comportement réel attendu, c'est-à-dire que le modèle est utilisé sur différents scénarios d'utilisation pour confirmer qu'il reflète avec précision le fonctionnement du système ou le phénomène qu'il représente (= le modèle est "fidèle"). Après les étapes de vérification et de validation (notées V&V), le modèle peut alors être utilisé en toute confiance pour prendre des décisions ou faire des prédictions dans le monde réel.

Dans le contexte du cycle de vie d'un système, la vérification et la validation correspondent à un ensemble de tâches en lien avec tout type d'exigences. Pour contribuer à la SdF d'un système, les tâches de V&V sont liées aux exigences FDMS. Nous regarderons plus spécifiquement dans ce mémoire celles liées aux exigences de sécurité. Les tâches de vérification sont incluses à chaque phase du cycle de vie avec la vérification qu'une phase intègre bien les sorties de la phase anté-

rieure. Par souci de lisibilité sur la figure II.4, les boucles de vérification pour une phase ne sont pas représentées. La validation quant-à elle, intervient en deux temps pour garantir que le système en cours d'examen satisfait les exigences spécifiées pour le système en réponse à un besoin client :

— À l'étape 4 du cycle de vie, la satisfaction est évaluée par la validation du raffinement du besoin client en exigences système.
— À l'étape 9 du cycle de vie, la satisfaction est évaluée pendant et suite à l'intégration du système en se référant notamment à la stratégie globale des essais.

L'utilisation de modèles dans ce contexte peut venir en support des deux étapes ci-dessus. Il convient de noter que la notion d'exactitude (*correctness*) est importante dans les tâches de V&V et peut se référer à un système, à une exigence ou à un modèle. L'exactitude d'un système se réfère à sa capacité à fonctionner conformément aux exigences. L'exactitude d'une exigence se concentre sur la qualité de la spécification des besoins. L'exactitude d'un modèle concerne la fidélité de la représentation du système dans le modèle.

Concernant l'**assurance sécurité**, elle se réfère ici aux résultats d'analyses, de simulations, et d'essais de terrain sur le logiciel et le matériel démontrant le respect des exigences de sécurité. Les éléments de sécurité au sein du plan de validation (document dédié à la stratégie de validation) et le rapport de validation (document dédié aux résultats de validation) sont référencés dans un dossier de sécurité.

4) Suivi des performances de sécurité en exploitation

Dans le domaine ferroviaire, le suivi des performances de sécurité en exploitation s'effectue par les autorités nationales de sécurité (ANS), l'EPSF étant l'ANS française. Elles surveillent les différents niveaux des indicateurs issus du retour d'expérience des exploitants, à savoir les indicateurs nationaux et les indicateurs de sécurité communs (ISC) [26], ces derniers étant transmis à l'Agence Ferroviaire Européenne. Les ANS reportent les accidents et incidents dans une base de données. Elles surveillent aussi si les dispositions de tout système de gestion de la sécurité (SGS) détenu par les exploitants ferroviaires sont appliquées. Un SGS est un processus systématique pour gérer et contrôler les risques des activités ferroviaires de façon continue. Il décrit l'organisation, les procédures, les méthodes et moyens techniques ou humains, ainsi que les règles techniques et nationales à mettre en œuvre pour satisfaire durablement, voire améliorer, les objectifs de sécurité en situation normale et dégradée.

Les indicateurs et SGS n'étant pas abordés dans ce mémoire, ils ne seront pas détaillés ici. Toutefois, dans l'annexe 2 sont reportés sur une carte mentale les textes législatifs s'y référant, ainsi que les différents textes mentionnés dans les sous-sections précédentes. En utilisant la version numérique de ce document, chaque branche principale de la carte indique des liens en ligne sur lesquels ces textes sont consultables.

II.1.4 Problématiques de recherche

1) Contexte ferroviaire actuel

Cette sous-section décrit le contexte de mes travaux liés à la sécurité des systèmes complexes critiques, ce contexte étant lié à l'amélioration et la croissance des transports ferroviaires. De manière générale, la stratégie privilégiée pour cela consiste en priorité à optimiser l'utilisation du réseau ferré existant sans étendre ses infrastructures. Dans cette optique, il est nécessaire d'améliorer les performances des systèmes ferroviaires tout en maintenant leur sécurité. L'évolution des systèmes de contrôle-commande et de signalisation (abrégés CCS) contribue significativement à cette amélioration de performances, comme expliqué ci-après. Cette évolution implique notamment l'intégration de nouvelles technologies sans fil de localisation satellitaire et de communication dans les CCS ferroviaires. Nous mettrons en évidence les avantages liés à l'intégration de ces technologies ainsi que les défis qui y sont associés, avant d'aborder les problématiques scientifiques associées.

Contexte lié à l'amélioration et la croissance des transports ferroviaires :

Favoriser l'utilisation des transports ferroviaires pour les trajets moyens et longs de voyageurs (8% des voyages en France sont effectués en train en 2020) et revitaliser le transport de marchandises par trains de fret (9% du transport intérieur français de marchandises en 2020) permettraient d'éviter une très large part d'émission de gaz à effet de serre (GES) actuellement responsables des problèmes climatiques. En effet, ce mode de transport permet le déplacement d'un grand nombre de passagers et de marchandises avec un taux d'émission mondial en 2019 de 1% (voir le 6$^{\text{ème}}$ rapport du GIEC de 2022), ce qui est nettement inférieur à celui de l'aviation civile (11%), des transports maritime/fluvial (11%) et routier (69%), la part du transport dans les émissions mondiales de GES étant de 15% (31% en France, selon les chiffres de l'ADEME). Par conséquent, augmenter l'offre ferroviaire est une nécessité impérieuse et un moyen puissant pour réduire significativement les émissions des GES des transports.

Cette augmentation est envisageable, sans accroître la taille du réseau, selon trois possibilités : *i)* en optimisant la capacité des lignes très fréquentées, *ii)* en renforçant la fréquence des trains (électrifiés ou équipés de solutions d'"énergie verte") sur les lignes régionales et de dessertes fines des territoires[8] (par exemple, passer d'une fréquence de trains en gare toutes les 1 à 2 heures à une fréquence de 30 minutes), et *iii)* en ré-exploitant certaines petites lignes actuellement fermées [74]. Ces options font aujourd'hui l'objet d'investigations et leur faisabilité dépendra de leur viabilité économique, en particulier si les coûts matériels, d'entretien, d'exploitation, et de consommation d'énergie sont maîtrisés.

Amélioration et évolution des CCS :

D'un point de vue technique, agir sur l'augmentation du trafic ferroviaire sur une ligne (en augmentant le nombre ou la fréquence des trains) revient en premier lieu à améliorer les performances du CCS, garant de l'espacement sûr des trains sur la ligne. Cette amélioration vise principalement à renforcer la fiabilité des équipements afin de prévenir les retards de train, à augmenter leur vitesse

8. Les lignes de dessertes fines, souvent appelées petites lignes (catégories UIC 7 à 9 dans le classement de l'Union internationale des chemins de fer – fiche UIC 714), se réfèrent aux lignes sur lesquelles circulent peu de trains, mais qui sont généralement les plus utiles pour les déplacements du quotidien ; elles jouent ainsi un rôle essentiel dans les questions d'aménagement du territoire.

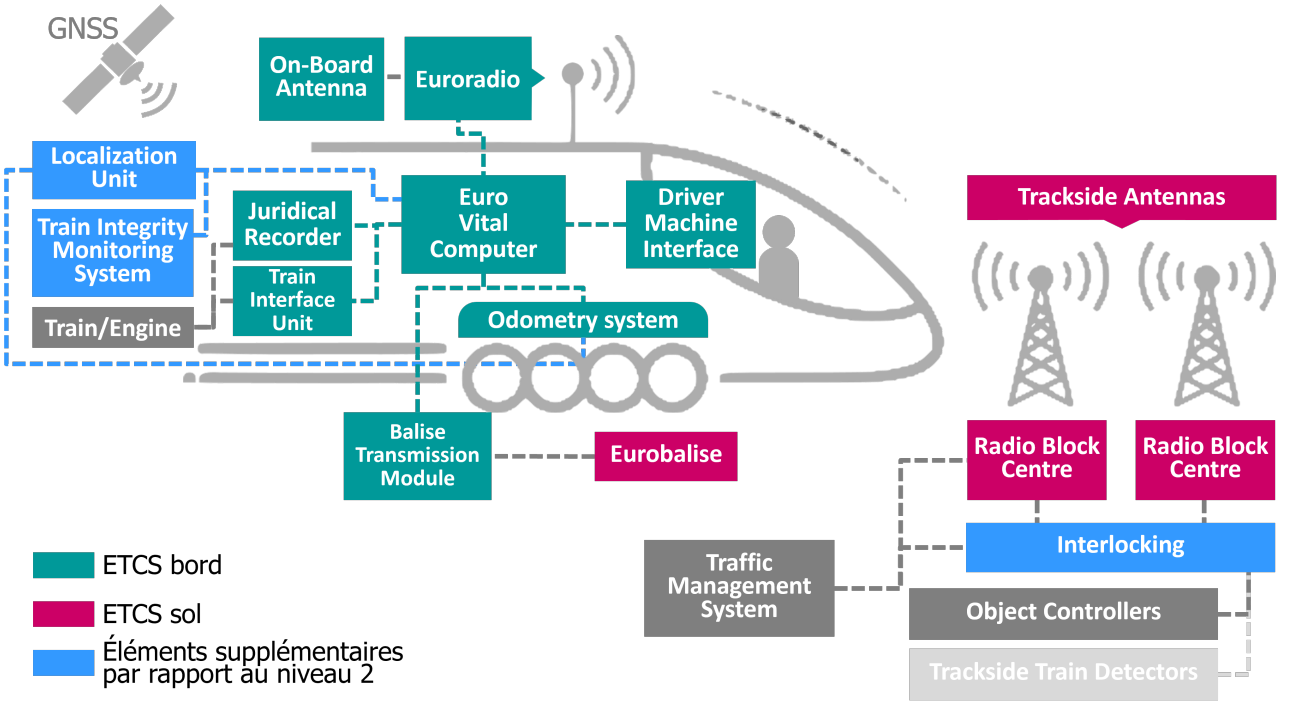


FIGURE II.7 – Vue composants des niveaux 2 et 3 de l'ETCS (avec la classification des niveaux antérieure à 2023)

en accord avec les capacités du matériel roulant (comprenant les capacités de freinage et les possibilités d'automatisation de la conduite) et de l'état de la voie, à réduire les arrêts en pleine voie, et à réduire la distance entre les trains. Pour ce dernier aspect, il est nécessaire de faire évoluer le fonctionnement du CCS afin de permettre la réalisation des nouveaux concepts opérationnels qui seront décrits par la suite.

Actuellement, l'ERTMS (*European Rail Traffic Management System*) est un CCS interopérable à l'échelle européenne, défini dans le cadre de l'harmonisation des systèmes européens ferroviaires conventionnels et grande vitesse. Son déploiement est requis d'ici 2030, notamment pour les 51 000 km de lignes ferroviaires des neufs corridors transeuropéens du réseau central (TEN-T) [2]. De forts risques existent toutefois liés à la non-réalisation de cet objectif chiffré. De plus, le déploiement de l'ERTMS est également requis pour tout nouveau système ou toutes modifications de système conformément au règlement européen (UE)2023/1695 [3]. À cet égard, les évolutions recherchées des CCS se concentrent principalement sur l'évolution de l'ERTMS. Il est toutefois important de noter que, pour certaines lignes envisageant la circulation de trains plus légers et innovants (actuellement en réflexion dans le cadre de projets nationaux tels que TELLi, Draisy, Flexy, Ferromobile, Ecotrain), la législation applicable relèvera davantage de celle associée aux transports guidés urbains.

Pour l'ERTMS, deux niveaux d'implémentation sont spécifiés dans la 4ème version des spécifications de l'ETCS datant de 2023. Ces niveaux 1 et 2 se rapportent plus précisément aux différentes implémentations que peut adopter son sous-système de contrôle et de protection automatique des trains, l'ETCS (*European Train Control System*) [93]. Ils sont définis pour permettre une migration progressive des systèmes nationaux non-interopérables vers l'ERTMS.

L'évolution du niveau 2 de l'ETCS fait l'objet de nombreuses recherches, notamment dans le cadre des initiatives européennes *Shift2Rail* et *Europe's Rail*. Les principes d'évolution de ce niveau reposent sur le transfert de fonctionnalités de protection des trains depuis les équipements existants installés sur l'infrastructure ferroviaire actuelle (sur ou aux abords des voies), 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) peuvent être issues des trains (plus précisément de leur sous-systèmes "bord") et non plus d'équipements de détection au sol reliés à l'ETCS (plus précisément à son sous-système "sol") . La radiocommunication bord / sol de l'ETCS permet alors à l'ETCS sol de connaître ces informations d'occupation de voie pour gérer en sécurité sur le réseau ferré, l'ensemble des itinéraires des trains. Ainsi, l'ETCS niveau 2 peut être mis en œuvre selon trois variants [93, 3] :

1) Avec détection des trains par l'ETCS sol,
2) Sans détection des trains par l'ETCS sol,
3) Avec une détection des trains réduite au niveau de l'ETCS sol.

Les spécifications relatives aux deux derniers variants étaient précédemment classées dans le "niveau 3" dans les versions des spécifications de l'ETCS datant d'avant 2023. Ce sont précisément ces deux variants qui concentrent les recherches actuelles. La figure II.7 illustre l'évolution de l'architecture haut niveau de l'ETCS entre le premier variant et les deux derniers. Elle utilise l'ancienne classification "niveau 2" / "niveau 3" par souci de clarté et de cohérence avec nos travaux présentés dans ce mémoire, antérieurs à 2023. La référence au "niveau 3" sera conservée par la suite.

Avantages de l'intégration de nouvelles technologies sans fil dans les CCS ferroviaires :

L'emploi de nouvelles technologies pour l'intégration de fonctionnalités à bord des trains, en particulier les technologies de localisation satellitaire (GNSS, *Global Navigation Satellite Systems*) en lien avec différents capteurs et traitements, ainsi que les technologies de communication sans fil, permet une exploitation des trains plus performante avec des approches opérationnelles plus flexibles et modulaires. Ces approches reposent sur des concepts novateurs tels que l'exploitation à l'aide de cantons virtuels [9], de cantons mobiles [10], et de trains couplés virtuellement [11]. En effet, les analyses de la communauté "gestion de trafic ferroviaire" ont démontré l'efficacité de ces concepts pour améliorer la capacité des lignes du réseau ferré [80]. La demande de leur mise en œuvre est importante pour répondre aux différents besoins des acteurs ferroviaires, notamment pour l'implémentation des cantons mobiles supportée par l'ERTMS/ETCS niveau 3.

Ces technologies permettent également de réduire les coûts d'installation des équipements sur voies, ce qui est particulièrement intéressant pour les petites lignes dont la rentabilité est limitée.

9. Cantons virtuels : ils permettent de diviser les cantons fixes utilisés classiquement sur une ligne, en plusieurs cantons virtuels, ceux-ci étant définis numériquement dans des espaces "digitalisés". Comme un canton ne peut être occupé que par un seul train, le découpage supplémentaire par cantons virtuels permet de placer davantage de trains sur une ligne.

10. Cantons mobiles : l'espacement entre les trains se ramène à un seul canton virtuel qui évolue avec chaque train et dont la longueur dépend uniquement de la distance de freinage absolue du train. L'espacement entre trains diminuant, la capacité augmente.

11. Couplage virtuel : un train adapte sa vitesse à celle du train de devant, par l'intermédiaire d'un lien radio entre eux, pour s'en rapprocher au maximum. Les trains sont alors considérés comme couplés non plus mécaniquement mais virtuellement, i.e. sans attelage.

Défis associés à cette intégration :

L'adoption de ces nouvelles technologies suscite des interrogations quant à leur impact en termes de sécurité, ce qui freine leur acceptation dans le domaine du contrôle-commande ferroviaire. D'une part, se pose la question de **comment spécifier** les exigences de sécurité et allouer les objectifs de sécurité aux équipements mettant en œuvre ces technologies et à ceux qui sécurisent leurs défauts, afin de rendre les risques associés acceptables. Cette tâche est d'autant plus difficile que les besoins utilisateurs sont souvent exprimés selon des critères propres aux technologies envisagées (par exemple, la précision pour la localisation) plutôt que spécifiquement en termes de sécurité.

D'autre part, se pose la question de **comment démontrer** le respect de ces exigences et objectifs de sécurité prévus pour atteindre un niveau de risque acceptable. Cela implique de prendre en compte les choix architecturaux de l'équipement technique implémentant ces technologies, ainsi que la sensibilité de ces technologies au contexte opérationnel ferroviaire. Cette tâche est ardue en raison de leurs spécificités liées au traitement de signaux. Cette question est en fait relative au **risque technique** associé aux équipements intégrant les technologies évoquées. De plus, dès lors que ces équipements interviennent dans un CCS, il est crucial de prendre en compte dans cette démonstration le **risque opérationnel** qu'ils peuvent générer. Évaluer ce risque opérationnel est une problématique délicate, d'autant plus qu'il convient également de considérer, dans les analyses de risques, la complexité fonctionnelle associée aux derniers concepts opérationnels novateurs évoqués précédemment.

Ces défis dépendant du contexte ferroviaire rejoignent des problématiques scientifiques plus générales liées à la "démarche sécurité" des systèmes complexes critiques. Ces problématiques sont décrites ci-dessous et sont examinées par la suite dans les trois grandes sections suivantes de ce mémoire de recherche. Ci-dessous, la première problématique aborde les questions relatives au processus d'appréciation des risques de la démarche sécurité d'un système complexe critique. La seconde problématique aborde les questions relatives aux analyses de risques techniques et opérationnels liées à la démarche sécurité d'un système complexe critique, tel qu'un CCS intégrant les nouvelles technologies évoquées, qualifié de CCS avancé.

2) Problématique d'allocation liée au processus d'appréciation des risques

La spécification des exigences et objectifs de sécurité, résultant du processus d'appréciation des risques, notamment par le biais d'allocations d'objectifs de sécurité aux situations dangereuses et l'allocation de SIL aux fonctions de sécurité, sont des points clés pour la démarche sécurité dans le domaine ferroviaire. Les exigences obtenues sont continuellement affinées et complétées tout au long du développement du système, en fonction des éléments issus de la conception détaillée. Cependant, établir ces exigences de manière aussi complète et rigoureuse que possible dès les premières étapes de développement reste un défi. L'enjeu majeur est d'obtenir un ensemble d'exigences le plus exhaustif possible à ce stade, afin d'éviter ultérieurement des adaptations ou correctifs chronophages, sources d'erreurs et, finalement, de risques découlant d'une analyse insuffisante en amont.

Néanmoins, lors de cette phase d'initialisation de la démarche sécurité, il demeure difficile d'identifier et d'articuler de manière intégrée les informations liées aux dangers en limite du système (*boundary hazards*), aux objectifs de sécurité et aux fonctions de sécurité à prévoir. Établir un lien structuré entre ces trois aspects, tout en restant en cohérence avec les textes réglementaires ferroviaires en vigueur et avec le cadre de sécurité général, constitue un défi. Nous nous sommes penchés sur cette problématique afin de contribuer à l'allocation d'objectifs de sécurité dans le domaine ferroviaire, tant dans le cadre général que dans le cadre spécifique des fonctions implémentées par des technologies sans fil.

Il convient de noter que même si des méthodes d'allocation existent, telles que le graphe de risque ou la matrice de gravité des événements dangereux (cf. figure II.3), celles-ci se concentrent sur une seule fonction analysée séparément des autres. Par conséquent, elles ne tiennent pas compte du fait que de multiples fonctions de sécurité exécutées, par différents systèmes de sécurité, coexistent dans un système ferroviaire global.

3) Problématique d'analyse de risques liée à la démonstration de sécurité

Lors de l'étape de démonstration de sécurité d'un système, l'analyse qualitative et quantitative des défauts liés aux composants techniques, impliquant l'évolution des états des composants dans le temps, ainsi que l'identification des impacts opérationnels dangereux liés aux états dégradés, constitue déjà un défi. Celui-ci est exacerbé par les effets multiples générés par l'environnement physique dans lequel les trains évoluent. Nous nous sommes alors penchés sur ces aspects dynamiques et les effets multiples de l'environnement afin de contribuer aux analyses de risques techniques et opérationnels dans le cadre général des systèmes complexes critiques ferroviaires. En particulier, la fonction de localisation utilisant des technologies de navigation par satellites (GNSS) occupe une place importante dans nos travaux.

Pour ces analyses de risques, il convient de noter que, de manière générale, dans les systèmes complexes, il est difficile, voire impossible, de prévoir tous les scénarios dangereux. Une pratique de plus en plus adoptée est de guider l'identification de ces scénarios dangereux par l'emploi de modèles intégrant les diverses interactions entre entités du système (techniques/humaines) et, aussi, entre le système et son environnement. Ces modèles reproduisent, par différentes méthodes d'ingénierie système, des comportements fonctionnels et/ou intègrent des défauts de composants avec des lois prévisionnelles de dysfonctionnement. Les analyses et résultats issus de ces modèles peuvent permettre de repérer des liens de causes-conséquences et aussi des séquences d'évènements menant à une situation dangereuse. Bien sûr, l'effort de modélisation dépend du niveau de complexité du système et du niveau de détails considérés. D'ailleurs, cette modélisation est elle-même source de problèmes à résoudre.

En ce qui concerne l'analyse des modèles, elle s'effectue généralement en déduisant des propriétés qualitatives ou quantitatives sur la base de leurs simulations, lesquelles reflètent une réalité future potentielle, c'est-à-dire différentes évolutions du système dans le temps. Cependant, la génération de scénarios aux conditions limites ou d'occurrence rare s'avère difficile en simulation, voire impossible. Nous nous sommes alors penchés sur l'obtention des modèles dotés de caractéristiques permettant d'y associer des raisonnements mathématiques pour leur analyse. Ainsi, en complément de la recherche de propriétés par simulation, la mise en œuvre sur des modèles d'algorithmes avan-

cés, notamment ceux intervenant au sein des techniques de vérification formelle, est étudiée. Ces techniques consistent à explorer tous les scénarios possibles de l'espace d'états atteignables afin de déduire des propriétés spécifiques d'un système. Il est à noter que les techniques de vérification formelle existent depuis une trentaine d'années pour des systèmes au comportement relativement simple et ont connu des progrès marquants au cours de la dernière décennie.

II.1.5 Conclusion

En conclusion, nos efforts de recherche ont ainsi pour objectif de contribuer aux activités de sécurité menant à la certification des CCS ferroviaires intégrant des fonctionnalités avancées de localisation et de communication. Les problématiques que nous avons identifiées dans cette section et qui seront traitées dans les sections suivantes de ce mémoire, s'accompagnent de travaux de recherche en sûreté de fonctionnement et gestion des risques sur la base des concepts et méthodes exposés dans cette section.

Parallèlement, avec ces travaux, il est possible de guider les différents organismes ferroviaires impliqués dans le contrôle de la sécurité, tels que les autorités nationales de sécurité ferroviaire comme l'EPSF, les organismes évaluateurs de sécurité comme CERTIFER, et l'Agence Ferroviaire Européenne. Il est possible aussi de fournir une expertise sur les points sensibles de sécurité liés aux systèmes évoqués.

Ces considérations soulèvent également des questions sur la compatibilité des approches de recherche développées avec le cadre réglementaire européen actuel de la gestion des risques ferroviaires (voir Annexe 2), voire même sur la manière de faire évoluer ce cadre de manière harmonisée. C'est pourquoi, dans les sections suivantes, il est toujours indiqué quand c'est possible, comment nos travaux s'inscrivent en cohérence avec ce cadre réglementaire.

II.2 Allocation d'exigences de sécurité dans un système critique ferroviaire

Les travaux présentés dans cette section ont pour objectif de contribuer à l'allocation d'exigences liées à la sécurité, cette activité intervenant à la fin de la macro-phase d'*appréciation des risques* décrite à la section II.1. Trois approches, proposées dans le cadre des post-doctorats de Kiswendsida Abel Ouedraogo et Thi Phuong Khanh Nguyen, ainsi qu'à travers une collaboration avec l'IRT Railenium et l'Université de Technologie de Compiègne, sont présentées. La première, décrite à la sous-section II.2.1, concerne l'élaboration d'une méthodologie générique pour l'allocation de SIL aux fonctions relatives à la sécurité d'un système critique ferroviaire. Les deux suivantes se concentrent plus spécifiquement sur la fonction de localisation des trains utilisant des signaux satellitaires, afin de prendre en compte les incertitudes associées aux erreurs ou aux défaillances liées aux GNSS.

Ainsi, la deuxième contribution, décrite à la sous-section II.2.2 repose sur une méthodologie d'allocation d'objectifs de sécurité imprécis. Cette approche vise à prendre en compte les incertitudes liées à l'apparition des dangers associés à la défaillance de la fonction de localisation d'ETCS intégrant le GNSS. Dans la troisième contribution détaillée à la sous-section II.2.3, une approche est proposée pour approfondir l'allocation fonctionnelle à un niveau plus détaillé, celui de l'architecture de l'ETCS et de ses constituants, dont l'unité de localisation.

II.2.1 Méthodologie générique pour l'allocation de SIL

La méthodologie générique a été proposée dans le cadre du post-doctorat de Kiswendsida Abel Ouedraogo. Ces travaux ont été réalisés dans le contexte du projet SIL, financé par l'EPSF, et ont abouti à la rédaction d'un article de revue [ACL6], ainsi que de quatre articles de conférence [ACTI14, ACTN6, ACTI18, ACTI22]. Les principes méthodologiques et applicatifs décrits dans ces publications reposent sur les retours d'expérience issus des échanges avec différents acteurs ferroviaires durant la réalisation du projet.

1) Contexte des travaux

La méthodologie générique pour l'allocation de niveaux d'intégrité de sécurité (SIL, *Safety Integrity Level*) abordée dans cette sous-section vise à expliciter et structurer les étapes de l'allocation des SIL dans une perspective ultérieure d'automatisation éventuelle. L'harmonisation de l'allocation des SIL à l'échelle européenne est un défi ancien dans le domaine ferroviaire, avec des initiatives d'analyse lancées dans des projets européens tels que MODTRAIN et MODURBAN [103]. Ce défi découle de la difficulté à fédérer les acteurs (exploitants, constructeurs, évaluateurs de sécurité) autour d'une seule méthodologie. Chacun membre de l'UE a ses pratiques, souvent diverses et bien établies, parfois avec des interprétations incorrectes des concepts liés au SIL en raison d'une mauvaise compréhension [77], ce qui rend l'harmonisation difficile. De plus, certaines méthodes d'allocation proviennent d'autres secteurs (nucléaire, sécurité des machines, automobile, etc.) avec des référentiels différents et parfois contradictoires, même si, au départ, ces référentiels s'appuient tous sur la norme internationale de sécurité fonctionnelle : la norme IEC 61508 [48]. En réalité, les incompréhensions entre acteurs découlent des différentes applications des concepts et méthodes présents dans cette norme "chapeau".

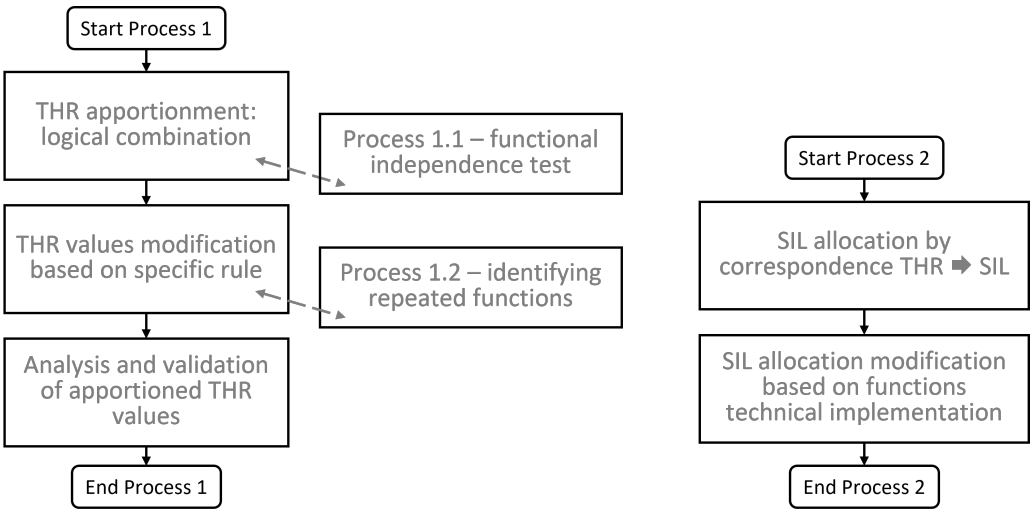


FIGURE II.8 – Aperçu des processus 1 et 2, resp., pour la répartition des THR et l'allocation des SIL

Pour la méthodologie proposée, un pré-requis important est de rester en cohérence avec les textes réglementaires et normatifs en vigueur suivants : *i)* la méthode de sécurité commune pour l'appréciation des risques présentée dans le règlement européen 402/2013 [4] (qui ne traite pas de l'allocation des SIL dans sa version actuelle), *ii)* les normes de sécurité ferroviaire EN 50126, EN 50128 et EN 50129 [30, 31, 32, 33]. Quant au champ d'application de la méthodologie, il porte sur l'ensemble des fonctions de sécurité présentes dans tout type de système ferroviaire critique ; l'EPSF se concentre en particulier sur les fonctions intervenant au sein d'un matériel roulant (i.e., les fonctions d'un système appelé TCMS, *Train Control and Monitoring System*). Les contributions proposées font écho à mes travaux de thèse sur lesquels j'ai pu m'appuyer [ACL13, ACTI33, ACTI32, ACTI34, ACTI35].

Comme introduit à la section II.1, un SIL a vocation à être alloué à chaque fonction d'un système critique dans le but de mettre en place la "sécurité fonctionnelle" du système. Ainsi, l'allocation de SIL aux fonctions de sécurité permet de fixer des exigences de sécurité qualitatives et quantitatives selon le niveau SIL 1 à SIL 4. Cette allocation s'effectue de manière à ce que les exigences attribuées à une fonction, en tenant compte du SIL retenu et de celui des autres fonctions présentes, puissent contribuer à réduire le niveau de risque du système global jusqu'à un niveau acceptable. Toutefois, plus l'architecture du système est complexe, plus l'allocation devient délicate avec des dépendances entres les fonctions à ne pas omettre. Les paragraphes ci-dessous décrivent le processus que nous avons développé pour cette allocation.

2) Processus développés

Aspects généraux sur la méthodologie :

La méthodologie proposée est déclinée en deux processus (cf. figure II.8) et leurs différentes étapes sont fondées sur des règles pratiques et des hypothèses à vérifier. Sa mise en œuvre débute par l'utilisation d'objectifs de sécurité quantitatifs, les THR supposés fixés par l'exploitant ferroviaire. Ces objectifs sont à répartir sur les différentes fonctions de sécurité selon les étapes formalisées par la méthodologie. Le fait de partir d'objectifs quantitatifs permet de tenir compte des objectifs de conception harmonisés à l'échelle européenne (CSM-DT) (cf. sous-section II.1.3.1). Même si les

THR sont des critères quantitatifs, ils sont à la fois utilisés pour spécifier des exigences quantitatives (sur l'intégrité de sécurité vis-à-vis des défaillances aléatoires) et des exigences qualitatives (sur l'intégrité de sécurité vis-à-vis des défaillances systématiques) (cf. sous-section II.1.3.2), la rigueur liée aux exigences qualitatives étant en lien avec l'ordre de grandeur des objectifs de THR. Il est important de noter que, lors du développement de la méthodologie proposée, la version de la norme EN50126 de 2017 n'était pas encore disponible car en projet d'évolution. Par conséquent, l'allocation d'objectifs de sécurité aux fonctions s'est effectuée sous la forme de THR, appelés "THR répartis". Aujourd'hui ceux-ci correspondent aux TFFR (cf. sous-section II.1.3.1) pour bien séparer la couche des dangers de la couche des fonctions.

La méthode de l'arbre de défaillances (AdD), couramment adoptée pour les analyses de fiabilité et de sécurité des systèmes (dont les fondements sont rappelés au §II.3.2), est employée pour représenter les liens causes/conséquences entre l'occurrence d'une situation dangereuse et les défaillances des fonctions relatives à la sécurité associées. La méthodologie se réfère donc à la combinaison d'événements de défaillance avec des portes logiques *ET* et *OU*. Il est important de noter que les hypothèses adoptées permettent d'utiliser la méthode de l'AdD avec des règles de combinaisons conjonctive et disjonctive acceptant des taux par heure en entrée.

La méthodologie requiert les données suivantes provenant d'une APR :

— la liste des situations dangereuses (des exemples de SD génériques sont listés dans l'annexe C17 de [35]),
— la liste des fonctions de sécurité ;
— la liste de scénarios incluant :
  - les combinaisons de défaillances de fonctions menant à chaque situation dangereuse,
  - les défaillances fonctionnelles menant directement à un risque de décès ;
— Les objectifs associés aux situations dangereuses (THR) et/ou aux fonctions (CSM-DT).

1er processus s'appuyant sur le THR :

Dans ce processus, les éléments du système sont considérés d'un point de vue fonctionnel étant donné que plusieurs architectures matérielles/logicielles sont possibles. Dans d'autres secteurs s'appuyant sur la norme générique IEC 61508, l'allocation des SIL peut impliquer des calculs fiabilistes sur des architectures techniques particulières réalisant une fonction de sécurité.

Des règles de répartition du THR associé à l'occurrence d'une situation dangereuse dans un scénario d'accident considéré sont appliquées lors d'une analyse "*Top-Down*" basée sur un arbre de défaillances, afin d'obtenir des objectifs sur les fonctions et sous-fonctions relatives à la sécurité.

D'une part, ces règles sont liées aux combinaisons logiques (conjonction ou disjonction) des fonctions relatives à la sécurité, empêchant l'occurrence d'une situation dangereuse (cf. 1ère étape du processus 1 dans les figures II.8 et II.9). Ce sont les défaillances des fonctions relatives à la sécurité en lien avec les situations dangereuses qui sont plutôt manipulées compte tenu des combinaisons entre causes dangereuses et conséquences identifiées.

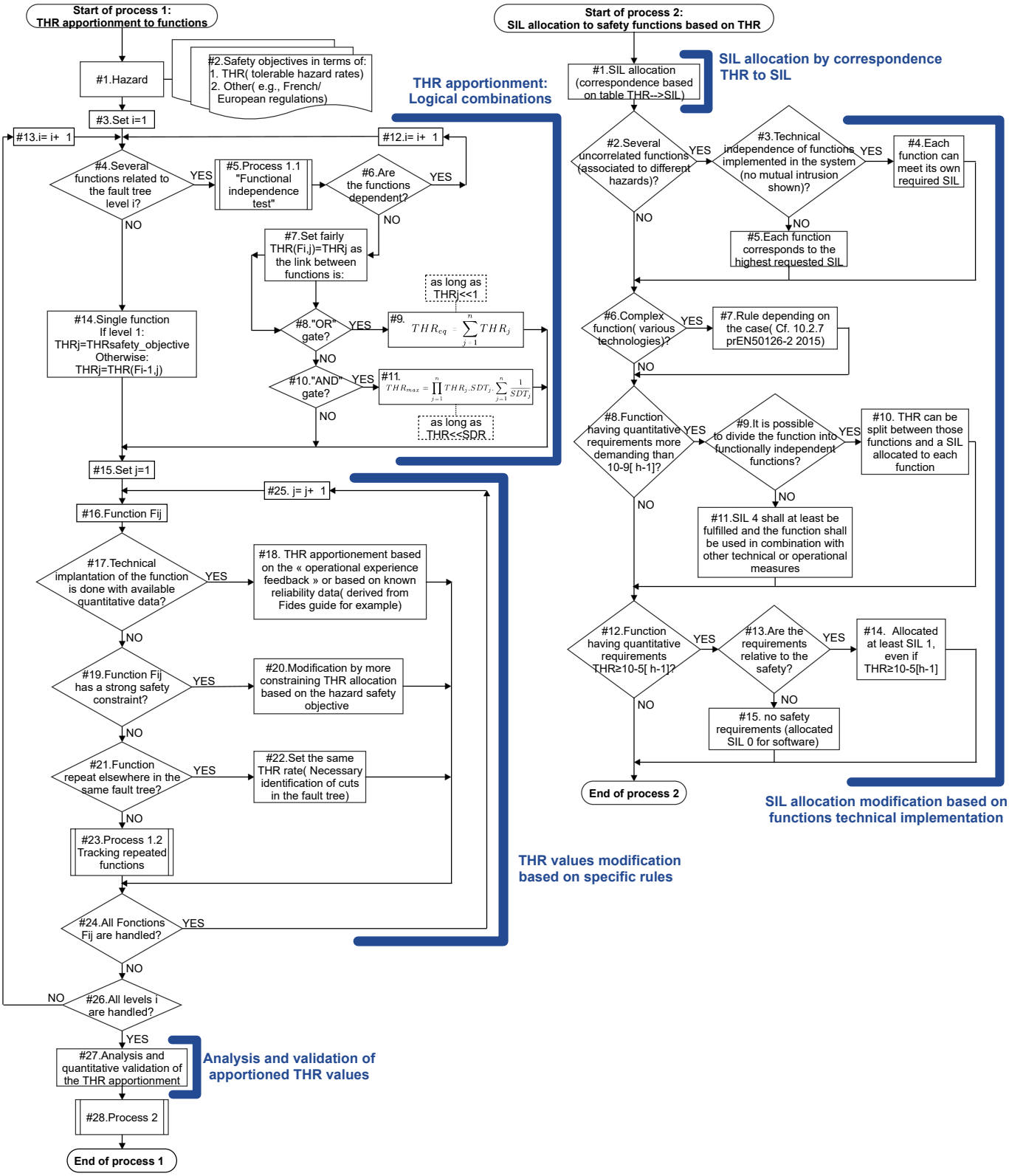


FIGURE II.9 – Méthodologie d'allocation des SIL

D'autre part, afin de prendre en considération divers aspects techniques tels le maillon le plus faible en matière de sécurité, dernier maillon de la chaîne de sécurité, les dépendances fonctionnelles, la complexité technologique, etc., des règles spécifiques implicitement utilisées dans les pratiques existantes sont définies. Ces règles ont pour but de réajuster certaines valeurs de THR, comme indiqué dans la 2ème étape du processus 1 dans les figures II.8 et II.9.

Après avoir apporté les modifications aux THR répartis conformément aux règles spécifiques, une analyse et une validation quantitative de type "*Bottom-Up*" sont réalisées. Cette étape vise à vérifier la conformité de la répartition du THR lié à l'objectif de sécurité de chaque situation dangereuse correspondante (cf. 3ème étape du processus 1 dans les figures II.8 et II.9). Cette validation a pour but d'apporter éventuellement des réductions ou des modifications explicites d'objectifs, en prenant en compte des architectures techniques particulières. Il est important de noter que si un objectif de sécurité n'est pas atteint, il faudra alors démontrer l'acceptabilité du risque, en utilisant par exemple un argumentaire d'expert, un raisonnement basé sur le principe GAMÉ, etc.

2nd processus d'allocation des SIL :
L'objectif de sécurité se rapporte à une défaillance de fonction, tandis que le SIL se rapporte à une fonction : pour chaque mode de défaillance d'une fonction donnée, un objectif de sécurité peut être attribué en terme de THR réparti. Ensuite, un SIL est attribué à cette fonction à partir du THR réparti le plus exigeant la concernant. L'allocation des SIL aux fonctions relatives à la sécurité, sur la base des THR répartis et validés dans le processus précédent, est alors mise en œuvre. Dans un premier temps, cette allocation aux fonctions relatives à la sécurité se fait par la correspondance entre THR répartis (équivalent du TFFR) et SIL (voir la table des SIL dans [33]).

La manière dont sont implémentées les fonctions sur les sous-systèmes d'un train (projection des fonctions sur l'architecture matérielle/logicielle) a également une incidence sur l'allocation des SIL. Des règles d'allocation spécifiques tenant compte de ces conditions d'implémentation (solutions techniques complexes, intrusion mutuelle des fonctions à implémenter, exigences de sécurité très fortes/faibles) sont également définies dans ce dernier processus. En particulier, pour une fonction présentant des exigences quantitatives plus sévères que 10^{-9}/h, il est nécessaire de lui associer des méthodes et des mesures techniques ou opérationnelles applicables au SIL 4. De même, il peut être requis d'allouer au moins un SIL 1 à une fonction présentant des exigences quantitatives relatives à la sécurité faibles, telles que $THR \geq 10^{-5}$/h.

Cette méthodologie générique d'allocation des SIL a été appliquée pour déterminer les exigences de sécurité du TIMS (*Train Integrity Monitoring System*, système observé dans la figure II.7), comme décrit dans l'article issu de nos travaux dans le cadre du projet européen X2Rail4-WP6 [Sub1]. Le TIMS réalise deux fonctions de sécurité essentielles au fonctionnement d'un CCS ferroviaire de dernière génération tel que l'ETCS niveau 3 : surveiller l'absence de rupture d'attelage entre les voitures d'un même train et déterminer la longueur d'un train, cette dernière pouvant varier, en particulier pour les trains de fret.

La partie suivante aborde un autre domaine d'application, celui lié à nouveau système de localisation de trains déterminant la position de l'avant d'un train grâce à l'utilisation des GNSS. Outre la question de la sécurité liée à l'intégration de ce type de système dans les CCS ferroviaires, nous avons voulu examiner la possibilité d'introduire des imprécisions dans le processus d'allocation, une intention qui sera justifiée ci-dessous.

II.2.2 Allocation fonctionnelle avec imprécisions pour des systèmes utilisant les GNSS

1) Introduction des types d'intégration du GNSS dans l'ETCS

La fonction de localisation des trains utilisée dans l'ETCS (cf. §II.1.4.1 introduisant l'ETCS) repose actuellement sur l'utilisation combinée d'équipements d'odométrie embarqués et de balises physiques installées entre les rails de la voie ferrée. L'estimation de la distance parcourue par le train, obtenue par les équipements d'odométrie, accumule une erreur croissante à mesure que le train progresse le long de la voie. Pour corriger de manière ponctuelle cette erreur par recalage, des balises physiques, espacées de quelques kilomètres, sont utilisées. Chaque balise transmet par induction sa position de référence, c'est-à-dire sa coordonnée absolue, lorsque le train la franchit.

Afin d'améliorer les performances de localisation à moindre coût, plusieurs projets de recherche européens ont exploré l'utilisation de systèmes de positionnement par satellite selon trois options [ACL7] :

— *Balises virtuelles* : Cette option implique l'utilisation d'un équipement GNSS pour jouer le rôle d'une balise virtuelle, rôle fonctionnellement équivalent à celui d'une balise physique [86]. En pratique, la position absolue fournie en continu par un récepteur GNSS embarqué sert de position de référence pour réduire l'erreur d'odométrie. L'avantage de cette approche réside dans le fait qu'elle ne nécessite aucune autre installation que les équipements GNSS embarqués dans les trains, réduisant ainsi les coûts en éliminant le recours aux balises physiques et permettant des recalages plus fréquents. Cependant, le recalage par balises virtuelles peut comporter des erreurs à maîtriser, par exemple en sélectionnant les zones de réception GNSS favorables et en hybridant le GNSS avec d'autres capteurs.

— *Odométrie avancée* : dans cette option, l'équipement d'odométrie est remplacé par un équipement GNSS fournissant une distance parcourue plus précise, nécessitant donc moins de recalage par balise physique. De même, les erreurs sont à corriger ou à minimiser .

— *Solution globale* : dans cette option, l'ensemble odométrie / balises physiques est remplacé par une solution globale de localisation GNSS assistée par d'autres dispositifs destinés à mesurer le mouvement d'un mobile (exemple, centrale inertielle). Avec une maîtrise justifiée des erreurs, ce type de solution peut présenter des coûts très réduits.

Actuellement, la première parmi ces trois options offre l'intégration la plus aisée, car elle permet de laisser inchangées les spécifications d'ETCS, en ajoutant uniquement un équipement VBTS (*Virtual Balise Transmission System*) possédant les mêmes spécifications d'interface que celles liées aux balises physiques [104]. Les deux autres alternatives nécessitent un changement plus profond d'ETCS, ce qui est délicat dès lors que l'on vise des spécifications interopérables. L'utilisation d'un VBTS pour l'ETCS niveau 2 sera considérée dans cette sous-section.

2) Objectif de l'ajout d'imprécisions dans l'allocation

L'utilisation des GNSS pour la fonction de localisation des trains dans l'ETCS introduit de nouveaux risques pour la sécurité du trafic ferroviaire. Les erreurs associées aux signaux GNSS, comme expliqué dans la section II.3 dédiée aux risques techniques au §II.3.1, peuvent entraîner une détection erronée d'une balise virtuelle, menant ainsi à un fonctionnement incorrect du système VBTS. Bien que des mécanismes de détection de défaillances aient été proposés pour atténuer ces risques, des hypothèses fortes sur les modèles de distributions liés aux erreurs de mesure du temps de propagation des signaux et aux effets de l'environnement (en particulier le fait de considérer des bruits blancs gaussiens) rendent ces processus de détection non garantis en termes de sécurité.

De plus, l'évaluation des performances de ces mécanismes ne prend pas suffisamment en compte la variabilité des conditions de réception des signaux GNSS en milieu opérationnel. Les tests opérationnels sont souvent restreints à l'analyse de mesures sur des portions de voie limitées, ce qui ne permet pas d'obtenir une représentativité globale du fonctionnement correct (i.e., l'erreur supposée de la position estimée est bornée correctement) ou défaillant des mécanismes (i.e., l'erreur de position est sous-estimée bien que suffisamment importante pour déclencher une alerte du mécanisme de détection). Le manque de données ferroviaires représentatives de l'ensemble des différents environnements traversés par un train limite la validation de ces mécanismes selon des exigences données, en particulier celles liées à la sécurité. La validation des exigences de sécurité est importante car elle conditionne l'autorisation de mise en service. Pour établir ces exigences, l'utilisation d'objectifs de sécurité exprimés en termes de THR pour un système intégrant le GNSS suppose que le récepteur GNSS possède un point de fonctionnement unique à partir duquel les déviations inacceptables (i.e., non détectées) peuvent être appréhendées avec un taux exprimé en fonction du temps. Comme expliqué précédemment, ces déviations ne sont pas entièrement caractérisées aujourd'hui. Par conséquent, l'utilisation d'un THR en tant que tel crée une forte contrainte de conception potentiellement irréalisable pour les constructeurs.

Dans le cadre de ces travaux, pour atténuer cette contrainte imposée par une valeur fixe de THR, nous avons considéré des THR imprécis pour laisser la possibilité de considérer une plage de fonctionnement pour le récepteur GNSS. Concrètement, le risque de s'écarter de cette plage de fonctionnement sera représenté par un intervalle de THR.

3) Principes

La méthode originale proposée dans ces travaux a fait l'objet d'une collaboration avec Railenium et l'université de technologie de Compiègne dans le cadre du projet européen X2Rail-2 (WP3), les réflexions avec l'UTC ayant débuté dans le projet ERSAT-GGC. Cette collaboration tripartite a permis de contribuer à un livrable de projet, une communication [COM3] et un papier [ACTI12] dans une conférence internationale de référence en sécurité des systèmes (ESREL).

Afin d'allouer des THR non plus comme des valeurs précises, mais comme des intervalles reflétant les incertitudes aléatoires et épistémiques des modèles utilisés pour la détection des défaillances et la prise en compte de l'impact de l'environnement, la méthode d'allocation proposée repose sur l'analyse de l'arbre de défaillances (décrite au §II.3.2) et sur les méthodes de propagation d'intervalles. Cette approche prend en compte les incertitudes liées au modèle et aux données en associant un

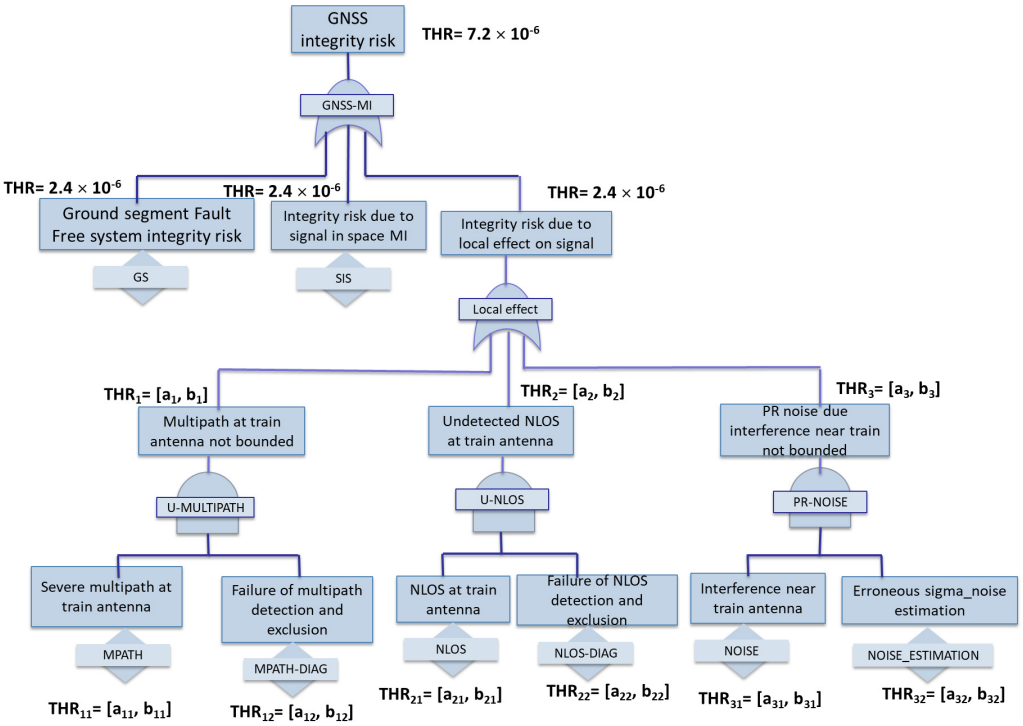


FIGURE II.10 – Extrait de l'AdD du VBTS englobant les événements de base relatifs aux erreurs GNSS

intervalle probabiliste aux événements de base d'un AdD. Ceci confère alors une plus grande polyvalence à la méthode d'allocation recommandée par la norme EN 50126 [31], laquelle a été affinée grâce à l'approche proposée au début de cette section.

Dans [17], différentes approches pour propager les incertitudes dans un AdD ont été comparées. Contrairement à la logique floue, l'approche par intervalles améliore la précision et évite le problème de la perte d'information sur l'incertitude. La théorie des fonctions de croyance proposée par Dempster-Shafer consiste à transformer les limites des intervalles en une forme à trois valeurs, tandis que l'approche par intervalles fournit des calculs plus simples équivalents à la théorie de Dempster-Shafer. Comparée aux simulations de Monte Carlo, l'approche par intervalles est plus rapide et fournit des limites garanties pour les résultats.

La méthode répond au besoin d'allouer des objectifs de sécurité (THR répartis, équivalents aux TFFR) aux fonctions du VBTS, en particulier des objectifs imprécis aux fonctions mettant en œuvre le GNSS. Toutefois, elle est également applicable dans tout autre contexte nécessitant l'allocation d'objectifs de sécurité imprécis. Dans le cadre spécifique du VBTS, la méthode sera appliquée à la partie d'AdD du système englobant les événements de base qui intègrent les erreurs GNSS, en particulier celles liées aux perturbations environnementales (cf. Figure II.10). Cet AdD est issu de l'allocation de THR aux fonctions du VBTS selon les mêmes principes de découpage fonctionnel et dysfonctionnel issus de l'analyse de sécurité de l'ETCS niveau 2 [95] (cf. travaux des projets européens ERSAT-GGC [RPRE9] et NGTC). Également, les mêmes valeurs pour les événements de haut niveau considérés dans l'analyse de sécurité d'ETCS sont utilisées : l'événement "*ETCS Core Hazard*" et les sous-événements "*Corruption Hazard*" (données de balise corrompues), "*Deletion Hazard*" (balise non détectée) et "*Insertion Hazard*" (lecture d'une balise incorrecte, par exemple,

celle de la voie adjacente). Le troisième sous-événement est décomposé plus en profondeur avec les erreurs liées aux GNSS, sachant que la notion de risque sur l'intégrité de la localisation observée dans cet AdD sera développée dans la section II.3 liée aux risques techniques des CCS avancés.

Dans la méthode d'allocation proposée, la propagation "*Top-Down*" de l'incertitude est réalisée en déterminant une enveloppe d'intervalle optimale pour les événements intermédiaires et les événements de base. Pour cela, une technique d'optimisation et l'arithmétique des intervalles (AI) sont utilisées et décrites ci-dessous. L'adoption d'une enveloppe d'intervalle permet d'éviter de faire des hypothèses qui pourraient altérer les résultats.

L'enveloppe d'intervalle optimale est obtenue pour chaque THR alloué aux événements intermédiaires en fonction du type de porte *ET* et *OU* de l'arbre. Dans un premier temps, les opérations d'AI sont utilisées et sont synthétisées dans l'ensemble d'équations II.1 . Ces équations représentent les formules associées aux bornes des intervalles X et Y, notées $[\underline{X}, \overline{X}]$ et $[\underline{Y}, \overline{Y}]$.

$$\begin{aligned}
&[\underline{X}, \overline{X}] + [\underline{Y}, \overline{Y}] = [\underline{X} + \underline{Y}, \overline{X} + \overline{Y}],\\
&[\underline{X}, \overline{X}] - [\underline{Y}, \overline{Y}] = [\underline{X} - \overline{Y}, \overline{X} - \underline{Y}],\\
&[\underline{X}, \overline{X}] \times [\underline{Y}, \overline{Y}] = [\min(\underline{X} \times \underline{Y}, \underline{X} \times \overline{Y}, \overline{X} \times \underline{Y}, \overline{X} \times \overline{Y}), \max(\underline{X} \times \underline{Y}, \underline{X} \times \overline{Y}, \overline{X} \times \underline{Y}, \overline{X} \times \overline{Y})],\\
&[\underline{X}, \overline{X}] : [\underline{Y}, \overline{Y}] = [\min(\underline{X} : \underline{Y}, \underline{X} : \overline{Y}, \overline{X} : \underline{Y}, \overline{X} : \overline{Y}), \max(\underline{X} : \underline{Y}, \underline{X} : \overline{Y}, \overline{X} : \underline{Y}, \overline{X} : \overline{Y})].
\end{aligned} \tag{II.1}$$

Même si l'AI peut être utilisée dans la méthode pour garantir des bornes sur le THR des événements de base, elle peut conduire à des bornes larges conservatives, donc potentiellement non utilisables. Si un tel intervalle est obtenu, ses bornes peuvent être contractées sans exclure de valeur qui soit en accord avec l'ensemble de contraintes associées. Un contracteur est défini comme un opérateur réduisant le domaine initial de valeurs, fournissant ainsi un intervalle moins conservatif. Plusieurs contracteurs existent, chacun fonctionnant de manière différente et étant efficace uniquement pour des cas spécifiques [54]. Certains algorithmes sont spécifiquement conçus avec l'AI pour trouver des bornes de qualité pour la solution obtenue, en particulier l'algorithme de Krawczyk [76]. C'est une méthode itérative qui définit une séquence d'intervalles convergeant vers une solution optimale unique. Celle-ci est utilisée par la suite.

Pour une porte logique *OU* dans la méthode d'allocation standard, le THR équivalent de l'événement de sortie, noté THR_{eq}, est tel que $THR_{eq} = \sum_{i=1}^{n} THR_i$ compte tenu des n événements de base. Pour déterminer les intervalles des THR_i, il est nécessaire de résoudre un système d'équations linéaires à variables réelles, l'algorithme d'optimisation de Krawczyk est utilisé pour cela.

Pour une porte logique *ET*, il est nécessaire de résoudre un système d'équations non linéaires. Dans la méthode d'allocation standard, le THR maximal de la porte *ET* est défini comme suit [31] :

$$THR_{max} \approx \prod_{i=1}^{n} THR_i \cdot SDT_i \cdot \sum_{j=1}^{n} \frac{1}{SDT_j} \tag{II.2}$$

La constante SDT_i, pour *Safe Down Time*, représente le temps de latence entre deux tests consécutifs lié à la fonction i, nécessaire pour vérifier la disponibilité de la fonction. Il est égal à la moyenne de la période de test de la fonction (= temps de détection) additionnée d'un temps de mise en sécurité si la fonction est défaillante (= temps de passivation). La méthode de Krawczyk est également utilisée pour résoudre le système d'équations non linéaires et obtenir une enveloppe d'intervalle.

Après avoir obtenu les intervalles des THR des événements de base, il est possible d'effectuer une propagation d'intervalles avec une analyse "*Bottom-Up*". Ce processus permet de vérifier les intervalles obtenus à partir du processus d'allocation. Il permet également de vérifier si l'objectif de sécurité initialement défini pour l'événement sommet de l'arbre de défaillances est contenu dans l'intervalle propagé des feuilles de l'arbre à son sommet. Ce processus est considéré comme une analyse d'incertitudes et peut être réalisé à l'aide de l'analyse d'intervalles. Toutefois, pour éviter le problème de surestimation d'intervalle, l'algorithme de Skelboe-Moore permet de calculer les raffinements d'intervalles [75].

Pour appliquer la méthode à l'AdD de la figure II.10, l'outil *INTLAB* implémentant les algorithmes évoqués [89], est utilisé. Le processus d'allocation d'intervalle de THR commence au niveau de l'événement "*Local effect*" de la figure. La solution fournie pour les trois évènements intermédiaires reliés par une porte "OU" consiste en des valeurs de THR_i pour $i \in 1,2,3$ appartenant à l'intervalle $\begin{bmatrix} a_i & b_i \end{bmatrix} = \begin{bmatrix} 3.33 \times 10^{-9}, & 8 \times 10^{-7} \end{bmatrix}$. Cet intervalle est ensuite propagé au niveau des évènements de base reliés par des portes *ET*. Pour la porte "ET" ayant les deux événements "*NLOS*" et "NLOS-DIAG", sachant que THR_{max} se situe dans $[3.33 \times 10^{-9}, 8 \times 10^{-7}]$ et $SDT_i = 1$ pour $i \in 1,2$ (valeurs arbitraires), les valeurs obtenues de THR_{2i} pour $i \in 1,2$ appartiennent à l'intervalle $[4.08 \times 10^{-5}, 2 \times 10^{-4}]$, en supposant que les intervalles de THR_{12} et THR_{22} sont égaux.

Pour illustrer les résultats du processus de validation, les intervalles obtenus lors de l'étape d'allocation sont utilisés en l'absence de taux provenant de données réelles. Le THR de l'événement sommet est calculé et appartient à l'intervalle $[5.5 \times 10^{-6}, 7.2 \times 10^{-6}]$, ce qui inclut bien la valeur déterminée dans le processus d'allocation. Ainsi, l'allocation de THR est validée.

II.2.3 Allocation d'objectifs FDMS : des fonctions à l'architecture

L'approche développée a été proposée dans le cadre du post-doctorat de Thi Phuong Khanh Nguyen. Elle a fait l'objet d'un article de revue [ACL4] valorisé au sein du projet Smarties.

1) Objectif et type d'approche d'allocation développée

La transformation des exigences de haut niveau, en particulier les exigences FDMS issues du besoin utilisateur, en exigences de niveau inférieur pour un système repose de manière générale sur un processus de répartition et de raffinement d'exigences le long de son cycle de vie. Ce processus débute par l'analyse des fonctions du système et s'étend jusqu'aux éléments matériels et logiciels qui le constituent. Les sous-sections précédentes ont mis l'accent sur la répartition d'objectifs de sécurité au niveau des fonctions. Nos travaux présentés ci-dessous approfondissent l'allocation au

niveau des éléments de l'architecture d'un système. Pour cela, une méthodologie est proposée pour allouer un objectif quantitatif de disponibilité à un sous-système à partir d'exigences quantitatives de plus haut niveau.

Cette méthodologie est appliquée dans le contexte de l'ETCS intégrant un sous-système de localisation autonome basé sur les GNSS (quel que soit le type d'intégration du GNSS dans l'ETCS). L'objectif est de proposer un moyen d'allouer un objectif quantitatif de disponibilité à une LU autonome (*Localisation Unit*). Nous prenons en compte les objectifs globaux de disponibilité de l'ETCS définis par l'EUG (*ERTMS User's Group*) [28][12]. Ces objectifs sont définis indépendamment du niveau d'implémentation d'ETCS.

Bien que cette partie ne se concentre pas spécifiquement sur les objectifs de sécurité, contrairement aux sous-sections précédentes, la méthodologie demeure applicable à tout type d'objectif quantitatif à répartir au niveau d'éléments constitutifs d'une architecture.

Pour déterminer un objectif en termes de FDMS, en particulier un objectif de disponibilité, pour un sous-système constitutif d'un système global, deux d'approches générales peuvent être adoptées : une approche "descendante" (*Top-Down*) ou une approche "ascendante" (*Bottom-Up)*. Cependant, la mise en place de ces approches est délicate pour un système complexe tel qu'un CCS. Dans le cas de l'approche descendante, il devient difficile de décomposer un objectif de disponibilité défini pour le système global en sous-objectifs pour les sous-systèmes. En effet, les interactions entre les entités et leur environnement peuvent avoir un impact plus important que prévu sur la disponibilité du système. Dans ce cas, l'approche ascendante, fondée sur l'utilisation des paramètres des composants prévus pour le système, sera alors préférée (cf. paragraphe suivant). De plus, pour un système étendu avec plusieurs niveaux hiérarchiques impliquant différentes équipes, il est ardu d'obtenir un objectif initial global avec une vue d'ensemble. Plutôt que d'adopter un point de vue global, plusieurs objectifs initiaux peuvent être définis en fonction de diverses perspectives d'analyse (ex., contexte particulier, hypothèse de bon fonctionnement d'un sous-système pour se concentrer sur un autre, etc.)

Dans le cas de l'approche ascendante, associée aux analyses quantitatives prévisionnelles de FDMS (cf. §II.1.1.2), les évaluations de propriétés liées à un système dépendent de paramètres associés aux éléments constitutifs de ce système, tels que les taux de défaillance et de réparation de composants, ainsi que de la structure et du comportement des éléments du système. Ce type d'approche a été appliqué dans plusieurs travaux autour de l'ETCS niveau 2 [37, 100, 82]. Néanmoins, estimer précisément les valeurs des paramètres FDMS des éléments de base d'un système, en particulier lors de l'utilisation de nouvelles technologies, est difficile en raison du manque de données. Par conséquent, il est préférable de prendre en compte les incertitudes associées à ces paramètres pour refléter l'état réel des connaissances sur ces données. La théorie des ensembles flous offre des concepts efficaces pour les analyses dépendantes de données incertaines, contrairement aux simulations de Monte Carlo plus communément utilisées, qui peuvent être chronophages, notamment lorsqu'elles impliquent des boucles de simulation supplémentaires pour prendre en compte les incertitudes paramétriques [83, 58, 107].

12. L'EUG, association regroupant plusieurs entités ferroviaires investissant significativement dans l'ERTMS, possède un groupe de travail sur la localisation. Ce groupe s'appuie sur les documents très récents de l'initiative OCORA (*Open CCS On-board Reference Architecture*) pour laquelle différents opérateurs cherchent à définir une base commune d'architecture pour la prochaine génération d'équipements embarqués d'ETCS. Aucune mise à jour des objectifs de disponibilité d'ETCS définis en 1998 dans [28] n'a pour le moment été proposée dans [79].

Compte tenu des avantages et inconvénients des approches évoquées, la méthodologie d'allocation proposée adopte une **approche hybride** en combinant les approches *Top-Down* et *Bottom-Up*. De plus, par rapport aux approches d'analyse prévisionnelle classiques, elle est capable de **gérer les incertitudes paramétriques** pour allouer un objectif imprécis au sous-système spécifique intervenant dans le système global, tel que le sous-système de localisation autonome par satellites, en fonction d'un objectif au niveau système. Étant donné que l'objectif alloué est imprécis, une **courbe de satisfaction** est estimée pour représenter le taux de satisfaction associé à chaque valeur d'imprécision par rapport à l'objectif initial.

2) Étapes de la méthodologie

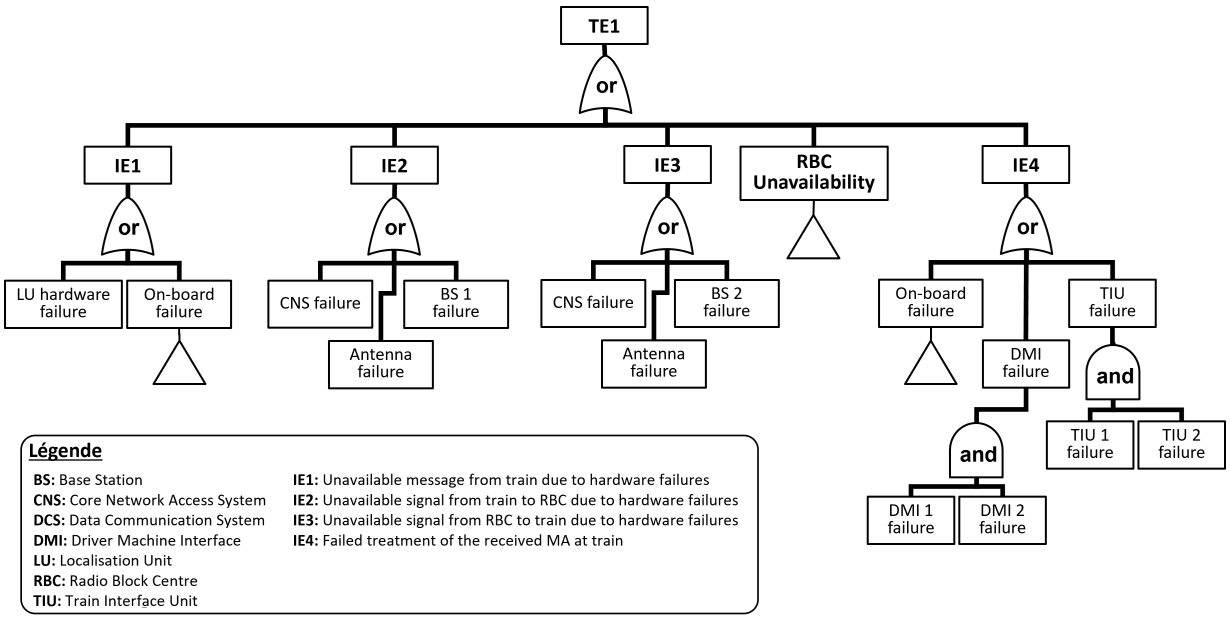
La méthodologie se rapporte, de manière générale, à l'identification d'un objectif de disponibilité pour un sous-système en tenant compte d'un objectif global. Toutefois, dans le contexte de ce mémoire et dans le but de faciliter la compréhension de la méthodologie, le système global se référera à un '*ETCS avancé intégrant les nouvelles technologies de localisation et de communication*' et le sous-système se référera à la '*LU autonome*'. Les trois étapes de la méthodologie sont présentées ci-dessous et seront détaillées par la suite.

- **Étape 1 – Allocation d'un (ou plusieurs) objectif(s) d'indisponibilité initial(aux) à l'ETCS :** L'(les) objectif(s) de disponibilité de l'ETCS, dérivé(s) de besoins utilisateurs, est(sont) converti(s) en seuil supérieur d'indisponibilité à répartir sur les différents sous-systèmes de l'ETCS qui sont sources de défaillances.
- **Étape 2 – Analyse des causes conduisant à l'indisponibilité de l'ETCS :** En se basant sur l'architecture du système global, les combinaisons de défaillances des sous-systèmes qui conduisent à l'indisponibilité du système sont analysées. Des valeurs imprécises caractérisant l'incertitude des paramètres intervenant dans le calcul de l'indisponibilité de chaque sous-système, à l'exception de la LU qui fait l'objet de l'allocation, sont déterminées.
- **Étape 3 – Détermination d'une courbe de satisfaction associée à(aux) l'objectif(s) de l'ETCS :** L'indisponibilité cible de la LU, nécessaire pour atteindre l'(les) objectif(s) initial(aux) de l'ETCS, est évaluée sous la forme d'une indisponibilité imprécise à travers une courbe de satisfaction. Cette courbe représente le taux de satisfaction à(aux) l'objectif(s) initial(aux) considéré(s) pour le système global par rapport à chaque valeur d'imprécision de l'indisponibilité du sous-système analysé (cf. sous-section suivante).

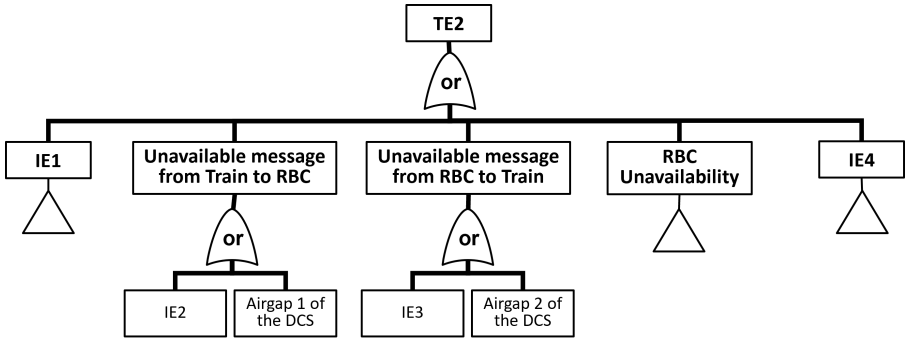
L'**étape 1** se réfère à différents objectifs de disponibilité de l'ETCS définis selon plusieurs angles de vue dans [28]. Dans le cadre de ces travaux, notre attention se porte sur les deux exigences suivantes, auxquelles la LU autonome peut contribuer :

R1 - *La contribution quantifiable de l'ERTMS/ETCS à la disponibilité opérationnelle, due aux défaillances matérielles, ne doit pas être inférieure à 0.999854*. Cela signifie que l'indisponibilité de l'ETCS due aux défaillances matérielles doit être inférieure à U_{R1} où $U_{R1} = 1.46 \cdot 10^{-4}$.

R2 - *La contribution quantifiable de l'ERTMS/ETCS à la disponibilité opérationnelle, due aux défaillances matérielles et aux erreurs de transmission, ne doit pas être inférieure à 0.99984*. Cela signifie que l'indisponibilité de l'ETCS due aux défaillances matérielles et aux erreurs de transmission doit être inférieure à U_{R2}, où $U_{R2} = 1.6 \cdot 10^{-4}$.



(a) Causes de l'évènement TE1 : indisponibilité de l'ETCS due aux défaillances matérielles



(b) Cause de l'évènement TE2 : indisponibilité de l'ETCS due aux défaillances matérielles et aux erreurs de transmission

FIGURE II.11 – Causes des évènements TE1 et TE2

Les objectifs d'indisponibilité associés à R1 et R2 sont respectivement liés aux événements sommets (*Top Event*) TE1 et TE2 des arbres de défaillances obtenus dans l'**étape 2** et présentés dans les figures II.11a et II.11b. Les causes apparaissant dans ces AdD sont décrites en détails dans [ACL4]. La détermination de la courbe de satisfaction de l'**étape 3** est décrite dans la sous-section qui suit.

3) Détermination de la courbe de satisfaction

La courbe de satisfaction est utilisée pour représenter le 'taux de satisfaction lié aux objectifs R1 et R2' en fonction des 'valeurs d'imprécision de l'indisponibilité de la LU'. Elle permet de déterminer l'indisponibilité imprécise de la LU, ainsi que le seuil maximum d'indisponibilité que la LU peut atteindre afin de satisfaire les objectifs de disponibilité de l'ETCS (par le biais des objectifs d'indisponibilité U_{R1} et U_{R2}). La démarche pour obtenir cette courbe sera expliquée en trois tâches dans cette sous-section, et la manière d'exploiter cette courbe sera détaillée.

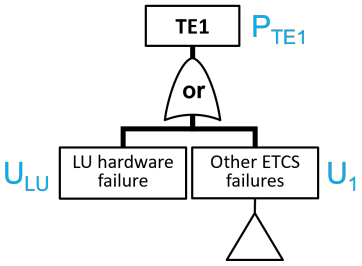


FIGURE II.12 – Forme réduite de l'arbre de défaillances lié à l'événement TE1

La **première tâche** consiste à déterminer l'indisponibilité imprécise de la LU par rapport à l'objectif R1. Pour ce faire, des arbres de défaillance utilisant des paramètres flous sont employés. Les bases théoriques pour l'évaluation de l'événement sommet d'un tel arbre sont détaillées en Annexe 3.

Pour réaliser cette tâche, l'indisponibilité imprécise associée aux défaillances des sous-systèmes de l'ETCS hors LU est évaluée en utilisant une forme réduite de l'arbre de défaillances de la figure II.11a. Cette forme isole la défaillance de la LU du reste des autres défaillances de l'ETCS (cf. figure II.12). Ainsi, l'évènement sommet TE1 est vu comme la combinaison de deux sous-évènements par le biais d'une porte OU : l'évènement de base "*LU hardware failure*", représentant la défaillance du sous-système qui nous intéresse (avec une probabilité d'indisponibilité floue notée U_{LU}) et l'événement intermédiaire "*Other ETCS failures*", combinant les coupes minimales liées aux défaillances des autres sous-systèmes de l'ETCS (avec une probabilité d'indisponibilité floue notée U_1).

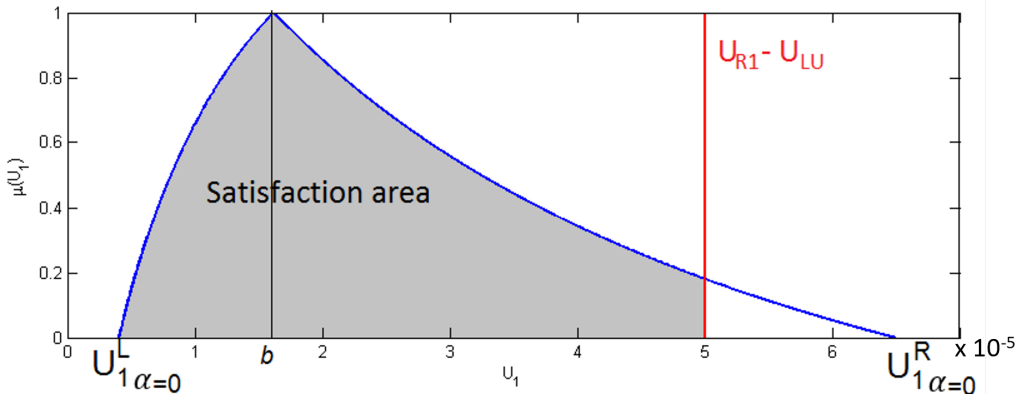


FIGURE II.13 – Fonction d'appartenance de U1 et zone d'exigence satisfaite

La fonction d'appartenance de U_1, c'est-à-dire $\mu_{\tilde{U_1}}(U_1)$, est évaluée à partir de l'application de la *Procedure Eval* décrite en Annexe 3 sur le sous-arbre de défaillances lié à U_1. Cet arbre prend en entrées les paramètres flous liés aux sous-systèmes d'ETCS hors LU. La représentation graphique de $\mu_{\tilde{U_1}}(U_1)$ est illustrée par la courbe bleue dans la figure II.13. Afin de satisfaire l'exigence R1 ($P_{TE1} \leq U_{R1}$), la limite supérieure de $\tilde{U_1}$ doit avoir comme limite supérieure $U_{R1} - U_{LU}$. Cette limite est caractérisée par la ligne verticale rouge dans la figure II.13 lorsque U_{R1} et U_{LU} sont des nombres précis.

Pour la **deuxième tâche**, nous définissons le taux de satisfaction à R1, noté SP (*Satisfaction Percentage)*, correspondant à l'une des valeurs de $\tilde{U}_1$. Ce taux correspond au rapport entre l'aire de la zone grise, notée S_{GA} (cf. figure II.13), et l'aire de la surface sous la fonction d'appartenance $\mu_{\tilde{U}_1}(U_1)$, notée $S_{\mu(U_1)}$. Si la ligne rouge est au delà de la courbe bleue (à droite), soit $U^R_{1_{\alpha=0}} \leq (U_{R1} - U_{LU})$, cela signifie que l'exigence R1 est satisfaite pour toutes les valeurs d'imprécision de U_1. Dans le cas contraire, le pourcentage de satisfaction SP est donné par :

$$SP = \frac{S_{GA}}{S_{\mu(U_1)}} \tag{II.3}$$

Afin de déterminer les valeurs d'indisponibilité floue de la LU (U_{LU}) conformément à l'exigence de l'ETCS (R1), la **troisième tâche** consiste à évaluer les valeurs de SP en fonction des valeurs de U_{LU} comme suit :

- Si $U_{LU} \leq U_{R1} - U^R_{1_{\alpha=0}}$, $SP = 100\%$
- Si $U_{LU} > U_{R1} - U^L_{1_{\alpha=0}}$, $SP = 0\%$
- Si $U_{R1} - U^R_{1_{\alpha=0}} < U_{LU} \leq U_{R1} - U^L_{1_{\alpha=0}}$, SP est évalué par la Procédure *SP* (cf. ci-dessous). Cette procédure comprend deux phases. Tout d'abord, un ensemble de valeurs SP sont évaluées pour toutes les valeurs de U_1 appartenant à $[U^L_{1_{\alpha=0}}, U^R_{1_{\alpha=0}}]$. Ensuite, dans la phase 2, la valeur de SP retenue pour une valeur de U_{LU}, est celle telle que à $U_1 = U_{R1} - U_{LU}$.

Procédure *SP* : Identification de la courbe de satisfaction à un objectif

procedure 1) EVALUATE SP SET
  Let d be the length of the vector B including obtained values of U_1 ; we have : $B = \{U^L_{1_{\alpha=0}}, U^L_{1_{\alpha=i\cdot\Delta}}, U^R_{1_{\alpha=i\cdot\Delta}}, U^R_{1_{\alpha=0}}\}$, where $(i = 1, 2, ..., n-1)$.
  for $i = 2 : 1 : d$ **do**
    Calculate $S_{\mu(U_1)}$, that is a vector having d elements, by the numerical integral following the trapezoidal rule : $S_{\mu(U_1)}(i) = S_{\mu(U_1)}(i-1) + 0.5 * [B(i) - B(i-1)] * (\alpha_{B(i)} + \alpha_{B(i-1)})$
  end for
  Evaluate vector SP : $SP = \frac{S_{\mu(U_1)}}{S_{\mu(U_1)}(d)}$
end procedure

procedure 2) IDENTIFYING $SP_{U_{LU}}$
  Set i=1
  while $(d \neq i+1)$ **do**
    h=round$((i+d)/2)$
    if $U_{R1} - U_{LU} < B(h)$ **then**
      d=h
    end if
    if $U_{R1} - U_{LU} > B(h)$ **then**
      i=h
    end if
    if $U_{R1} - U_{LU} = B(h)$ **then**
      i=h ; d=h ; Break
    end if
  end while
  $SP_{U_{LU}} = \frac{SP(i) + SP(d)}{2}$
end procedure

Suite à l'évaluation des valeurs de SP en fonction des valeurs de $\tilde{U}_{LU}$, il est possible de tracer une courbe de satisfaction liée à l'exigence R1. De manière similaire, nous pouvons obtenir la courbe correspondant à l'exigence R2. Au final, la courbe de satisfaction liée aux exigences R1 et R2 est déterminée en considérant les valeurs minimales issues des deux courbes précédentes. Un cas d'étude décrit ci-dessous permet d'illustrer l'approche.

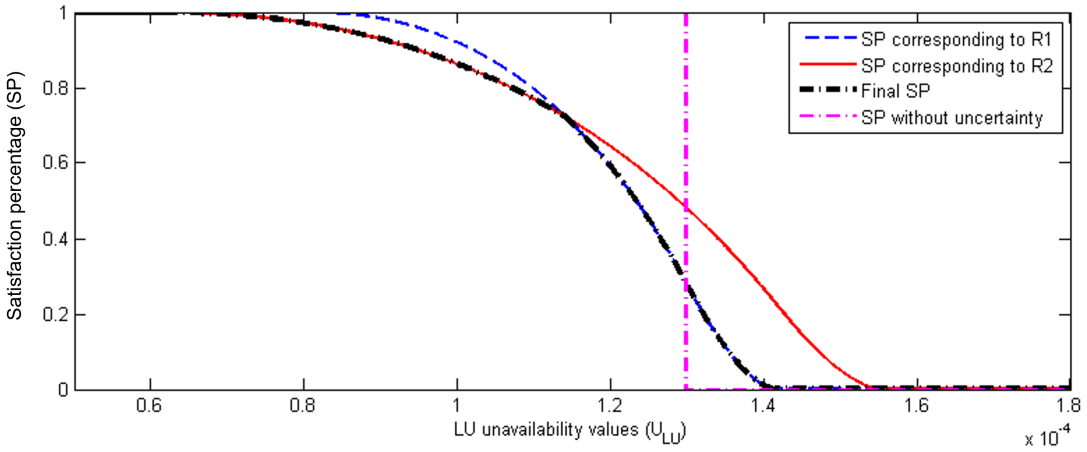


FIGURE II.14 – Courbes de satisfaction liée à l'indisponibilité imprécise de la LU

4) Illustration sur un cas d'étude

Le choix des taux de défaillance et de réparation imprécis, liés aux paramètres d'entrées des arbres de défaillances illustrés dans les figures II.11a et II.11b, est décrit dans notre article [ACL4]. La courbe de satisfaction liée à l'exigence R1 est déterminée grâce à la Procédure *SP* décrite précédemment et est illustrée par la ligne en pointillés bleus à la figure II.14. De manière similaire, la courbe de satisfaction liée à l'exigence R2 est illustrée par la ligne rouge à la figure II.14. La courbe de satisfaction finale liée aux exigences R1 et R2 est illustrée par la courbe en pointillés noirs.

Nous observons que lorsque l'indisponibilité de la LU est inférieure à $6.17 \cdot 10^{-5}$, le SP est de 100 %, tandis que les exigences de l'ETCS ne peuvent pas être satisfaites lorsque l'indisponibilité de la LU dépasse $1.42 \cdot 10^{-4}$. D'autre part, sans tenir compte de l'incertitude paramétrique, le seuil supérieur d'indisponibilité de la LU est de $1.3 \cdot 10^{-4}$. Cela signifie que les exigences de l'ETCS sont également satisfaites lorsque l'indisponibilité de la LU autonome est de $1.3 \cdot 10^{-4}$. Cependant, en tenant compte de l'incertitude paramétrique, la SP correspondante à cette valeur n'est que de 28.53 %. Il y a donc un risque élevé que l'ETCS ne réponde pas aux exigences de disponibilité.

En revanche, si les paramètres d'entrée les plus pessimistes sont considérés, les résultats de l'approche précise traditionnelle pourraient entraîner des dépenses inutiles pour le développement de la LU, et cela pourrait être difficile à réaliser en pratique.

II.2.4 Conclusion

Dans cette section II.2, les efforts engagés pour structurer de manière générique et harmonisée les étapes d'un processus d'allocation de SIL aux fonctions de sécurité d'un système critique ferroviaire ont abouti à l'élaboration d'un cadre méthodologique formalisé. Ce cadre, conçu pour guider divers acteurs du secteur ferroviaire tels que les exploitants, constructeurs, évaluateurs de sécurité, vise à remédier aux incompréhensions et aux mésusages associés au concept de SIL, comme discutés avec certains de ces acteurs.

L'introduction, dans ce processus, d'imprécisions sur les objectifs de sécurité liés aux dangers et aux fonctions, nous permet de prendre en compte le cas des systèmes pour lesquels la quantification des objectifs alloués est délicate en raison de conditions de fonctionnement accompagnées d'incerti-

tudes. C'est notamment le cas pour les systèmes de localisation par satellites dont les signaux utilisés sont sujets à des perturbations aléatoires. Pour considérer ces imprécisions, nous avons développé une méthode d'allocation fonctionnelle, venant alors enrichir le processus d'allocation générique.

Enfin, pour approfondir l'allocation fonctionnelle à un niveau plus détaillé, une dernière approche manipulant également des objectifs imprécis a été proposée. Dans le cadre de ce mémoire, cette dernière approche permet d'allouer des objectifs quantitatifs aux éléments de l'architecture de l'ETCS et de ses constituants, dont l'unité de localisation. Ces approches contribuent ainsi à la macro-phase d'*appréciation des risques*.

Les deux sections suivantes visent à présenter nos contributions aux activités de sécurité de la macro-phase "*réalisation et démonstration de la conformité aux exigences de sécurité*" pour les CCS avancés intégrant des nouvelles technologies de localisation satellitaire et de communication. Comme abordé dans la section II.1 au début du mémoire de recherche, cette macro-phase a deux finalités : affiner, voire compléter, l'analyse des dangers avec les risques découlant des spécificités liés au système à concevoir, et maîtriser les situations dangereuses résultant du système conçu.

Au vu de ces finalités, la section II.3 expose nos recherches sur l'analyse des **nouveaux risques techniques** liés aux évolutions technologiques évoquées et prévues pour améliorer les performances d'un CCS. Ensuite, la section II.4 se consacre aux **nouveaux risques opérationnels** engendrés par l'utilisation de ces technologies dans les CCS pour la mise en œuvre de principes d'exploitation plus efficaces.

II.3 Analyse des risques techniques de CCS avancés

Les travaux présentés dans cette section ont pour objectif de contribuer à l'analyse quantitative des risques au niveau de systèmes techniques implémentant les nouvelles technologies évoquées dans les sections précédentes. Les évaluations prévisionnelles qui en découlent visent à statuer sur le fait que les systèmes techniques développés, ainsi que leurs mesures de sécurité associées, sont capables de répondre aux exigences de sécurité ou, dans le cas contraire, nécessitent des évolutions pour réduire davantage les risques.

L'approche proposée dans le cadre des travaux de post-doctorat de Thi Phuong Khanh Nguyen et celle proposée dans le cadre des travaux de thèse de Cyril Legrand sont toutes deux associées à des résultats applicatifs concernant les systèmes de localisation avec GNSS. Il est à noter que les recherches sur l'utilisation sécuritaire des systèmes de télécommunications que j'ai entreprises sont moins développées en raison de contraintes de ressources et de priorisation des travaux. Ces recherches ne seront pas détaillées mais discutées en conclusion de cette section.

La sous-section II.3.1 décrit le périmètre d'analyse et les questions de recherche issues de mes travaux de post-doctorat. Ces aspects, mettant en évidence un lien interdisciplinaire entre les trois communautés scientifiques de la sécurité des systèmes, des transports intelligents et des GNSS, ont orienté les travaux présentés dans cette section. Bien que les problématiques soulignées soient spécifiques au GNSS utilisé en milieu ferroviaire, nous montrons qu'elles sont généralisables, ouvrant la voie à l'adaptation des approches développées à d'autres systèmes.

En partant du constat établi qu'un dispositif de localisation embarqué ne peut reposer uniquement sur un récepteur GNSS en raison des défauts de ces systèmes (qui seront précisés par la suite), les travaux ont porté sur les systèmes multi-capteurs utilisant les signaux satellitaires et d'autres technologies de localisation. Au-delà de la considération de ce domaine applicatif, l'approche d'évaluation détaillée dans la sous-section II.3.2 vise à appréhender les situations de pannes multiples de faible probabilité d'occurrence.

Une autre orientation de recherche, issue des problématiques spécifiques identifiées dans la première sous-section, a consisté à se référer et s'appuyer sur des techniques existantes d'évaluation de critères de performance propres aux technologies GNSS analysées, sans passer par l'utilisation de modèles dont l'élaboration même est délicate (cet aspect sera abordé dans la section II.4). Une démarche visant à formaliser des liens entre des propriétés liées au critère de sécurité et des propriétés spécifiques liées à l'"intégrité de la localisation", sera décrite à la sous-section II.3.3.

II.3.1 Problématiques d'analyse de SdF liées aux systèmes embarqués avec GNSS

1) Fonctionnement des GNSS en milieu ferroviaire

Sans entrer dans les détails du fonctionnement des GNSS afin de mettre l'accent sur les éléments qui entreront en jeu dans les analyses de SdF (quelques détails seront toutefois donnés ponctuellement par la suite, lorsque cela est nécessaire pour la compréhension), notons que ces systèmes comportent trois catégories de défauts pouvant impacter le service de localisation fourni. Il est important de noter que ces défauts ne sont principalement pas imputables à des aspects fonctionnels

ou dysfonctionnels du matériel et / ou du logiciel classiquement considérés dans les analyses de SdF, mais plutôt à des phénomènes de propagation de signaux et à des algorithmes de traitement de données :

— Ceux potentiellement présents dans les informations transmises par les satellites ;
— Ceux concernant les informations reçues par l'équipement utilisateur en raison de dégradations subies par les signaux satellitaires avant leur réception ;
— Ceux liés au traitement des informations reçues.

Différentes mesures de sécurité préventives existent pour pallier ces défauts, en particulier pour les premiers qui peuvent être corrigés. Les axes d'amélioration de ces mesures portent principalement sur le contrôle des dégradations avant réception attribuables aux perturbations que les signaux satellitaires peuvent subir dans l'environnement de propagation ferroviaire. Sans considérer les interférences possibles (intentionnelles ou non), ces perturbations résultent de phénomènes de propagation locaux liés au milieu environnemental dans lequel évolue un train. En effet, ce milieu peut masquer ou perturber la réception des signaux satellitaires au niveau de l'antenne fixée sur le train, notamment lorsque le train traverse une zone entourée de bâtiments, de végétation, de montagnes ou lorsqu'il passe dans une tranchée ferroviaire.

En situation normale, un récepteur embarqué a besoin de recevoir les signaux d'au moins quatre satellites différents pour estimer une position aux coordonnées (x, y, z), ainsi que le décalage Δt entre les horloges très précises des satellites et celle, beaucoup moins précise, du récepteur. Dans les domaines aéronautique ou maritime, cette condition sur le nombre de signaux est toujours vérifiée puisque, en l'absence d'obstacle, un avion en vol ou un bateau en mer reçoit l'ensemble des signaux disponibles sur leur zone de couverture, et cette réception s'effectue en visibilité directe sans déviation. Ceci n'est plus le cas dans les domaines ferroviaire et du transport terrestre en général, où la visibilité satellitaire peut être réduite en raison du milieu, pouvant même manquer, notamment dans les tunnels.

Les phénomènes de propagations locaux (multi-trajets, signaux reçus en visibilité indirecte ou dite "*non-line of sight*", interférences) posent problème dans le cas des transports terrestres, car ils sont imprévisibles. Ces phénomènes ont un impact sur la fonction de localisation, celle-ci se référant à l'estimation périodique de la position qu'un récepteur embarqué effectue à partir des informations reçues des satellites. Même si une position estimée comporte toujours un écart par rapport à la position réelle du véhicule, en raison des imprécisions inhérentes aux algorithmes de calcul, cet écart peut devenir important avec la dégradation des informations reçues. Cela peut s'accentuer jusqu'à conduire à une position dont l'erreur n'est plus acceptable pour l'utilisateur, c'est-à-dire une défaillance.

Pour anticiper ou parer ces phénomènes locaux spécifiques aux environnements contraints, de nombreux travaux au sein de la communauté GNSS portent sur la caractérisation des erreurs locales, leur compensation par l'hybridation des récepteurs GNSS à d'autres capteurs, leur compensation par le recalage de position sur une carte numérique munie de différentes informations géographiques en deux ou trois dimensions (se référant aux SIG, *Systèmes d'Informations Géographique*), et leur détection par des algorithmes de surveillance signalant et / ou corrigeant l'erreur détectée [ACL7, 15].

À noter que des systèmes d'augmentations par le sol (ex. *differential GNSS*) ou par satellites (ex. EGNOS, *European Geostationary Navigation Overlay Service*) permettent de compenser uniquement les erreurs globales (ex. celles liées aux effets de l'atmosphère).

2) Périmètre des travaux et problématiques de SdF

La délimitation du périmètre d'analyse et les problématiques associées aux approches de SdF présentées dans les sous-sections II.3.2 et II.3.3, s'appuient sur les travaux effectués durant mon post-doctorat. Ces travaux visaient à établir les bases d'analyses de SdF de solutions GNSS prévues pour être utilisées dans des applications ferroviaires sécuritaires. Dans le cadre de ces travaux, nous avons réalisé une revue de l'état de l'art et maintenu une veille continue du contexte ferroviaire sur l'utilisation sécuritaire des GNSS, sujet progressivement formalisé par l'Agence Européenne des GNSS [13] dans une "*roadmap*" [14] où figurent des projets dans lesquels nous avons contribué et pu échanger avec les partenaires sur le contexte évolutif du domaine. L'ensemble de ces activités nous a permis de mettre en évidence les dispositifs techniques à considérer en priorité dans un équipement GNSS venant intégrer un sous-système de contrôle-commande embarqué, ainsi que les problématiques d'évaluation de SdF qui en découlent. Les paragraphes ci-dessous abordent ces deux aspects, en résumant au préalable les bases d'analyses évoquées.

Les travaux qui servent de base aux analyses de SdF ultérieures ont été menés en partie dans le cadre du projet Tr@in-MD piloté par la SNCF et en partie dans le cadre de la collaboration avec l'université de Pardubice.

Ces travaux préalables, bien qu'ils ne soient pas détaillés dans ce mémoire, seront cités durant la description des approches présentées. Notons qu'ils ont permis :

- D'identifier les trois catégories de défauts liés aux GNSS (évoquées ci-dessus) pouvant altérer les informations de localisation ;
- D'identifier les sources possibles de ces défauts ;
- D'identifier les divers moyens existants (évoqués ci-dessus), susceptibles de pallier ou compenser ces défauts, jouant ainsi le rôle de mesures de sécurité ;
- De mettre en place deux catégories d'approches capables de quantifier des performances FDMS du service rendu par le système de localisation : l'une est fondée sur des comportements prévisionnels, et l'autre est fondée sur les principes d'analyse de données de retour d'expérience [ACL11, ACLN3, ACTI26, ACTI27, ACTI28, ACTI30, ACTI29, ACTN7] ;
- D'identifier des liens entre les critères FDMS et les critères de performances propres aux systèmes de navigation par satellites [ACL12, ACLN4, ACTI28, ACTI31, COM4, COM6, COM5].

Périmètre des travaux :

L'utilisation de systèmes de localisation multi-capteurs, combinée à des techniques de surveillance de l'intégrité de la localisation (notion définie au §II.3.3.1), sera analysée en priorité dans les travaux

13. Ex-GSA (*European GNSS Agency*) devenue EUSPA (*European Union Agency for the Space Programme*) en mai 2021

14. Accès à la feuille de route élaborée par l'EUSPA montrant différents projets passés et en cours, ainsi que les principaux liens entre acteurs, pour aller vers l'utilisation des GNSS européens dans l'ERTMS : https://www.euspa.europa.eu/sites/default/files/roadmap_2021.pdf

qui suivent. Il est à noter qu'il s'agit d'une option d'intégration possible des GNSS dans les CCS ferroviaires, à savoir l'option d'intégration *globale*, comme décrit à la section II.2 au §II.2.2.1. Cette option, liée au couplage d'un récepteur GNSS à d'autres dispositifs indépendants des signaux GNSS, est celle qui suscite le plus de réflexions en raison de son caractère en rupture par rapport à l'existant, d'autant plus lorsqu'il s'agit d'entamer une démarche d'évaluation des risques techniques. En effet, les autres options basées sur l'emploi de "balises virtuelles" et d'"odométrie avancée", en tant qu'améliorations des équipements de l'ETCS, peuvent être associées à un approfondissement et à une adaptation des analyses de sécurité actuelles en lien avec l'ETCS [95, 96].

Les solutions multi-capteurs correspondent à des systèmes de localisation qualifiés d'"hybrides", car ils combinent plusieurs technologies, dont celle relative aux GNSS, au sein d'une même architecture de système, ainsi que des algorithmes de fusion de données. Ainsi, comme argumenté ci-dessous, cette stratégie d'hybridation permet aux faiblesses des dispositifs de localisation utilisés d'être indépendantes et de se contrebalancer entre-elles. En particulier, les principales faiblesses des GNSS, provenant de leur utilisation en environnement contraint et leur incapacité à fournir une position dans les zones sans visibilité satellitaire telles que les tunnels, nécessitent d'être compensées. Les dispositifs supplémentaires comblent alors les discontinuités de service.

De nombreuses combinaisons entre un récepteur GNSS et d'autres types de capteurs indépendants des signaux GNSS sont possibles, avec différents types de redondance matérielle ou d'hybridation de données (ex., couplage de données lâche ou serré, prenant en compte ou pas les données d'une carte géographique) [39]. Ces combinaisons vont des plus couramment utilisées, impliquant par exemple un odomètre ou un système de navigation inertielle (INS, *Inertial Navigation System*), aux plus expérimentales, impliquant par exemple des capteurs à courants de Foucault (ECS, *Eddy Current Sensors*). Chaque solution comporte ses avantages et ses limitations en termes de fonctionnalités, de performances, de maintenance, de coûts et de consommation d'énergie. Même si la description de ces systèmes dépasse le cadre de ce mémoire, il convient de noter que, par rapport aux solutions les plus courantes, les INS sont souvent privilégiés en raison de leur polyvalence et de leurs caractéristiques (suivi tridimensionnel du mouvement, fourniture d'informations sur la direction et l'orientation du véhicule, miniaturisation à moindre coût). Cependant, les INS nécessitent un étalonnage et leurs mesures peuvent être affectées par différents biais et bruits. D'un autre côté, les odomètres sont des solutions sur essieux peu coûteuses mais susceptibles de présenter des erreurs en raison de phénomènes de glissement et de patinage. Au vu de ces considérations et en tenant compte des solutions privilégiées dans les projets auxquels nous avons participé, les études de cas liées aux travaux présentés ci-après impliqueront des INS ou ECS, en tant que dispositifs redondants et indépendants des signaux GNSS.

Problématiques de recherche en SdF :

Les problématiques identifiées se rapportent aux aspects suivants :

— *La prise en compte de la forte variabilité des situations rencontrées*. En effet, les défauts causés par l'environnement ne sont pas les mêmes d'un endroit à un autre et d'un moment de la journée à un autre. Plus précisément, étant donné que les satellites d'un GNSS forment une constellation en mouvement, la visibilité des signaux satellitaires à un point fixe sur le globe terrestre change constamment. De plus, les trains étant mobiles, le point de réception n'est

pas fixe. Ces éléments soulignent les aspects dynamiques d'un système embarqué utilisant les GNSS. De manière générale, cela implique **l'analyse de l'évolution des états du système dans le temps**, ce qui complique l'évaluation des critères FDMS du système. La dynamique d'un système, l'une des facettes de la complexité des systèmes, constitue un enjeu majeur pour les analyses de sûreté de fonctionnement.

— *Le fait qu'une défaillance de la fonction de localisation ne soit pas visible*, la défaillance correspondant à une erreur de position supérieure à une limite maximale tolérée par l'utilisateur. En effet, lorsque le système de localisation fournit une position sans autre indication, il est impossible pour un utilisateur de déterminer si celle-ci est correcte ou hors limites. Cela soulève la question générale de la **caractérisation des événements et états liés à une fonction ou un système, étant donné que ces états ne sont pas directement observables lors du fonctionnement d'un système**. Cette question de la caractérisation conduit ensuite à celle de **l'évaluation de l'occurrence de ces états ou événements**, en particulier ceux à caractère dangereux qui touchent la sécurité du système. Pour la fonction de localisation, ces états correspondent respectivement à 'position correcte' et 'position défaillante', états pour lesquels un service est délivré et utilisé, bien que potentiellement dangereux en fonction de l'erreur. Un troisième état, 'service interrompu', existe nécessairement et se rapporte à une indisponibilité de la fonction. Cette indisponibilité correspond à une absence de sortie de la fonction qui peut être causée par des pannes matérielles ou l'insuffisance du nombre de signaux GNSS reçus au niveau du récepteur. Comme cette absence de sortie est observable, elle peut être maîtrisée par l'utilisateur ou tout système connexe capable d'agir en conséquence.

Les techniques de surveillance de l'intégrité de la localisation, mentionnées précédemment et dont les principes généraux seront détaillés au §II.3.3.1, contribuent à répondre à la seconde problématique. Ces techniques sont dédiées au contrôle et à la détection de conditions contraires à la sécurité. Bien qu'elles soient prévues avec un niveau de performances attendues, elles présentent également un risque de fonctionnement incorrect voire dangereux, qu'il convient de prendre en compte. En envisageant l'ajout d'une fonction supplémentaire de surveillance de la localisation, la seconde problématique se rapporte alors à *la caractérisation et l'évaluation des états dangereux de la fonction de localisation compte tenu de la présence d'un mécanisme de détection dans le système de localisation avec GNSS*. Cette question peut être traitée, de manière empirique, par l'évaluation de paramètres liés au système. En effet, cette évaluation peut bénéficier des pratiques d'analyse employées pour les systèmes de navigation. Les paramètres évalués, issus de ces pratiques, sont intéressants à considérer car ils ne reposent pas sur l'emploi de modèles à base d'événements, d'états ou de comportements, compliqués à obtenir dans un contexte où la variabilité opérationnelle et la dynamique des systèmes sont importantes. Néanmoins, ils mènent à des critères de performances propres aux systèmes de navigation, différents des critères FDMS. De ce fait, *comprendre ces critères spécifiques aux GNSS, identifier les liens possibles avec les critères FDMS, et formaliser ces liens* constitue une problématique attachée à la problématique d'évaluation précédente.

Ainsi, l'approche d'évaluation proposée dans la sous-section II.3.2 contribue à répondre à la première problématique et aborde la seconde en utilisant des paramètres hypothétiques pour caractériser les événements de défaillance. La démarche présentée dans la sous-section II.3.3 s'attache uniquement à la seconde problématique et permet de formaliser des liens entre classes de critères. À noter que même si cette dernière contribution n'inclut pas la formalisation de comportements complexes, elle permet de formaliser explicitement les paramètres influents liés à l'intégrité de la localisation, une notion souvent délicate à appréhender dans le domaine ferroviaire. Ces éléments seront particulièrement utiles dans la section II.4 qui se concentre sur les risques opérationnels liés à l'exploitation des trains en plus des risques techniques.

II.3.2 Méthode d'évaluation par arbre de défaillances étendu

L'approche d'évaluation a été proposée dans le cadre du post-doctorat de Thi Phuong Khanh Nguyen. Elle a été appliquée au système embarqué satellitaire multi-capteurs d'architecture redondante du projet GaLoROI, projet piloté par la *spin-off* iQST de la TU Braunschweig (cf. §I.6.1). Elle a fait l'objet d'un article de revue [ACL10], ainsi que de deux articles de conférence [ACTI21, ACTI25].

1) Objectif et type d'approche d'évaluation développée

Pour développer une approche d'évaluation FDMS pour un système embarqué satellitaire multi-capteurs, nos travaux se sont appuyés sur une démarche de modélisation à base d'arbre de défaillances étendu, celui-ci prenant en compte l'évolution dans le temps des différents états de fonctionnement et de panne des composants d'un système.

L'arbre de défaillances (AdD) est une méthode largement employée pour l'analyse qualitative et quantitative de SdF d'un système. En effet, elle permet une représentation claire et structurée de liens causaux entre un événement sommet (défaillance du système) et des événements qui y mènent (défaillances des composants) à partir de l'utilisation de portes logiques ET et OU principalement. De ce fait, elle offre un cadre adapté pour les analyses déductives menant à l'identification des combinaisons critiques de défaillances. Cette méthode, par l'utilisation de la formule de Poincaré, mène également à des évaluations quantitatives probabilistes du système à partir de la connaissance des probabilités des évènements de base [64].

L'analyse avec AdD repose sur les hypothèses que tous les composants doivent être dans un état booléen (fonctionnement ou panne) et que les événements de défaillance des composants surviennent indépendamment les uns des autres. Ces hypothèses permettent d'évaluer les probabilités de défiabilité et d'indisponibilité de systèmes à l'aide de l'approche combinatoire des défaillances. Cependant, cela ne suffit pas à rendre compte des comportements réels des systèmes complexes puisque les hypothèses ne sont pas adaptées aux systèmes dynamiques. De ce fait, des extensions d'AdD ont été investiguées. Puis, une méthode fondée sur la définition de l'"AdD étendu" qui combine les avantages de différentes extensions d'AdD a été proposée afin de structurer les défaillances liées à un enchaînement d'événements (ex., durée ou ordre d'événements menant à la défaillance du système). Enfin, un processus permettant d'évaluer l'AdD étendu a été développé.

Ce processus est fondé sur les réseaux de Petri (RdP) et s'appuie sur les états de panne mis en évidence par l'AdD étendu. Les RdP se rapportent à un formalisme graphique et mathématique de modélisation des systèmes à événements discrets pouvant intégrer des aspects temporels et probabilistes. En particulier, les DSPN (*Deterministic Stochastic Petri Net*) permettent de prendre en compte les interactions entre événements de nature stochastique et déterministe en considérant aussi des dépendances temporelles. Les DSPN sont donc appropriés pour considérer les aspects dynamiques liés à l'enchaînement d'événements, ces derniers caractérisant les différents états d'un système. Toutefois, leur construction est délicate à gérer et leur simulation, selon les principes de la simulation de Monte Carlo, devient peu performante lorsqu'elle doit générer des évènements liés à la sécurité, de fréquence faible.

Pour une durée de traitement efficace, le processus d'évaluation associe alors aux RdP une nouvelle approche analytique pour les événements critiques qui dépendent du temps. Les performances du nouveau processus proposé ont, au final, été démontrées à l'aide d'un exemple théorique d'AdD étendu et l'utilisation pratique de la méthode a été illustrée sur un système ferroviaire utilisant les signaux satellitaires. Quelques éléments d'état de l'art sur l'évaluation des extensions d'AdD sont donnés ci-dessous et l'approche proposée est ensuite décrite.

2) Approches existantes pour l'évaluation d'extensions d'AdD

En définissant des portes supplémentaires, une extension d'AdD, appelée "AdD dynamique" (DFT, *Dynamic Fault Tree*) a été proposée pour la première fois dans [27] pour tenir compte de séquences ordonnées de défaillances (porte PAND), de redondances passives de composants (porte Spare) et de dépendances fonctionnelles (porte FDEP). Cette méthode a ensuite été développée dans de nombreuses études [10, 40, 71, 72, 84] qui, néanmoins, ne tiennent pas compte de composants ayant des états multiples dus à des processus de dégradation, ainsi que des conditions temporelles entre causes qui conduisent à un événement redouté.

[13, 55, 53] ont présenté une autre extension d'AdD, appelé "AdD à états multiples" (mFT, *multi-state Fault Tree*). Le mFT permet de considérer des composants dégradés dont les états sont dépendants et permet également de prendre en compte les événements de réparation. D'autre part, les extensions d'AdD avec des aspects temporels (conditions temporelles menant à un événement redouté, délai entre la cause et l'effet) sont utiles pour l'analyse des systèmes techniques dynamiques. [81] a exprimé des relations temporelles quantitatives entre les causes et les effets en définissant de nombreuses portes temporelles supplémentaires. Cette extension se nomme "AdD temporel" (TFT, *Temporal Fault Tree*). [56] a également pris en compte la relation temporelle entre les causes et les effets avec "l'AdD état-événement" (SEFT, *State-Event Fault tree*). Pour cet AdD, les entrées des portes sont à la fois des événements instantanés et des états qui durent dans le temps. [68] a présenté un "AdD à dépendances temporelles" (TdFT, *Time dependencies Fault Tree*) et s'est concentré sur l'analyse temporelle des événements dangereux. Dans ce dernier article, les événements ne sont pas considérés comme instantanés mais sont exprimés par leur durée. Les auteurs définissent ensuite les portes causales caractérisées par les délais entre les causes et les conséquences.

TABLE II.3 – Approches existantes pour l'évaluation d'AdD étendus

	Multistate compo-nents	Repairable compo-nents	Temporal depen-dencies	Failure sequence depen-dency	Various kinds of failure probability distribution	Type of fault Tree
Analytic approach (exact evaluation)						
Combinatorial method (discrete structure function between input and output gate)	✓	⚠	✗	✗	✓	mFT
Continuous Time Markov Chain	⚠	⚠	✗	✓	✗	DFT
Input/output Interactive Markov chain	⚠	✓	✗	✓	✗	DFT
Algebraic approach (for obtaining minimal cut sets)	⚠	⚠	✗	✓	✓	DFT
Combinatorial method by converting TFT into FT	✓	⚠	✓	✓	✓	TFT
Approximate analytic approach						
	⚠	✓	✗	✓	✗	DFT
Simulation approach (statistical evaluation)						
State chart	⚠	⚠	✓	✓	✓	TdFT
Monte Carlo Simulation and Petri Net	✓	✓	✓	✓	✓	eFT*

⚠ = Not appropriate * mFT, DFT, TFT, SEFT, TdFT

Afin d'identifier une approche d'évaluation la plus adaptée à la prise en compte : *i)* de composants multi-états réparables, *ii)* de séquences d'évènements dépendants, et *iii)* de conditions de durée sur les causes qui mènent à un événement critique, une investigation des approches possibles a été menée. Elle est résumée au tableau II.3.

3) Principes de l'approche proposée

Suite à l'analyse de travaux antérieurs évoqués précédemment, il en ressort que l'approche d'évaluation la plus appropriée pour un "AdD étendu" tirant avantage des mFT, DFT, TFT SEFT et TdFT, repose sur la simulation des parties dynamiques de l'AdD étendu, c'est-à-dire des sous-arbres ayant des caractéristiques dynamiques. Cette simulation s'effectue à la fois par réseaux de Petri, pour modéliser les aspects dynamiques, et par simulation de Monte Carlo (SMC) pour l'échantillonnage des lois de probabilité et les évaluations statistiques. La solution est intégrée dans l'évaluation globale de l'arbre. L'approche adopte ainsi un caractère modulaire.

Avant d'arriver à l'étape de simulation pour évaluer l'AdD étendu, les trois étapes suivantes sont considérées. Elles permettent de convertir l'AdD étendu du système considéré en RdP :

— **Étape 1** : Cette étape concerne les évènements de base de l'AdD étendu. Elle porte sur la modélisation en DSPN de l'évolution dans le temps des états des composants reliés aux feuilles de l'arbre.
— **Étape 2** : Cette étape concerne les portes de l'arbre. Elle sert à transformer les portes temporelles et dynamiques de l'arbre en DSPN [56, ACTI25].
— **Étape 3** : Cette étape combine des RdP issus des étapes précédentes. Elle permet d'évaluer la probabilité de l'événement sommet de l'arbre en simulant le RdP "combiné" selon les principes de la SMC.

Cependant, le temps de simulation du RdP combiné s'est avéré problématique comme les états des parties du système que le RdP modélise sont examinés à chaque pas d'échantillonnage de T_0 secondes, durée très petite devant le temps de mission du système. Cela peut mener à un grand nombre de séquences d'événements ne menant à aucun événements dangereux susceptible d'engendrer la défaillance du système. Ces séquences sont donc inutiles pour l'évaluation. Dans les systèmes de localisation considérés, un événement dangereux coïncide le plus souvent avec le fait qu'un état de panne de composant dure un certain temps, à la place de l'occurrence instantanée de la panne (ex. la panne d'un capteur pendant plus de 10 secondes mène à l'événement dangereux). Pour pallier ce problème de temps d'exécution, la loi de probabilité qu'un composant soit dans un état critique pendant une durée définie a été formalisée mathématiquement. Elle a alors été utilisée dans certaines transitions du RdP (comme le montrera l'exemple plus loin). La densité de probabilité d'un tel événement critique a été déterminée en utilisant une chaîne de Markov pour caractériser le processus stochastique de changements d'états du composant. La densité de probabilité p obtenue est définie par l'ensemble d'équations II.4 lié à la probabilité $Q_{CE}(m)$ que l'évènement critique CE soit présent à la $m^{ième}$ période (cf. éq. II.5). Dans ces équations, i est l'indice de l'état qui peut mener à CE s'il dure n périodes ($m \geq n+1$ et $n \geq 2$) et P_{trans} représente la matrice de transition de la chaîne de Markov pour laquelle les transitions au temps m sont homogènes en temps (la probabilité p ne dépend pas de m).

$$
\begin{aligned}
\forall\, m < n: \quad & p(n_{CE} = m) = 0, \\
m = n: \quad & p(n_{CE} = m) = P_{occ}(i) \cdot p_{ii}^{n}, \\
n < m \leq 2n+1: \quad & p(n_{CE} = m) = Q_{CE}(m) - \sum_{a=n}^{m-1} p(n_{CE} = a) \cdot p_{ii}^{m-a} \\
\forall\, m \geq 2n+2: \quad & p(n_{CE} = m) = Q_{CE}(m) - \sum_{a=m-n-1}^{m-1} p(n_{CE} = a) \cdot p_{ii}^{(m-a)} \\
& \quad - \sum_{a=n}^{m-n-2} p(n_{CE} = a) \times P_{from\_i} \times P_{trans}^{(m-a-n-2)} \times P_{to\_i} \cdot p_{ii}^{n}
\end{aligned}
\tag{II.4}
$$

$$
Q_{CE}(m) = P_{occ} \times P_{trans}^{(m-n-1)} \times P_{to\_i} \cdot p_{ii}^{n} \tag{II.5}
$$

La fonction de répartition correspondante est définie dans l'équation II.6. Le tirage aléatoire, selon cette distribution, de la période de temps m lors de laquelle se produit l'événement critique, est effectué à l'aide de l'algorithme détaillé dans [ACL10]. Celui-ci, validé sur des exemples, est codé en langage C pour être utilisé dans certaines transitions du RdP.

$$P(n_{CE} \leq m) = \sum_{j=0}^{m} p(n_{CE} = j) \tag{II.6}$$

avec :
- n_{CE} : Période de 1ère occurrence de l'événement critique (le composant reste dans l'état i pendant plus de n périodes de temps)
- $P_{occ}(i)$: Probabilité d'occurrence de l'état i d'un composant à l'instant initial
- p_{ii} : Probabilité de rester dans l'état i après T_0 secondes

4) Résultats applicatifs pour un système de localisation multi-capteurs

Dans le contexte du projet européen GaLoROI (cf. §I.6.1), le système de localisation développé fusionne des données de position issues des signaux de Galileo et d'ECS [ACTI16]. Il est ici considéré comme cas d'étude. Ce système dont l'architecture est construite selon le principe de sécurité composite [15], est représenté à la figure II.15. Dans cette architecture, il y a deux canaux de données qui permettent d'implémenter en sortie un contrôle de cohérence. Par la suite, un seul canal de données est utilisé pour illustrer l'approche d'évaluation proposée.

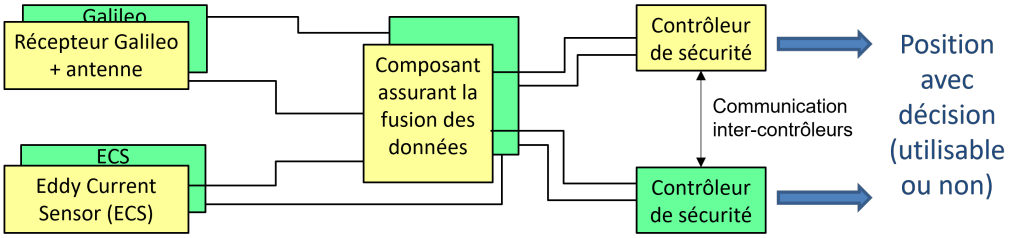


FIGURE II.15 – Architecture du système de localisation dans le projet GaLoROI [ACTI16]

L'analyse de la défaillance ou l'interruption du service de localisation fourni par l'un des canaux constituant le système Galileo / ECS mène à l'AdD étendu de la figure II.16. Selon les étapes de conversion d'AdD étendu en RdP, les évènements de base (EB) sont examinés pour en particulier modéliser sous forme de RdP, ceux qui se réfèrent à un comportement dynamique. La figure II.17 montre le RdP modélisant les modes de défaillance associés au récepteur GNSS, ceux se rapportant aux EB entourés d'un cadre bleu dans l'arbre de la figure II.16. Dans ce RdP, certaines transitions peuvent être franchies selon une condition utilisant la nouvelle distribution de probabilité formulée précédemment (conditions surlignées en vert). En effet, comme cette distribution a pour but de modéliser le fait qu'un composant soit dans un état critique pendant une durée définie, elle permet de modéliser les situations suivantes :

15. Selon le principe de sécurité composite, chaque fonction relative à la sécurité du système est réalisée par au moins deux entités redondantes indépendantes. Toute panne matérielle dangereuse aléatoire d'une entité doit être détectée et passivée dans un délai suffisant pour éviter l'occurrence d'une autre panne de la deuxième entité sur ce laps de temps [33].

- Dans la branche “Case B” dédiée aux causes de défaillance de la position en sortie du système :
  - *Non disponibilité des données ECS et GNSS* : s’il n’y a pas de données ECS et GNSS pendant plus de T_1 s, la sortie du composant assurant la fusion est considérée comme fausse.
  - *Non disponibilité des données GNSS* : si les données GNSS sont manquantes pendant plus de T_2 s (avec des mesures ECS valides), l’intervalle de confiance lié aux données de sortie augmentera rapidement. Dans ce cas, la sortie du composant assurant la fusion est considérée comme fausse ($T_1 < T_2$).
- Dans la branche “Case C” dédiée au fait qu’une erreur de position est non détectée (i.e., l’erreur de position PE_{system} est supérieure à une limite de tolérance donnée) :
  - Au moins k erreurs de position consécutives du récepteur GNSS supérieures à x mètres ($PE_{GNSS} > x$) peuvent conduire à PE_{system} > limite de tolérance.
  - Si les données ECS sont manquantes, au moins l erreurs de position consécutives du récepteur GNSS qui sont supérieures à x mètres ($PE_{GNSS} > x$) peuvent conduire à PE_{system} > limite de tolérance ($k > l$).

Suite à la simulation du RdP obtenu pour l’ensemble du système [RPRE13], des résultats de fiabilité et de disponibilité pour différents milieux de propagation des signaux GNSS ont été obtenus et sont représentés à la figure II.18. Les valeurs de paramètres utilisés sont également indiqués dans

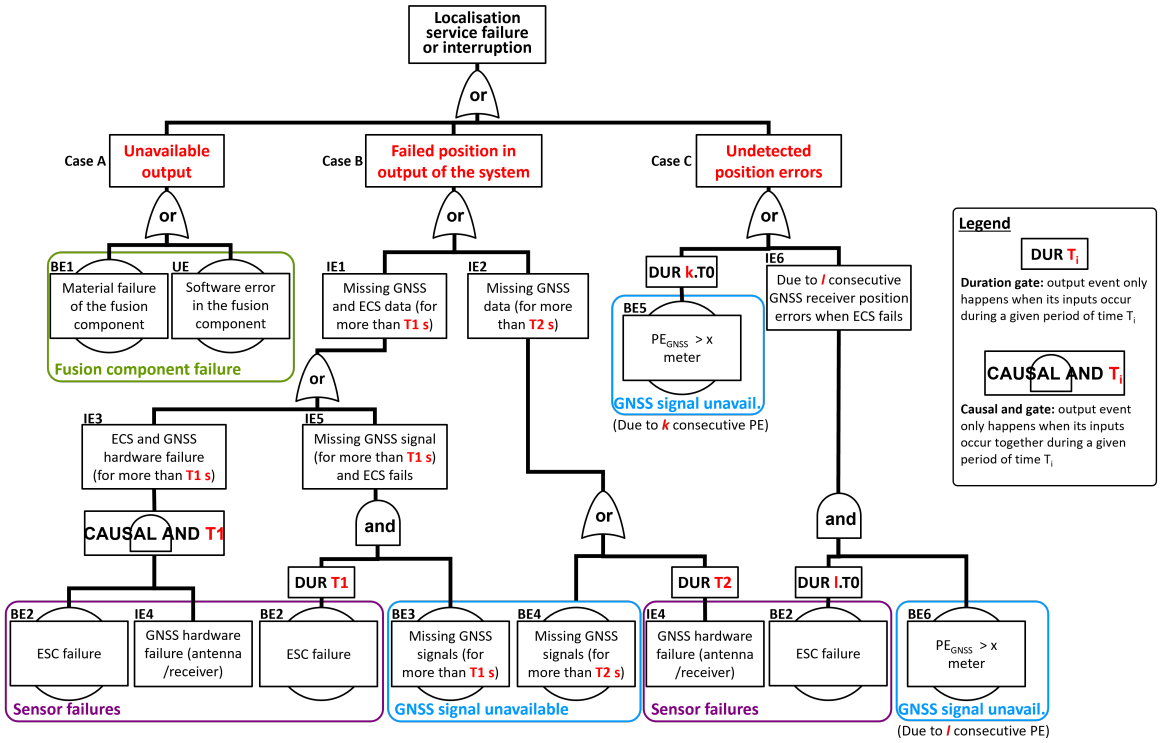


FIGURE II.16 – Arbre de défaillances étendu du système de localisation du projet GaLoROI

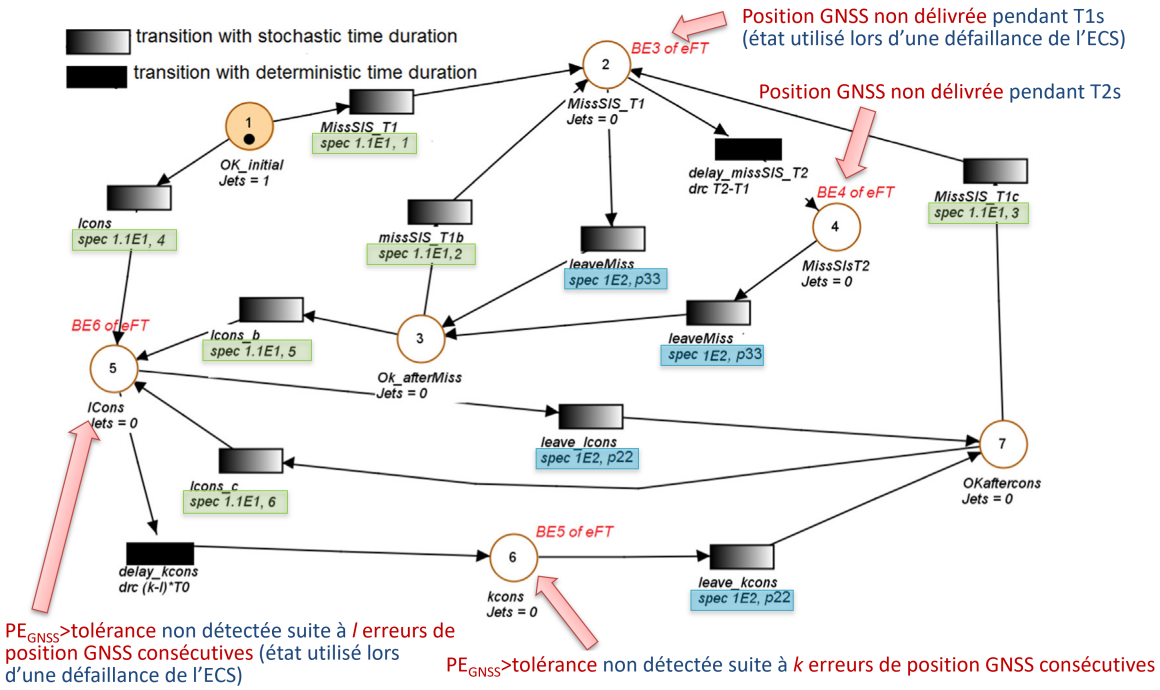
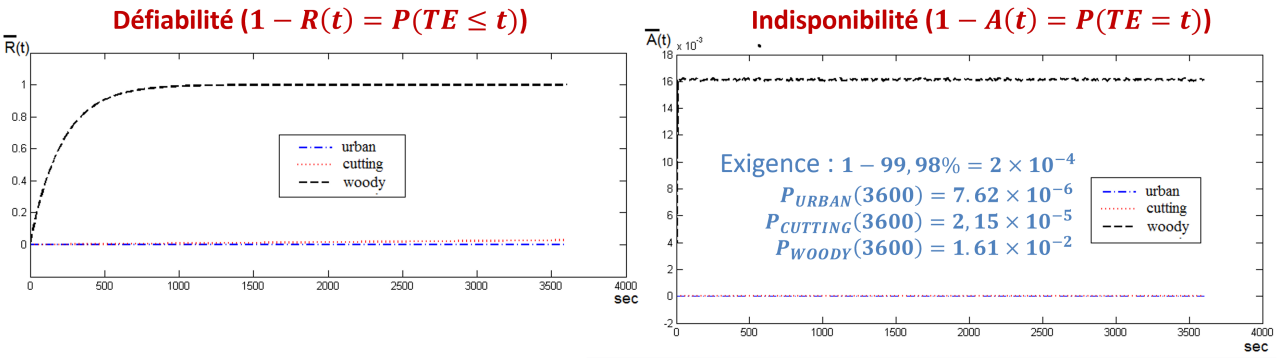


FIGURE II.17 – Extrait du modèle dynamique en RdP lié aux modes de défaillance GNSS



Temps d'indispo. GNSS et nb de PE_r consécutifs	T1	T2	l	k
	4	10	4	10
Taux de défaillance /10^{-9} (s)	$\alpha_{antenne}$	$\alpha_{récepteur}$	α_{ECS}	α_{fusion}
	1.11	1.13	0.6	1.7

La matrice de transition entre les états 1/2/3 est issue des données de [ACL11] où des positions GNSS sont estimées dans des milieux urbains / boisés / de tranchée ferroviaire simulés.

1. Position correcte, $PE_{GNSS} < x$
2. Position incorrect, $PE_{GNSS} > x$
3. Position indisponible due à l'indisponibilité des signaux
4. Position indisponible due à une défaillance matérielle

FIGURE II.18 – Résultats d'évaluation avec des environnements urbains, boisés, de tranchée ferroviaire

cette figure. TE correspond à l'instant où l'événement sommet (*Top Event*) de l'AdD survient pour la première fois. À noter que les valeurs employées sont uniquement utilisées pour illustrer l'approche et ne sont pas issues de données réelles.

En résumé, l'approche proposée dans nos travaux permet de fournir une évaluation performante de critères de SdF pour les systèmes de localisation multi-capteurs au comportement dynamique. Elle permet également d'orienter la conception du système en fonction des exigences attendues.

En effet, les paramètres k, l, T_1 et T_2 peuvent être calculés pour atteindre une exigence de sécurité requise pour la fonction de localisation, celle-ci étant ici exprimée soit par la disponibilité, soit par la fiabilité de la fonction relative à la sécurité.

La partie suivante explique la démarche d'évaluation de sécurité à partir des critères de performance propres aux GNSS.

II.3.3 Critères de sécurité et d'intégrité de la localisation : évaluations croisées

La démarche permettant de quantifier des propriétés liées à la sécurité à partir de critères de performance GNSS est issue de la thèse de Cyril Legrand [60]. Deux articles de revue y sont associés [ACL8, ACL5], ainsi que trois articles de conférence [ACTI15, ACTI19, ACTI24].

1) Intégrité de la localisation : définition et utilisation

Contexte aéronautique :

Le critère d'*intégrité de la localisation* est l'un des quatre critères de performance caractérisant les systèmes avec GNSS. Les normes aéronautiques, établies par l'Organisation Internationale de l'Aviation Civile [44] et par le RTCA (*Radio Technical Commission for Aeronautics*) [88], ont également défini les concepts de *précision*, de *continuité*, de *disponibilité*, pour les systèmes de navigation en général, y compris ceux basés sur les GNSS.

Nos travaux se sont concentrés spécifiquement sur le premier critère évoqué car il introduit la notion de confiance à la fois dans les informations fournies par les GNSS (c'est-à-dire l'intégrité des signaux émis) et dans le service délivré (c'est-à-dire l'intégrité de la position estimée). Dans la suite, nous supposerons que les signaux émis au niveau des satellites sont intègres.

Définition et paramètres associés :

La notion *d'intégrité de localisation* est une performance qui permet de caractériser spécifiquement la "capacité d'un système de navigation à alerter, en temps utile, l'utilisateur" d'un éventuel fonctionnement défaillant d'un de ses sous-systèmes. Pour les applications GNSS, cette définition porte en particulier sur l'évaluation de la confiance accordée à l'équipement de localisation embarqué muni d'un dispositif de détection, communément appelé "contrôle de l'intégrité". Cette évaluation de confiance est précieuse pour apprécier la sécurité, ou inversement le niveau de risque associé à l'équipement. Son importance est d'autant plus notable pour les applications de sécurité, parmi lesquelles figurent les CCS ferroviaires. Le contrôle de l'intégrité repose sur trois paramètres :

- La **limite d'alerte** (notée AL, *Alert Limit*) : il s'agit du seuil de tolérance au-delà duquel l'erreur de position (notée PE, *Position Error*) n'est plus acceptable par l'utilisateur. Le franchissement de ce seuil déclenche une alerte.
- Le **risque sur l'intégrité** (notée IR, *Integrity Risk*) : c'est la probabilité que la fonction de contrôle identifie comme acceptable une position qui ne l'est pas, sans avertir l'utilisateur dans un temps donné.
- Le **temps d'alerte** (notée TTA, *Time To Alert*) : il représente le temps accepté entre le moment où une défaillance survient et le moment où l'alerte est donnée.

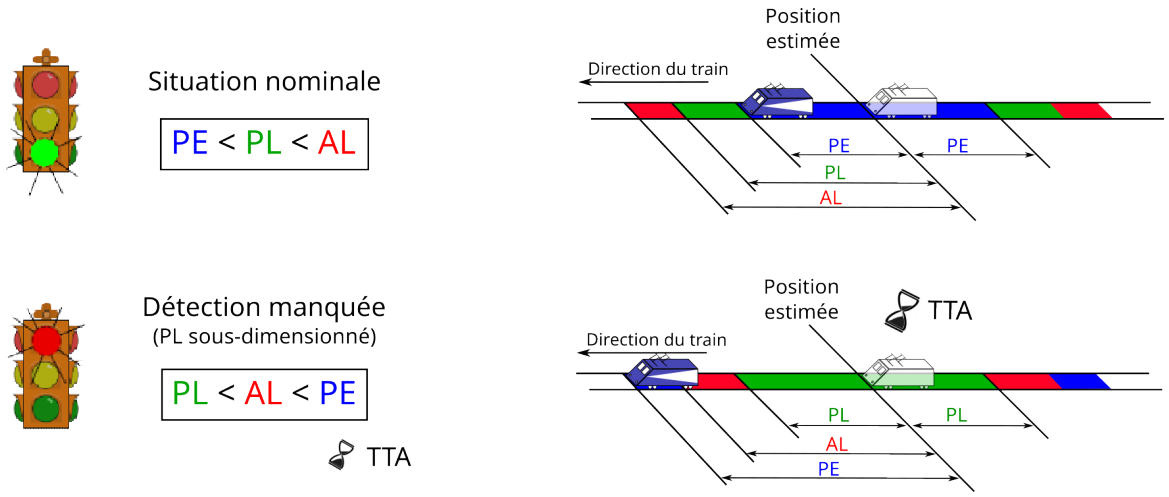


FIGURE II.19 – Contrôle de l'intégrité de la localisation en situation normale et risquée

En opération normale, l'erreur réelle PE ne peut pas être directement mesurée ; elle demeure inconnue. Par conséquent, les processus de contrôle, issus du domaine aéronautique, utilisent des modèles statistiques pour estimer un majorant de cette erreur, appelé **niveau de protection** et noté PL (*Protection Level*). Ce niveau de protection représente l'erreur de position maximale garantie par le contrôle de l'intégrité. Le risque associé à une estimation incorrecte du majorant (i.e. PL sous-dimensionné par rapport à PE) correspond à la probabilité IR.

Utilisation des paramètres dans le cas général :

Si le niveau de protection calculé PL estimé par le contrôle de l'intégrité dépasse la limite d'erreur acceptable AL, une alerte est émise. Le système de localisation est alors considéré comme indisponible et ne doit pas être utilisé en opération. Il s'agit d'un comportement sécuritaire. En revanche, si PL est inférieur à AL, même si le système est disponible, il existe un risque que PE ne soit pas correctement borné par PL, et que PE dépasse AL (comme illustré à la figure II.19 dans un référentiel unidimensionnel). Cette situation correspond à une défaillance dangereuse susceptible d'entraîner des conséquences critiques si elle persiste dans le temps.

Pour estimer PL, des modèles statistiques sont utilisés dans les processus de contrôle d'intégrité pour borner les incertitudes (voire les biais) de mesures des récepteurs GNSS. Ces modèles sont bien connus pour les environnements totalement dégagés d'obstacles et sont intégrés dans les mécanismes de détection, tels que le RAIM (*Receiver Autonomous Integrity Monitoring*) [105]. Cependant, l'estimation devient plus difficile pour les environnements contraints en raison de la variabilité des configurations de réception satellitaire. Des travaux de recherche sont actuellement menés, dans la communauté GNSS, pour développer des modèles robustes et efficaces adaptés à ces environnements. De plus, des modèles encore plus sophistiqués sont nécessaires dans le cas de systèmes multicapteurs avec GNSS, afin de prendre en compte les incertitudes et biais liés aux autres capteurs combinés au récepteur GNSS. Le développement de ces modèles est un des éléments clés pour les applications ferroviaires de sécurité du GNSS [91].

En ce qui concerne l'exigence IR liée à un système de navigation muni d'un contrôle d'intégrité, elle est généralement vérifiée de manière statistique. À partir des données d'une campagne de mesures comportant suffisamment d'échantillons, les informations relatives à PE, PL et AL sont représentées dans un diagramme de Stanford. Ce dernier comporte plusieurs zones (position disponible / indisponible, position dangereuse / non-dangereuse mais bornée de manière incorrecte) qui permettent de classifier les données et d'estimer le risque sur l'intégrité IR, à partir du nombre de points situés dans la zone dangereuse.

Discussion sur l'utilisation des paramètres dans le domaine ferroviaire :

Il convient de noter que le critère d'*intégrité de la localisation* est légèrement différent de la notion plus générale d'*intégrité de la sécurité*. En effet, cette dernière est dédiée à l'allocation d'exigences de sécurité à un système E/E/PE à partir de l'analyse des défaillances dangereuses de ses fonctions. Plus le risque associé aux défaillances d'une fonction est élevé, plus les exigences qui doivent lui être associées, devront être rigoureuses. L'échelle des SIL de 1 à 4 traduit ce niveau de rigueur à la fois de manière qualitative (indépendance entre matériels / logiciels redondants, contrôle des processus, etc.) et quantitative (objectif de sécurité sous la forme d'un TFFR pour une fonction et d'un THR pour le danger associé).

La fonction de localisation est une fonction de sécurité dans un CCS et fait l'objet d'une allocation de SIL. Le risque sur l'intégrité IR apparaît comme étant un objectif de sécurité lié au danger de cette fonction. Toutefois, le fait qu'il fasse référence à la probabilité qu'une défaillance de position dure pendant un laps de temps TTA soulève des interrogations dans le domaine ferroviaire. En effet, dans le cadre d'une évaluation de sécurité dans ce secteur, une probabilité est attribuée à l'occurrence d'un événement dangereux, mais pas à sa durée. Une probabilité par heure peut être utilisée, mais elle ne concerne pas le fait qu'un événement dure une heure, plutôt le fait qu'il puisse apparaître pendant cette période.

Dans le domaine aéronautique, le TTA fait généralement référence au temps dont les infrastructures de surveillance au sol ont besoin pour analyser l'intégrité des signaux fournis par les satellites et transmettre un message d'alerte à l'utilisateur pour l'informer d'un problème. Dans ce contexte, le TTA est lié à l'intégrité des signaux émis. Lorsque la surveillance se concentre sur les signaux reçus au niveau utilisateur et s'effectue à l'aide d'un processus de détection intégré au récepteur GNSS, le traitement pour détecter la condition $PL > AL$ est quasi-instantané. Une alerte peut alors être déclenchée immédiatement. Cependant, dans ce contexte et en cohérence avec sa définition donnée plus haut, le TTA peut correspondre au délai maximal entre l'apparition d'une condition dangereuse à l'entrée d'un récepteur GNSS et le déclenchement d'une alerte par le mécanisme de détection. Afin de démontrer si ce délai maximum est respecté par le dispositif de contrôle développé, il sera nécessaire d'analyser l'intervalle de temps entre : le moment où le mécanisme de détection n'émet pas d'alerte (i.e. $PL \leq AL$) alors que la position n'est plus intègre (i.e. $PE > AL$), et le moment où une réaction est déclenchée, sachant que la défaillance de position a persisté entre les deux instants. Si l'analyse montre que tout intervalle de ce type est inférieur à TTA, l'exigence de sécurité sera démontrée.

Enfin, en ce qui concerne la spécification de l'exigence sur le risque IR, il convient de noter que plus ce risque est contraignant (c'est-à-dire une probabilité plus faible), plus l'intervalle de confiance (PL) sera étendu. Dans ce cas, la localisation ne pourra être disponible qu'avec une marge de tolérance AL spécifiée à une valeur élevée. Dans le domaine ferroviaire, cette contrainte pourrait entraîner une augmentation de l'intervalle de sécurité entre les trains, ce qui rendrait leur exploitation moins performante. Cela rejoint le fait de trouver un compromis entre sécurité et disponibilité.

Compte tenu de ces éléments, la démarche d'évaluation proposée est détaillée ci-dessous. Elle nécessite la mise en place d'un mécanisme de détection adapté à un système multicapteurs avec GNSS, composé d'un récepteur GNSS combiné à une centrale inertielle. Une partie des travaux de thèse de Cyril Legrand s'est concentrée sur le développement d'un algorithme de contrôle de l'intégrité étendu au système GNSS / INS [ACL8]. L'algorithme associé ne sera pas détaillé dans ce mémoire afin de mettre l'accent sur le type de situations dangereuses qu'il permet d'identifier en fonction d'un raisonnement propre à la démarche. Ce raisonnement s'appuiera sur les paramètres AL, PL et IR.

2) Démarche d'évaluation de sécurité

La méthodologie d'évaluation repose sur une approche empirique fondée sur une analyse de données de localisation mesurées dans des conditions ferroviaires spécifiques. La démarche comprend quatre étapes visant à évaluer la probabilité qu'une situation dangereuse critique, c'est-à-dire non maîtrisée, se produise. Ces situations dangereuses sont caractérisées, d'une part, par l'occurrence de détections de défauts spécifiques au système GNSS / INS, tels que les biais instantanés et les biais cumulatifs (ces derniers seront notés SGE–*Slowly Growing Errors*) [ACL8]. La détection d'un défaut par le mécanisme développé dans ces travaux, est considérée comme menant au franchissement de l'exigence utilisateur AL. D'autre part, lorsqu'aucun défaut n'est détecté, les incertitudes de position sont quantifiées par un paramètre PL adapté. Ce paramètre, noté PL_{extend}, permet d'établir la disponibilité du mécanisme de détection s'il est inférieur à AL, en tenant compte du risque IR_{extend} associé. Ces trois paramètres contribuent à définir le critère d'"*intégrité de localisation étendue*", utilisé par la suite pour l'évaluation de sécurité. Cette évaluation, fondée en particulier sur l'estimation du risque IR_{extend}, sera exprimée selon des propriétés de sécurité qui sont en lien avec les critères FDMS des normes de sécurité ferroviaire.

Avant d'aborder ces quatre étapes, il est important de souligner que la caractérisation d'une situation dangereuse nécessite de prendre en compte le contexte opérationnel dans lequel le système de localisation évolue. Dans les travaux présentés ci-dessous, notre objectif n'est pas d'évaluer les risques opérationnels, c'est-à-dire l'éventualité qu'un accident se produise sur une ligne ferroviaire en raison de causes liées au système gérant l'exploitation des trains en sécurité (le système de contrôle-commande). L'objectif principal est de se concentrer sur un système technique de localisation et sur ses défaillances dangereuses. Dans le cas où certaines défaillances dangereuses pourraient ne pas être maîtrisées, le but est d'estimer la probabilité d'occurrence des situations critiques associées et de vérifier si cette probabilité ne dépasse pas une valeur d'exigence spécifiée.

À ce jour, aucun tableau d'exigences FDMS n'est harmonisé pour la fonction de localisation dans le domaine ferroviaire. Certaines exigences de localisation ont été spécifiées dans le cadre de l'ERTMS, notamment avec des critères de performance concernant le niveau de précision [94], tandis que les exigences de sécurité font souvent référence, dans l'absolu, au SIL 4. Les différents projets axés sur les GNSS pour les applications de sécurité ferroviaire ont introduit leurs propres exigences pour chaque solution spécifique basée sur les GNSS développées [ACL7]. Les exigences les plus récentes connues sur un ensemble représentatif d'applications GNSS pertinentes pour la sécurité ferroviaire sont celles formulées par un panel ferroviaire constitué par l'EUSPA [36]. Cependant, la façon dont elles sont exprimées, en particulier à travers les paramètres d'intégrité de la localisation, n'est pas facilement exploitable par les utilisateurs ferroviaires. C'est ce qui nous a conduit, comme évoqué dans les problématiques présentées au début de cette section, à formaliser les liens entre les critères de sécurité et d'intégrité de la localisation afin d'obtenir une évaluation croisée entre ces différents critères.

Ainsi, les quatre étapes de la démarche d'évaluation proposée se résument comme suit ; elles sont développées juste après :

- **Étape 1** : *Acquisition d'un ensemble de données de localisation*. Cet ensemble de données est lié à une ou plusieurs zones typiques du réseaux ferré. Il est acquis en conditions d'essais, c'est-à-dire que l'écart entre chaque position estimée d'un train et sa position réelle associée, est connu, ce qui n'est pas le cas en conditions opérationnelles classiques.
- **Étape 2** : *Identification des situations dangereuses*. Cette étape consiste à analyser les données acquises afin de distinguer les instants où des situations dangereuses se produisent. Ces situations sont identifiées en se basant sur les états de localisation risqués et leur persistance dans le temps. Un état risqué est spécifiquement défini en fonction des différents états du contrôle d'intégrité associé au système GNSS / INS, c'est-à-dire le contrôle d'intégrité étendu développé dans le cadre de ces travaux.
- **Étape 3** : *Estimation de la probabilité d'occurrence d'une situation dangereuse critique* : Cette probabilité correspond à l'estimation du risque sur l'intégrité IR_{extend}. À partir du nombre d'occurrences de situations dangereuses critiques identifiées à l'étape précédente, les expressions de la valeur moyenne et de la valeur instantanée de IR_{extend} sont formalisées.
- **Étape 4** : *Relation entre les critères de sécurité et d'intégrité de la localisation*. Cette étape permet de formaliser les liens entre les expressions de IR_{extend} obtenues précédemment et certaines propriétés liées au critère 'sécurité', telles que définies dans les normes de sécurité ferroviaire.

Étape 1 *Acquisition d'un ensemble de données de localisation*

Pendant cette étape, des données de localisation sont collectées à l'aide de l'équipement GNSS / INS installé sur le train, alors qu'il parcourt un itinéraire donné. Cet itinéraire comprend plusieurs zones caractéristiques telles que celles où le train est à l'approche d'une station, d'un nœud ferroviaire, ou se trouve en pleine voie (entre deux nœuds / gares). Le parcours effectué par le train sur cet itinéraire et la collecte de données associée constituent un scénario.

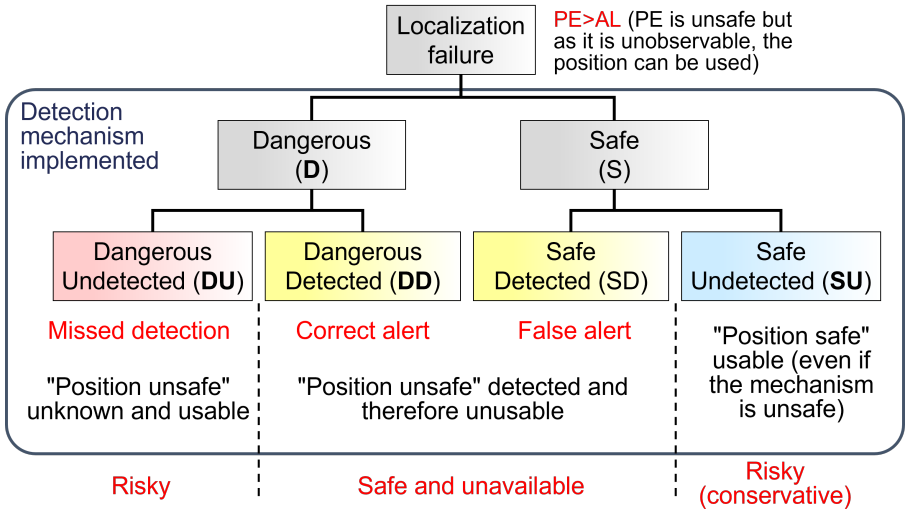


FIGURE II.20 – Classification des états de localisation

Dans les étapes suivantes, les états de localisation risqués seront identifiés à chaque instant discrétisé t_i pendant la période de temps T_m du scénario. i est un entier représentant le $i^{\text{ème}}$ pas de temps, et T_e est la taille du pas de temps, de sorte que $0 \leq i \leq int(T_m/T_e)$ (l'unité de temps est supposée être la seconde par la suite). Les évaluations des indicateurs quantitatifs liés à la sécurité seront effectuées sur la période T_m qui correspond à la durée de mission du système. Ces évaluations nécessitent une observation prolongée du système en fonctionnement pour obtenir des valeurs statistiques significatives.

Pendant la collecte des données, les mesures peuvent être acquises lors d'expérimentations sur site ou lors de simulations reproduisant les conditions de réception des GNSS sur l'itinéraire parcouru. Les positions de référence, associées aux positions estimées par l'équipement GNSS / INS, sont supposées être disponibles, soit grâce à une technique fournissant ce que l'on appelle communément la "vérité terrain" lors de mesures sur site, soit par le biais de l'outil de simulation. Cela permet de déterminer l'erreur sur la position PE.

Étape 2 *Identification des situations dangereuses*

Pour identifier les situations dangereuses en fonction de l'occurrence ou non de détections de défauts, il est utile de s'appuyer sur les états de la fonction de localisation. Nos travaux antérieurs ont permis d'identifier les différents états de localisation (et leur probabilités associées en fonction de AL, IR et PE) à partir de l'étude des défaillances dangereuses et non dangereuses de cette fonction [ACLN4, ACL12]. Ces défaillances sont représentées dans les rectangles colorés de la figure II.20. Elles mènent à des états de localisation sécuritaires ou risqués, qui sont liés aux quatre états du mécanisme de détection : détection manquée / détection correcte / fausse alerte / non-détection. Dans cette figure, l'événement DU (dangereux non-détecté) est inévitablement associé à un état risqué. Dans le domaine aéronautique, l'événement SU (sécuritaire non-détecté) est souvent considéré comme risqué car, même si l'erreur de position reste inférieure à une limite d'erreur tolérable, le mécanisme de détection ne fonctionne pas correctement (PL ne majore pas correctement PE), ce qui peut entraîner des problèmes ultérieurs ; c'est un point de vue conservateur [87].

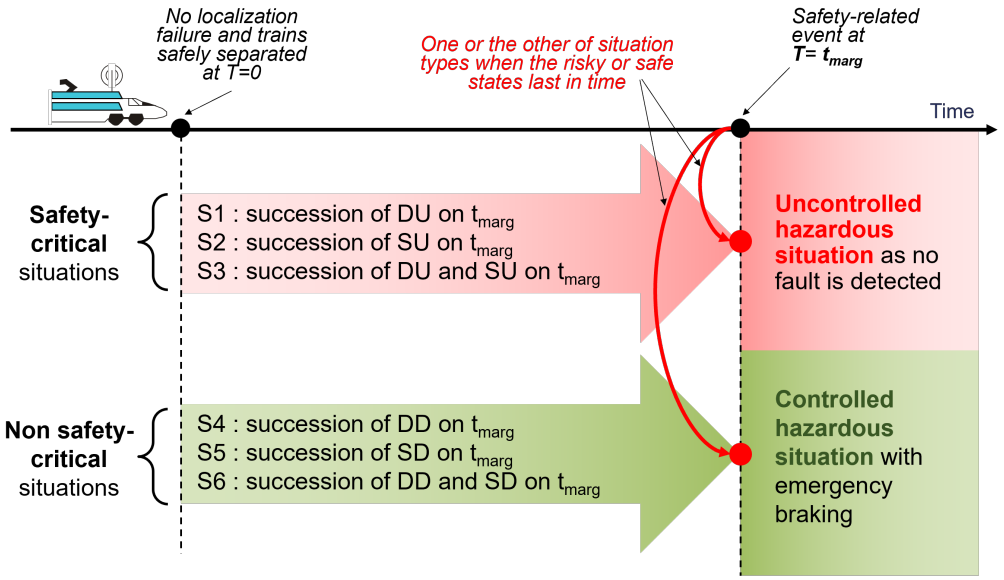


FIGURE II.21 – Types de situations dangereuse rencontrées en contexte ferroviaire (critiques ou non) selon les états de localisation

Dans cette figure, les événements DU et SU sont vus indépendamment de leur occurrence ou de leur durée dans le temps. Cependant, dans le domaine ferroviaire, la dimension temporelle, ainsi que la dimension spatiale, sont importantes pour caractériser une situation dangereuse. En effet, une telle situation est liée à un contexte opérationnel ferroviaire précis, caractérisé essentiellement par trois aspects : la phase opérationnelle du train (ex. service nominal, maintenance), le mode de fonctionnement du train (ex. marche à vue à une vitesse inférieure à 30 km/h), et la zone exploitée sur le réseau ferré [9].

Compte tenu du fait qu'un train se trouve sur une zone spécifique du réseau (ex. à l'approche d'une station), il est important de souligner qu'une défaillance de position qui survient et ne dure qu'un pas de temps d'échantillonnage du système (ex. 1 seconde) n'aura pas d'impact critique sur l'exploitation ferroviaire en raison de son caractère furtif. Par conséquent, les cas où les états de localisation risqués persistent pendant une certaine durée sont à analyser pour cette étape 2. La figure II.21 illustre, sur une zone quelconque, la progression d'un train à partir d'une position estimée à T=0 (avec une erreur correctement bornée), sachant que la position réelle du train est soit en amont soit en aval. Lors de sa progression, la succession dans le temps d'états de localisation risqués permet de caractériser les situations dangereuses possibles. En effet, étant donné un point cible que le système de contrôle-commande embarqué du train (*CCS Bord*) n'autorise pas à franchir (point fixe ou mobile non représenté sur la figure, le point mobile correspondant à l'arrière d'un autre train), et étant donné un intervalle d'imprécision maximum, le *CCS Bord* détermine un point critique (2nd point de la figure) au-delà duquel le non déclenchement d'une réaction de sécurité mène à une situation non maîtrisée. La condition de durée entre les deux points est notée t_{marg} et correspond au temps pour parcourir une marge de sécurité. Par conséquent, les événements DU et SU ne créent une situation dangereuse critique que s'ils se maintiennent suffisamment longtemps pour dépasser le délai de sécurité t_{marg} (cf. situations $S1$, $S2$ ou $S3$ sur la figure II.21). Cette durée apparaît comme une contrainte opérationnelle ferroviaire à préciser selon la zone parcourue. La durée t_{marg} a alors la

même finalité que le paramètre TTA défini précédemment. Il convient de noter que les événements DD (événement dangereux détecté) et SD (événement incorrectement détecté comme dangereux) permettent au train de rester dans une situation maîtrisée, en freinant par exemple (cf. situations $S4$, $S5$ ou $S6$ sur la figure II.21).

L'objectif final de cette étape est donc d'identifier les événements DU et SU dans l'ensemble des données collectées en fonction des résultats de détection liés aux paramètres d'intégrité étendue. Pour identifier ces événements, des propositions logiques sont utilisées et établies en fonction des événements d'alerte délivrés par le processus de détection. La transition vers l'état SU est reconnue lorsque :

$$\left[(PE \leq AL) \text{ and } \left((PL < PE) \text{ and } \quad test_{bias} = false \quad \text{and} \quad test_{SGE} = false\right)\right] \tag{II.7}$$

La transition vers l'état DU est reconnue lorsque :

$$\left[(PE > AL) \text{ and } \left((PL \leq AL) \text{ and } \quad test_{bias} = false \quad \text{and} \quad test_{SGE} = false\right)\right] \tag{II.8}$$

$test_{bias}$ et $test_{SGE}$ sont deux variables booléennes dont la valeur est *true* lorsque, respectivement, un biais instantané ou un SGE est détecté, et *false* sinon.

Étape 3 : *Estimation de la probabilité d'occurrence d'une situation dangereuse critique*

Cette étape permet d'estimer la probabilité qu'une situation critique se produise en raison du système de localisation GNSS / INS. Comme expliqué précédemment, cette probabilité se définit en fonction de l'occurrence des états DU et SU, sous la condition qu'ils se succèdent dans le temps selon l'une des trois situations S_1, S_2 ou S_3. Cette définition se rapporte au risque sur l'intégrité du système muni d'un contrôle d'intégrité étendu, il est noté IR_{extend}.

Une valeur moyenne de IR_{extend}, notée IR_{extend_avg}, peut être estimée à partir du nombre moyen d'occurrences de S_1, S_2 et S_3 sur la période T_m. Pour exprimer IR_{extend_avg} en fonction des événements SU et DU, notons ces événements de manière indifférenciée avec $A = \{SU \cup DU\}$. En utilisant le nombre de pas de temps dans la période T_m, calculé par $int(T_m/T_e)$, IR_{extend_avg} peut alors être défini par l'équation II.9.

$$IR_{extend\_avg} \approx \frac{\#(\text{S1 OR S2 OR S3}) \text{ is observed on } T_m}{int(T_m/T_e)} \tag{II.9}$$

Pour exprimer IR_{extend} sur chaque pas de temps t_i, nous considérons la persistance de l'événement A entre t_i et $t_i + TTA$, plus précisément entre t_i et $t_{i+int(TTA/T_e)}$ pour tenir compte de la discrétisation des mesures. Une formulation de $IR_{extend}(t_i)$ est alors obtenue selon l'équation II.10 (en supposant que les événements A_{t_j} sont indépendants).

$$IR_{extend}(t_i) = \prod_{j=i}^{i+int(TTA/T_e)} P(A_{t_j}) \tag{II.10}$$

$IR_{extend}(t_i)$ peut être estimé à partir de plusieurs ensembles de données associés à des répétitions du même scénario. L'estimation se rapporte alors au nombre de fois où l'événement $(A_{t_i}, ..., A_{i+int(TTA/T_e)})$ se produit à t_i sur chacun des scénarios, moyenné sur le nombre de répétitions du scénario.

En résumé pour cette étape 3 :

- Les états SU et DU sont traités de manière indifférenciée à l'aide de l'événement A.
- La persistance de l'évènement A entre t_i et $t_{i+int(TTA/T_e)}$ permet de décrire n'importe quelle situation $S1$, $S2$ ou $S3$.
- L'expression de $IR_{extend}(t_i)$ est donnée par l'équation II.10.
- La valeur moyenne de IR_{extend}, formulée à l'équation II.9, peut être exprimée en tenant compte de l'événement A, selon la formulation de l'équation II.11.

$$IR_{extend\_avg} \approx \frac{\#(A_{t_i}, ..., A_{i+int(TTA/T_e)}) \text{ is observed on } T_m}{int(T_m/T_e)} \tag{II.11}$$

Étape 4 : *Relation entre les critères de sécurité et d'intégrité de la localisation*

L'étape 4 permet de formaliser le lien entre l'expression de IR_{extend} et deux propriétés de sécurité rencontrées dans le domaine ferroviaire : P_{wsf} et PFH.

P_{wsf} (*Probability of wrong-side failure*) est une propriété définie dans la norme de sécurité ferroviaire EN 50126 [30]. Elle représente la probabilité de défaillances contraire à la sécurité qu'un système peut provoquer. Pour le système de localisation, elle s'écrit alors comme suit : $P_{wsf}(t_i) = P_{DU}(t_i) + P_{SU}(t_i) = P_A(t_i)$. Ainsi, le lien entre P_{wsf} et IR_{extend} peut s'exprimer selon l'équation II.12, en considérant que P_{wsf} est constant.

$$IR_{extend}(t_i) = \prod_{j=i}^{i+int(TTA/T_e)} P_{wsf}(t_j) \tag{II.12}$$

$$\Rightarrow P_{wsf}(t_i) = (IR_{extended}(t_i))^{\frac{1}{int(TTA/T_e)}}$$

De plus, une valeur moyenne de P_{wsf} peut être estimée et formulée selon l'équation II.13.

$$P_{wsf\_avg} \approx \frac{\#\text{ of time } A_{t_i} \text{ is observed}}{int(T_m/T_e)} \tag{II.13}$$

PFH (*frequency of Dangerous Failure per Hour*) est l'une des deux principales propriétés définies dans la norme de sécurité fonctionnelle IEC 61508 [48], aux côtés de PFD_{avg} (*average Probability of Failure on Demand*). Cette norme étant générique, elle est applicable au domaine ferroviaire. PFD_{avg} et PFH se distinguent par le mode de fonctionnement de la fonction de sécurité qu'ils caractérisent. Alors que PFD_{avg} est dédié aux fonctions faiblement sollicitées, PFH concerne les fonctions fortement sollicitées (plus d'une fois par an), allant jusqu'à une demande continue, comme c'est le cas dans les systèmes de sécurité ferroviaires. PFH est défini par la fréquence moyenne à laquelle une défaillance dangereuse se produit sur une période continue d'utilisation de la fonction. Elle est exprimée en nombre de défaillances dangereuses par heure.

Dans la norme IEC 61508, une défaillance dangereuse est considérée menant directement à une situation dangereuse. Cependant, dans le domaine ferroviaire, où plusieurs mesures de sécurité peuvent se combiner pour éviter une situation dangereuse, la notion de THR est plutôt utilisée pour caractériser le fait que l'ensemble de ces mesures peut être en défaut, ceci dans un contexte opérationnel donné. Dans cette étape, le PFH peut être assimilé à un THR comme il est utilisé pour évaluer la fréquence d'occurrence des situations dangereuses issues de la fonction de localisation. Toutefois, le contexte opérationnel est uniquement considéré de manière générale ; seule la persistance dans le temps des défaillances dangereuses de la fonction de localisation caractérise ce contexte. Celui-ci sera examiné plus en détail dans la section II.4.

Au final, une estimation de la propriété PFH peut s'écrire telle que $PFH = IR_{extend\_avg}/T_m$. Comme il s'agit d'une fréquence horaire et que T_m est en secondes, l'équation II.14 est finalement obtenue.

$$PFH = \frac{3600.IR_{extend\_avg}}{T_m} \tag{II.14}$$

Pour conclure sur la démarche d'évaluation proposée, il est important de noter qu'elle nécessite de prendre en compte un nombre important de données afin de fournir une estimation précise des quantités recherchées. Les résultats présentés ci-dessous montrent l'applicabilité de cette démarche. Ils sont issus d'un système GNSS / INS dont le modèle de représentation d'état constitue un 'cas d'école' non optimisé, sur lequel le raisonnement de sécurité lié à la démarche peut être mené.

3) Résultats applicatifs de la démarche d'évaluation

L'architecture du système de localisation GNSS / INS utilisé pour le cas d'étude est issue de [39]. Il s'agit d'une solution d'hybridation très serrée au sein de laquelle un filtre de Kalman étendu (EKF) permet d'estimer une position. Un filtre de Kalman est un algorithme récursif de traitement de données en temps réel utilisé pour estimer les états d'un système linéaire dynamique compte tenu de mesures de capteurs bruitées, c'est-à-dire comportant une erreur. Dans un EKF, les équations d'état et de mesure se rapportent à un système non linéaire. L'algorithme EKF génère des résidus qui sont traités par l'algorithme de contrôle d'intégrité développé dans ces travaux de thèse. En confrontant les résultats du mécanisme de détection (alerte ou absence d'alerte à chaque pas de temps) à l'erreur de position connue dans les conditions expérimentales, il est possible d'identifier et de quantifier l'occurrence de situation dangereuses critiques selon la démarche d'évaluation proposée.

Pour l'étape 1 de l'approche, l'acquisition de données avec ce système n'est pas possible car il s'agit d'un système théorique issu de la littérature. Cependant, grâce à l'aide du laboratoire GEOLOC du Campus de Nantes de l'université Gustave Eiffel, nous avons pu accéder à des données réelles provenant d'un récepteur GNSS monté sur un véhicule routier utilisé pour des essais. Bien que ces données ne soient pas collectées le long d'une ligne ferroviaire, elles peuvent être considérées comme représentatives pour l'analyse, car les environnements rencontrés par un train sont similaires à ceux rencontrés par une voiture (présence de végétation, bâtiments, etc). Deux jeux de données ont été enregistrés à Paris sur le même itinéraire. L'environnement urbain dense rencontré est une source de perturbations pour les signaux GNSS. Les erreur de position PE sont connues grâce à un dispositif de mesure très précis installé sur le véhicule. Étant donné l'absence de données INS réelles pour l'analyse du système GNSS / INS, des données INS simulées sont générées selon les modèles

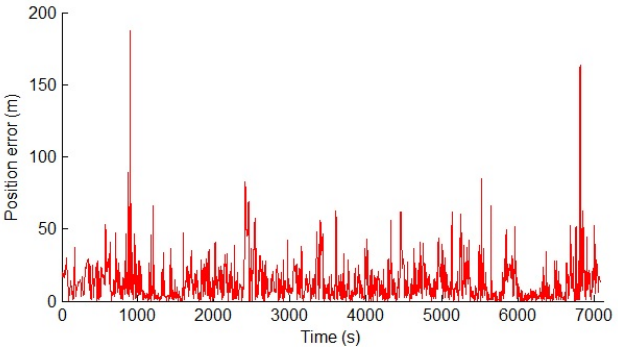


FIGURE II.22 – Erreur de position PE obtenu avec le 1er jeu de données

	1er jeu de données	2nd jeu de données
Erreur moyenne (en m)	13.35	12.09
Précision (à 95 %)	37.43	32.16

TABLE II.4 – Caractéristiques de PE associée à chaque cas

fournis dans [39], puis bruitées. Ces données sont utilisées dans les routines de calcul fournies (sous licence BSD) pour estimer les positions en sortie de la solution intégrée. La figure II.22 représente l'erreur de position du système obtenue pour le 1er jeu de donnée GNSS couplé aux données INS, tandis que le tableau II.4 présente la précision associée à chaque jeu de données.

Pour mener l'étape 2, le niveau d'alerte AL est fixé à 20 mètres et le temps d'alerte TTA est fixé à 4 secondes. Ces valeurs ont été établies en tenant compte du contexte de gestion de l'inter-distance entre trains dans le cadre de l'ETCS niveau 3, comme expliqué dans notre article décrivant l'obtention des résultats qui suivent [ACL5]. Au cours de cette étape, le nombre d'états de localisation risqués obtenus lorsque le système utilise le contrôle d'intégrité développé est quantifié.

La succession dans le temps des états de localisation risqués est analysée dans l'étape 3 pour identifier les situations dangereuses $S1$, $S2$ et $S3$ (cf. tableau II.5). Cette étape considère une fenêtre glissante de TTA secondes sur le temps de mission de chaque scénario. Cette identification permet d'évaluer la moyenne du risque sur l'intégrité étendu IR_{extend_avg}. Les résultats de cette étape sont présentés dans le tableau II.6 pour chaque scénario.

Suite à la mise en œuvre de l'étape 4, le tableau II.6 présente également les valeurs de p_{wsf_avg} et de PFH associées à chaque scénario, ainsi que des valeurs globales considérant l'ensemble des deux scénarios obtenus sur le même itinéraire. Ces valeurs sont des approximations de probabilités qui peuvent être réduites avec un plus grand plus grand nombre de scénarios et, également, avec un plus grand nombre de points dans ces scénarios.

La sécurité du système GNSS / INS dans cette analyse peut être discutée à partir de la valeur PFH obtenue, égale à $3.16\,\text{E-}2$. En référence à la norme IEC 61508, nous pouvons conclure que le système GNSS / INS évalué dans cet exemple doit être considéré comme dangereux et inutilisable car le PFH associé est supérieur à tous les intervalles de PFH liés au SIL définis dans la norme. Cependant, il est important de noter que ces résultats s'expliquent par les performances médiocres du contrôle d'intégrité telles qu'analysées dans [ACL5]. Cela provient principalement du fait que l'algorithme de détection mis en place et l'EKF de la solution GNSS / INS, tel que configuré pour estimer une position, supposent des erreurs gaussiennes, ce qui n'est pas le cas en réalité. Cependant, la

TABLE II.5 – Nombre de situations critiques (S1 à S3) et probabilités d'occurrence approchées

	1er jeu de données	2nd jeu de données
Nombre de situations critiques		
# de $S1$	170	112
# de $S2$	268	262
# de $S3$	61	45
Probabilité approchée sur T_m		
Situation $S1$	2.4 E-2	1.51 E-2
Situation $S2$	3.78 E-2	3.53 E-2
Situation $S3$	8.6 E-3	6.1 E-3
Probabilité approchée sur 1h		
Situation $S1$	1.22 E-2	7.3 E-3
Situation $S2$	1.92 E-2	1.71 E-2
Situation $S3$	4.4 E-3	2.9 E-3

TABLE II.6 – Propriétés de sécurité obtenues avec la démarche d'évaluation

	1er jeu de données	2nd jeu de données
IR_{extend_avg} sur T_m	7.04 E-2	5.65 E-2
P_{wsf_avg} sur T_m	0.175	0.128
PFH sur 1h	3.58 E-2	2.74 E-2

	Considération des 2 jeux de données
IR_{extend_avg} sur T_m	6.35 E-2
P_{wsf_avg} sur T_m	0.152
PFH sur 1h	3.16 E-2

recherche de modèles d'erreur fidèles à la réalité et l'estimation d'un PL dimensionné au plus juste par rapport à l'erreur de position, restent des questions de recherche dans la communauté GNSS. Ce travail de thèse s'est concentré en priorité sur la formulation d'un raisonnement de sécurité permettant l'évaluation de critères ferroviaires. À l'avenir, il sera nécessaire d'envisager des algorithmes plus performants en suivant également les progrès des recherches issues des communautés traitant de l'intégrité de la navigation par satellite et de la modélisation des systèmes intégrés multicapteurs.

II.3.4 Conclusion

Cette section s'est concentrée sur la caractérisation et l'évaluation de l'occurrence des états risqués d'un système technique au comportement dynamique, notamment dans le cas où un état risqué peut être non observable mais avoir des conséquences néfastes. Les méthodes d'évaluation développées, l'une à partir d'arbres de défaillance étendus, l'autre concentrée sur l'évaluation de propriétés d'intégrité, permettent de contribuer à l'enjeu de l'analyse de sécurité de systèmes complexes critiques. Elles ont été appliquées aux systèmes de localisation utilisant les GNSS, ceux-ci étant particulièrement intéressants pour la mise en œuvre des concepts opérationnels ferroviaires avancés de contrôle-commande, tels que les cantons mobiles et les cantons virtuels, envisagés pour l'ETCS niveau 3 (cf. section II.1).

Cette mise en œuvre de CCS avancés repose également fortement sur les systèmes de télécommunications permettant l'échange d'informations entre les trains et l'infrastructure. L'évaluation de la sécurité des services fournis par ces systèmes peut ainsi bénéficier des approches proposées, comme démontré dans les travaux que nous avons réalisés dans le cadre du projet Systuf, piloté par Nokia. Des recommandations pour la mise en œuvre d'études de sûreté de fonctionnement liées aux fonctions de communications de véhicules de transport guidé urbain exploités avec un système de contrôle-commande de type CBTC (*Communication Based Train Control*) ont été formulées, et des

travaux analysant les aspects fonctionnels, dysfonctionnels, et critiques du lien sans fil LTE utilisé (*Long Term Evolution* ou 4G) ont été publiés [ACL9, ACTI20]. Ces recherches n'ont pas été poursuivies, pour le moment, en raison d'un manque de temps, notamment pour suivre les évolutions rapides de ces systèmes, telles que les avancées vers la 6G et le cadre ferroviaire FRMCS–*Future Railway Mobile Communication System*.

Au final, les méthodes développées dans cette section contribuent à la démonstration de sécurité de CCS avancés en évaluant les risques techniques pouvant apparaître lors du fonctionnement d'un équipement analysé. Toutefois, l'identification et la caractérisation des scénarios de dangers liés à l'utilisation en exploitation de ces systèmes techniques représentent un autre aspect primordial et difficile de la démonstration de sécurité, surtout lorsqu'il s'agit de considérer l'évolution d'un système complexe dans un environnement d'exploitation aux conditions très variées, tel que l'environnement ferroviaire. La section suivante est dédiée à l'analyse de ces risques opérationnels.

II.4 Analyse des risques opérationnels de CCS avancés

Cette section porte sur l'analyse des risques opérationnels liés à l'utilisation de systèmes complexes critiques intégrant des technologies nouvelles, notamment de localisation et de communication, en mettant en évidence les défis rencontrés lors de l'analyse de leurs scénarios opérationnels dangereux. À travers cette section, je rends compte des travaux de thèse de Ouail Himrane et des travaux de post-doctorat de Rim Saddem, dans lesquels nous nous concentrons sur certaines techniques de vérification formelle. Ces techniques sont capables d'explorer de manière approfondie les divers scénarios opérationnels qu'un système peut rencontrer, et certaines d'entre elles permettent également d'évaluer la probabilité d'occurrence de ces scénarios.

La sous-section II.4.1 explique ce qui caractérise un scénario opérationnel dangereux, et les grandes familles d'analyses de ces scénarios, en particulier les techniques de vérification formelle. Ces techniques sont confrontées à différents défis lorsqu'elles sont appliquées à des systèmes complexes. Après avoir présenté ces défis, des stratégies possibles pour les surmonter sont mises en évidence et intégrées dans une approche générique menant à l'obtention de modèles pour l'analyse de scénarios. De plus, étant donné que les conditions opérationnelles et environnementales variables peuvent avoir une incidence sur certains systèmes, une adaptation de l'approche précédente est présentée pour tenir compte de ces conditions.

Avant de détailler l'approche et son adaptation, la sous-section II.4.2 présente le contexte opérationnel dans lequel elle sera mise en œuvre. Il se réfère aux principes opérationnels prévus pour l'exploitation de lignes ferroviaires à l'aide du système de contrôle-commande ERTMS/ETCS niveau 3, tels qu'ils ont été décrits dans les projets européens auxquels nous avons participé.

La sous-section II.4.3 présente les fondements de l'approche proposée. Elle repose sur un processus générique de modélisation visant à développer des modèles de système vérifiables quant à diverses propriétés de sécurité. Cette vérification s'appuie sur l'ensemble des scénarios issus des modèles. Ce processus prend en considération un ensemble de spécifications qui, dans le contexte de ce mémoire, se rapportent à une sélection de celles existant aujourd'hui pour l'ETCS niveau 3. Ensuite, cette approche est adaptée pour prendre en compte l'influence des conditions opérationnelles ferroviaires changeantes. Cette adaptation est orientée vers la vérification de propriétés liées à l'une des fonctions clés des CCS ayant des impacts en termes de sécurité : la localisation. Comme expliqué à la section II.2, pour permettre à cette fonction d'être réalisée par des équipements techniques embarqués à bord du train, l'utilisation des GNSS est privilégiée. Trois options d'intégration sont envisageables et valables à la fois pour l'ERTMS/ETCS niveau 2 et niveau 3. Parmi ces options, celle basée sur des balises virtuelles est actuellement la plus mature. Par conséquent, ses principes opérationnels seront considérés, ainsi que les incertitudes qui leur sont associées, en particulier celles spécifiques aux GNSS principalement liées à l'environnement.

II.4.1 Caractériser et analyser les scénarios opérationnels dangereux

1) Caractérisation des scénarios

En ingénierie des systèmes, un **scénario opérationnel** est une "*description d'une séquence imaginaire d'événements ou d'activités qui inclut l'interaction d'un produit ou d'un service avec son environnement et ses utilisateurs, ainsi que l'interaction entre les composants du produit ou du service,*

lorsque cela revêt une importance pour l'utilisateur final" [52]. Concrètement, cette description de séquence d'événements ou d'activités permet de détailler les fonctionnalités d'un système ainsi que les interactions attendues entre le système et son environnement, ses utilisateurs et d'autres systèmes, étant donné un "*contexte d'utilisation*". Ce contexte peut comprendre les utilisateurs cibles, les tâches à accomplir, les logiciels et matériels impliqués, ainsi que l'environnement physique et social dans lequel le système évolue. Selon le contexte d'utilisation, les scénarios opérationnels peuvent correspondre aux cas suivants :

- Scénario d'exploitation normale,
- Scénario d'exploitation en mode dégradé,
- Scénario de transition du système entre deux modes (ex. manuel, automatique) ou phases d'exploitation (ex. maintenance),
- Scénario d'initialisation du système,
- Scénario de réponse à l'occurrence d'une situation anormale.

L'analyse des **scénarios opérationnels dangereux** permet d'étudier les réponses sécuritaires d'un système face à des situations dangereuses, notamment les mesures de sécurité prises ou à prendre pour revenir à un état normal, dégradé, ou de blocage du système en sécurité. Ces scénarios, liés à la sécurité, prennent en compte à la fois des aspects fonctionnels et dysfonctionnels, ainsi que l'environnement spécifique dans lequel le système opère et les événements dangereux externes susceptibles de se produire.

Pour contextualiser l'utilisation de scénarios dangereux dans les activités de sécurité du cycle de vie des systèmes critiques (cf. section II.1), la macro-phase d'appréciation des risques initie l'exploration de ces scénarios. Cette analyse exploratoire préliminaire permet d'évaluer les risques potentiels associés à chaque situation dangereuse identifiée et de définir des mesures générales de réduction du risque tenant déjà compte du lieu, du mode et/ou de la phase de fonctionnement du système, ainsi que certaines conditions de fonctionnement (ex. vitesse de véhicules). Ces mesures seront ensuite affinées et suivies de manière traçable tout au long du développement du système. Pendant les activités de vérification de la macro-phase de démonstration de sécurité, une fois que les fonctions attendues du système, notamment celles liées à la sécurité, sont définies et que les choix de conception techniques sont arrêtés, divers scénarios opérationnels détaillés (dangereux ou non) sont testés, soit sur le terrain dans des conditions réelles, soit en simulation. Les résultats de ces scénarios seront finalement utilisés lors de la macro-phase de validation.

2) Types d'analyses

Les scénarios liés à la sécurité sont généralement testés en simulation à partir d'un modèle du système, étant donné qu'il n'est évidemment pas envisageable de provoquer un accident ferroviaire réel. La simulation permet également de répéter un même scénario selon un large éventail de conditions environnementales, y compris les plus rares, ainsi qu'avec différentes valeurs de paramètres liés au système, y compris celles relatives aux limites de fonctionnement du système. L'analyse peut alors être présentée sous la forme d'une analyse de sensibilité permettant de déterminer quelles gammes de conditions ou paramètres font basculer le scénario opérationnel de non dangereux à dangereux.

Pour évaluer des indicateurs prévisionnels de performances ou de sécurité liés à un scénario dangereux spécifique, caractérisé par des conditions environnementales et paramètres de configurations définis, les approches fondées sur la simulation de Monte Carlo se révèlent utiles. Ces approches reposent sur la répétition du même scénario sur la durée de mission du système afin d'évaluer des indicateurs tels que la fréquence d'occurrence d'un événement particulier. Il convient de noter qu'avec les capacités numériques actuelles, les simulations offrent l'avantage de pouvoir être réalisées sur une durée de mission très longue et permettent un grand nombre de répétitions, ce qui contribue à resserrer l'intervalle de confiance des analyses statistiques associées.

3) Recours aux méthodes de vérification formelle

Comme évoqué dans les problématiques générales de ce mémoire (cf. section II.1), prévoir l'ensemble des scénarios dangereux susceptibles de se produire lors de l'utilisation d'un système complexe est illusoire. Toutefois, des techniques existent pour explorer automatiquement l'ensemble des séquences d'événements possibles issues d'un modèle de comportement dynamique. Il s'agit des techniques dites de *Model-Checking* [21], appartenant à la famille des méthodes formelles.

De manière générale, les méthodes formelles sont des techniques reposant sur des fondements mathématiques et logiques pour décrire et analyser rigoureusement le comportement d'un système. Contrairement au langage naturel, ces méthodes établissent une description explicite du système à l'aide de notations spécifiques non ambiguës, telles que celles de langages (comme Z, B, Ada, VHDL, Verilog), de logiques (telles que la logique des prédicats du premier ordre, les logiques temporelles), ou de formalismes (tels que les automates à états finis, les réseaux de Petri, l'algèbre des processus). De telles représentations permettent, d'une part, d'éviter les malentendus et les erreurs résultant des différentes interprétations potentielles d'une même information, ce qui est particulièrement bénéfique pour décrire, spécifier, concevoir et vérifier les systèmes avec un niveau élevé de précision. D'autre part, ces représentations explicites se prêtent à différents traitements automatiques. Les points suivants listent les deux principales catégories d'utilisation des méthodes formelles dans le domaine de la sûreté de fonctionnement, sans entrer dans les détails du vaste domaine scientifique associé aux méthodes formelles :

- Les **approches formelles pour la conception sûre** impliquant l'utilisation de méthodes basées sur différents langages, la plus connue étant la méthode B [14].
- Les **approches de vérification formelles de propriétés**, parmi lesquelles figurent :
  - Les techniques de démonstration de théorème ou *Theorem-Proving* [78],
  - Les techniques de vérification de modèles ou *Model-Checking* [21], qui englobent les techniques classiques basées sur des modèles d'automates à états finis (ou transposables dans ce formalisme, comme c'est le cas des réseaux de Petri ou du formalisme BIP, *Behavior, Interaction, Priority*), ainsi que les techniques basées sur des modèles décrits dans des langages spécifiques (par exemple, en langage B, en Real-Time Maude, en PROMELA).

Les algorithmes de *Model-Checking* (MC) explorent automatiquement l'ensemble de l'espace d'états lié à un modèle formel reflétant le comportement d'un système. Toutes les séquences d'événements sont explorées en fonction de propriétés d'intérêt à vérifier. Ces propriétés, exprimées à travers des logiques spécifiques, peuvent être des propriétés temporelles, des propriétés d'invariant de sécu-

rité (exemple, un évènement redouté ne se produit jamais), des propriétés de vivacité (absence de blocage d'évolution du système), des propriétés de violation d'assertion ou des propriétés d'atteignabilité de certains états. De telles propriétés représentent un comportement correct/incorrect à vérifier. Les algorithmes de MC confrontent la propriété examinée avec le modèle du système. Si la propriété n'est pas satisfaite, l'algorithme fournit une trace de contre-exemple qui démontre un chemin d'événements possible menant à une violation de cette propriété. Une telle possibilité est particulièrement intéressante puisqu'elle permet d'identifier des scénarios risqués pouvant être passés inaperçus lors de l'analyse de risque. La vérification automatisée permet, au final, de réduire le temps et les efforts nécessaires pour analyser de manière exhaustive les scénarios liés à un système.

4) Défis rencontrés

Défi lié à l'explosion combinatoire :

Les approches basées sur l'exploration exhaustive de l'espace d'état souffrent du problème d'explosion combinatoire lorsque la taille de l'espace d'état est grande. C'est en particulier le cas des systèmes complexes puisqu'ils comportent de multiples variables d'état liées par exemple à des valeurs de paramètres temporels ou stochastiques et à des conditions déterministes ou probabilistes de franchissement de seuil, en fonction de l'état des composants ou d'impacts de l'environnement. Des méthodes existent pour réduire la taille de l'espace d'état et éviter une non-convergence des algorithmes de MC lors de la vérification [20]. Citons la représentation symbolique de l'espace d'état, les méthodes de réduction basées sur la symétrie, ou les méthodes de réduction d'ordre partiel. Ces méthodes de réduction font encore l'objet d'investigations aujourd'hui pour rendre la vérification plus efficace et réduire la complexité de l'analyse elle-même.

Lorsque l'exploration exhaustive de l'espace d'état est impossible ou n'est pas nécessaire car des résultats avec une erreur tolérée sont acceptables, la vérification statistique de modèles ou **Statistical Model-Checking** (SMC), introduite dans [42], représente une alternative intéressante au MC classique. Contrairement à ce dernier qui produit un résultat binaire (la propriété est satisfaite ou non), le SMC fournit un résultat quantitatif. En effet, il permet l'évaluation de mesures de performance ainsi que de propriétés probabilistes pouvant être liées à la sécurité. Plus précisément, il permet de déterminer la probabilité que la propriété examinée soit satisfaite par le modèle avec un intervalle de confiance. De même, un intervalle de confiance est associé à une mesure de performance. Les algorithmes de SMC reposent en fait sur les principes de la simulation Monte Carlo.

Bien que le SMC repose sur des simulations pour estimer des probabilités et des mesures de performance, il peut néanmoins être considéré comme une technique formelle. En effet, il utilise des modèles reposant sur des notations mathématiques, tels que les automates stochastiques, pour représenter le comportement d'un système. De plus, il fournit une indication sur l'incertitude des données de sortie, ce qui apporte une caractérisation précieuse en termes de confiance associé au résultat obtenu. Les techniques de SMC fondées sur des simulations sont également considérées comme un compromis entre les techniques de test traditionnelles et la vérification complète d'un modèle [12].

Les techniques de SMC continuent d'évoluer, notamment pour prendre en compte des éléments tels que les boucles de rétro-action trouvées dans le cadre de systèmes cyber-physiques [57]. Malgré leur évolution toujours en cours, ces techniques sont aujourd'hui largement acceptées et la recherche

se concentre davantage sur leurs applications aux systèmes critiques [59, 5], y compris les systèmes de contrôle-commande ferroviaires (des exemples sont décrits dans [16] et [8]). Leur utilisation devient également plus accessible grâce à la disponibilité d'outils intégrant des interfaces graphiques pour la construction de modèles et l'analyse des résultats, tel qu'UPPAAL, ce qui était auparavant principalement réalisé à l'aide de scripts informatiques.

Au final, les techniques de SMC apparaissent particulièrement pertinentes dans le cadre de l'analyse de scénarios opérationnels de systèmes complexes et seront adoptées dans les approches développées par la suite.

Défi lié à l'élaboration de modèles formels :

Pour analyser des scénarios par le biais des techniques de MC, il est primordial de développer des modèles formels 'corrects' et 'fidèles' (voir §II.1.3.3) pour obtenir des résultats fiables et exploitables. Dans le cas des systèmes complexes, développer des modèles tout en garantissant leur exactitude est une tâche qui se révèle ardue. L'activité de modélisation apparaît donc comme un défi qui dépend fortement de l'expertise de l'analyste, à la fois en termes de modélisation et de connaissances 'métier' sur le système.

Pour élaborer un modèle formel reflétant le comportement d'un système complexe, il est préférable de mettre en place une approche de modélisation adoptant les principes suivants :

— Recourir à des **modèles intermédiaires** pour obtenir les modèles formels. Ces modèles intermédiaires sont élaborés à l'aide de formalismes semi-formels plus intuitifs, tels que ceux des diagrammes UML (*Unified Modeling Language*) ou SysML (*Systems Modeling Language*), afin de faciliter les échanges entre les experts métier et les analystes concernant le fonctionnement attendu du système.

— Adopter une **approche modulaire** pour permettre de se concentrer sur le développement d'un module à la fois, c'est-à-dire un sous-modèle représentant une partie spécifique du système, plutôt que sur l'ensemble du système. Chaque module développé peut facilement être affiné et étendu de manière itérative pour intégrer progressivement des détails plus avancés sur le système, sans avoir d'incidence sur les autres modules. La composition des modules s'effectue ensuite en gérant les interfaces entre-eux.

— Favoriser une **approche paramétrable** en développant un modèle générique comportant des paramètres d'entrée ajustables. Cela permet d'analyser différentes configurations d'un même système à partir d'un seul modèle (ou groupe de sous-modèles/modules). Le nombre de composants du système ainsi que certaines caractéristiques de performances peuvent alors être ajustés selon les besoins.

L'application de ces principes de modélisation permet, au final, de répartir l'effort de modélisation lié à la complexité entre plusieurs personnes issues de divers horizons, qu'elles soient du métier ou spécialisées en modélisation. Ces principes seront adoptés dans l'approche développée par la suite.

Avant de détailler cette approche, les principes opérationnels liés à l'ETCS niveau 3 qui serviront de base à son application sont présentés ci-dessous, en mettant en avant l'implication des GNSS pour la fonction de localisation.

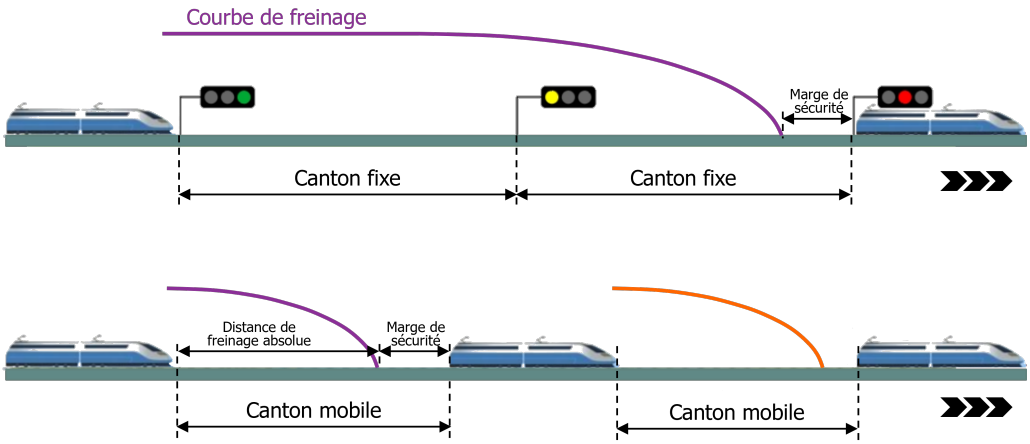


FIGURE II.23 – Des cantons fixes aux cantons mobiles

II.4.2 Modes d'exploitation avancés d'ETCS et implications des GNSS

Comme évoqué dans la section II.1 dédiée au contexte de ces travaux de recherche (cf. § II.1.4.1), la stratégie de migration des systèmes de contrôle/commande et de signalisation des trains vers l'ERTMS, visant à harmoniser progressivement tous les CCS à l'échelle européenne, prévoit trois niveaux d'implémentation. Le concept de "train intelligent" caractérise le dernier niveau dans le sens où les véhicules peuvent exécuter plusieurs fonctions de manière autonome ne nécessitant plus le concours d'équipements d'infrastructure au sol. En particulier, les technologies de localisation satellitaire apportent une réponse efficace et interopérable, étant compactes et utilisables en tout point du globe, pour mettre en œuvre la fonction de 'localisation autonome' de *l'ensemble* du train (de la position avant à la position arrière du véhicule) dans le sous-système bord de l'ETCS niveau 3.

En fournissant les informations de localisation au sous-système sol de l'ETCS, en particulier à un RBC (*Radio Block Center*), via un système de télécommunication de données, les équipements de localisation autonome avec GNSS permettent au RBC de déterminer dynamiquement et au plus juste les distances de sécurité entre les trains, selon le concept opérationnel de canton mobile (introduit au § II.1.4.1 et représenté à la figure II.23), contribuant ainsi à améliorer la capacité du réseau ferroviaire. La mission principale du RBC ne change pas de manière significative par rapport à celle de son premier déploiement dans l'ETCS niveau 2. Le RBC reçoit des informations des trains, surveille l'état de la zone ferroviaire qu'il contrôle et, sur la base de ces informations, génère une autorisation de mouvement (MA, *Movement Authority*) avec des données d'itinéraire et de vitesse.

Dans le niveau 2, la détection des trains sur une zone et l'établissement des itinéraires s'effectuent toutefois par le biais d'un système qui n'est pas encore directement intégré au RBC, à savoir le système d'enclenchement (cf. figure II.7 dans la section II.1). Ce système s'appuie sur des installations fixes de détection de train situées le long des rails, telles que les circuits de voie et les compteurs d'essieux, pour déterminer l'occupation des zones délimitées par des cantons fixes, et ensuite établir des itinéraires sûrs. Ces dispositifs de détection sont coûteux et deviennent superflus dans le niveau 3, étant donné que les informations transmises par l'*ECTS bord* permettent directement à l'*ETCS sol* de déterminer l'occupation des voies. Cela entraîne une réduction de coûts supplémen-

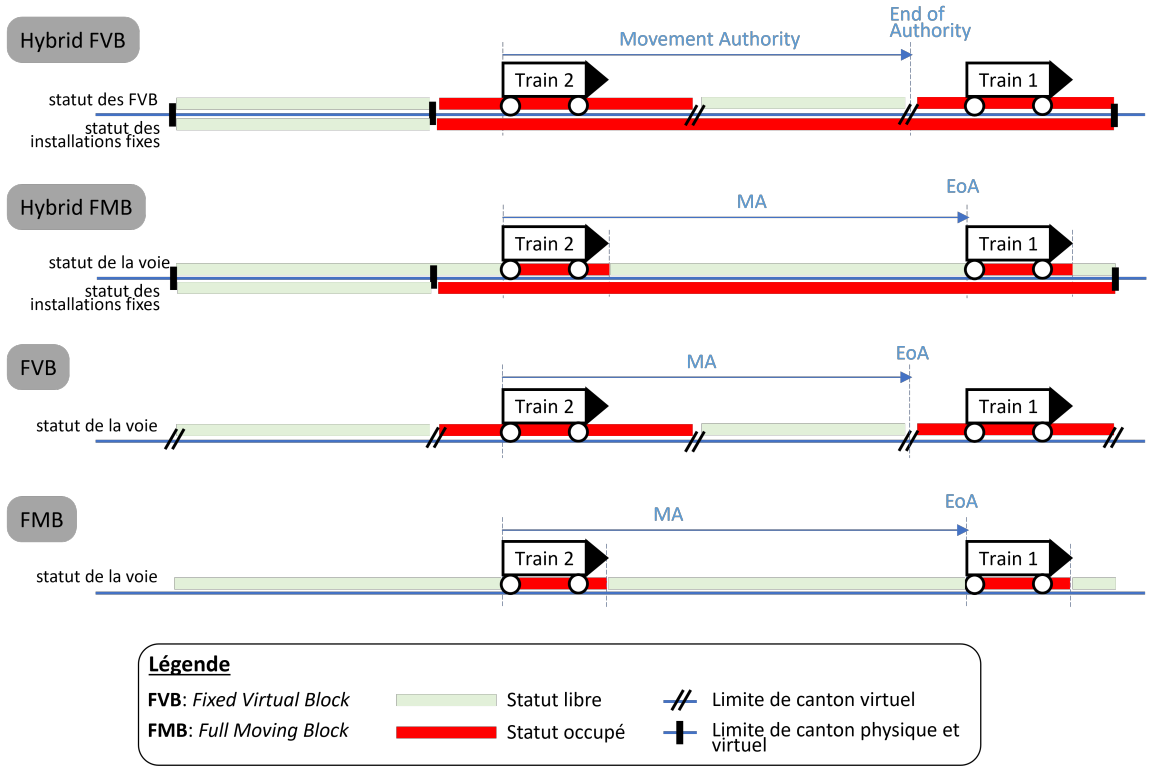


FIGURE II.24 – Exploitation en cantons mobiles selon 4 variants définis pour l'ETCS niveau 3

taire, notamment par rapport aux suppressions possibles de balises physiques sur les voies, rendues également envisageables par l'utilisation des GNSS dans les niveaux 2 et 3, comme expliqué dans la section II.2 au §II.2.2.1.

Cependant, afin de faciliter la transition de l'ETCS niveau 2 vers l'ETCS niveau 3, une phase de circulation mixte, où des trains équipés et non équipés du système bord avec cantons mobiles coexistent, est possible en utilisant des configurations hybrides. Pour assurer le contrôle-commande des trains, l'*ETCS sol* doit alors être en mesure d'utiliser les deux types de fonctionnement : celui avec des cantons fixes en exploitant les installations fixes, et celui avec les cantons mobiles en utilisant les données embarquées transmises. Cette transition, de l'utilisation d'équipements physiques à un fonctionnement numérique, peut ainsi s'effectuer de manière progressive. Il est également possible de combiner le principe de découpage des lignes en cantons fixes avec celui en cantons virtuels pour définir ce que l'on appelle des cantons fixes virtuels. Ces derniers sont des cantons représentés sous une forme logique dans les bases de données de l'*ETCS sol*. Ils permettent une subdivision plus fine d'une ligne ferroviaire par rapport à celle autorisée par les cantons fixes physiques, en découpant la voie en sections plus petites grâce à la manipulation de données numériques. Ainsi quatre variants de l'ETCS niveau 3 ont été définis, comme illustré dans la figure II.24 : FMB (*Full Moving Block*, en cantons mobiles complets), FVB (*Fixed Virtual Block*, en cantons virtuels fixes), *Hybrid* FMB, et *Hybrid* FVB. Cette figure représente également, au travers de zones aux statuts libre ou occupé, les informations d'occupation de voie disponibles pour l'*ETCS sol*.

Le développement de l'ETCS niveau 3 est actuellement en cours selon deux orientations complémentaires. La première, dirigée par les partenaires de *Europe's Rail* (programme européen visant à coordonner et gérer les investissements de recherche et d'innovation dans le domaine ferro-

viaire), se concentre sur le développement des quatre variantes du système avec cantons mobiles. La deuxième, sous la direction du groupe EUG (*ERTMS Users' Group*) [38], se focalise plus spécifiquement sur la variante appelée '*Hybrid FVB*', également connue sous le nom d'ETCS niveau 3 hybride [29], celle-ci étant actuellement la plus mature en termes d'implémentation.

Les travaux de recherche décrits ci-dessous abordent maintenant l'approche axée sur le développement de modèles de système vérifiables selon différentes propriétés de sécurité. L'application de cette approche vise à contribuer à l'analyse des risques pour toutes les variantes de l'ETCS niveau 3. Dans une seconde partie, une adaptation de cette approche prenant en compte des aspects liés au contexte opérationnel ferroviaire est détaillée. Cette approche adaptée a été appliquée à l'analyse des risques opérationnels liés à l'utilisation de balises virtuelles dans le cas de l'ETCS niveau 3 avec FVB.

II.4.3 Approche d'analyse fondée sur la modélisation et la vérification formelle

1) Processus générique applicable à l'ETCS niveau 3

L'approche décrite dans ce paragraphe a été proposée dans le cadre des travaux de post-doctorat de Rim Saddem. Ces travaux ont contribué à structurer les activités de modélisation formelle dans le projet européen PERFORMINGRAIL piloté par l'université de Birmingham. Quatre articles de conférence y sont associés [ACTI1, ACTI3, ACTI4, ACTI5, ACTI6].

Pour répondre au défi posé par l'application des techniques de vérification formelle, notamment la difficulté de modéliser les systèmes complexes et de passer à l'échelle des modèles formels dans des contextes industriels, l'objectif de ces travaux est de définir une méthodologie générique de modélisation et d'analyse formelle pour de tels systèmes fonctionnant dans différentes configurations.

Cette méthodologie permet de fournir des **lignes directrices** pour le développement de modèles semi-formels intermédiaires liés au système examiné, suivis de modèles formels paramétrables, réutilisables, et adaptés aux techniques de vérification formelle automatique. Son objectif est de garantir un fonctionnement conforme du système aux attentes des utilisateurs en mettant en évidence d'éventuelles failles, telles que des erreurs dans les données échangées ou dans le séquencement des réponses fonctionnelles, pouvant avoir un impact critique sur la sécurité du système. L'identification de ces failles permet alors de se concentrer soit sur les corrections pour remédier aux insuffisances fonctionnelles associées, soit sur la mise en place de mesures supplémentaires de réduction du risque dans le système pour faire face aux scénarios dangereux détectés et non identifiés initialement.

L'applicabilité de cette méthodologie a été démontrée par les partenaires du projet PERFORMINGRAIL dans le groupe de travail dédié à la modélisation, au sein duquel nous avons proposé ce cadre méthodologique (WP2). Comme les modèles développés, destinés à l'analyse du fonctionnement de l'ETCS niveau 3, sont trop vastes pour être décrits dans ce mémoire, seuls quelques résultats des étapes de l'approche seront illustrés à la figure II.26 par rapport au cas d'utilisation "perte d'intégrité du train". Cela permet de se concentrer sur les détails de ces étapes, comme présentés ci-dessous. Toutefois, une description complète des modèles élaborés ainsi que différentes vérifications asso-

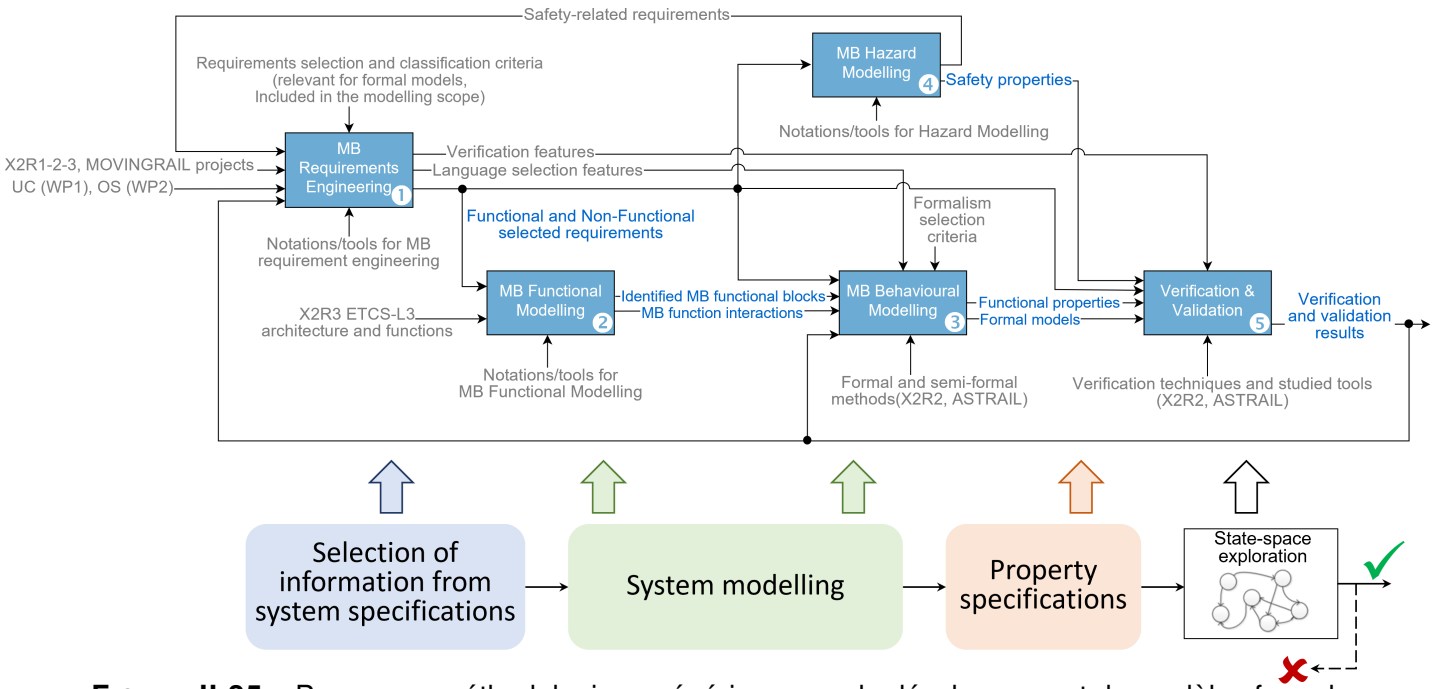


FIGURE II.25 – Processus méthodologique générique pour le développement de modèles formels vérifiables

ciées est fournie dans les rapports suivants : [RPRE7, RPRE1, RPRE3]. De plus, pour entrevoir la complexité du système, l'architecture fonctionnelle fournie à l'annexe 4 illustre les 56 interactions et les 13 fonctions identifiées, sans entrer dans les détails du fonctionnement interne des blocs, lesquels dépendent du type de variant d'ETCS niveau 3 considéré.

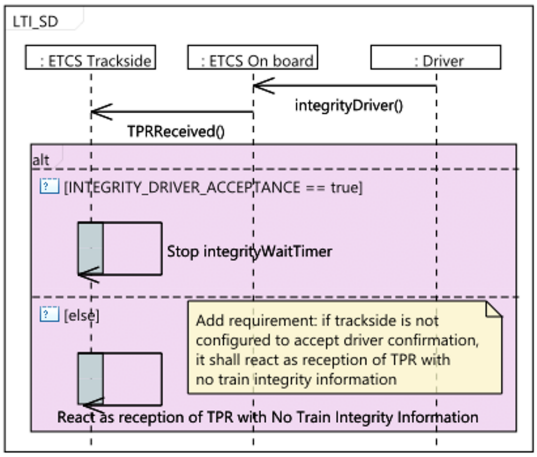
Cette méthodologie correspond à un processus en cinq étapes, représentées par les boîtes bleues de la figure II.25 (en bas de la figure sont indiqués les types d'activités associées aux étapes). Chaque entrée/sortie de ces étapes est associée à des éléments génériques applicables à tout système, ainsi qu'à des éléments concrets tirés de projets récents menés dans le cadre de Shift2Rail entre 2016 et 2023 (X2Rail-1, X2Rail-2, X2Rail-3, MOVINGRAIL, ASTRail). Ces éléments concrets permettent d'illustrer le type d'entrées pouvant alimenter la méthodologie sans tomber dans un cadre trop général et moins explicite. Dans la figure, 'MB' fait référence à *Moving Block* (cantons mobiles), tout comme dans l'acronyme 'MBS' (*Moving Block System*) utilisé pour désigner l'ETCS niveau 3. Les éléments en gras de la figure représentent les résultats de chaque étape du processus. Les cinq étapes sont détaillées comme suit :

— L'étape 1, dénommée **ingénierie des exigences**, vise à identifier et à classer les exigences les plus pertinentes pour le système (par exemple, celles décrivant un comportement, une interaction entre deux éléments, un type de configuration). Elles sont issues de cas d'utilisation (UC) et de scénarios opérationnels (OS) attendus, issus des projets de Shift2Rail évoqués. Les exigences sélectionnées peuvent être illustrées à l'aide de diagrammes d'exigences SysML. Les résultats sont un ensemble de caractéristiques identifiées à prendre en compte dans la méthodologie de modélisation et une liste d'exigences fonctionnelles et non fonctionnelles sélectionnées.

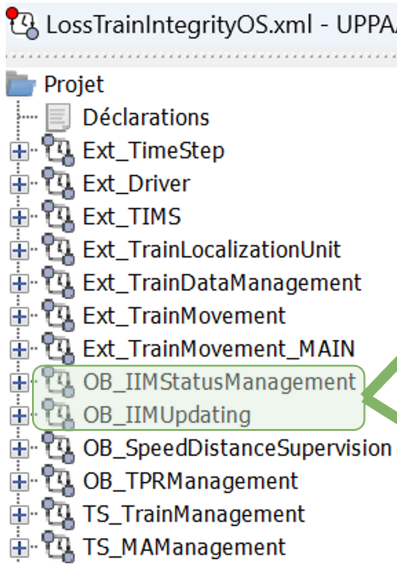
Étape 1) Exigences sélectionnées – Table d'allocation SysML

	id : String [1]	/satisfiedBy : NamedElement [*]	text : String [1]
LossTI-1	REQ-LossTI-1	LTI_TIMS_Integrity_SD	When receiving a position report from a train with the information 'Train integrity lost', the L3 Trackside shall change the Track Status Area associated with this train to Unknown.
LossTI-2	REQ-LossTI-2	LTI_TIMS_Integrity_SD	When the L3 Trackside considers that the integrity is lost for a train, the L3 Trackside shall change the Track Status Area associated with this train to Unknown.
LossTI-3	REQ-LossTI-3	LTI_TIMS_Integrity_SD	When the L3 Trackside considers that the Train Integrity is lost for a train, the L3 Trackside shall react as configured.
LossTI-4	REQ-LossTI-4	LTI_TIMS_Integrity_SD	The L3 Trackside shall consider the Train Integrity as lost when 'No train integrity information' is reported longer than a configurable time (Integrity Wait Timer).
LossTI-5	REQ-LossTI-5	LTI_TIMS_Integrity_SD	When receiving a message from a train with the information 'Train integrity confirmed by external device', the L3 Trackside shall start/restart the Integrity Wait Timer.
LossTI-6	REQ-LossTI-6	LTI_DriverIntegrity_SD	When receiving a message from a train with the information 'Train integrity confirmed by Driver', if the L3 Trackside is configured to accept confirmation by Driver and the Integrity Wait Timer is running, then the L3 Trackside shall stop the Integrity Wait Timer.
LossTI-7	REQ-LossTI-7	LTI_TIMS_Integrity_SD	After a loss of integrity, the driver shall be made aware of the situation via an indication in the cab.
LossTI-8	REQ-LossTI-8	LTI_DriverIntegrity_SD	The L3 Trackside shall be able to be configured whether to accept Train Integrity confirmation by the driver.

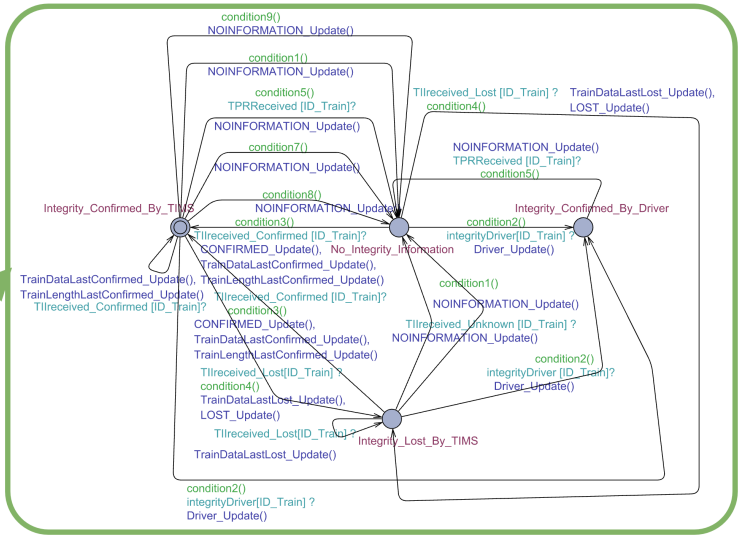
Étape 2) Interactions de haut niveau – Diagramme de séquence SysML



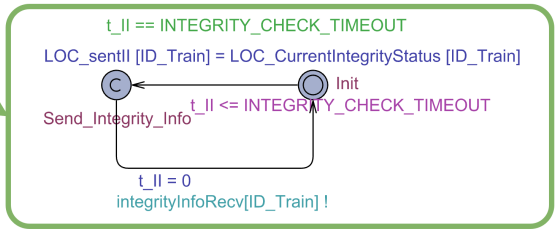
Étape 3) Modèle formel paramétrable (automates)



Détermination du statut d'intégrité (9 conditions)



La MàJ périodique du statut d'intégrité



Étapes 4) et 5)

Exemple de propriétés vérifiables :

- **Atteignabilité de l'état** $Lost\_By\_TIMS$: $E <> IIM\_Process\_A.Lost\_By\_TIMS \;\&\&\; LOC\_AbsTime > 60$
- **Vitesse à laquelle évolue le train dans le temps** : $simulate\ [LOC\_AbsTime <= 300; 1]\{V\_int[0] * 0.1, V\_int[1] * 0.1\}$
- **Vitesse connue par ETCS-Sol** : $simulate[LOC\_AbsTime <= 300; 1]\{(msgTPRReceived[0].positionReport.V\_TRAIN) * 0.1,\ (msgTPRReceived[1].positionReport.V\_TRAIN) * 0.1\}$

Vérification sur le modèle : Vitesse connue par ETCS-Sol

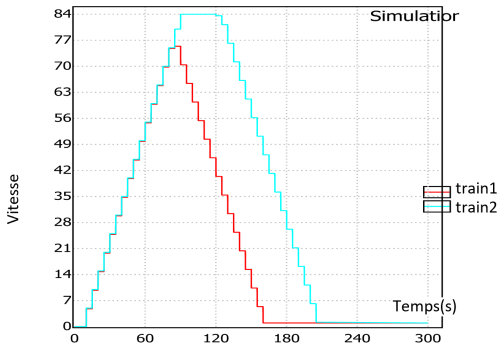


FIGURE II.26 – Illustration de l'approche pour le cas d'utilisation "perte d'intégrité du train"

— L'étape 2, dénommée **modélisation fonctionnelle**, vise à identifier, à partir des exigences sélectionnées, les différentes fonctions du système, ainsi que les interactions entre elles. Il est possible d'utiliser des notations standards semi-formelles telles que, par exemple, le diagramme de classes d'UML / le diagramme de définition de blocs de SysML, et/ou le diagramme de composants d'UML / le diagramme de paquets de SysML, et/ou le diagramme de blocs internes de SysML.

— L'étape 3, dénommée **modélisation comportementale**, vise à développer une bibliothèque de modèles semi-formels et formels pour les différentes fonctions. Dans un premier temps, le comportement des fonctions identifiées et les interactions qu'elles induisent, notamment celles liées aux équipements et composants techniques utilisés pour réaliser ces fonctions, sont modélisés à l'aide de notations graphiques semi-formelles. Par exemple, les machines d'état SysML peuvent être employées pour modéliser le comportement des fonctions, tandis que les diagrammes de séquence SysML peuvent servir à représenter les interactions fonctionnelles. Basés sur ces modèles semi-formels, les modèles formels sont ensuite développés pour prendre en compte des aspects difficiles à considérer d'emblée ensemble lors de la modélisation d'un système complexe. Ces aspects, qui sont progressivement identifiés à travers les notations graphiques semi-formelles et précisés avec les notations formelles, comprennent : les aspects temporels, probabilistes, déterministes, séquentiels, concurrents, de dépendances, les structures de données échangées, et les paramètres de fonctionnement. Afin de rendre ces modèles formels réutilisables et ainsi limiter les efforts de modélisation pour les différentes configurations du système identifiées, ils sont conçus pour être paramétrables en fonction des configurations, ainsi que des caractéristiques de performance du système.
  Deux formalismes issus du domaine des systèmes dynamiques à évènements discrets, permettant d'élaborer des modèles formels qui intègrent les différents aspects mentionnés, ont été identifiés : les **automates stochastiques temporisés**, implémentables à l'aide de l'outil UPPAAL [22], et les **réseaux d'activités stochastiques** (SAN, *Stochastic Activity Networks*), implémentables à l'aide de l'outil Möbius [90]. Ces formalismes présentent des caractéristiques de modularité et de paramétrisation, permettant la composition de sous-modèles et la configuration du système.
  Cette étape vise également à spécifier les propriétés à vérifier qui peuvent être classées dans les catégories qui suivent, les performances étant une catégorie à part qui résulte de simulations à partir des modèles :
  - **Propriétés logiques**, ce sont des assertions faites sur les variables du système et qui doivent être respectées par le système (par exemple, un invariant, des pré/post-conditions, l'atteignabilité d'un état),
  - **Propriétés fonctionnelles**, ce sont des propriétés du système directement dérivées de ses exigences fonctionnelles,
  - **Performances**, elles se réfèrent à des critères tels que la capacité de la ligne ferroviaire, les intervalles d'attente.

— L'étape 4, dénommée **modélisation des situations dangereuses**, vise à modéliser les dangers liés au système identifiés en phase initiale d'appréciation des risques. Cette étape vise également à spécifier les propriétés de sécurité à vérifier, c'est-à-dire les conditions de danger / de sécurité (exemple, les trains sont suffisamment espacés dans tous les cas) ou l'état des mécanismes de protection garantissent un fonctionnement opérationnel sûr.
— L'étape 5, dénommée **vérification et de validation**, vise à vérifier et à valider les modèles formels produits par rapport aux propriétés déterminées. Les modèles formels liés au système sont instanciés avec différentes valeurs de leurs paramètres pour pouvoir vérifier les propriétés non pas sur les modèles génériques mais sur des modèles concrets.

Les travaux ci-dessous adaptent l'approche présentée en détaillant comment intégrer l'influence du contexte opérationnel ferroviaire sur l'évolution du système de contrôle-commande.

2) Approche adaptée à l'influence du contexte opérationnel

L'approche et son application liée à l'utilisation des technologies GNSS sont issues de la thèse de Ouail Himrane [43]. Un article de revue y est associé [ACL3], ainsi que trois articles de conférence [ACTN4, ACTI11, ACTI8]. Les modèles issus de ces travaux de thèse ont pu être valorisés dans le cadre du projet européen PERFORMINGRAIL.

Ces travaux se concentrent d'une part sur l'adaptation de l'étape 1 (ingénierie des exigences) et de l'étape 3 (modélisation comportementale d'un système complexe) de l'approche précédemment décrite. L'objectif est d'élargir le champ de modélisation de cette approche au-delà du comportement interne des fonctions du système et de leurs interactions entre elles, en prenant spécifiquement en compte les aspects opérationnels ferroviaires susceptibles d'affecter à la fois les fonctions et les technologies spécifiques qui les mettent en œuvre.

Des lignes directrices de modélisation additionnelles sont formulées pour intégrer ces aspects opérationnels, en mettant l'accent sur leur application à la fonction de localisation des CCS ferroviaires. Des modèles que nous avons spécifiquement développés pour l'utilisation de balises virtuelles basées sur les GNSS sont employés pour obtenir des résultats d'analyse par vérification formelle. Ces résultats contribuent à démontrer non seulement des propriétés de sécurité, mais aussi des objectifs de performance spécifiques.

Lignes directrices pour le développement de modèles intégrant les aspects opérationnels :

La figure II.27 illustre les éléments ajoutés au processus représenté à la figure II.25. Les mêmes codes couleur sont utilisés dans les deux figures : bleu ciel pour les descriptions et spécifications liées au système, vert pour la modélisation du système, et orange pour la spécification des propriétés à vérifier. Les éléments ajoutés à l'étape 1 (caractérisation de l'environnement dans le rectangle bleu) et à l'étape 3 (impact de la situation opérationnelle dans le rectangle vert) du processus générique sont respectivement les suivants :

— **Informations pour caractériser l'environnement ferroviaire** : Cela implique d'identifier toutes les informations pertinentes exprimant les conditions liées à l'environnement issues des spécifications du systèmes, formulées par des experts ou issues de la littérature scientifique. Ces informations, tout comme les exigences systèmes, seront utilisées comme entrées

des étapes de modélisation fonctionnelle et comportementale. Plus particulièrement, en ce qui concerne la fonction de localisation, il est nécessaire de préciser les conditions de réception dans l'environnement ferroviaire. En effet, comme expliqué dans la section II.3 au §II.3.1.1, ces conditions ont un impact direct sur l'utilisation des GNSS permettant l'implémentation de cette fonction.

— **Rendre les modèles paramétrables en fonction de différentes situations opérationnelles, en plus du paramétrage lié à la configuration du système**. Cela permet de tenir compte, dans la modélisation, des impacts variables de divers aspects opérationnels sur le comportement du système. Deux types d'aspects opérationnels sont considérés :

- **Les aspects liés à l'évolution d'un train**. La position relative des trains les uns par rapport aux autres impacte l'état de certaines fonctions du système, rendant ainsi nécessaire la modélisation de leur mouvement. En effet, certaines conditions liées aux systèmes, en particulier les conditions de sécurité, dépendent des variables de mouvement, telles que la position et la vitesse. Ces variables à leur tour dépendent de paramètres liés aux trains, tels que leurs coefficients d'accélération ou de freinage.
- **La variabilité des conditions environnementales**. L'impact de l'environnement ferroviaire sur la fonction de localisation se traduit par l'apparition d'erreurs additionnelles dans les positions estimées. L'*écart maximum possible* entre positions estimées et position réelles, qualifié d'incertitude, est une variable qui doit être prise en compte dans les modèles comportementaux à des fins d'évaluation de sécurité. Cette variable regroupe plusieurs sources d'incertitudes dont celles liées à l'utilisation d'équipement avec GNSS. Toutefois, les erreurs imputées à ces équipements varient selon le types d'architecture technique choisie, certaines solutions ayant plus de capacité que d'autres à réduire les incertitudes. Afin de garantir l'applicabilité de l'approche à toute solution technique et sa réutilisabilité, la solution avec GNSS est considérée comme une boite noire caractérisée uniquement par des paramètres de performances.

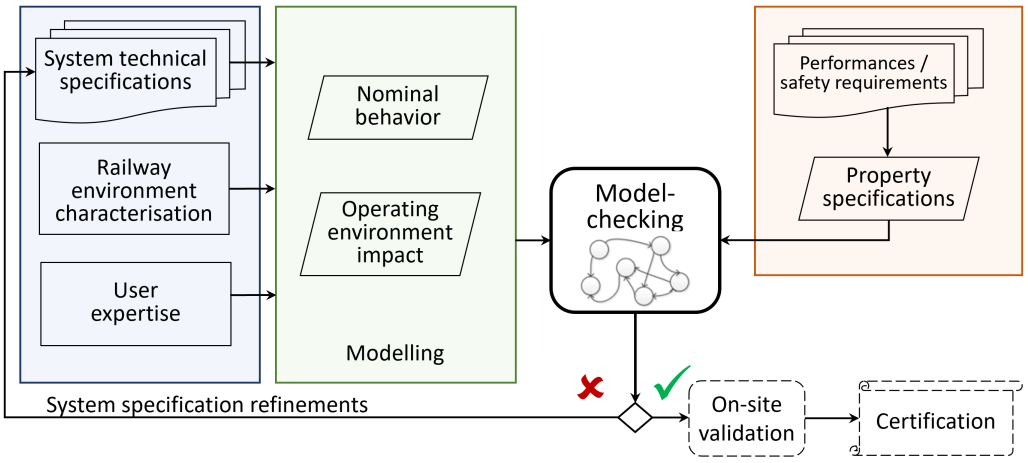


FIGURE II.27 – Adaptation de l'approche avec des conditions opérationnelles et environnementales variables

Les lignes directrices de l'approche adaptée avec la prise en compte des aspects opérationnels, sont appliquées pour analyser la fonction de localisation de l'ETCS niveau 3 basée sur l'utilisation de balises virtuelles, comme présenté dans notre papier [ACL3]. Une synthèse de cette application est faite ci-dessous, en précisant, au préalable, plusieurs principes opérationnels liés à l'utilisation de balises virtuelles. Ces principes, associés à quelques détails techniques importants, constituent un résumé des spécifications utilisées dans les modèles développés.

Comme expliqué à la section II.2 au §II.2.2.1, l'idée derrière l'utilisation de balises virtuelles (VB, *Virtual Balises*) est d'émuler le comportement des balises physique (PB, *Physical Balises*) sans recours à des dispositifs matériels. En général, les balises physiques sont placées aux limites des cantons (*blocks*). Lorsque les cantons sont des cantons fixes virtuels (les FVB, cf. §II.4.2), la ligne ferroviaire est virtuellement subdivisée en sections plus courtes sur lesquelles des VB peuvent être placées, comme illustré à la figure II.28. À noter, toutefois, que PB et VB co-existeront lors de la migration progressive de CCS existants vers l'ETCS niveau 3 avec l'utilisation de VB, d'où la modélisation également des PB par la suite.

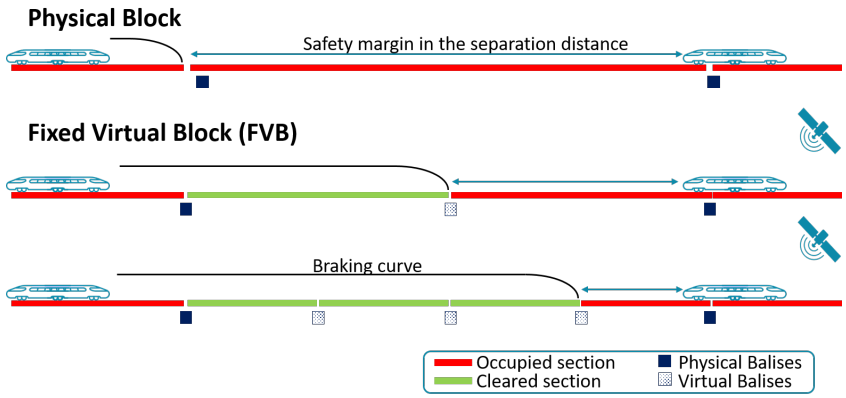


FIGURE II.28 – Exemple d'implantation de balises au sein d'*ETCS Sol*

Chaque VB correspond à une position de référence stockée dans l'*ETCS bord* [66]. Depuis un équipement de localisation intégrant une technologie indépendant de l'odométrie, ici le GNSS, l'*ETCS bord* récupère des estimations de position du train dans la zone où il s'attend à rencontrer une balise virtuelle ; cette zone est appelé "fenêtre d'anticipation" (*expectation window*) dans les spécifications de l'ERTMS [93]. Ainsi, lorsque la distance parcourue estimée à bord par l'odométrie (y compris les incertitudes associées, jusqu'à un maximum de 5% de la distance parcourue par le train) atteint cette fenêtre d'anticipation, l'*ETCS bord* vérifie en permanence si la position estimée par l'équipement GNSS correspond à la position de la VB. Dès que cette correspondance est constatée, la VB est *activée* émulant l'activation d'une PB. La position de la VB et son erreur associée sont utilisées pour réajuster l'erreur d'odométrie. Pour cela, un niveau de protection (PL, *Protection Level*), c'est-à-dire l'erreur maximale garantie par un mécanisme de surveillance lié à l'équipement GNSS (cf. section II.3 au §II.3.3.1), est associé à la position issue de l'équipement au moment de l'activation de la VB. Ce PL correspond à l'"*erreur résiduelle maximale*" liée à l'emplacement de la VB. Il est garanti, par définition, avec un niveau de confiance fixé et exprimé sous la forme d'une probabilité (par exemple, $Integrity\_Risk = 10^{-5}$).

La valeur de l'erreur résiduelle maximale dans le cas de la PB est fixe et limitée à 5 mètres [94]. En revanche, la valeur de l'erreur résiduelle liée à l'activation de la VB est inconnue et limitée par le PL, qui peut dépasser 5 mètres. De plus, le PL peut varier d'une balise à une autre, et d'un passage sur la balise à un autre, en fonction de plusieurs paramètres principalement liés à l'environnement d'exploitation. Par conséquent, comme il n'est pas possible de prédire avec certitude la valeur du PL qui sera utilisée pour réajuster la distance parcourue fournie par l'odométrie, une variable d'incertitude apparaît.

Application des lignes directrices à la fonction de localisation

— **Informations pour caractériser l'environnement ferroviaire** : Dans la littérature, la plupart des travaux à ce sujet sont principalement basés sur des campagnes de mesure pour évaluer, dans un contexte opérationnel donné, les performances des solutions avec GNSS en termes de précision, disponibilité, continuité, et intégrité de la localisation (cf. II.3.3). Cependant, comme discuté dans le projet ASTRail qui a précédé le projet PERFORMINGRAIL, plusieurs classes d'environnement peuvent être distinguées : l'environnement ouvert (*Open Sky*) où tous les satellites sont visibles au niveau utilisateur sans perturbation de leur signaux, l'environnement urbain, caractérisé par une visibilité partielle ou indirecte des satellites avec des perturbations de leurs signaux, et l'environnement restreint où la visibilité des satellites est inexistante, comme dans un tunnel.
Ainsi, un train se déplaçant sur un itinéraire traverse différentes classes d'environnement, qui peuvent être pré-déterminées par les campagnes de mesures. Ces classes sont considérées comme ayant des impacts différents en termes d'incertitudes sur la localisation. Ce changement de classe d'environnement selon la section de voie parcourue constitue une entrée pour la partie modélisation. Un état spécifique dans le modèle doit être réservé par train pour la classe d'environnement active.

— **Différents types de paramètres opérationnels identifiés** : Les paramètres considérés pour modéliser la dynamique du train sont mentionnés dans la figure II.29. En ce qui concerne l'impact des conditions environnementales, il est observé par les incertitudes introduites par l'usage des GNSS dans les VB. Ainsi, la variation du nombre de VB par rapport au nombre de PB, des distances entre balises (PB et/ou VB), ainsi que des paramètres de distribution de probabilité caractérisant le niveau de protection (PL) associé à une VB (dans une classe d'environnement donnée), traduisent la variabilité des conditions environnementales (cf. figure II.29).

— **Modélisation** : Associés au module mettant à jour les variables liées à la dynamique du train, plusieurs modules paramétrables ont été développés avec l'outil UPPAAL pour représenter les différents mécanismes créant de l'incertitude. Les principaux modules se rapportent à l'activation d'une VB, l'activation d'une PB et l'évolution de l'incertitude au niveau de l'odométrie. Seule l'évolution continue de l'erreur de position *maximale* autorisée est considérée pour chaque mécanisme, comme un point de vue axé sur la sécurité est adopté. Ainsi, une incertitude globale sur la position d'un train peut être analysée à l'aide de ces modèles, en prenant en compte les différentes sources d'incertitudes identifiées.

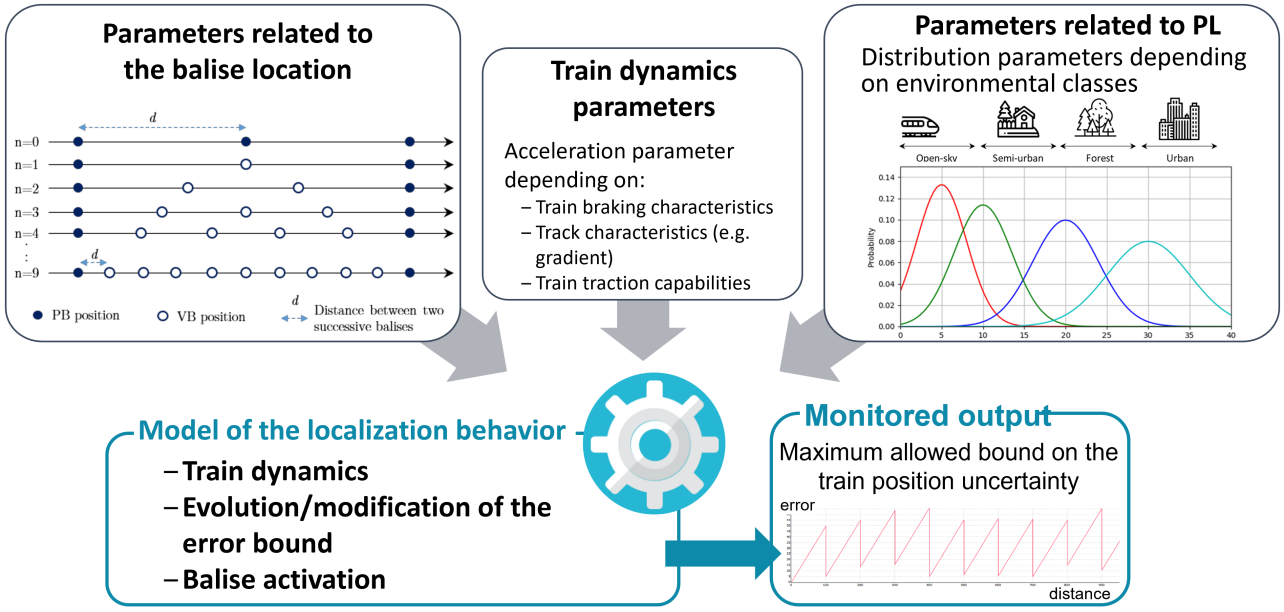
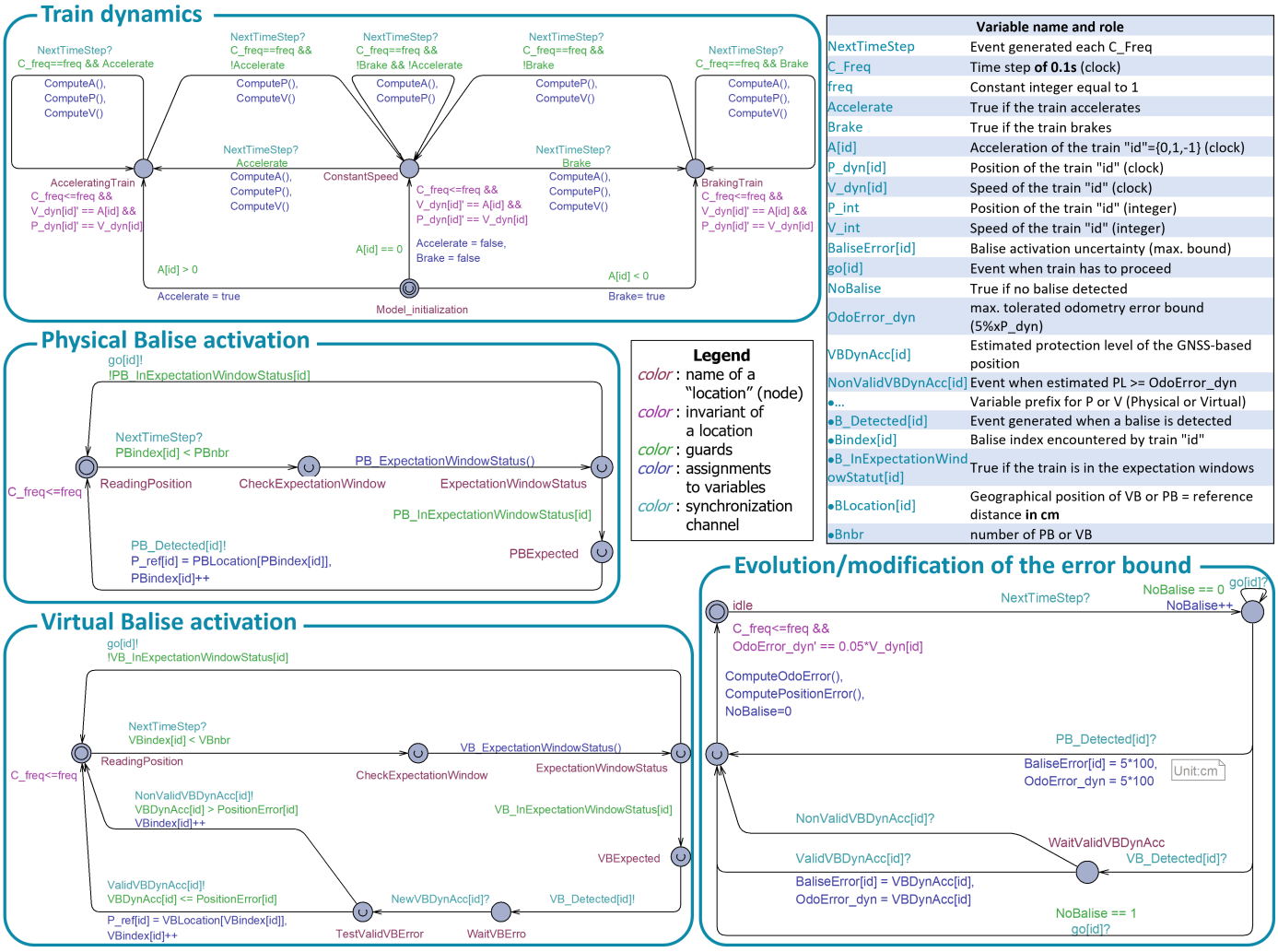


FIGURE II.29 – Paramètres opérationnels identifiés



Variable name and role	
NextTimeStep	Event generated each C_Freq
C_Freq	Time step **of 0.1s** (clock)
freq	Constant integer equal to 1
Accelerate	True if the train accelerates
Brake	True if the train brakes
A[id]	Acceleration of the train "id"={0,1,-1} (clock)
P_dyn[id]	Position of the train "id" (clock)
V_dyn[id]	Speed of the train "id" (clock)
P_int	Position of the train "id" (integer)
V_int	Speed of the train "id" (integer)
BaliseError[id]	Balise activation uncertainty (max. bound)
go[id]	Event when train has to proceed
NoBalise	True if no balise detected
OdoError_dyn	max. tolerated odometry error bound (5%xP_dyn)
VBDynAcc[id]	Estimated protection level of the GNSS-based position
NonValidVBDynAcc[id]	Event when estimated PL >= OdoError_dyn
•...	Variable prefix for P or V (Physical or Virtual)
•B_Detected[id]	Event generated when a balise is detected
•Bindex[id]	Balise index encountered by train "id"
•B_InExpectationWindowStatut[id]	True if the train is in the expectation windows
•BLocation[id]	Geographical position of VB or PB = reference distance **in cm**
•Bnbr	number of PB or VB

FIGURE II.30 – Principaux modules développés pour modéliser la fonction de localisation

L'instanciation de chaque module avec des valeurs de paramètres permet ainsi d'obtenir un modèle global pour la fonction de localisation attendue dans l'ETCS niveau 3. Ce modèle est spécifique à un train donné dans une classe d'environnement particulière. La prise en compte de plusieurs classes d'environnement est possible, comme expliqué dans notre article [ACTI11]. De plus, l'article [ACTI8] aborde l'utilisation de distributions de probabilité caractérisant l'incertitude de position liée à PL. Ces distributions dépendent de la classe d'environnement et peuvent être adaptées en fonction de l'avancée des recherches de la communauté GNSS sur ce sujet. La sous-section ci-dessous détaille les résultats d'analyses effectuées avec ce modèle.

3) Résultats d'analyse par vérification formelle

Dans cette sous-section, des propriétés de sécurité et de performance sont analysées sur la base du modèle obtenu précédemment. Pour cela, les fonctions de vérification de l'outil UPPAAL SMC (*Statistical Model-Checking*) sont utilisées et un cas d'étude est considéré.

Type de propriété de sécurité analysée :

Nous analysons la probabilité que l'incertitude globale sur la position d'un train dépasse un certain seuil pendant son trajet, en prenant en compte un agencement spécifique des PB et VB sur la voie, ainsi que des classes d'environnement données. Cette propriété de sécurité, liée au *risque que le train se trouve en dehors de sa zone d'autorisation de mouvement*, est exprimée ci-dessous sous la forme d'une formule logique temporelle pouvant être vérifiée par l'algorithme de Model-Checking.

$$Pr\ [<= bound\ ]\ (<>\ Allowed\_Position\_Error > threshold) \tag{II.15}$$

Sachant que :

- $bound$ correspond au temps limite considéré dans la simulation,
- $Allowed\_Position\_Error$ est l'amplitude de l'erreur de position autorisée pour chaque train,
- $threshold$ est la valeur limite d'erreur autorisée (par exemple, $105\ m$),
- $<>$ correspond à l'opérateur temporel *eventually* (occurrence d'une condition dans un état futur indéterminé)

Des résultats sont obtenus pour différentes valeurs du paramètre de simulation $threshold$, puis agrégés sous la forme d'une courbe représentant la probabilité de satisfaction de cette propriété (avec un intervalle de confiance associé).

Description du cas d'étude

Pour quantifier les valeurs de probabilité associées à la propriété ci-dessus, c'est-à-dire pour quantifier le risque précédemment évoqué, nous considérons une ligne ferroviaire exploitée à l'aide de l'ERTMS niveau 3 fonctionnant avec des cantons fixes virtuels (notée L3-FVB). Ce risque, lié au franchissement d'une limite sécuritaire, dépend à la fois de l'agencement des PB/VB et de l'incertitude associée à chaque VB. D'une part, l'agencement des PB/VB est caractérisé par des paramètres opérationnels qui, comme mentionné précédemment, incluent le rapport entre le nombre de PB et de VB, ainsi que la distance entre balises. Ce sont des paramètres de configuration de la ligne liés à la fois à l'emplacement des balises, mais aussi à la taille des FVB, compte tenu de l'hypothèse d'une seule balise par FVB. D'autre part, l'incertitude associée à chaque VB est associée à une valeur de PL caractérisée par une distribution de probabilité liée à une classe d'environnement spécifique.

Avec l'hypothèse qu'une seule classe d'environnement est associée à l'ensemble de la ligne L3-FVB, il est alors possible d'analyser l'influence des paramètres de configuration sur le risque en effectuant une analyse de sensibilité. De cette dernière peuvent être dérivés :

— Le rapport optimal entre le nombre de PB nécessaires et celui de VB, ceci afin de réduire le nombre de PB. Cela se réfère à la **performance de coût**, traduisant les dépenses d'installation et d'entretien liées aux équipements physiques.

— La distance possible entre les balises, et par extension, la taille des FVB (avec l'hypothèse d'une balise par canton). Cela se réfère à la **performance de capacité de la ligne**, sachant que, globalement, plus les cantons sont petits, plus le nombre de trains sur la ligne augmente, en accord avec le principe de sécurité opérationnelle classique selon lequel un canton fixe ne peut être occupé que par un seul train.

Ce rapport optimal et cette distance entre balises peuvent alors être déterminés grâce à l'exploitation du modèle par Model-Checking, tout en respectant à la fois les spécifications et les conditions de sécurité pour maintenir un profil de risque acceptable.

La performance de capacité peut être comparée par rapport à celle obtenue en considérant une ligne exploitée sous ERTMS niveau 2 équipée de PB. Elle est exprimée ici en termes de taille de cantons. Dans ce cas d'étude, nous considérons des PB séparées de manière équidistante de 2 kilomètres, ce qui correspond à une taille moyenne de cantons fixes généralement évoquée par les experts ferroviaires (bien que sur une ligne réelle, cela puisse varier d'un canton à l'autre). Cette configuration implique, en accord avec les spécifications existantes sur l'ERTMS niveau 2, que l'incertitude globale sur la position du train varie entre $5\ m$ (immédiatement après l'activation d'une PB) et $105\ m$ ($5 + 5\% \cdot d$ avec $d = 2000\ m$, juste avant l'activation d'une autre PB). Dans le cas d'étude, ces deux valeurs sont constantes étant donné des cantons de taille identique considérés.

Nous considérons, comme autre hypothèse, que les trains circulent à la même vitesse sur les lignes L2 et L3-FVB du cas d'étude, et possèdent les mêmes caractéristiques dynamiques (le modèle gérant la variation des paramètres dynamiques du train n'est donc pas pris en compte ici mais a été étudié dans [ACTI8]). Pour la ligne L3-FVB analysée, nous choisissons arbitrairement d'utiliser 10% de PB sur l'ensemble des balises.

L'analyse ci-dessous porte, au final, sur la quantification de la propriété de sécurité définie précédemment, en tenant compte d'un motif de configuration de balises répété *(1PB - 9VB)*, et également, en considérant une même classe d'environnement. Trois réglages possibles sont utilisés pour les distributions de probabilité relatives à PL liées à l'activation des VB.

Résultats d'analyse et discussion :

Avant d'exposer les résultats, quelques notations nécessaires à leur explication sont introduites. Dans le cadre du modèle présenté précédemment, l'incertitude globale sur la position du train, représentant l'erreur de position autorisée pour un train ($Allowed\_Position\_Error$), est modélisée de façon à respecter la formule dans l'encadré ci-dessous. Cette formule inclut deux termes : l'un est une variable représentant l'erreur résiduelle maximale après l'activation d'une balise ($Max\_Balise\_Activation\_Error$), tandis que l'autre est une variable représentant l'erreur accumulée

d'odométrie ($5\% \times distance\_from\_the\_last\_reference\_position$). La première variable dépend du PL associé aux VB, tandis que la seconde atteint sa valeur maximale juste avant l'activation d'une balise (PB ou VB), ce point d'activation marquant la fin d'un canton.

$$Allowed\_Position\_Error = Max\_Balise\_Activation\_Error + 5\% \times distance\_from\_the\_last\_reference\_position$$

La variation de $Allowed\_Position\_Error$ peut alors être examinée en détails, en tenant compte uniquement dans un premier temps de la variation de l'erreur résiduelle maximale associée à l'activation des balises (variable $Max\_Balise\_Activation\_Error$), grâce à la vérification formelle de la propriété exprimée à l'équation II.15. Cette propriété est traduite en une requête dans UPPAAL SMC.

Pour chaque valeur de $threshold$ (par exemple, de 1 à 35 mètres), l'algorithme SMC traite la requête correspondante et estime la probabilité que la variable $Max\_Balise\_Activation\_Error$ dépasse une valeur de $threshold$. Les résultats obtenus pour les différentes valeurs de seuil sont illustrés à la figure II.31, où les courbes oranges représentent spécifiquement les valeurs obtenues pour la variable $Max\_Balise\_Activation\_Error$. Les courbes violettes représentent un décalage des courbes oranges pour tenir compte d'une erreur d'odométrie maximale supplémentaire associée, par exemple, à des cantons de 2 kilomètres. La signification des rectangles rouges est expliquée ci-dessous.

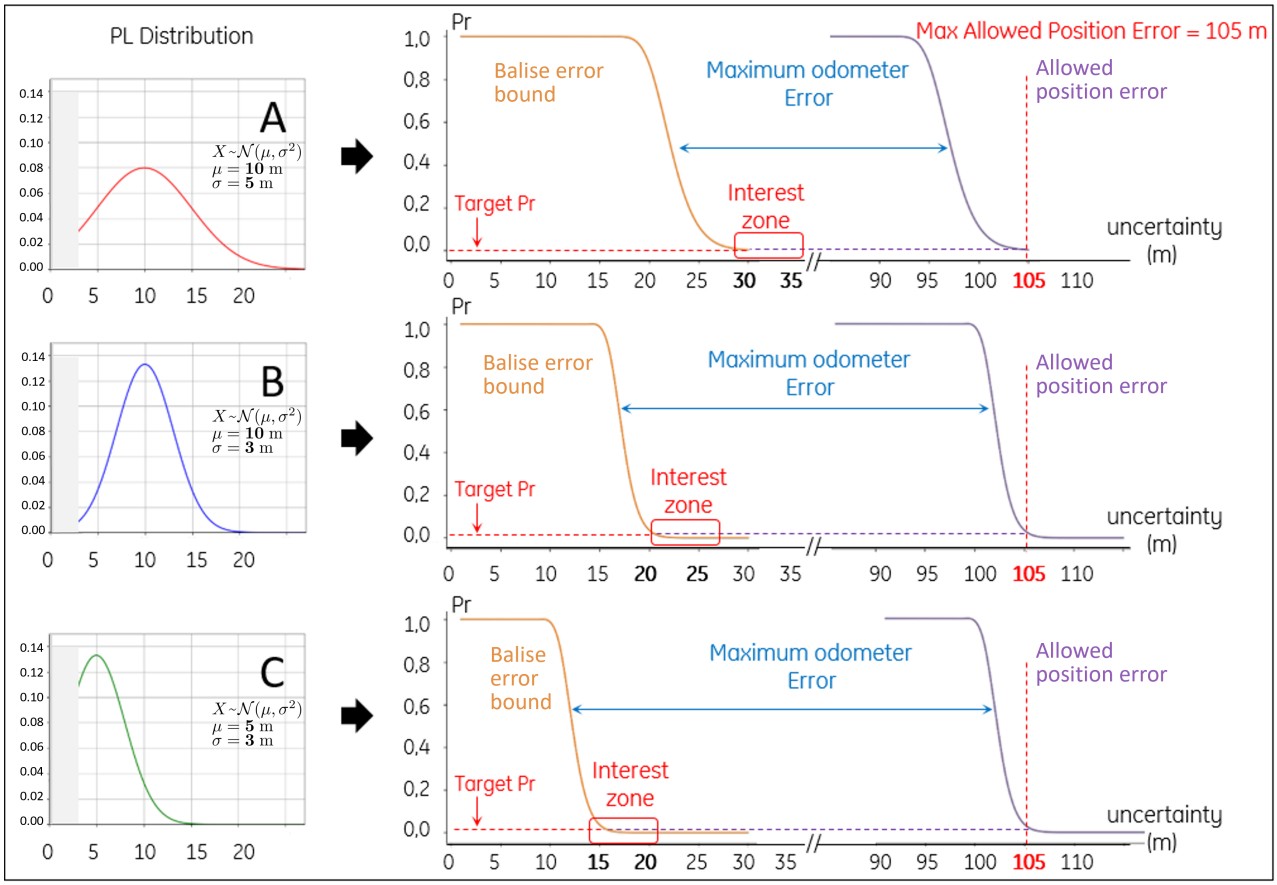


FIGURE II.31 – Résultats de l'algorithme SMC pour 3 distributions de PL : probabilités Pr obtenues pour différentes valeurs d'erreur résiduelle maximale associée à l'activation des balises

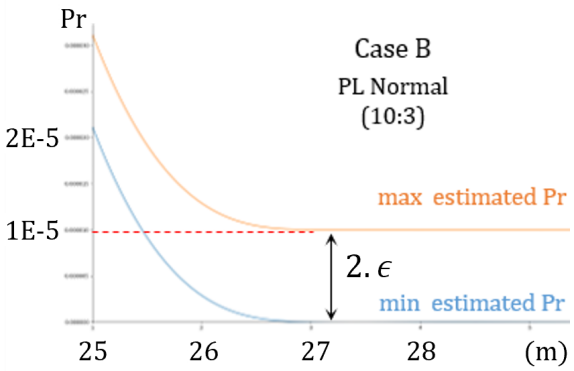


FIGURE II.32 – Zone d'intérêt pour PL~$\mathcal{N}(10,3)$ avec $\alpha = 10^{-5}$ et $\varepsilon = 5 \cdot 10^{-6}$

Distribution PL *mean* (m) : *std* (m)	$Max\_Balise\_Activation\_Error$ (m)	d'_{max} (m)	PB rate L3 vs. L2
Distrib. A (10,5)	37	1360	14,7 %
Distrib. B (10,3)	27	1560	12,8 %
Distrib. C (5,3)	22.5	1650	12 %

TABLE II.7 – Résultats d'erreur maximale d'activation de VB, de distance maximale entre balises, et pourcentage de PB L3/PB L2 en fonction de PL

Soit $TargetPr$ représentant le risque associé à PL, c'est-à-dire le fait que l'erreur résiduelle maximale associée à l'activation d'une VB ait été sous-estimée. L'estimation de ce risque peut être effectuée par l'algorithme SMC avec un certain niveau de confiance. Supposons que le risque que l'erreur résiduelle dépasse PL soit inférieur à 10^{-5} avec un niveau de confiance de $0,99999$. Des zones d'intérêt particulières sont alors identifiées sur la figure II.31 autour de la probabilité 10^{-5} (les rectangles rouges). Une exploration approfondie est alors réalisée dans ces zones avec l'outil de SMC, en réglant les paramètres de l'outil suivants : $\alpha = 1 - 0,99999$ (probabilité de faux négatifs) et $2 \cdot \varepsilon = 10^{-5}$ (incertitude sur la probabilité). Par exemple, la zone d'intérêt liée à un PL suivant une loi normale $\mathcal{N}(10,3)$ (distribution 'B') est agrandie dans la figure II.32. Les autres distributions de PL sont traitées de la même manière.

Après avoir obtenu les valeurs de $Max\_Balise\_Activation\_Error$, la deuxième partie de l'analyse se concentre sur l'incertitude globale sur la position du train pour déterminer la distance maximale entre balises, et par conséquent la taille d'un FVB. Si d' représente l'erreur d'odométrie accumulée depuis la dernière balise rencontrée par le train, d'_{max} représente l'erreur maximum accumulée au point marquant la fin d'un canton. Chaque canton étant considéré comme ayant une longueur fixe identique, d'_{max} est obtenu comme suit :

$$Max\_Allowed\_Position\_Error = Max\_Balise\_Activation\_Error + 5\% \times d'_{max}$$
$$\Rightarrow d'_{max} = \frac{1}{5\%} \times (Max\_Allowed\_Position\_Error - Max\_Balise\_Activation\_Error) \quad \text{(II.16)}$$

Les résultats obtenus pour les différentes distributions de PL sont présentés dans le tableau II.7. La dernière colonne du tableau présente le nombre de PB nécessaires à la ligne L3-FVB par rapport à celui utilisé dans la ligne de référence L2. On constate une réduction significative du nombre de PB de plus de 85% dans les trois cas étudiés. De plus, étant donné que les longueurs des FVB (d'_{max}) sont inférieures à la longueur des cantons fixes de la ligne de référence L2 de référence $(2\ km)$, la capacité de la ligne est augmentée. Il convient de noter que ces valeurs d'_{max} représentent la distance *maximale* séparant des balises successives. Par conséquent, la distance réelle de séparation

des balises à adopter peut être inférieure à la valeur d'_{max} calculée. En particulier, l'augmentation du nombre de balises est particulièrement importante puisque 90% des balises sont virtuelles. Par conséquent, l'accumulation d'erreurs d'odométrie est moindre et il est possible d'obtenir des FVB encore plus courts, ce qui permet d'augmenter encore la capacité de la ligne. Néanmoins, une limite physique à l'augmentation de la capacité de la ligne est liée aux capacités de freinage des trains exploités.

Enfin, il convient de noter qu'un raisonnement analogue peut être adopté pour étudier différents tracés de lignes et distributions de PL, de manière à déterminer le rapport coût/bénéfice optimal, tout en gardant la maîtrise sur les risques associés.

II.4.4 Conclusion

Des travaux visant à évaluer des propriétés de sécurité de CCS avancés à partir de modèles formels de comportement ont été présentés dans cette section. Pour surmonter les difficultés rencontrées lors de la modélisation de systèmes complexes, une approche d'analyse générique menant à des modèles formels de CCS avancés a été proposée et a ensuite été adaptée pour prendre en compte les conditions opérationnelles entraînant des incertitudes dans les données des modèles. Les modules correspondants sont conçus pour être paramétrables, ce qui permet d'étudier divers scénarios opérationnels couvrant une large variété de configurations.

Cette capacité d'analyse est particulièrement intéressante pour évaluer l'impact de différentes conditions environnementales sur les performances des GNSS pouvant être utilisés dans l'ETCS niveau 3. Des résultats d'analyse obtenus dans le cadre de l'ETCS niveau 3 hybride, basés sur des modèles développés, sont discutés. Nous montrons comment les modèles peuvent être avantageusement réutilisés pour étudier différents agencements de balises virtuelles sur une ligne ferroviaire, ces balises facilitant la réalisation de la localisation dans l'ETCS niveau 3 hybride à partir de GNSS. De plus, les évaluations obtenues prennent en compte les incertitudes sur la localisation par satellites et garantissent (par Model-Checking statistique) que les configurations testées sont sécuritaires et conformes aux spécifications.

Les évolutions possibles de ces travaux sont discutées dans les perspectives de ce mémoire. Des réflexions ont déjà conduit à plusieurs échanges avec des experts dans le cadre de la chaire "Sécurité des Systèmes Ferroviaires" et ces discussions s'alignent avec le démarrage de travaux d'une nouvelle thèse dès la rentrée universitaire 2024-2025.

CONCLUSION

Depuis 2007, mes activités de recherche ont été motivées par ma volonté de contribuer au développement des transports ferroviaires, en accordant une attention particulière à la sûreté de fonctionnement de leurs systèmes critiques. La démonstration de la sécurité des systèmes complexes constitue une problématique de recherche générale et ardue au sein de la communauté de l'ingénierie de la sécurité, que j'ai explorée tout au long de mon parcours en me concentrant sur les systèmes de contrôle-commande ferroviaire. Poursuivre des recherches dédiées à cette problématique a été un objectif que j'ai pu atteindre en accédant, en 2011, au poste de chercheure que j'occupe aujourd'hui, après avoir été chercheure contractuelle. C'est au cours de ce premier poste que j'ai identifié et commencé à m'attaquer aux défis liés à l'intégration sécuritaire de nouvelles technologies sans fil de localisation et de communication dans les systèmes critiques ferroviaires. Ces défis, qui ont été et demeurent le moteur de mes travaux, restent d'actualité avec les réflexions sur l'évolution des systèmes de contrôle-commande, notamment en ce qui concerne l'application de principes opérationnels novateurs exploitant ces technologies, tels que celui fondé sur les cantons mobiles.

Les approches originales présentées dans la partie II de ce mémoire ont été développées en tenant compte du cadre réglementaire européen de la sécurité ferroviaire. Elles visent à soutenir les activités de sécurité liées aux différentes phases du processus de développement d'un système critique, tout en prenant en compte la complexité et les propriétés spécifiques des technologies sans fil. De plus, les méthodologies ont été conçues pour être également applicables aux systèmes critiques complexes rencontrés dans d'autres secteurs que le ferroviaire. Ces méthodologies ont été valorisées dans différents projets nationaux et européens, comme indiqué au cours du mémoire.

La section II.1 a d'abord permis de synthétiser l'enchaînement des différentes activités liées à la démonstration de sécurité et de mettre en lumière leurs problématiques dans le cadre des systèmes complexes. Ces activités sont regroupées en quatre macro-phases, servant de fil directeur au mémoire : *1)* l'appréciation des risques pour l'allocation d'exigences de sécurité, *2)* la démonstration de sécurité intégrant à la fois des aspects techniques et opérationnels, *3)* la vérification et la validation du respect des exigences de sécurité, et *4)* le suivi des performances de sécurité en exploitation. Nos travaux ont particulièrement contribué aux deux premières macro-phases, la troisième s'appuyant sur les résultats des deux premières et la quatrième sur des indicateurs opérationnels pertinents dérivés du travail de démonstration de la sécurité.

Dans la section II.2 consacrée à la première macro-phase, j'ai présenté en détail une méthodologie générique proposée pour l'allocation de SIL aux fonctions de sécurité. Cette méthodologie a été développée dans le cadre des travaux post-doctoraux de Kiswendsida Abel Ouedraogo et d'un projet mené en collaboration avec l'autorité nationale de sécurité ferroviaire, l'EPSF. Son élaboration a permis de confronter différentes techniques d'allocation existantes issues de plusieurs secteurs d'activités critiques. Elle a également permis de mettre en lumière des utilisations incorrectes du concept

de SIL, principalement le fait de considérer un SIL autrement que d'un point de vue fonctionnel et de l'associer uniquement à des propriétés quantitatives de fiabilité. Cette démarche permet au final d'articuler les dangers, les objectifs de sécurité liés à chaque danger, les fonctions de sécurité (ou fonctions relatives à la sécurité), et les SIL. Elle ne repose pas uniquement sur la répartition quantitative d'un objectif en termes de poids de risques supporté par chaque fonction, mais également sur des considérations qualitatives intégrant des règles d'implémentation techniques. L'application de cette méthodologie et de ses principes s'est avérée efficace lors de leur utilisation dans plusieurs projets européens.

Après avoir identifié, formalisé et intégré dans la méthodologie les règles implicitement employées dans le domaine ferroviaire pour l'allocation des niveaux d'intégrité de sécurité (SIL), nous avons également cherché à faire évoluer la méthodologie en tenant compte de l'imprécision dans les allocations. En particulier, cette adaptation de la méthode permet de considérer les cas où l'utilisation d'une valeur fixe pour un objectif de sécurité lié à un danger ou une fonction, peut créer une contrainte forte de conception pour l'équipement réalisant la fonction, contrainte qui pourrait ne pas être satisfaite et alors mener à un objectif inatteignable. Nous avons exposé comment prendre en compte cette imprécision pour relâcher cette contrainte tout en s'assurant que les poids de risques distribués permettent de respecter un objectif initial lié au danger. Ainsi, les principes de l'approche d'allocation précédente ont été étendus pour allouer des objectifs de sécurité quantitatifs imprécis à certaines fonctions de sécurité, notamment celles impliquées dans la localisation des trains lorsque des équipements basés sur le GNSS sont utilisés (Global Navigation Satellite Systems). Par conséquent, cette approche étendue permet de tenir compte des incertitudes associées à l'apparition de dangers dus à des défaillances de l'équipement GNSS.

Pour affiner l'allocation d'objectifs fonctionnels à un niveau plus détaillé, notamment lors de l'intégration d'un équipement de localisation satellitaire dans l'architecture du système européen de contrôle des trains (ETCS), une approche capable de gérer l'incertitude paramétrique a été proposée. Cette méthode d'allocation permettant de décliner des objectifs de sûreté de fonctionnement du niveau fonctionnel au niveau composants a été proposée dans le cadre des travaux post-doctoraux de Thi Phuong Khanh Nguyen.

Dans les sections II.3 et II.4 consacrées à la deuxième macro-phase, les approches développées concernent à la fois l'analyse des risques techniques et opérationnels associés aux systèmes avancés de contrôle-commande ferroviaire, incluant des technologies sans fil de localisation et de communication. La section II.3 a permis d'exposer nos travaux sur la caractérisation et l'évaluation de l'occurrence des états risqués d'un système technique au comportement dynamique, notamment dans le cas où un état risqué peut être non observable mais avoir des conséquences néfastes. Les méthodes d'évaluation développées – l'une à partir d'arbres de défaillance étendus, proposée dans le cadre des travaux de post-doctoraux de Thi Phuong Khanh Nguyen, l'autre centrée sur l'évaluation de propriétés d'intégrité, proposée dans le cadre de la thèse de Cyril Legrand – ont contribué à l'enjeu de l'analyse des risques techniques de systèmes complexes critiques. Elles ont été appliquées aux systèmes de localisation utilisant les GNSS.

Au-delà de la considération de ce domaine applicatif, l'approche d'évaluation basée sur des arbres de défaillance étendus permet d'appréhender les situations de pannes multiples de faible probabilité d'occurrence. La seconde approche d'évaluation illustre, d'une part, des étapes utiles pour identifier des situations dangereuses impliquant la persistance d'événements critiques dans le temps. D'autre part, en se référant et en s'appuyant sur des techniques existantes d'évaluation de critères de performance propres aux technologies analysées, cette approche démontre qu'il est possible de réaliser des évaluations sans recourir nécessairement à l'utilisation de modèles dont l'élaboration est délicate. Toutefois, ce parti pris n'est plus possible lorsque l'évaluation porte non plus seulement sur l'équipement technique mais aussi sur ses interactions avec le contexte opérationnel.

Étendre le contexte d'analyse au système ferroviaire global permet d'investiguer les scénarios dangereux, éléments clés de l'analyse des risques opérationnels, objet de la section II.4. Pour cela, les travaux menés dans le cadre du post-doctorat de Rim Saddem ont conduit au développement d'une approche formelle de modélisation et de vérification capable d'analyser les séquences d'événements risqués liés à l'utilisation de systèmes critiques complexes. Une version étendue de cette approche, proposée dans le cadre de la thèse de Ouail Himrane, a permis la prise en compte de conditions opérationnelles variables. Cette extension, mise en œuvre en modélisant un ensemble de spécifications relatives au système de contrôle-commande ETCS niveau 3 intégrant le GNSS, a suscité dernièrement l'intérêt de plusieurs départements de recherche et d'innovation industriels du secteur ferroviaire, notamment dans le cadre de la chaire "Sécurité des Systèmes ferroviaires", pour approfondir ses bases et son utilisation.

Pour finir, les résultats des activités de sécurité (appelés preuves de sécurité) intervenant à des phases spécifiques du cycle de vie d'un nouveau système ferroviaire, les processus et méthodes permettant de les obtenir, ainsi que l'argumentaire expliquant en quoi ces résultats démontrent la satisfaction des exigences et objectifs de sécurité, constituent les éléments clés examinés pour la certification du système avant sa mise en service. Par conséquent, la certification de systèmes complexes ne peut être obtenue qu'à l'issue d'un long processus d'ingénierie, comprenant plusieurs étapes de synthèse documentaire résumant les conclusions en termes de sécurité à chaque phase. Cela justifie, au-delà des travaux de recherche entrepris pour la sécurité des systèmes critiques, la durée parfois de plusieurs années entre la définition et la mise en service d'un système ferroviaire. C'est le prix indispensable de l'assurance sécurité des systèmes critiques.

PERSPECTIVES

Les travaux développés dans ce mémoire ouvrent plusieurs perspectives applicatives et méthodologiques en matière de recherche en ingénierie de la sécurité pour les systèmes critiques de contrôle-commande ferroviaire. Elles sont axées, d'une part, sur la continuité des travaux concernant l'utilisation sûre des technologies sans fil pour assurer des fonctionnalités avancées liées à la circulation des trains et, d'autre part, sur la sécurité des trains autonomes. La première section décrit le contexte menant aux perspectives que j'envisage de suivre, tandis que les deux sections suivantes présentent les pistes de recherche que j'ai identifiées pour approfondir ces aspects.

Contexte applicatif et méthodologique

Les perspectives de recherche en ingénierie de la sécurité pour les systèmes critiques de contrôle-commande ferroviaire sont nombreuses, en raison de la volonté de mettre en œuvre de manière sûre des concepts opérationnels performants visant à augmenter l'offre et la compétitivité du transport ferroviaire. Nos travaux présentés dans ce mémoire, ont mis en avant les concepts de cantons mobiles et virtuels. Avec l'essor accru des recherches sur la mobilité autonome, particulièrement dans le secteur automobile, la conduite autonome des trains est également envisagée pour répondre aux besoins actuels d'optimisation des réseaux de transport ferroviaire et d'amélioration des services de mobilité.

En effet, les nouvelles technologies de l'information, de la communication et du traitement des données ont atteint un niveau de développement tel qu'elles rendent désormais possible l'émergence de solutions embarquées avancées pour la conduite autonome. Ces solutions, dont certaines reposent sur l'intelligence artificielle, visent à analyser et évaluer diverses situations opérationnelles, qu'elles soient ordinaires ou dangereuses. Elles visent également à prendre des décisions complexes dans un environnement ouvert (c'est-à-dire non maîtrisé en conception) et à intervenir automatiquement face aux risques potentiels, sans action humaine, à la fois pour percevoir le contexte opérationnel et réagir en conséquence. À moyen et long termes, mon intention est de me concentrer sur la sécurité des trains autonomes et sur l'établissement d'un cadre d'assurance sécurité adapté à ces systèmes, compte tenu de mon expertise et de mon positionnement dans les domaines de la sécurité ferroviaire et de l'ingénierie de la sûreté de fonctionnement. En particulier, les risques potentiels liés à l'incertitude et à l'interprétation des données issues des différents capteurs de mouvement et de perception des véhicules autonomes, ainsi que les interactions de ces véhicules avec leur environnement, sont difficiles à caractériser. Ce cadre applicatif est compatible avec l'évolution de mes recherches actuelles sur la sécurité des technologies de localisation et de communication utilisées dans les systèmes de contrôle-commande ferroviaire, tout en abordant la question de l'analyse des problèmes opérationnels associés à l'introduction de l'autonomie dans les trains et leur gestion en sécurité.

D'un point de vue méthodologique, il me paraît également judicieux d'explorer et d'enrichir un type d'approches jugées comme prometteuses par la communauté d'ingénierie de la sécurité pour la gestion de la complexité : les "approches d'évaluation de la sécurité basées sur des modèles" ou approches MBSA (*Model-Based Safety Assessment*). En effet, en réutilisant dans les analyses de sécurité les artefacts de modélisation développés pour l'aide à la conception d'un système, les approches MBSA permettent de faciliter, voire d'optimiser l'analyse de sécurité du système complexe examiné. L'analyste de sécurité se concentre alors plus spécifiquement sur les comportements dysfonctionnels pour construire les modèles d'analyses soit par injection de fautes dans le modèle de conception, soit par extension du modèle, soit en se référant aux détails d'architecture de ce modèle pour construire un modèle de sécurité dédié [97].
Pour cela, ces approches comportent *a minima* les quatre activités principales suivantes :

1. Modéliser les défaillances des composants, leur facteurs de causalité et leur propagation dans le système,
2. S'appuyer sur des algorithmes de traitement permettant l'automatisation des analyses de sécurité et reposant sur des langages de modélisation capables d'intégrer des comportements dysfonctionnels,
3. Assurer la cohérence, jusqu'au niveau de détail de l'architecture et des composants du système, entre les modèles utilisés pour la conception (issus par exemple d'approches de type MBSE, *Model-Based Systems Engineering*, ou MDE *Model-Driven Engineering*) et les modèles utilisés pour l'analyse de sécurité,
4. Démontrer que les risques pour la sécurité dus aux défaillances des composants restent acceptables.

Les efforts de modélisation en conception peuvent alors être mis à contribution pour atteindre à la fois les objectifs complémentaires de la conception et de la sécurité : d'une part, assurer une construction correcte d'un système pour qu'il réponde aux besoins des utilisateurs, et d'autre part, garantir que le fonctionnement opérationnel du système en exploitation ne génère pas de risque inacceptable.

Dans un but d'efficacité d'analyse de sécurité vis-à-vis de comportements complexes, j'envisage le développement d'une approche MBSA explorant les spécificités techniques et contextuelles des technologies sans fil de localisation et de communication présentées dans ce mémoire. Cela permet une réflexion sur la prise en compte, dans ces méthodes, de conditions environnementales et de comportements dynamiques, tout en apportant une méthodologie dont peut bénéficier le domaine ferroviaire. Ces aspects méthodologiques, examinés à échéance proche, sont abordés ci-dessous avant l'évolution des activités de sécurité pour les systèmes de conduite autonome à plus long terme.

Évolution des approches MBSA pour considérer les défauts des technologies sans fil

Les travaux présentés dans ce mémoire ont éclairé et formalisé différents aspects fonctionnels et dysfonctionnels liés à la fonction de localisation des trains utilisant les technologies satellitaires, en particulier les conditions environnementales ferroviaires liées à ces technologies. L'évolution de ces conditions est intimement liée au mouvement d'un train, pour lequel différents modèles ont été

fournis et construits de façon à être paramétrables selon l'approche générique présentée à la section II.4. Suite à ces travaux, je souhaite investiguer l'intégration de modèles représentant l'évolution dynamique du contexte opérationnel, comme ceux évoqués, dans une approche MBSA. La thèse de Araaf Dinullah Recta, qui démarrera à l'automne 2024 en collaboration avec l'équipe MOFED (Modèles et Formalismes à Évènements Discret) du LIS de l'Université d'Aix-Marseille, donne l'occasion d'explorer cette piste.

De manière plus générale, les comportements dysfonctionnels liés aux liens sans fil peuvent être intégrés dans les modèles. Des aspects dysfonctionnels liés à l'utilisation de balises virtuelles ou d'unités de localisation multi-capteurs avec GNSS ont été décrits et représentés à l'aide des notations classiques d'arbres de défaillances dans les sections II.2 et II.3) ; et d'autres travaux que nous avons menés et qui ne sont pas présentés dans ce mémoire ont également formalisé certaines erreurs liées à des systèmes de communication utilisés en contrôle-commande [ACTI20, RPRE11]. De plus, dans les sections II.3 et II.4, des types d'évaluations ont été proposés en lien avec des situations dangereuses. Les travaux futurs pourront se référer à nos travaux actuels et aux perspectives évoquées dans les travaux de thèses de Cyril Legrand et Ouail Himrane (voir ci-dessous). Ils pourront également s'appuyer sur l'expertise des communautés associées pour inclure les dernières avancées dans ces technologies sans fil. Citons en particulier mes liens avec les collègues de Railenium, du LEOST et du CRIStAL, ainsi qu'avec les partenaires des projets européens, tels que SAFESAT4X, projet proposé cette année (incluant notamment la participation du DLR allemand et du CEIT espagnol).

Les perspectives issues des travaux des thèses évoquées se résument comme suit :

— Modélisation et analyse de conditions fonctionnelles supplémentaires, telles que la non-activation d'une ou plusieurs balises virtuelles, et de conditions opérationnelles dégradées, telles que l'occurrence de comportements non-nominaux associés à l'estimation du niveau de protection (*PL*) et du risque sur l'intégrité d'une position GNSS, source de situations qualifiées de *Hazardous Misleading Information* dans le domaine du GNSS.
— Établissement de règles d'ingénierie sur les marges de sécurité associées aux distances entre trains, compte tenu de l'analyse des impacts liés aux conditions précédentes et des discussions issues des projets européens X2Rail-x.
— Analyse d'impact et évaluation comparative, en termes de FDMS, de solutions de *Fault Detection and Exclusion* en tant que barrière de sécurité liée à la fonction de localisation, en s'appuyant sur la formalisation de liens entre les critères FDMS et performances de disponibilité, continuité, précision et intégrité de la localisation, dans la continuité des évaluations croisées entreprises dans nos travaux.
— Évaluation probabiliste de scénarios dangereux incluant la fonction de localisation, les délais de communication sol-bord et les temps de réponse, ainsi que l'identification des événements initiateurs de ces scénarios dans le cadre de l'utilisation des principes opérationnels avancés de cantons mobiles et de couplage virtuel des trains.

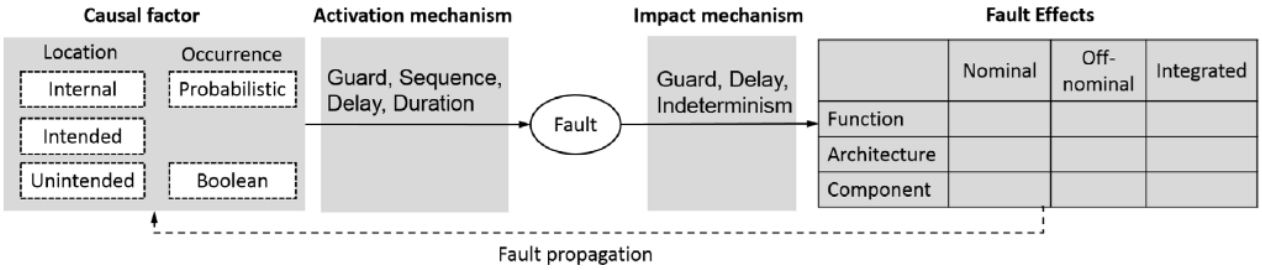


FIGURE II.33 – Schéma générique pour caractériser l'activation et les impacts des pannes d'un composant (*fault model pattern*) [97]

Il est important de noter que les approches MBSA utilisent des langages de modélisation (exemple, AltaRica, Hip-HOPS *Hierarchically Performed Hazard Origin and Propagation Studies*), voire des notations formelles, s'appuient sur des schémas génériques de pannes, et emploient des techniques de traitement automatique des modèles (ex. *Model-Checking*) pour réaliser les analyses, et par la même occasion, repérer les incomplétudes, incohérences ou erreurs dans les modèles.

Pour les technologies sans fil qui sous-tendent le fonctionnement des CCS ferroviaires avancés, les échanges de flux d'informations peuvent être perturbés en complément des problèmes matériels possibles. Étendre et enrichir les structures génériques de pannes existantes, telles que celle présentée à la figure II.33 est envisageable. Tout comme la possibilité de paramétrer les modules modélisant séparément différentes parties d'un système, une structure générique pourrait être paramétrée pour considérer différents types de défauts. La manière de considérer la structure étendue dans les modèles et les traitements automatiques associés aux approches MBSA est ensuite à investiguer.

Évolution des activités de sécurité pour les systèmes de conduite autonome

Les travaux de thèse de Mohammed Chelouati [18], soutenus en juin 2024 et contribuant à l'assurance de la sécurité des trains autonomes, ont permis de préciser et d'apporter des réponses à plusieurs verrous scientifiques associés à la démonstration de sécurité des systèmes de conduite autonome intégrés dans les trains. De manière générale, les défis spécifiques à la sécurité du train autonome sont liés principalement au transfert de tâches et de responsabilités du conducteur vers les automatismes, à la transition entre les modes de conduite et la gestion des modes dégradés, ainsi qu'à l'introduction de l'intelligence artificielle dans ces systèmes.

J'ai choisi de ne pas détailler ces travaux de thèse dans ce mémoire d'HDR afin de suivre le fil directeur retenu pour la période 2007-2024, lequel permet de présenter mes différentes contributions aux activités de sécurité des systèmes critiques ferroviaires qui assurent des fonctionnalités avancées de contrôle-commande par le biais de systèmes sans fil. Toutefois, ce chapitre de perspectives offre l'occasion de mettre en avant les éléments nécessitant un approfondissement à partir des réflexions que nous avons menées et des trois approches développées durant la thèse de Mohammed Chelouati :

— Une approche pour la structuration de l'argumentation de sécurité des trains autonomes à partir de notations GSN (*Goal Structuring Notation*) [ACL2, ACTN2],
— Une méthodologie modélisant la conscience de la situation (*situational awareness*) du système de conduite autonome du train (ADS, *Autonomous Driving System*) intégrant une analyse de risque dynamique [ACTI2],
— Une approche de prise de décision orientée risques et fondée sur la mise en œuvre de POMDP (*Partially Observable Markov Decision Processes*) [ACL1, ACTN1].

Les éléments d'approfondissement sont présentés ci-dessous selon deux axes qui permettent de poursuivre de récents travaux de recherche et de proposer de nouvelles pistes. Les aspects exploratoires suggérés ouvrent la voie à de riches travaux futurs et collaborations, tant en matière méthodologique qu'en appui aux organismes réglementaires et de certification. Les collaborations scientifiques en cours (notamment avec Railenium) et prévues (notamment avec le laboratoire Heudyasic de l'Université de Technologie de Compiègne, avec le centre allemand de recherche sur le transport ferroviaire DZSF) mobiliseront des compétences complémentaires. Enfin, des formations en lien avec ces sujets, seront possibles dans le cadre de la Chaire "Sécurité des Systèmes Ferroviaires".

Évolution du processus d'appréciation des risques

Les travaux visés permettant d'identifier et d'évaluer les dangers liés au train autonome comprennent :

— L'adaptation du processus d'appréciation des risques à chacun des quatre degrés d'autonomie des trains autonomes (de GoA1 à GoA4 – *Grades of Automation*). Pour cela, un cadre d'assurance sécurité au niveau système est proposé avec plusieurs collègues de l'équipe sécurité d'ESTAS et de Railenium pour analyser les nouveaux dangers en fonction du niveau d'analyse et du degré d'autonomie. Ce cadre méthodologique est élaboré de manière à pouvoir être précisé au niveau composants du train autonome, en particulier pour ceux à base d'intelligence artificielle (IA). L'intention est de continuer à approfondir l'approche sur la base des travaux effectués [ACLN1, ACTI7, ACTI9].

  Le premier niveau d'analyse proposé dans ce cadre est le niveau système. Celui-ci inclut la spécification de l'environnement opérationnel sur lequel les activités de conception s'appuient. Cet environnement est nommé "domaine opérationnel de conception" (ODD, *Operational Design Domain*). Les scénarios de conduite du système sont fondés sur l'ensemble des évènements susceptibles de survenir dans l'ODD. Cette spécification d'ODD, qui s'avère délicate et importante pour la sécurité, permet de définir le périmètre à considérer pour l'appréciation des risques ainsi que pour toutes les activités d'assurance sécurité, en particulier en ce qui concerne les composants à base d'IA du train autonome. Je ne souhaite pas investiguer l'évaluation de fonctions de sécurité intégrant de l'IA, étant donné que d'autres collègues de l'équipe approfondissent ce sujet, notamment avec des techniques de vérification formelles [11]. Nous collaborons toutefois au sein d'un groupe interne pour partager nos avancées et les résultats

en cours, qui pourront notamment être considérés au niveau système, celui sur lequel je me positionne. Une problématique prioritaire à aborder, à ce niveau, porte alors sur la preuve que la définition d'ODD est complète et cohérente, cela conditionne l'argumentation de sécurité [102].

— La spécification de mesures de sécurité permettant d'assurer que le niveau de sécurité des trains autonomes soit globalement au moins équivalent à celui des systèmes existants. La définition du concept de "globalement au moins équivalent", principe d'acceptation du risque utilisé en France pour les trains autonomes et issu de la norme EN 50126, doit être formalisée avec précision, étant donné les débats réguliers sur le sujet.

Aide à la mise en place de mesures de sécurité et démonstration

Pour démontrer que les mesures spécifiées à haut niveau sont adaptées aux situations dangereuses susceptibles d'être rencontrées par le train autonome, et ainsi contribuer à une couverture suffisante des risques identifiés, les travaux visés comprennent :

— L'intégration dans l'automatisme de conduite du train autonome (ADS) de fonctions de sécurité capables de contrôler les risques en temps réel face aux différentes situations opérationnelles rencontrées par le train. Elles sont en lien avec les fonctions de l'ADS permettant la conscience de la situation, à savoir les fonctions de perception, décision & compréhension, intégration & action. L'intégration d'une fonction d'anticollision reposant sur un modèle de prise de décision orientée risques a été investiguée dans la thèse de Mohammed Chelouati. Ce modèle utilisant les POMDP est capable d'effectuer une analyse dynamique des risques en exploitation pour couvrir le risque de collision avec un obstacle. Toutefois, d'autres risques restent à couvrir comme la considération de conditions météorologiques changeantes, la variabilité des trajectoires d'obstacles mobiles pouvant se trouver face au train, la perception erronée de la signalisation latérale. Ce type de modèle pourra alors être approfondi en fonction de ces éléments.

— De nouvelles approches sont nécessaires pour faire face au fait que les dangers associés aux trains autonomes peuvent être causés par des facteurs autres que des défaillances. C'est ce que traite la norme internationale SOTIF (*Safety of the Intended Functionality*), publiée par la communauté de la conduite autonome automobile. Cette norme cible spécifiquement les facteurs de causalité autres que la défaillance, qualifiés d'"insuffisance" [51]. L'analyse de sécurité doit prendre en compte ces facteurs causaux non liés aux défaillances, et des travaux sont nécessaires pour étendre les analyses traditionnellement orientées sur les défaillances afin d'identifier des mesures reposant non seulement sur des mécanismes classiques de type *fail-safe* ou *fault-tolerant*, mais aussi sur des mécanismes de type *fail-operation*. Une direction prometteuse consiste à utiliser la méthode STPA (*System-Theoretic Process Analysis*), dérivée du cadre de travail STAMP (*System-Theoretic Accident Model and Processes*) [61]. La méthode STPA est connue pour sa capacité à identifier les facteurs de causalité autres que les défaillances qui peuvent conduire à des événements qualifiés d'accidents fonctionnels (*dangerous successes*).

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] (UE)2015/1136 : *Règlement d'exécution de la Commission du 13 juillet 2015 modifiant le règlement d'exécution (UE) n°402/2013 concernant la méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques*, 2015. adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32015R1136.

[2] (UE)2017/6 : *Règlement d'exécution (UE) 2017/6 de la Commission du 5 janvier 2017 relatif au plan européen de déploiement du système européen de gestion du trafic ferroviaire*, 2017. adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32017R0006&qid=1702025769503.

[3] (UE)2023/1695 : *Règlement d'exécution (UE) 2023/1695 de la Commission du 10 août 2023 relatif à la spécification technique d'interopérabilité concernant les sous-systèmes "contrôle-commande et signalisation" du système ferroviaire dans l'Union européenne et abrogeant le règlement (UE) 2016/919*, 2023. adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32023R1695.

[4] (UE)402/2013 : *Règlement d'exécution de la Commission du 30 avril 2013 concernant la méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques et abrogeant le règlement (CE) n°352/2009*, 2013. adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32013R0402.

[5] G. AGHA et K. PALMSKOG, « A survey of statistical Model-Checking, » *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, t. 28, nº 1, p. 1-39, 2018. DOI : 10.1145/3158668.

[6] J.-F. AUBRY et N. BRINZEI, *Systems Dependability Assessment : Modeling with Graphs and Finite State Automata* (Risk Management and Dependability Series). Hoboken, NJ, USA & London, UK : co-publisher : Wiley & ISTE, 2015. DOI : 10.1002/9781119053996.

[7] J.-F. AUBRY, N. BRINZEI et M.-H. MAZOUNI, *Systems Dependability Assessment – Volume 1 : Benefits of Petri Net Models* (Systems and Industrial Engineering Series). Hoboken, NJ, USA & London, UK : co-publisher : Wiley & ISTE, 2016. DOI : 10.1002/9781119262114.

[8] D. BASILE, A. FANTECHI, L. RUCHER et G. MANDÒ, « Analysing an autonomous tramway positioning system with the UPPAAL Statistical Model Checker, » *Formal Aspects of Computing*, t. 33, p. 957-987, 2021.

[9] A. BLAS et J. BOULANGER, « Comment améliorer les méthodes d'analyse de risques et l'allocation des THR, SIL et autres objectifs de sécurité, » in *20ème congrès Lambda-Mu*, Saint-Malo, France, 2016.

[10] A. BOBBIO et D. RAITERI, « Parametric fault trees with dynamic gates and repair boxes, » in *Reliability and Maintainability symposium*, 2004.

[11] F. BOUDARDARA, A. BOUSSIF, P.-J. MEYER et M. GHAZEL, « A Review of Abstraction Methods Toward Verifying Neural Networks, » *ACM Transactions on Embedded Computing Systems*, t. 23, nº 4, p. 1-19, 2024. DOI : 10.1145/3617508.

[12] M. BROY, B. JONSSON, J.-P. KATOEN, M. LEUCKER et A. PRETSCHNER, *Model-Based Testing of Reactive Systems*. Lecture Notes in Computer Science, Volume 3472, Springer, 2005.

[13] K. BUCHAKER, « Modeling with Extended Fault Trees, » in *5th IEEE International Symposium on High Assurance Systems Engineering (HASE)*, 2000.

[14] M. BUTLER, P. KÖRNER, S. KRINGS, T. LECOMTE, M. LEUSCHEL, L.-F. MEJIA et L. VOISIN, « The first twenty-five years of industrial use of the B-method, » in *International Conference on Formal Methods for Industrial Critical Systems*, 2020, p. 189-209.

[15] B. CAI, B. WU et D. LU, « Survey of Performance Evaluation Standardization and Research Methods on GNSS-Based Localization for Railways, » *Chinese Journal of Electronics*, t. 29, n° 1, p. 22-33, 2020. DOI : 10.1049/cje.2019.09.003.

[16] Q. CAPPART, C. LIMBRÉE, P. SCHAUS, J. QUILBEUF, L.-M. TRAONOUEZ et A. LEGAY, « Verification of Interlocking Systems Using Statistical Model Checking, » in *IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*, Singapore, 2017.

[17] C. CARRERAS et I. WALKER, « Interval methods for fault-tree analysis in robotics, » *IEEE Transactions on Reliability*, t. 50, n° 1, p. 3-11, 2001.

[18] M. CHELOUATI, « Contributions à l'assurance de sécurité des trains autonomes, » thèse de doct., Informatique et Automatique, Université Gustave Eiffel, 2024.

[19] L. CIANI, G. GUIDI et G. PATRIZI, « Human reliability in railway engineering : Literature review and bibliometric analysis of the last two decades, » *Safety Science*, t. 151, 2022. DOI : 10.1016/j.ssci.2022.105755.

[20] E. CLARKE, O. GRUMBERG, S. JHA, Y. LU et H. VEITH, « Progress on the state explosion problem in Model-Checking, » in *Lecture Notes in Computer Science*, 2001, p. 176-194.

[21] E. M. CLARKE, T. HENZINGER, H. VEITH et R. BLOEM, *Handbook of Model-Checking*. Springer, 2019. DOI : 10.1007/978-3-319-10575-8.

[22] A. DAVID, K. G. LARSEN, A. LEGAY, M. MIKUČIONIS et D. BØGSTED POULSEN, « UPPAAL SMC Tutorial, » in *Technical report of Aalborg University, Denmark, and INRIA/IRISA lab in Rennes, France*, 2018.

[23] DÉCISION 2009/460/CE : *Décision de la Commission du 5 juin 2009 relative à l'adoption d'une méthode de sécurité commune pour évaluer la réalisation des objectifs de sécurité*, 2009. adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32009D0460.

[24] DÉCISION 2012/226/UE : *Décision de la Commission du 23 avril 2012 relative à la seconde série d'objectifs de sécurité communs pour le système ferroviaire*, 2012. adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32012D0226.

[25] DIRECTIVE (UE)2016/798 : *Directive du Parlement Européen et du Conseil du 11 mai 2016 relative à la sécurité ferroviaire*, 2016. adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L0798.

[26] DIRECTIVE 2004/49/CE : *Directive du Parlement Européen et du Conseil du 29 avril 2004 concernant la sécurité des chemins de fer communautaires et modifiant les directives 95/18/CE et 2001/14/CE (abrogée par la directive (UE) 2016/798)*, 2013. adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32004L0049#.

[27] J. DUGAN, J. SALVATOR et M. BOYD, « Fault trees and sequence dependencies, » in *Annual Reliability and Maintainability Symposium*, 1990.

[28] EEIG-EUG, *ERTMS/ETCS RAMS Requirements specification*. reference 96S126, version 6, EEIG-EUG – European Economic Interest Grouping - ERTMS Users' Group, sept. 1998.

[29] EEIG-EUG, *Hybrid ERTMS/ETCS Level 3*. European Economic Interest Grouping - ERTMS Users' Group, reference 16E042, version 1D, 2020.

[30] EN 50126-1 : « Railway Applications – The Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 1 : generic RAMS process, » European Committee for Electrotechnical Standardisation (CENELEC), European Standard, oct. 2017.

[31] EN 50126-2 : « Railway Applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 2 : systems approach to safety, » European Committee for Electrotechnical Standardisation (CENELEC), European Standard, oct. 2017.

[32] EN 50128 : « Railway Applications – Communication, signalling and processing systems - Software for railway control and protection systems, » European Committee for Electrotechnical Standardisation (CENELEC), European Standard, oct. 2011.

[33] EN 50129 : « Railway applications – Communication, signalling and processing systems - Safety related electronic systems for signalling, » European Committee for Electrotechnical Standardisation (CENELEC), European Standard, nov. 2018.

[34] EN 50159 : « Railway applications – Communication, signalling and processing systems - Safety-related communication in transmission systems, » European Committee for Electrotechnical Standardisation (CENELEC), European Standard, août 2011.

[35] ERA, *collection of examples of risk assessments and of some possible tools supporting the CSM regulation*. European Union Agency for Railways, 2009.

[36] EUSPA-USER CONSULTATION PLATFORM, *Report on Rail User Needs and Requirements - Outcome of the European GNSS user consultation platform*, 2019. adresse : https://www.euspa.europa.eu/euspace-applications/euspace-users/user-consultation-platform-2020,%20EUSPA--European%20Union%20Agency%20for%20the%20Space%20Programme.

[37] F. FLAMMINI, « Model-based dependability evaluation of complex critical control systems, » Doctor thesis, University of Naples Federico II, Naples, Italia, nov. 2006.

[38] N. FURNESS, H. VAN HOUTEN, L. ARENAS et M. BARTHOLOMEUS, « ERTMS Level 3 : the Game-Changer, » *IRSE–Institute of Railway Signal Engineers, April*, p. 2-9, 2017.

[39] P. GROVES, *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems*. 2nd ed. Norwood, MA, USA : Artech House, 2013.

[40] R. GULATI et J. DUGAN, « A modular approach for analyzing static and dynamic fault trees, » in *Reliability and Maintainability symposium*, 1997.

[41] A. HAIDER et A. NADEEM, « A Survey of Safety Analysis Techniques for Safety Critical Systems, » *International Journal of Future Computer and Communication*, t. 2, n° 2, p. 134-137, 2013. DOI : 10.7763/IJFCC.2013.V2.137.

[42] L. S. Y. HÅKAN et G. S. REID, « Verification and planning for stochastic processes with asynchronous events, » in *AAAI'04 – 19th conference on Artifical Intelligence*, 2004.

[43] O. HIMRANE, « Contribution to Safety and Operational Performance Evaluation of GNSS-based Railway Localization Systems Using a Formal Model-based Approach, » thèse de doct., Automatique, Génie Informatique, Traitement du Signal et des Images, Université Gustave Eiffel, 2022.

[44] ICAO, *International Standards and Recommended Practices, Annex 10 - Aeronautical Telecommunications, Volume 1 (Radio Navigation Aids), Technical report, International Civil Aviation Organization*, 2023. adresse : https://standart.aero/en/icao/book/annex-10-v-1-aeronautical-telecommunications-volume-i-radio-navigation-aids-en-cons.

[45] IEC 60050-192 : « International Electrotechnical Vocabulary – Part 192 : Dependability, » International Electrotechnical Commission (IEC), International Standard, fév. 2015.

[46] IEC 60050-903 : « International Electrotechnical Vocabulary – Part 903 : Risk assessment, » International Electrotechnical Commission (IEC), International Standard, juin 2013.

[47] IEC 60300-1 : « Dependability management – Part 3-1 : Application guide - Analysis techniques for dependability - Guide on methodology, » International Electrotechnical Commission (IEC), International Standard, août 2005.

[48] IEC 61508 : « Functional safety of electrical/electronic/programmable electronic safety-related systems, » International Electrotechnical Commission (IEC), International Standard, avr. 2010.

[49] IEC 61703 : « Mathematical expressions for reliability, availability, maintainability and maintenance support terms, » International Electrotechnical Commission (IEC), International Standard, août 2016.

[50] IEEE 1012 : « IEEE Standard for System, Software and Hardware Verification and Validation, » The Institute of Electrical et Electronics Engineers (IEEE), IEEE Standard, 2016. DOI : 10.1109/IEEESTD.2017.8055462.

[51] ISO 21448 : « Road Vehicles – Safety Of The Intended Functionality, » International Organization for Standardization (ISO), ISO Standard, 2022.

[52] ISO/IEC/IEEE 29148 : « ISO/IEC/IEEE Standard for system and software engineering – Life cycle processes – Requirements engineering, » International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), The Institute of Electrical et Electronics Engineers (IEEE), ISO/IEC/IEEE Standard, 2018. DOI : 10.1109/IEEESTD.2018.8559686.

[53] X. JANAN, « On multistate system analysis, » *IEEE Transactions on Reliability*, t. R-34, n° 4, p. 329-337, 1985. DOI : 10.1109/TR.1985.5222178.

[54] L. JAULIN, M. KIEFFER, O. DIDRIT et E. WALTER, *Applied Interval Analysis*. Springer, 2001.

[55] Y. KAI, « Multistate fault-tree analysis, » *Reliability Engineering & System Safety*, t. 28, n° 1, p. 1-7, 1990.

[56] B. KAISER et C. GRAMLICH, « State-event-fault-trees – a safety analysis model for software controlled systems, » in *23rd conference on computer safety, reliability, and security – SafeComp*, 2004.

[57] K. KALAJDZIC, C. JEGOUREL, A. LUKINA, E. BARTOCCI, A. LEGAY, S. SMOLKA et R. GROSU, « Feedback control for statistical model checking of cyber-physical systems, » in *International Symposium on Leveraging Applications of Formal Methods*, 2016, p. 46-61.

[58] K. KUMAR et P. KUMAR, « Fuzzy availability modeling and analysis of biscuit manufacturing plant : a case study, » *International Journal of System Assurance Engineering and Management*, t. 2, n° 3, 2011. DOI : 10.1007/s13198-011-0076-3.

[59] A. LEGAY, B. DELAHAYE et S. BENSALEM, « Statistical Model Checking : An Overview, » in *First International Conference RV 201, Runtime Verification*, St Julians, Malta, 2010.

[60] C. LEGRAND, « Contribution à l'évaluation de la sécurité de systèmes de localisation ferroviaires basés sur les GNSS par la formalisation des concepts d'intégrité étendue, » thèse de doct., Automatique, Génie Informatique, Traitement du Signal et des Images, Université de Lille, 2016.

[61] N. LEVESON, *Engineering a Safer World : Systems Thinking Applied to Safety (Engineering Systems)*. The MIT Press, 2016. DOI : 20.500.12657/26043.

[62] A. LEVESON N., « A new accident model for engineering safer systems, » *Safety Science journal*, t. 42, n° 4, p. 237-270, 2004. DOI : 10.1016/S0925-7535(03)00047-X.

[63] X. LI, M. ZUO et R. YAM, « Reliability analysis of a repairable k-out-of-n system with some components being suspended when the system is down, » *Reliability Engineering & System Safety*, t. 91, n° 3, 2006. DOI : 10.1016/j.ress.2005.01.010.

[64] N. LIMNIOS, *Arbre de défaillances*. Paris : Hermès-Lavoisier, 2005.

[65] H. LIU, G. ZHENG, H. WANG et C. FENG, « Research on Integrity Monitoring For Integrated GNSS/SINS System, » in *IEEE International Conference on Information and Automation*, Harbin, China, 2010.

[66] L. LO PRESTI et S. SABINA, *GNSS for rail transportation, challenges and opportunities*. PoliTO Springer Series, 2018.

[67] D. LU et E. SCHNIEDER, « Performance Evaluation of GNSS for Train Localization, » *IEEE Transactions on Intelligent Transportation Systems*, t. 16, nº 2, p. 1054-1059, 2015. DOI : 10.1109/TITS.2014.2349353.

[68] J. MAGOTT et P. SKROBANEK, « Timing analysis of safety properties using fault trees with time dependencies and timed state-charts, » *Reliability Engineering & System Safety*, t. 97, nº 1, p. 14-26, 2012. DOI : 10.1016/j.ress.2011.09.004.

[69] Q. MAHBOOB et E. ZIO, *RAMS in Railway Systems : Theory and Practice*. Boca Raton, FL, USA : CRC Press, 2018. DOI : 10.1201/b21983.

[70] Y. MAHMOOD, A. AHMADI, A. VERMA, A. SRIVIDYA et U. KUMAR, « Fuzzy fault tree analysis : a review of concept and application, » *International Journal of System Assurance Engineering and Management*, t. 4, nº 1, p. 19-32, 2013. DOI : 10.1007/s13198-013-0145-x.

[71] G. MERLE, J.-M. ROUSSEL et J.-J. LESAGE, « Algebraic determination of the structure function of Dynamic Fault Trees, » *Reliability Engineering & System Safety*, t. 96, nº 2, p. 267-277, 2011. DOI : https://doi.org/10.1016/j.ress.2010.10.001.

[72] L. MESHKAT, J. DUGAN et J. ANDREWS, « Dependability analysis of systems with on-demand and active failure modes using dynamic fault trees, » *ProcIEEE*, t. 77, nº 4, p. 240-251, 2002.

[73] MIL-STD-882D : « Standard practice for system safety, » United States Department of Defense (DoD), DoD Standard, fév. 2000.

[74] MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE ET SOLIDAIRE, « Petites lignes ferroviaires : des plans d'actions régionaux (Rapport Philizot en annexe), » *Dossier de presse de février 2020*,

[75] R. MOORE, R. KEARFOTT et M. CLOUD, *Introduction to interval analysis*. Siam, 2009, t. 110.

[76] R. E. MOORE, *Interval analysis*. Prentice-Hall Englewood Cliffs, NJ, 1966, t. 4.

[77] R. MUTTRAM et C. KESSELL, *Understanding SIL*. Institution of Railway Signal Engineers (IRSE) News, oct. 2015.

[78] M. NAWAZ, M. MALIK, Y. LI, M. SUN et M. LALI, « A Survey on Theorem Provers in Formal Methods, » *CoRR : a computing research repository - ACM Digital Library*, 2019. DOI : 10.48550/arXiv.1912.03028.

[79] OCORA, *Localisation On-Board (LOC-OB), High-level Requirements*, version 3.1, OCORA project – *Open CCS On-board Reference Architecture*, document of interest for EEIG-ERTMS Users Group, mai 2022. adresse : https://ertms.be/activities/localisation-working-group.

[80] J. PACHL, *Railway Operation and Control*. Mountlake Terrace, USA : 4th edition, VTD Rail Publishing, 2018.

[81] G. K. PALSHIKAR, « Temporal fault trees, » *Information and Software Technology*, t. 44, nº 3, p. 137-150, 2002. DOI : 10.1016/S0950-5849(01)00223-3.

[82] S. QIU, M. SALLAK, W. SCHÖN et Z. CHERFI-BOULANGER, « Availability assessment of railway signalling systems with uncertainty analysis using Statecharts, » *Simulation Modelling Practice and Theory*, t. 47, p. 1-18, 2014. DOI : 10.1016/j.simpat.2014.04.004.

[83] S. QIU, M. SALLAK, W. SCHÖN et Z. CHERFI-BOULANGER, « Epistemic parametric uncertainties in availability assessment of a Railway Signalling System using Monte Carlo simulation, » in *ESREL - European Safety and Reliability Conference*, Amsterdam, The Netherlands, 2013.

[84] K. D. RAO, V. GOPIKA, V. RAO, H. KUSHWAHA, A. K. VERMA et A. SRIVIDYA, « Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment, » *Reliability Engineering & System Safety*, t. 94, nº 4, p. 872-883, 2009.

[85] S. RAVIKUMAR et C. SUBRAMANIAM, « A Survey on Different Software Safety Hazard Analysis and Techniques in Safety Critical Systems, » *Middle-East Journal of Scientific Research, (Special Issue on Innovations in Information, Embedded and Communication Systems), 2016*, t. 24, p. 90-97, 2016. DOI : 10.5829/idosi.mejsr.2016.24.IIECS.23145.

[86] F. RISPOLI, G. SICILIANO et C. BRENNA, « GNSS for ERTMS train localization, a step-change technology and new business model, » *Inside GNSS*, p. 48-54, 2017.

[87] B. ROTURIER, E. CHATRE et J. VENTURA-TRAVESET, « The SBAS Integrity Concept standardised by ICAO. Application to EGNOS, » in *5th International Symposium on Global Navigation Satellite Systems, Seville, Spain*, 2001.

[88] RTCA, *Minimum Operational Performance Standards (MOPS) for Global Positioning System / Satellite-based Augmentation System Airborne Equipment. DO229D standard, Radio Technical Commission for Aeronautics*, 2013.

[89] S. RUMP, « INTLAB - INTerval LABoratory, » in *Developments in Reliable Computing*, http://www.tuhh.de/ti3/rump/intlab/, Dordrecht : Kluwer Academic Publishers, 1999, p. 77-104.

[90] W. SANDERS et J. MEYER, « Stochastic Activity Networks : formal definitions and concepts, » in *Lectures on Formal Methods and Performance Analysis : First EEF/Euro Summer School on Trends in Computer Science*. Berlin, Heidelberg : Springer-Verlag, 2002, p. 315-343.

[91] W. SCHÖN, J.-N. BENSO, G. LARRAUFIE, G. MOËNS et J. PORÉ, *Railway signalling and automation*. Vol 4., La Vie du Rail & IRSE, 2023.

[92] J.-P. SIGNORET et A. LEROY, *Reliability Assessment of Safety and Production Systems – Analysis, Modelling, Calculations and Case Studies*. Cham, Switzerland : Springer, 2021. DOI : 10.1007/978-3-030-64708-7.

[93] SUBSET 026, *ERTMS-ETCS – System Requirements Specifications*. UNISIG – Union of Signalling Industry , issue 4.0.0, 2023-05-07, 2023.

[94] SUBSET 041, *ERTMS-ETCS – Performance Requirements for Interoperablity*. UNISIG – Union of Signalling Industry , issue 4.0.0, 2023-05-07, 2023.

[95] SUBSET 088, *ETCS Application Levels 1 & 2 - Safety Analysis - Part 3 - THR Apportionment*. UNISIG – Union of Signalling Industry , issue 3.7.0, 2019-12-16, 2019.

[96] SUBSET 091, *Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2*. UNISIG – Union of Signalling Industry , issue 4.0.0, 2023-07-05, 2023.

[97] M. SUN, S. GAUTHAM, Q. GE, C. ELKS et C. FLEMING, « Defining and characterizing model-based safety assessment : A review, » *Safety Science*, t. 172, 2024. DOI : 10.1016/j.ssci.2024.106425.

[98] D. TRENTESAUX, R. DAHYOT, A. OUEDRAOGO, D. ARENAS, S. LEFEBVRE, W. SCHÖN, B. LUSSIER et H. CHÉRITEL, « The Autonomous Train, » in *13th Annual Conference on System of Systems Engineering (SoSE)*, 2018. DOI : 10.1109/SYSOSE.2018.8428771.

[99] K. TRIVEDI et A. BOBBIO, *Reliability and Availability Engineering : Modeling, Analysis, and Applications*. Cambridge, UK : Cambridge University Press, 2017.

[100] D. VERNEZ et F. VUILLE, « Method to assess and optimise dependability of complex macro-systems : Application to a railway signalling system, » *Safety Science*, t. 47, p. 382-394, 2009. DOI : 10.1016/j.ssci.2008.05.007.

[101] P. WEBER et C. SIMON, *Systems Dependability Assessment – Volume 2 : Benefits of Bayesian Network Models* (Systems and Industrial Engineering Series). Hoboken, NJ, USA & London, UK : co-publisher : Wiley & ISTE, 2015. DOI : 10.1002/9781119347316.

[102] G. WEISS, M. ZELLER, H. SCHOENHAAR, C. DRABEK et A. KREUTZ, « Approach for Argumenting Safety on Basis of an Operational Design Domain, » in *CAIN 2024 - 3rd IEEE ACM International Conference on AI Engineering*, Lisbon, Portugal, 2024. DOI : 10.1145/3644815.3644944.

[103] P. WIGGER, « MODSafe-Modular Urban Transport Safety and Security Analysis, » *Procedia - Social and Behavioral Sciences, Transport Research Arena 2012*, t. 48, p. 2616-2625, 2012. DOI : 10.1016/j.sbspro.2012.06.1232.

[104] C. WULLEMS, F. SPERANDIO, M. BASSO, S. STURARO et 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)*, 2018.

[105] N. ZHU, J. MARAIS, D. BÉTAILLE et M. BERBINEAU, « GNSS Position Integrity in Urban Environments : A Review of Literature, » *IEEE Transactions on Intelligent Transport Systems*, 2018. DOI : 10.1109/TITS.2017.2766768.

[106] A. ZIMMERMANN et G. HOMMEL, « Towards modeling and evaluation of ETCS real-time communication and operation, » *Journal of Systems and Software*, t. 77, nº 1, p. 47-54, 2005. DOI : 10.1016/j.jss.2003.12.039.

[107] H.-J. ZIMMERMANN, « Fuzzy set theory, » *Wiley Interdisciplinary Reviews : Computational Statistics*, t. 2, nº 3, p. 317-332, 2010.

ANNEXE 1 – LISTE DES PUBLICATIONS

Mémoire de thèse

[TH1] J. BEUGIN, *Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé*, Mémoire de doctorat, LAMIH, Université de Valenciennes, https://theses.hal.science/tel-00132452, 2006.

Articles de revue répertoriée (ACL)

[Sub1] I. SASSI, E.-M. EL-KOURSI, J. BEUGIN, S. IOVINO et N. RICEVUTO, « Defining Safety Requirements of New On-Board Functions Essential to ETCS Level 3 Operation : The Train Integrity and Train Length Determination, » *IEEE Access*, article soumis en 2024.

[ACL1] M. CHELOUATI, A. BOUSSIF, J. BEUGIN et E.-M. EL-KOURSI, « A Risk-Based Decision-Making Process for Autonomous Trains Using POMDP : Case of the Anti-Collision Function, » *IEEE Access*, t. 12, p. 5630-5647, 2024. DOI : 10.1109/ACCESS.2023.3347500.

[ACL2] M. CHELOUATI, A. BOUSSIF, J. BEUGIN et E.-M. EL-KOURSI, « Graphical safety assurance case using Goal Structuring Notation (GSN) - challenges, opportunities and a framework for autonomous trains, » *Reliability Engineering & System Safety (RESS)*, t. 230, 2023. DOI : 10.1016/j.ress.2022.108933.

[ACL3] O. HIMRANE, J. BEUGIN et M. GHAZEL, « Implementation of a Model-Oriented Approach for Supporting Safe Integration of GNSS-Based Virtual Balises in ERTMS/ETCS Level 3, » *IEEE Open Journal of Intelligent Transportation Systems*, t. 4, p. 294-310, 2023. DOI : 10.1109/OJITS.2023.3267142.

[ACL4] T. P. K. NGUYEN, J. BEUGIN, M. BERBINEAU et J. MARAIS, « Application of fuzzy theory for identifying the required availability of an autonomous localisation unit in European Train Control System, » *Journal of Intelligent Transportation Systems : Technology, Planning, and Operations*, t. 23, n° 3, p. 265-281, 2019. DOI : 10.1080/15472450.2018.1525533.

[ACL5] J. BEUGIN, C. LEGRAND, J. MARAIS, M. BERBINEAU et E.-M. EL-KOURSI, « Safety Appraisal of Localization Systems Based on GNSS Used in Train Spacing Control, » *IEEE-Access*, t. 6, n° 1, p. 9898-9916, 2018. DOI : 10.1109/ACCESS.2018.2807127.

[ACL6] K.-A. OUEDRAOGO, J. BEUGIN, E.-M. EL-KOURSI, J. CLARHAUT, D. RENAUX et F. LISIECKI, « Toward an application guide for Safety Integrity Level allocation in railway systems, » *Risk Analysis journal*, t. 38, n° 8, p. 1634-1655, 2018. DOI : 10.1111/risa.12972.

[ACL7] J. MARAIS, J. BEUGIN et M. BERBINEAU, « A survey of GNSS-based Research and Developments for the European railway signaling, » *IEEE-Transactions on Intelligent Transportation Systems*, t. 18, n° 10, p. 2602-2618, 2017. DOI : 10.1109/TITS.2017.2658179.

[ACL8] C. LEGRAND, J. BEUGIN, B. CONRARD, J. MARAIS, M. BERBINEAU et E.-M. EL-KOURSI, « From extended integrity monitoring to the safety evaluation of satellite-based localisation, » *Journal of Reliability Engineering and System Safety (RESS)*, t. 155, p. 105-114, 2016. DOI : 10.1016/j.ress.2016.04.011.

[ACL9] T. P. K. NGUYEN, J. BEUGIN, M. BERBINEAU et M. KASSAB, « A new analytical approach to evaluate the critical-event probability due to wireless communication errors in Train Control Systems, » *IEEE-Transactions on Intelligent Transportation Systems*, t. 18, n° 6, p. 1380-1392, 2016. DOI : 10.1109/TITS.2016.2604043.

[ACL10] T. P. K. NGUYEN, J. BEUGIN et J. MARAIS, « Method for evaluating an extended Fault Tree to analyse the dependability of complex systems : application to a satellite-based railway system, » *Journal of Reliability Engineering & System Safety (RESS)*, t. 133, p. 300-313, 2015. DOI : 10.1016/j.ress.2014.09.019.

[ACL11] J. BEUGIN et J. MARAIS, « Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization, » *Journal of Transportation Research, part C (Emerging Technologies)*, t. 22, p. 42-57, 2012. DOI : 10.1016/j.trc.2011.12.002.

[ACL12] J. BEUGIN, A. FILIP, J. MARAIS et M. BERBINEAU, « Galileo for railway operations : question about the positioning performances analogy with the RAMS requirements allocated to safety applications, » *European Transport Research Review (ETRR)*, t. 2, n° 2, p. 93-102, 2010. DOI : 10.1007/s12544-010-0032-3.

[ACL13] J. BEUGIN, D. RENAUX et L. CAUFFRIEZ, « A SIL Quantification Approach based on an Operating Situation Model for Safety Evaluation in Complex Guided Transportation Systems, » *Journal of Reliability Engineering & System Safety (RESS)*, t. 92, n° 12, p. 1686-1700, 2007. DOI : 10.1016/j.ress.2006.09.022.

Articles de revue non répertoriée (ACLN)

[ACLN1] A. BOUSSIF, A. TONK, J. BEUGIN et S. COLLART-DUTILLEUL, « Operational Risk Assessment of Railway Remote Driving System, » *Safety and Reliability journal*, 2023. DOI : 10.1080/09617353.2023.2226965.

[ACLN2] D. DE ALMEIDA PEREIRA, O. HIMRANE, P. BON et J. BEUGIN, « From French National Signalling Systems to ERTMS : Considering the Evolution of Trackside Systems, » *International Journal of Signal Processing Systems*, t. 9, n° 2, p. 12-16, 2021. DOI : 10.18178/ijsps.9.2.11-16.

[ACLN3] J. BEUGIN et J. MARAIS, « Application des principes de la sûreté de fonctionnement à l'évaluation du service de localisation par satellites dans le domaine ferroviaire, » *Recherche Transports Sécurité (RTS), Lavoisier*, t. 99, p. 89-103, 2008. DOI : 10.3166/rts.99.89-103.

[ACLN4] A. FILIP, J. BEUGIN, J. MARAIS et H. MOCEK, « Interpretation of the Galileo Safety-Of-Life Service by Means of Railway RAMS Terminology, » *Transactions on Transport Sciences, Ministère des transports Tchèques*, t. 1, n° 2, p. 61-68, 2008. DOI : 10.5507/tots.2008.009.

Article dans revue sans comité de lecture (ASCL)

[ASCL1] J. BEUGIN, N. VIANDIER, J. MARAIS et M. BERBINEAU, « GNSS pour la localisation sûre des transports terrestres guidés ou publics de type bus en site propre ou tramways, » *Revue Navigation de l'Institut Français de Navigation (IFN)*, t. 57, n° 225, p. 5-24, 2009.

Conférences données à l'invitation du comité d'organisation (INV)

[INV1] J. BEUGIN et P.-Y. GILLIERON, *Satellite positioning in the transport domain : applications and challenges*, Workshop 4 : Navigation Technologies and Geographic Information System for a better traffic management, Data Science and Mobility Conference supported by SBB/CFF/FFS, January 31, Lausanne, Switzerland, 2018.

[INV2] J. BEUGIN et C. STEIN, *RAMS Terminology in Standardization*, Tutorial session at the 9th FORMS-FORMAT symposium (Formal Methods for Automation and Safety in Railway and Automotive Systems), December 11-13, Braunschweig, Germany, 2012.

[INV3] J. BEUGIN et J. MARAIS, *INRETS activities on GALILEO, results of recent scientific research*, the 7th Munich Satellite Navigation Summit 2009, session panel "GNSS on tracks : railroad", 3-5 March, Germany, 2009.

[INV4] J. BEUGIN, A. FILIP et J. MARAIS, *A dependability approach for integrating a satellite positioning system in a railway application*, invited lecture for Braunschweiger Verkehrskolloquium, DLR -Deutsches Zentrum für Luft und Raumfahrt- (centre aérospatial allemand), Braunschweig, Allemagne, 7 Février, 2008.

[INV5] A. FILIP, J. BEUGIN, J. MARAIS et H. MOCEK, *Galileo Safety of Life Service for Railway Signalling*, invited lecture for Braunschweiger Verkehrskolloquium, DLR -Deutsches Zentrum für Luft und Raumfahrt- (centre aérospatial allemand), Braunschweig, Allemagne, 7 Février, 2008.

Communications avec actes dans un congrès international (ACTI)

[ACTI1] R. SADDEM-YAGOUBI, J. BEUGIN et M. GHAZEL, « ERTMS/ETCS L3 : Usable Formal Models for the "Loss of Train Integrity" Operation Scenario, » in *VECoS'24 - 17th International Conference on Verification and Evaluation of Computer and Communication Systems*, (15 oct. 2024-18 oct. 2022), Djerba, Tunisie, 2024.

[ACTI2] M. CHELOUATI, A. BOUSSIF, J. BEUGIN et E.-M. EL-KOURSI, « A framework for risk-awareness and dynamic risk assessment for autonomous trains, » in *ESREL 2022 - 32nd European Safety and Reliability Conference*, (28 août-1er sept. 2022), Dublin, Ireland, 2022.

[ACTI3] R. SADDEM-YAGOUBI, J. BEUGIN et M. GHAZEL, « A Formal Modelling Framework for Moving Block Systems in the PERFORMINGRAIL project, » in *RAILWAYS 2022 - 5th International Conference on Railway Technology : Research, Development and Maintenance*, (22-25 août 2022), Montpellier, France, 2022.

[ACTI4] R. SADDEM-YAGOUBI, J. BEUGIN et M. GHAZEL, « Methodology Framework for Modelling ETCS-L3 Moving Block System, » in *TRA 2022 - 9th Transport Research Arena*, (14-17 nov. 2022), Lisbon, Portugal, 2022.

[ACTI5] R. SADDEM-YAGOUBI, J. BEUGIN et M. GHAZEL, « Verification Framework for Moving Block System Safety : Application on the Loss of Train Integrity Use Case, » in *11th TRISTAN conference, Triennal Symposium on Transportation Analysis*, (19-25 juin 2022), Mauritius Island, 2022.

[ACTI6] R. SADDEM-YAGOUBI, M.-U. SANWAL, S. LIBUTTI, M. BENERECETTI, J. BEUGIN, F. FLAMMINI, M. GHAZEL, B. JANSSEN, S. MARRONE, F. MOGAVERO, R. NARDONE, A. PERON, C. SECELEANU et V. VITTORINI, « Toward Usable Formal Models for Safety and Performance Evaluation of ERTMS/ETCS Level 3 : The PERFORMINGRAIL Project, » in *ESREL 2022 - 32nd European Safety and Reliability Conference*, (28 août-1er sept. 2022), Dublin, Ireland, 2022.

[ACTI7] A. TONK, M. CHELOUATI, A. BOUSSIF, J. BEUGIN et E.-M. EL-KOURSI, « A Safety Assurance Methodology for Autonomous Trains, » in *TRA 2022 - 9th Transport Research Arena*, (14-17 nov. 2022), Lisbon, Portugal, 2022.

[ACTI8] O. HIMRANE, J. BEUGIN et M. GHAZEL, « Toward Formal Safety and Performance Evaluation of GNSS-based Railway Localisation Function, » in *CTS 2021, 16th IFAC Symposium on Control in Transportation Systems*, (8-10 juin 2021), Lille, France, 2021.

[ACTI9] A. TONK, A. BOUSSIF, J. BEUGIN et S. COLLART-DUTILLEUL, « Towards a Specified Operational Design Domain for a Safe Remote Driving of Trains, » in *ESREL 2021 - 31st European Safety and Reliability Conference*, (19-23 sept. 2021), Angers, France, 2021.

[ACTI10] D. I. DE ALMEIDA PEREIRA, O. HIMRANE, P. BON et J. BEUGIN, « From French National Signalling Systems to ERTMS : Considering the Evolution of Trackside Systems, » in *ICCSIT 2020 - 13th International Conference on Computer Science and Information Technology, virtual attendance*, (14-16 oct. 2020), The Netherlands, 2020.

[ACTI11] O. HIMRANE, J. BEUGIN et M. GHAZEL, « Towards a Model-Based Safety Assessment of Railway Operation Using GNSS Localization, » in *ESREL 2020 and PSAM 15 - 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference, virtual attendance*, (1er-5 nov. 2020), Venice, Italy, 2020.

[ACTI12] I. SASSI, J. BEUGIN, M. SALLAK et N. AIT TMAZIRTE, « Allocating imprecise safety targets in satellite-based localization systems used in railway signaling operations, » in *ESREL 2020 and PSAM 15 - 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference, virtual attendance*, (1er-5 nov. 2020), Venice, Italy, 2020.

[ACTI13] J. MARAIS, J. BEUGIN, J. POUMAILLOUX et M. GANDARA, « EGNOS service evaluation in railway environment for safety-critical operations, » in *7th Transport Research Arena (TRA)*, (16-19 avr. 2018), Vienna, Austria, 2018.

[ACTI14] K.-A. OUEDRAOGO, J. BEUGIN, E.-M. EL-KOURSI, J. CLARHAUT, D. RENAUX et F. LISIECKI, « Safety Integrity Level Allocation shared or Divergent Practices in the Railway Domain, » in *IRSC - International Railway Safety Council*, (2-7 oct. 2016), Paris, France, 2016.

[ACTI15] C. LEGRAND, J. BEUGIN, B. CONRARD, J. MARAIS, M. BERBINEAU et E.-M. EL-KOURSI, « Approach for evaluating the safety of a satellite-based train localisation system through the extended integrity concept, » in *ESREL 2015 - European Safety and Reliability conference*, (7-10 sept. 2015), Zürich, Switzerland : in Podofillini et al. Eds, Taylor & Francis Group, London, ISBN 978-1-138-02879-1, 2015, p. 1297-1305.

[ACTI16] H. MANZ, E. SCHNIEDER, D. STEIN, M. SPINDLER, M. LAUER, C. SEEDORFF, A. BAUDIS, U. BECKER, J. BEUGIN, T. P. K. NGUYEN et J. MARAIS, « GaLoROI : Satellite-based localization in railways, » in *IC-ARE'15, International Congress on Advanced Railway Engineering*, (2-4 mars 2015), Istanbul, Turkey, 2015.

[ACTI17] T. P. K. NGUYEN, J. BEUGIN, M. KASSAB et M. BERBINEAU, « Analytical approach for evaluating LTE communication errors in train control application, » in *IEEE ICC-DVC, International Conference on Communications- 1st workshop on Dependable Vehicular Communications*, (8-12 juin 2015), London, UK, 2015.

[ACTI18] K.-A. OUEDRAOGO, J. BEUGIN, E.-M. EL-KOURSI, J. CLARHAUT, D. RENAUX et F. LISIECKI, « Harmonized methodology for Safety Integrity Level allocation in a generic TCMS application, » in *ESREL 2015 - European Safety and Reliability conference*, (7-10 sept. 2015), Zürich, Switzerland : in Podofillini et al. Eds, Taylor & Francis Group, London, ISBN 978-1-138-02879-1, 2015, p. 3579-3587.

[ACTI19] C. LEGRAND, J. BEUGIN, B. CONRARD, J. MARAIS, M. BERBINEAU et E.-M. EL-KOURSI, « Causal analysis methodology of multisensor systems based on GNSS, » in *Railways 2014, the 2nd International Conference on Railway Technology : Research, Development and Maintenance*, (8-11 avr. 2014), Ajaccio, Corsica, France, 2014.

[ACTI20] T. P. K. NGUYEN, J. BEUGIN, M. KASSAB et M. BERBINEAU, « Modelling Communication Based Train Control system for dependability analysis of the LTE Communication network in train control application, » in *IEEE EMS-8th European Modelling Symposium on Mathematical Modelling and Computer Simulation*, (21-23 oct. 2014), Pisa, Italy, 2014.

[ACTI21] T. P. K. NGUYEN, J. BEUGIN et J. MARAIS, « RAMS analysis of GNSS based localisation system for the train control application, » in *IEEE ComManTel 2014, the 2nd International Conference on Computing, Management and Telecommunications*, (27-29 avr. 2014), Da Nang, Vietnam, 2014.

[ACTI22] K.-A. OUEDRAOGO, J. BEUGIN, E.-M. EL-KOURSI, J. CLARHAUT, D. RENAUX et F. LISIECKI, « Allocation rules of Safety Integrity Levels in a generic TCMS application, » in *10th FORMS-FORMAT symposium (Formal Methods for Automation and Safety in Railway and Automotive Systems)*, (30 sept. 2014-2 oct. 2015), Braunschweig, Germany, 2014.

[ACTI23] O. HOINARU, J. BEUGIN et J. MARAIS, « Contribution to a terminology related to dependability for the qualification of an on-board satellite-based system, » in *In proceedings of the 2nd ICTIS conference (International Conference on Transportation Information and Safety)*, (28 juin-1er juill. 2013), Wuhan, China, 2013.

[ACTI24] C. LEGRAND, J. BEUGIN, B. CONRARD, J. MARAIS, M. BERBINEAU et E.-M. EL-KOURSI, « Sensitivity Assessment to Analyse Dependability of a Multisensor Localisation System based on GNSS, » in *IEEE ITS-T, Intelligent Transportation Systems-Telecommunications conference*, (5-7 nov. 2013), Tampere, Finland, 2013.

[ACTI25] T. P. K. NGUYEN, J. BEUGIN et J. MARAIS, « Dependability evaluation of a GNSS and ECS based localisation unit for railway vehicles, » in *IEEE ITS-T, Intelligent Transportation Systems-Telecommunications conference*, (5-7 nov. 2013), Tampere, Finland, 2013.

[ACTI26] J. MARAIS et J. BEUGIN, « Evaluation method of GNSS-based positioning functions for safety applications in operational conditions, » in *Transport Research Arena - TRA conference*, (23-26 avr. 2012), Athens, Greece, 2012.

[ACTI27] J. MARAIS et J. BEUGIN, « Integrity in safe railway GNSS-based applications, » in *ITST 2010 - 10th International Conference on Intelligent Transport Systems Telecommunications*, (9-11 nov. 2010), Kyoto, Japan, 2010.

[ACTI28] J. BEUGIN, A. FILIP et J. MARAIS, « Simulation approaches to evaluate dependability of satellite-based positioning services in railway transportation applications, » in *ESREL 2009 - European Safety and Reliability conference*, (7-10 sept. 2009), Prague, Czech Republic : in Briš, Guedes & Martorell Eds,Taylor & Francis Group, ISBN 978-0-415-55509-8, 2009, p. 2331-2337.

[ACTI29] J. BEUGIN et J. MARAIS, « An Approach to Quantify the Satellite-Based Train Location Service Using a Petri-Nets Model, » in *The 8th World Congress on Railways Research*, (18-22 mai 2008), Séoul, Corée du Sud, 2008.

[ACTI30] J. BEUGIN, J. MARAIS et J.-P. LOZAC'H, « A dependability analysis for integrating a satellite positioning system in a rail freight application, » in *ENC-GNSS 2008 - European Navigation Conference*, (22-25 avr. 2008), Toulouse, France, 2008.

[ACTI31] A. FILIP, J. BEUGIN, J. MARAIS et H. MOCEK, « Safety Concept of Railway Signalling Based on Galileo Safety of Life Service, » in *COMPRAIL-11th international conference on Computer System Design and Operations in the Railway and Other Transit Systems*, (15-17 sept. 2008), Toledo, Espagne, 2008.

[ACTI32] J. BEUGIN, L. CAUFFRIEZ et D. RENAUX, « Prise en compte du contexte opérationnel dans l'évaluation de la sécurité d'un système de transport guidé, » in *PENTOM 2007 - Performances et Nouvelles Technologies en Maintenance*, (juill. 2007), Mons, Belgique, 2007.

[ACTI33] J. BEUGIN, D. RENAUX et L. CAUFFRIEZ, « A safety assessment method for guided transportation systems : a dynamic approach using Monte Carlo and discrete event simulations, » in *IMACS - 17th congress on Scientific Computation, Applied Mathematics and Simulation*, (juill. 2005), Paris, France : in Borne, Benrejeb, Dangoumau & Lorimier Eds, ISBN 2-915913-02-1, 2005.

[ACTI34] J. BEUGIN et L. RENAUX D.and Cauffriez, « A SIL quantification approach to complex systems for guided transportation, » in *ESREL 2005 - European Safety and Reliability conference*, (juin 2005), Gdansk, Pologne : in Kolowrocki Eds, Taylor & Francis Group, 2005, p. 197-204.

[ACTI35] D. RENAUX, J. BEUGIN et L. CAUFFRIEZ, « Allocation et évaluation de la sécurité globale d'un système de transports guidés, » in *PENTOM 2005 - Performances et Nouvelles Technologies en Maintenance*, (avr. 2005), Marrakech, Maroc, 2005, p. 289-303.

[ACTI36] D. RENAUX, J. BEUGIN et L. CAUFFRIEZ, « Proposal for a neural network approach and ordering heuristic for the fault tree evaluation, » in *ESREL 2003 - European Safety and Reliability conference*, (juin 2003), Maastricht, The Netherlands : in Bedford & van Gelder Eds, ISBN 90-5809-551-7, 2003, p. 1301-1306.

Communications avec actes dans un congrès national (ACTN)

[ACTN1] M. CHELOUATI, A. BOUSSIF, J. BEUGIN et E.-M. EL-KOURSI, « Une approche orientée risques pour la prise de décision dans les trains autonomes : Cas de la fonction anti-collision, » in *24ème congrès Lambda-Mu*, (14-17 oct. 2024), Bourges, France, 2024.

[ACTN2] M. CHELOUATI, A. BOUSSIF, J. BEUGIN et E.-M. EL-KOURSI, « Argumentaire de sécurité graphique pour l'assurance de sécurité des trains autonomes, » in *23ème congrès Lambda-Mu*, (11-13 oct. 2022), Paris-Saclay, France, 2022.

[ACTN3] A. BOUSSIF, S. COLLART-DUTILLEUL, F. BARANOWSKI, J. BEUGIN et W. SCHÖN, « Démonstration de la sécurité opérationnelle de la téléconduite des trains : contexte, méthodologie et défis, » in *22ème congrès Lambda-Mu, e-congrès*, France, 2020.

[ACTN4] O. HIMRANE, J. BEUGIN et M. GHAZEL, « Proposition d'une approche orientée modèles pour évaluer la sécurité des systèmes de signalisation ferroviaire utilisant les GNSS, » in *22ème congrès Lambda-Mu, e-congrès*, (13 oct. 2020), France, 2020.

[ACTN5] D. MAILLAND, M. SCHAFF, A. THIONVILLE et J. BEUGIN, « Comparaison de l'approche sécurité multi-domaines, » in *21ème congrès Lambda-Mu*, (16-18 oct. 2018), Reims, France, 2018.

[ACTN6] J. BEUGIN, K.-A. OUEDRAOGO, E.-M. EL-KOURSI, J. CLARHAUT, D. RENAUX et F. LISIECKI, « Pratiques partagées ou divergentes d'allocation de niveaux d'intégrité de sécurité dans le domaine ferroviaire, » in *20ème congrès Lambda-Mu*, (11-13 oct. 2016), Saint-Malo, France, 2016.

[ACTN7] J. BEUGIN et J. MARAIS, « Propriétés de sûreté de fonctionnement d'un système embarqué de localisation par satellites dédié à la sécurité ferroviaire, » in *18ème congrès Lambda-Mu*, (16-18 oct. 2012), Tours, France, 2012.

[ACTN8] J. BEUGIN, D. RENAUX et L. CAUFFRIEZ, « Modélisation d'arbres de fautes par réseaux neuronaux pour l'évaluation de la sûreté de fonctionnement de systèmes complexes, » in *PENTOM 2003 - Performances et Nouvelles Technologies en Maintenance*, (26-28 mars 2003), Valenciennes, France : Presses Universitaires de Valenciennes, ISBN 2-905725-51-6, 2003, p. 315-327.

Communications orales sans actes dans un congrès international ou national (COM)

[COM1] R. SADDEM-YAGOUBI, J. BEUGIN et M. GHAZEL, « Vérification formelle d'un système de signalisation ferroviaire à base de cantons mobiles, » in *MSR'23 - Modélisation des Systèmes Réactifs*, (23 nov. 2023), Toulouse, France, 2023.

[COM2] I. SASSI, E.-M. EL-KOURSI, J. CLARHAUT, D. RENAUX et J. BEUGIN, « Safety Requirements of the New Onboard Train Integrity Function, » in *4th SmartRacon scientific workshop, organised by CEIT*, (20 oct. 2022), San Sebastian, Spain, 2022.

[COM3] I. SASSI, J. BEUGIN, N. AIT TMAZIRTE et M. SALLAK, « Extended method for safety target apportionment for the certification of satellite-based railway localization system, » in *2nd SmartRacon scientific workshop, organised on-line by CEIT, online*, (24 nov. 2020), 2020.

[COM4] J. BEUGIN, A. FILIP et J. MARAIS, « Analysis of the Galileo satellite-based location function in terms of railway safety requirements, » in *CERGAL-Certification of GNSS Systems & Services*, (2-3 avr. 2008), Braunschweig, Allemagne, 2008.

[COM5] A. FILIP, J. BEUGIN, J. MARAIS et H. MOCEK, « A Relation among GNSS Quality Measures and Railway RAMS Attributes, » in *CERGAL-Certification of GNSS Systems & Services*, (2-3 avr. 2008), Braunschweig, Allemagne, 2008.

[COM6] A. FILIP, J. BEUGIN, J. MARAIS et H. MOCEK, « Galileo Safety-of-Life Service and railway RAMS, » in *EURNEX-ZEL-GNSS 2008, workshop on GNSS-Based Train Position Detection Device*, (6 juin 2008), Stary Smokovec, Slovaquie, 2008.

Séminaires (SEM)

[SEM1] R. SADDEM-YAGOUBI, J. BEUGIN et M. GHAZEL, *Moving Block System : Verification Framework*, journée commune du comité techniques SED du GDR-MACS (Systèmes à Événements Discrets) et du comité technique AFSEC (Approches Formelles des Systèmes Embarqués Communicants) du GDR-GPL, Paris, 11 Avril, 2023.

[SEM2] J. BEUGIN, *Approches d'évaluation de sûreté de fonctionnement de systèmes sans fil dans le domaine ferroviaire*, 1ère journée d'échanges réseau thématique de l'IFSTTAR "Transfiab", outils probabilistes pour l'analyse de la fiabilité, Marne-la-Vallée, 7 Déc. 2016.

[SEM3] J. BEUGIN, *Évaluations de sûreté de fonctionnement de systèmes sans fil dans le domaine ferroviaire, approches pour les systèmes satellitaires*, webinaire scientifique du département COSYS de l'IFSTTAR, en visioconférence, 7 Déc. 2015.

[SEM4] J. BEUGIN et J. MARAIS, *Méthodes de sûreté de fonctionnement appliquées aux GNSS*, séminaire du GERI GNSS - Groupes d'Echanges et de recherches Ifsttar sur la Géolocalisation et la Navigation par un Système de Satellites, Villeneuve d'Ascq, 17 Nov. 2011.

[SEM5] J. BEUGIN et J. MARAIS, *L'intégrité dans les applications de localisation ferroviaire*, séminaire de la PFI GNSS - Plateformes Intégratrices sur la Géolocalisation et la Navigation par un Système de Satellites, Villeneuve d'Ascq, 4 Mai, 2010.

[SEM6] J. BEUGIN, J. MARAIS et M. BERBINEAU, *Approches de sûreté de fonctionnement pour des systèmes sans fil : le cas de Galileo*, journée ConecsSdF – Co-design de systèmes commandés en réseaux Sûrs de Fonctionnement, GdR MACS, Paris, 24 Sept. 2009.

[SEM7] J. BEUGIN, *Utilisation des GNSS dans le ferroviaire : la problématique de sûreté de fonctionnement*, 16ème réunion de la Commission du CNIG-Conseil National de l'Information Géographique- géo-positionnement, Paris, 27 Mars, 2008.

Rapports de recherche (RPRE)

[RPRE1] S. MARRONE, F. FLAMMINI, B. JANSSEN, R. SADDEM-YAGOUBI, J. BEUGIN, M. GHAZEL, C. SECELEANU, U. SANWAL, M. BENERECETTI, S. LIBUTTI, E. NAPOLITANO, F. MOGAVERO, R. NARDONE, A. PERON, L. STARACE et V. VITTORINI, *Deliverable D2.2-Moving Block Specification Development*. PERFORMINGRAIL project - PERformance-based Formal modelling et Optimal tRaffic Management for movING-block RAILway signaling, Shift2Rail - H2020 European programme, September, 2023, 171 p.

[RPRE2] E. QUAGLIETTA, N. VERSLUIS, J. BEUGIN, M. GHAZEL et D. KIRKWOOD, *Deliverable D1.2-Best Practices, Recommendations and Standardisation to Definition of the Railway Minimum Operations Performance Standards*. PERFORMINGRAIL project - PERformance-based Formal modelling et Optimal tRaffic Management for movING-block RAILway signaling, Shift2Rail - H2020 European programme, September, 2023, 31 p.

[RPRE3] R. SADDEM-YAGOUBI, J. BEUGIN, M. GHAZEL, S. MARRONE, B. JANSSEN, F. FLAMMINI, C. SECELEANU, U. SANWAL, M. BENERECETTI, S. LIBUTTI, E. NAPOLITANO, F. MOGAVERO, R. NARDONE, A. PERON, V. VITTORINI et J. AOUN, *Deliverable D2.3-Moving Block Verification and Validation*. PERFORMINGRAIL project - PERformance-based Formal modelling et Optimal tRaffic Management for movING-block RAILway signaling, Shift2Rail - H2020 European programme, September, 2023, 87 p.

[RPRE4] I. SASSI, S. IOVINO, G. DE MIGUEL, E.-M. EL-KOURSI, J. BEUGIN, M. GHAZEL et P. GARDY, *Deliverable D7.1-Demonstration and assessment of the On-board Train Integrity systems*. X2Rail-4 project - "Advanced signaling, automation system – Completion of activities for enhanced automation systems, train integrity, traffic management evolution et smart object controllers", Shift2Rail - H2020 European programme, April, 2023.

[RPRE5] M. SAMRA, J. BEUGIN, M. GHAZEL, S. MARRONE, V. VITTORINI, L. STARACE, R. NARDONE, S. DI MARTINO, A. PERON, M. BENERECETTI, R. GOVERDE, C. SECELEANU, F. FLAMMINI, A. MAZINI et M. GARCIA, *Deliverable D1.1-Baseline System Specification and Definition for Moving Block Systems*. PERFORMINGRAIL project - PERformance-based Formal modelling et Optimal tRaffic Management for movING-block RAILway signaling, Shift2Rail - H2020 European programme, November, 2022, 90 p.

[RPRE6] M. GARCIA, V. SUVORKIN, E. QUAGLIETTA, M. SAMRA, J. BEUGIN et S. DI MARTINO, *Deliverable D3.1-Design document of the Location algorithms*. PERFORMINGRAIL project - PERformance-based Formal modelling et Optimal tRaffic Management for movING-block RAILway signaling, Shift2Rail - H2020 European programme, October, 2021, 56 p.

[RPRE7] C. SECELEANU, F. FLAMMINI, S. MARRONE, F. MOGAVERO, R. NARDONE, L. STARACE, V. VITTORINI, R. SADDEM-YAGOUBI, M. GHAZEL, J. BEUGIN, R. GOVERDE, N. VERSLUIS, B. JANSSEN, M. SAMRA, A. MAZINI et M. GARCIA, *Deliverable D2.1-Modelling guidelines and Moving Block Use Cases characterization*. PERFORMINGRAIL project - PERformance-based Formal modelling et Optimal tRaffic Management for movING-block RAILway signaling, Shift2Rail - H2020 European programme, June, 2021, 142 p.

[RPRE8] D. RICCI, I. SASSI et J. BEUGIN, *Deliverable D3.7 - V&V Process Definition, Functional and Non-Functional Test Specification for the Fail-Safe Train Positioning Subsystem*. X2RAIL-2 project - "Enhancing railway signalling systems based on train satellite positioning, on-board safe train integrity, formal methods approach et standard interfaces, enhancing Traffic Management System functions", Shift2Rail - H2020 European programme, 2020, 61 p.

[RPRE9] F. SPERANDIO, S. STURARO, S. SABINA et J. BEUGIN, *Deliverable D3.2 - GNSS Quantitative Analysis for ERSAT-GGC Project*. ERSAT-GGC project - ERTMS on SATELLITE Galileo Game Changer, H2020 European programme, 2018, 46 p.

[RPRE10] J. MARAIS, J. BEUGIN, F. RISPOLI, P. GURNIK et A.-B. TOMA, *State of the art of EGNSS projects for the rail application*. Delivrable D5.1 of the STARS project - Satellite Technology for Advanced Railway Signalling, H2020 European programme, 2017, 61 p.

[RPRE11] T. NGUYEN, J. BEUGIN, M. KASSAB et M. BERBINEAU, *Recommandations pour la mise en œuvre des études de sûreté de fonctionnement des fonctions CBTC sur un lien LTE*. Livrable 6.5.1 du projet Systuf - SYStème Télécom pour les Transports Urbains du Futur, Programme d'Investissements d'Avenir, 2015, 49 p.

[RPRE12] K. OUEDRAOGO, J. BEUGIN, E.-K. EL-KOURSI, J. CLARHAUT et D. RENAUX, *Méthodologie générique d'allocation des SIL aux fonctions de sécurité – Guide d'application*. Livrable L4 du Projet SIL - Safety Integrity Level, sur l'analyse des méthodes de détermination des niveaux de SIL des fonctions critiques de sécurité, projet financé par l'EPSF, 2015, 57 p.

[RPRE13] T. NGUYEN, J. BEUGIN et J. MARAIS, *RAMS parameter analysis*. Deliverable D6.1 of the GaLoROI project - Galileo Localisation for Railway Operation Innovation, 7th European Framework Programme, 2014, 52 p.

[RPRE14] K. OUEDRAOGO, J. BEUGIN, E.-K. EL-KOURSI, J. CLARHAUT et D. RENAUX, *Analyse et comparaison des méthodes et pratiques – Application à deux cas d'études – Système d'accès voyageur et le sous-système de freinage*. Livrable L3 du Projet SIL - Safety Integrity Level, sur l'analyse des méthodes de détermination des niveaux de SIL des fonctions critiques de sécurité, projet financé par l'EPSF, 2014, 36 p.

[RPRE15] K. OUEDRAOGO, J. BEUGIN, E.-K. EL-KOURSI, J. CLARHAUT et D. RENAUX, *État de l'art sur les méthodes d'allocation et de combinaison des SIL*. Livrable L2 du Projet SIL - Safety Integrity Level, sur l'analyse des méthodes de détermination des niveaux de SIL des fonctions critiques de sécurité, projet financé par l'EPSF, 2014, 64 p.

[RPRE16] J. BEUGIN, E.-K. EL-KOURSI, J. CLARHAUT et D. RENAUX, *Plan de gestion de projet*. Livrable L1 du Projet SIL- Safety Integrity Level, sur l'analyse des méthodes de détermination des niveaux de SIL des fonctions critiques de sécurité, projet financé par l'EPSF, 2013, 12 p.

[RPRE17] J. BEUGIN, O. HOINARU, J. MARAIS, D. SCHNÄPP et M. WEGENER, *Structuring of terms describing the quality of GNSS*. Deliverable D1.1 of the QualiSaR project - Development of a Qualification Procedure for the Usage of Galileo Satellite Receivers for Safety Relevant Applications, 7th European Framework Programme, 2012, 31 p.

[RPRE18] J. BEUGIN et J. MARAIS, *Projet GARA : Application de Galileo à la localisation ferroviaire*. Étude financée par la Direction Générale des Infrastructures, des Transports et de la Mer et soutenue par le Predit 4, septembre, 2010, 57 p.

[RPRE19] J. BEUGIN et J. MARAIS, *Étude de sûreté de fonctionnement de la fonction de localisation par satellites*. Livrable L2.2.2 du projet ANR Tr@in-MD - Transport intelligent par fer des Marchandises Dangereuses - soutenu par le PREDIT Go9, 2009, 58 p.

[RPRE20] J. MARAIS et J. BEUGIN, *Étude des performances de Galileo pour des applications ferroviaires, notamment à caractère sécuritaire*. Étude financée par la Direction Générale des Infrastructures, des Transports et de la Mer. N° ISRN : INRETS/RE-09-709-FR, 2009, 43 p.

[RPRE21] L. CAUFFRIEZ, J. BEUGIN, D. RENAUX et P. MILLOT, *Design of Urban Guided Transport Management System : A dependability point of view*. UGTMS Project - Urban Guided Transport Management System, part of Deliverable D6, Safety conceptual approach & guidelines, 5th European Framework Programme, 2003.

Rapports d'étude (RPED)

[RPED1] J. BEUGIN, *Démonstrations de sécurité des systèmes de localisation ferroviaires utilisant les GNSS : contexte et problématique*, Projet SatRail - Étude de faisabilité de l'utilisation des satellites de navigation et de communication pour le contrôle-commande ferroviaire, Railenium, 32 p. 2017.

Rapports d'expertise (RPEX)

[RPEX1] F. BARANOWSKI, J. BEUGIN, M. CUVELIER et J. MARIANO, *Rapport d'évaluation intermédiaire, GO4-Phase de conception générale industrielle, système automatisme de conduite et commandes centralisées*, Projet Grand Paris Express L15-16-17, mission ISA, version 2, 15 p. 2022.

[RPEX2] F. BARANOWSKI, J. BEUGIN, M. CUVELIER et J. MARIANO, *Rapport d'évaluation intermédiaire, GO4.1-Phase de conception générale industrielle, système automatisme de conduite et commandes centralisées - automatismes de conduite*, Projet Grand Paris Express L15-16-17, mission ISA, version 1, 16 p. 2021.

[RPEX3] F. BARANOWSKI, J. BEUGIN, M. CUVELIER et J. MARIANO, *Rapport d'évaluation intermédiaire, plans méthodologiques, système automatisme de conduite et commandes centralisées*, Projet Grand Paris Express L15-16-17, mission ISA, version 1, 6 p. 2020.

[RPEX4] J. BEUGIN, *Évaluation de l'axe stratégique n°6 du CETU "Analyser et maîtriser les risques en exploitation"sur la période 2010-2018*, CETU - Centre d'Études des Tunnels, 2018.

[RPEX5] J. BEUGIN, *Remarks on the parts 2 and 3 of the document entitled "Engineering / safety requirements and SIL allocation" (MP-0-18-SPF-109 REV. 2 170320), Msheireb Downtown Doha Tramway*, Évaluation effectuée pour Certifer, 2017.

[RPEX6] J. BEUGIN, *Expertise de projet*, Appel à projet JCJC (programme blanc Jeunes Chercheuses et Jeunes Chercheurs) – comité SIMI 3 (Matériels et logiciels pour les systèmes et les communications), 2013.

Article de vulgarisation (OV)

J. BEUGIN, *Galileo : applications ferroviaires sécuritaires*, Article de la lettre scientifique AXES de l'INRETS num. 40, octobre 2008, rubrique Valorisation, 2008.

ANNEXE 2 – RÉGLEMENTATIONS ET NORMES DE SÉCURITÉ FERROVIAIRE

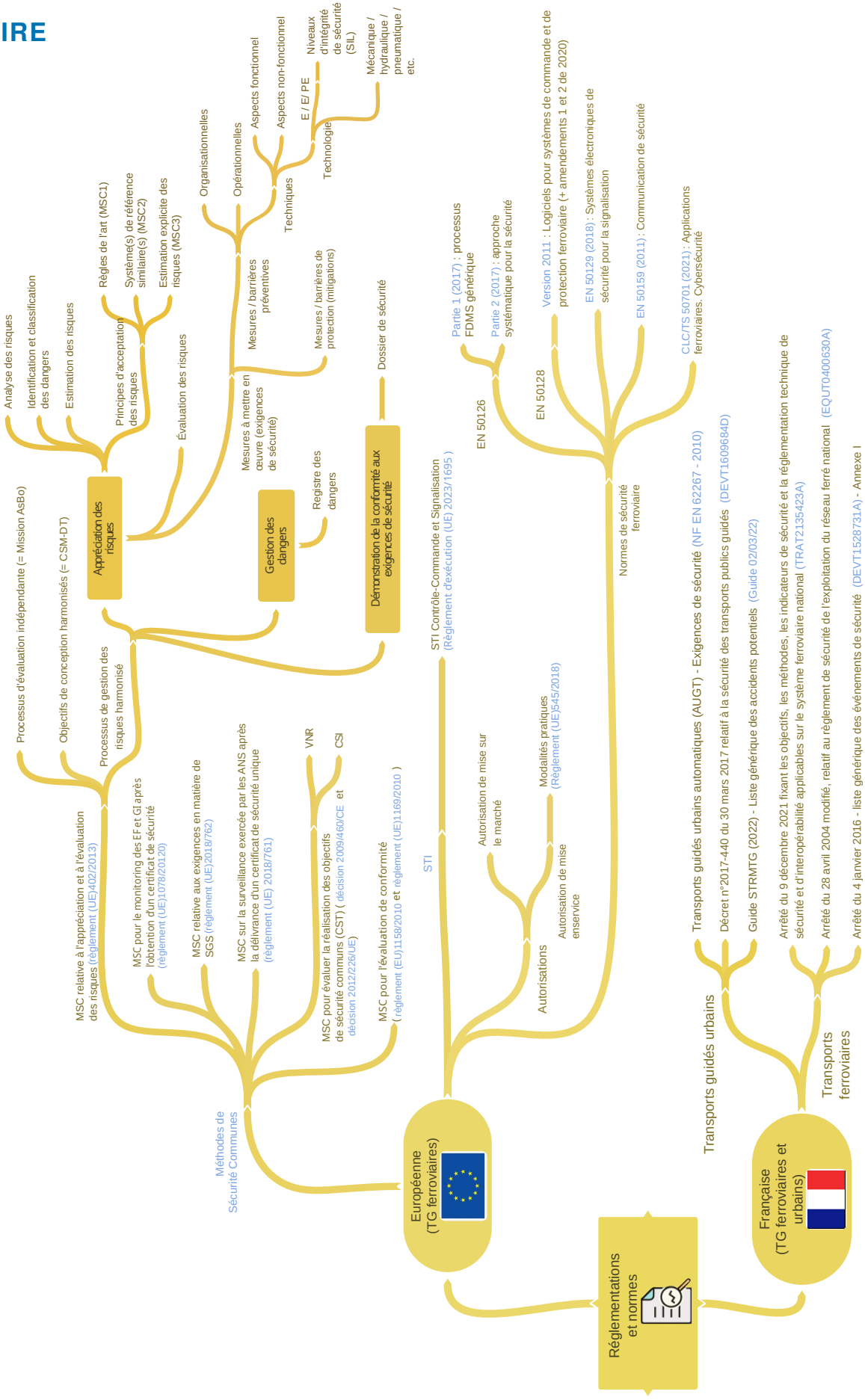


FIGURE II.34 – Réglementations et normes de sécurité ferroviaire

ANNEXE 3 – ÉVALUATION D'ARBRES DE DÉFAILLANCES UTILISANT DES PARAMÈTRES FLOUS

Dans cette annexe, nous exposons les formules communément utilisées avec la méthode de l'arbre de défaillances pour calculer l'indisponibilité d'un système en fonction de l'indisponibilité des ses composants. Les indisponibilités individuelles des composants ainsi que celles liées à leurs combinaisons seront exprimées en fonction des taux de défaillance et de réparation (valeurs constantes) associés aux composants. Lorsqu'il est difficile de définir une valeur précise pour ces taux en raison du manque de données, cette valeur peut être modélisée par un intervalle allant d'une borne inférieure a à une borne supérieure c, avec une valeur plus probable $b \in [a, c]$. Une telle valeur peut être représentée par un nombre flou, une quantité imprécise permettant de tenir compte de cette incertitude [107]. Ainsi, nous rappelons les fondements théoriques des nombres flous et de leur combinaison (les nombres flous triangulaires seront considérés). Enfin, les formules classiques utilisées pour évaluer l'événement sommet d'un arbre de défaillances sont adaptées à l'utilisation des nombres flous.

Indisponibilité d'un événement sommet

Soit un composant i dont la durée de vie et le temps de réparation suivent une distribution exponentielle avec un taux de défaillance λ_i et un taux de réparation ν_i, l'indisponibilité du composant en régime stationnaire est donnée par :

$$U_i = \frac{\lambda_i}{\nu_i + \lambda_i} \tag{II.17}$$

En supposant que les composants défaillants sont immédiatement réparés et que les défaillances de composants sont indépendantes entre-elles, la probabilité de la sortie d'une porte OU, d'une porte ET, et d'une porte K-parmi-N de l'arbre de défaillances est évaluée de manière similaire à l'indisponibilité des systèmes connectés en série, en parallèle ou selon une structure KooN, comme suit [63] :

1. *Lorsque n composants sont connectés en série avec une disponibilité A_i, un taux de défaillance λ_i, et un taux de réparation ν_i, alors l'indisponibilité du système (sortie d'une porte OU) est donnée par :*

$$U_S = 1 - \prod_{i=1}^{n} A_i = 1 - \prod_{i=1}^{n} \frac{\nu_i}{\nu_i + \lambda_i} \tag{II.18}$$

2. *Lorsque le système est composé de n composants identiques ayant un taux de défaillance λ, et un taux de réparation ν, alors l'indisponibilité du système (sortie d'une porte ET avec des entrées identiques) est donnée par :*

$$U_S = \prod_{i=1}^{n} (1 - A_i) = \frac{(\lambda)^n}{(\nu + \lambda)^n} \tag{II.19}$$

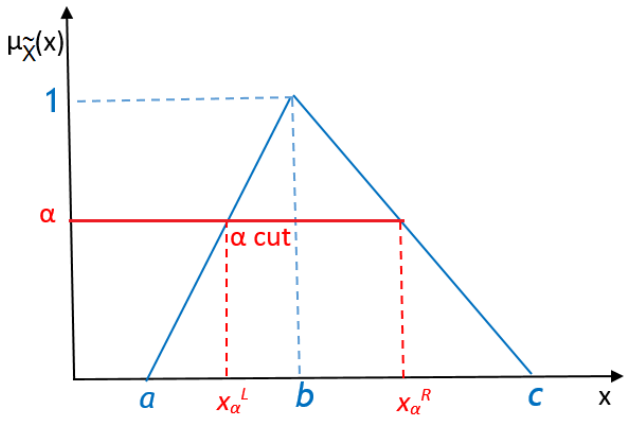


FIGURE II.35 – Illustration d'une α-coupe pour un nombre flou triangulaire

3. *Lorsque le système a une configuration redondante de K parmi N composants identiques ayant un taux de défaillance λ, et un taux de réparation ν, alors l'indisponibilité du système (sortie d'une porte KooN avec des entrées identiques) est donnée par :*

$$U_S = \frac{\lambda^n}{(\lambda+\nu)^n} \sum_{r=0}^{n-k} \binom{n}{r} (\frac{\nu}{\lambda})^r \tag{II.20}$$

Pour un système avec une configuration redondante 2oo3, l'indisponibilité en sortie d'une porte 2oo3 est donnée par :

$$U_S = \frac{3\lambda^2\nu + \lambda^3}{(\nu+\lambda)^3} \tag{II.21}$$

Nombres flous et arithmétique des nombres flous

Définition II.4.1. *Nombre flou*
Soit X un ensemble universel, alors un nombre flou $\tilde{X}$ est un ensemble flou convexe normalisé, défini par sa fonction d'appartenance : $\mu_{\tilde{X}} : X \to [0,1]$. $\mu_{\tilde{X}}(x)$ est le degré d'appartenance de x à $\tilde{X}$. Cette fonction d'appartenance attribue un nombre réel $\mu_{\tilde{X}}(x)$ dans l'intervalle $[0,1]$ à chaque élément $x \in X$.

Définition II.4.2. *Ensemble des α-coupes*
Soit un ensemble flou $\tilde{X}$ dans X et un nombre réel $\alpha \in [0,1]$, alors une α-coupe de $\tilde{X}$, noté $\tilde{X}_\alpha$, est un intervalle défini par : $\tilde{X}_\alpha = \{x \in X, \mu_{\tilde{X}}(x) \geq \alpha\}$ (cf. figure II.35).

Définition II.4.3. *Arithmétique floue avec l'ensemble des α-coupes*
Soient $[x_\alpha^L, x_\alpha^R]$ et $[y_\alpha^L, y_\alpha^R]$ respectivement les α-coupes de $\tilde{X}$ et $\tilde{Y}$, alors l'α-coupe de $\tilde{Z} = f(\tilde{X}, \tilde{Y})$ est définie par $[z_\alpha^L, z_\alpha^R]$ où :

$$\begin{cases} z_\alpha^L = \min_{\{x \in [x_\alpha^L, x_\alpha^R], y \in [y_\alpha^L, y_\alpha^R]\}} f(x,y) \\ z_\alpha^R = \max_{\{x \in [x_\alpha^L, x_\alpha^R], y \in [y_\alpha^L, y_\alpha^R]\}} f(x,y) \end{cases} \tag{II.22}$$

De l'équation (II.22), les α-coupes de fonctions de nombres flous positifs, peuvent être dérivées comme suit :

$$\tilde{Z} = \tilde{X} + \tilde{Y}; \qquad \tilde{Z}_\alpha : [x_\alpha^L + y_\alpha^L, x_\alpha^R + y_\alpha^R] \tag{II.23}$$

$$\tilde{Z} = \tilde{X}.\tilde{Y}; \qquad \tilde{Z}_\alpha : [x_\alpha^L.y_\alpha^L, x_\alpha^R.y_\alpha^R] \tag{II.24}$$

$$\tilde{Z} = 1 - \tilde{X}; \qquad \tilde{Z}_\alpha : [1 - x_\alpha^R, 1 - x_\alpha^L] \tag{II.25}$$

Indisponibilité d'un arbre de défaillances et nombres flous

Les concepts et applications de l'analyse par arbres de défaillances utilisant des paramètres flous a été discuté dans [70]. Soit $\tilde{P}_i$ $(i = 1, 2...n)$ la probabilité floue de l'événement i. Les α-coupes pour la probabilité en sortie de portes ET et OU d'un arbre de défaillances sont comme suit :

$$\tilde{P}_{AND_\alpha}^L = \prod_{i=1}^{n} \tilde{P}_{i_\alpha}^L; \qquad \tilde{P}_{AND_\alpha}^R = \prod_{i=1}^{n} \tilde{P}_{i_\alpha}^R \tag{II.26}$$

$$\tilde{P}_{OR_\alpha}^L = 1 - \prod_{i=1}^{n} (1 - \tilde{P}_{i_\alpha}^L); \qquad \tilde{P}_{OR_\alpha}^R = 1 - \prod_{i=1}^{n} (1 - \tilde{P}_{i_\alpha}^R) \tag{II.27}$$

Les lemmes suivants s'intéressent à la forme de la fonction d'appartenance de la probabilité en sortie d'une porte ET/OU, celle-ci étant en lien avec des taux de défaillance et de réparation flous.

Lemme II.4.1. *Soit $\tilde{X}_i$ le nombre flou dont $x_{i_\alpha}^L$ est non-décroissant et $x_{i_\alpha}^R$ est non-croissant en α, $\tilde{Z}$ étant la probabilité de sortie de la porte ET/OU liée à n nombres flous $\tilde{X}_i$ en entrée, alors z_α^L est non-décroissant et z_α^R est non-croissant en α.*

Ensuite, les α-coupes de la probabilité de sortie de la porte sont évaluées lorsque l'indisponibilité d'un composant de base est calculée à l'aide d'un taux de défaillance flou $(\tilde{\lambda}_i)$ et d'un taux de réparation flou $(\tilde{\nu}_i)$.

Lemme II.4.2. *1. Soit $\tilde{Z}$ l'indisponibilité du composant i, alors une α-coupe de $\tilde{Z}$ est donnée par :*

$$z_\alpha^L = \frac{\lambda_{i_\alpha}^L}{\nu_{i_\alpha}^R + \lambda_{i_\alpha}^L}; \qquad z_\alpha^R = \frac{\lambda_{i_\alpha}^R}{\nu_{i_\alpha}^L + \lambda_{i_\alpha}^R} \tag{II.28}$$

2. Soit $\tilde{Z}$ la probabilité de sortie d'une porte OU, alors une α-coupe de $\tilde{Z}$ est donnée par :

$$z_\alpha^L = 1 - \prod_{i=1}^{n} \frac{\nu_{i_\alpha}^R}{\nu_{i_\alpha}^R + \lambda_{i_\alpha}^L}; \qquad z_\alpha^R = 1 - \prod_{i=1}^{n} \frac{\nu_{i_\alpha}^L}{\nu_{i_\alpha}^L + \lambda_{i_\alpha}^R} \tag{II.29}$$

3. Soit $\tilde{Z}$ la probabilité de sortie d'une porte ET, alors une α-coupe de $\tilde{Z}$ est donnée par :

$$z_\alpha^L = \prod_{i=1}^{n} \frac{\lambda_{i_\alpha}^L}{\nu_{i_\alpha}^R + \lambda_{i_\alpha}^L}; \qquad z_\alpha^R = \prod_{i=1}^{n} \frac{\lambda_{i_\alpha}^R}{\nu_{i_\alpha}^L + \lambda_{i_\alpha}^R} \tag{II.30}$$

4. Soit $\tilde{Z}$ la probabilité de sortie d'une porte 2oo3, alors une α-coupe de $\tilde{Z}$ est donnée par :

$$\begin{cases} z_\alpha^L = \dfrac{(\lambda_\alpha^L)^3 + 3(\lambda_\alpha^L)^2 \nu_\alpha^R}{(\lambda_\alpha^L + \nu_\alpha^R)^3} \\ z_\alpha^R = \dfrac{(\lambda_\alpha^R)^3 + 3(\lambda_\alpha^R)^2 \nu_\alpha^L}{(\lambda_\alpha^R + \nu_\alpha^L)^3} \end{cases} \tag{II.31}$$

Lemme II.4.3. *Soit un composant ayant un taux de défaillance flou $\tilde{\lambda}$ et un taux de réparation flou $\tilde{\nu}$, où λ_α^L, ν_α^L sont non-décroissants en α et λ_α^R, ν_α^R sont non-croissants en α, alors son indisponibilité $\tilde{Z}$ est un nombre flou dont z_α^L est non-décroissant et z_α^R est non-croissant en α.*

Théorème II.4.1. *Soit un système en série/parallèle comprenant des composants ayant des paramètres de fiabilité flous $\tilde{X}_i$, avec $x_{i_\alpha}^L$ non-décroissant et $x_{i_\alpha}^R$ non-croissant en α, l'indisponibilité de ce système est également un nombre flou $\tilde{Z}$, avec $z_{i_\alpha}^L$ non-décroissant et $z_{i_\alpha}^R$ non-croissant en α.*

Ceci est également vrai pour les systèmes avec une configuration 2oo3 ayant des composants identiques.

En résumé, l'arbre de défaillances ayant des paramètres d'entrée flous peut-être évalué selon la **Procédure *Eval*** ci-dessous. D'autre part, d'après le Théorème II.4.1, la fonction d'appartenance de la probabilité de l'événement sommet, $\mu_{\tilde{Z}}(z)$, comporte un côté gauche monotone non-décroissante en z et un côté droit monotone non-croissant en z.

Procédure *Eval* : Évaluation d'un AdD utilisant des paramètres flous

1: Set $\alpha = 0$
2: **while** $\alpha \leq 1$ **do**
3: Determine α-cut set for all input fuzzy numbers.
4: Calculate the α-cut sets for all gate outputs (by eq. (II.28),(II.29),(II.30),(II.31)) until the α-cut set of the top event is obtained.
5: $\alpha = \alpha + \Delta$, where Δ is a small amount (*e.g.* 10^{-4}).
6: **end while**
7: Construct the membership function of the top event by aggregation of all α-cut sets.

ANNEXE 4 – MODÉLISATION DE L'ARCHITECTURE FONCTIONNELLE DE L'ETCS NIVEAU 3

Cette annexe illustre, à l'aide de deux figures, l'architecture fonctionnelle de l'ETCS niveau 3 telle que nous l'avons modélisée dans le cadre du projet européen PERFORMINGRAIL. La première figure présente un schéma illustrant les 13 blocs fonctionnels, les 56 interactions et les 6 acteurs externes identifiés pour le système. La seconde figure utilise le formalisme des diagrammes de blocs internes de SysML (à l'aide de l'outil Papyrus) pour modéliser cette architecture fonctionnelle.

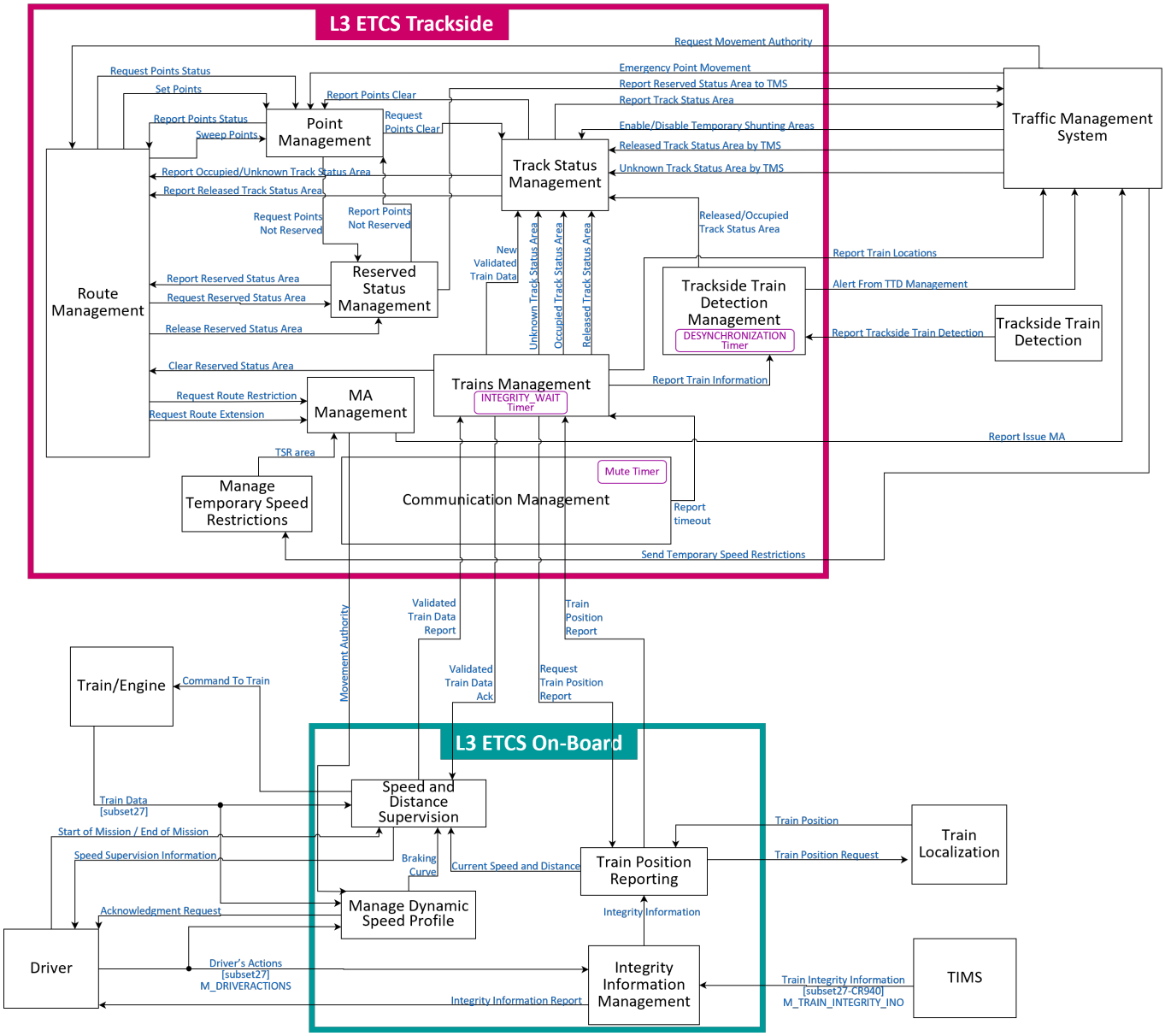


FIGURE II.36 – Schéma illustrant les 13 blocs fonctionnels et les 56 interactions identifiées dans l'ETCS niveau 3

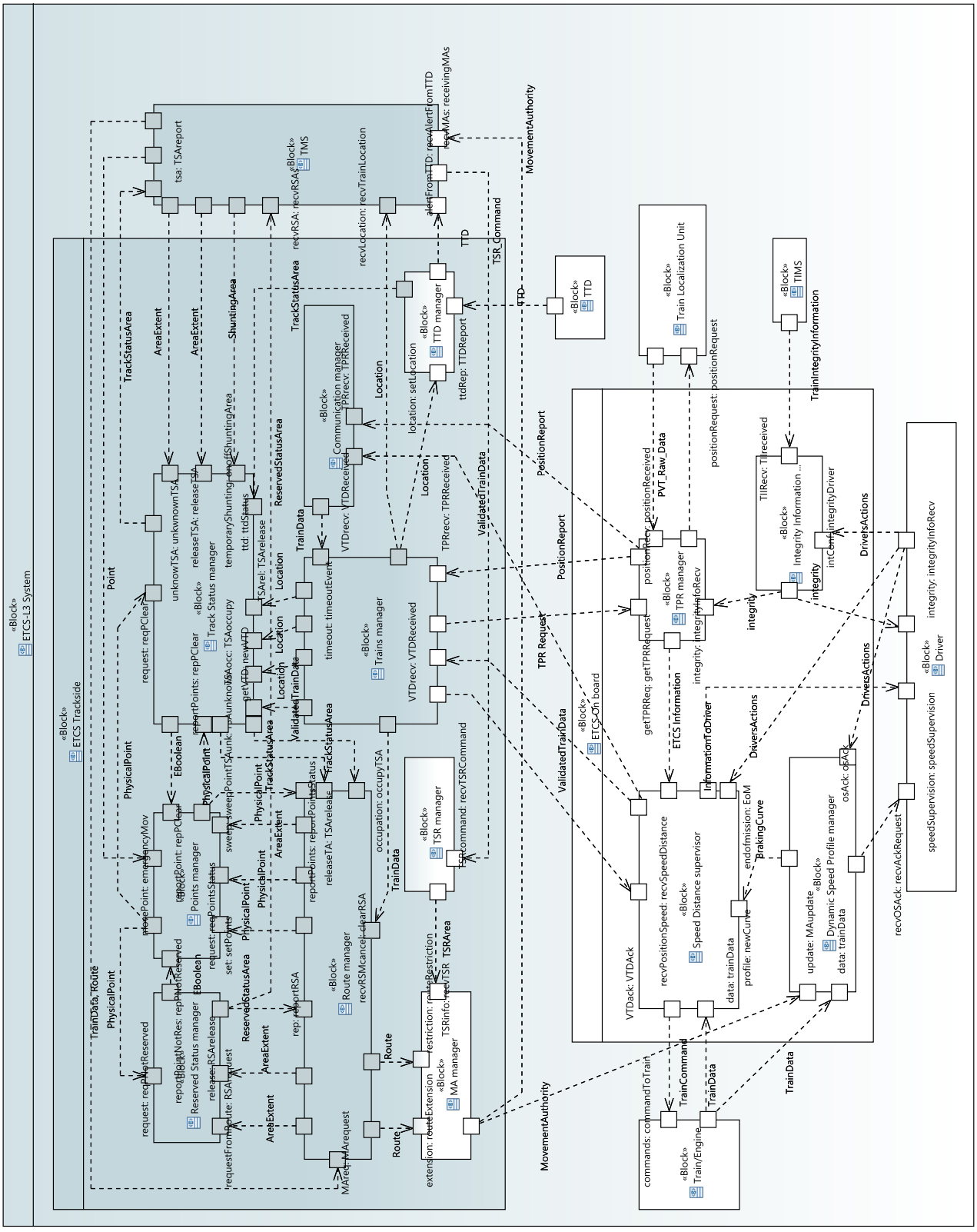


FIGURE II.37 – Diagramme de blocs internes de SysML modélisant l'architecture fonctionnelle d'ETCS niveau 3

RÉSUMÉ

Contributions aux Activités de Sécurité des Systèmes Complexes Critiques Ferroviaires – Cadre des Systèmes de Contrôle-Commande Avancés

L'évolution des systèmes de contrôle-commande ferroviaires, conçus pour gérer les circulations sur le réseau ferré de manière optimisée et en toute sécurité, constitue un levier important pour augmenter l'offre de transport ferroviaire, contribuant ainsi à l'enjeu central de décarbonation de nos mobilités. Les mutations technologiques de ces systèmes permettent une exploitation plus performante des trains. Cependant, elles soulèvent également des questions sur les mesures et conditions de sécurité à adapter face aux changements envisagés. En effet, le nombre croissant d'éléments interconnectés, principalement en raison de l'intégration des nouvelles technologies issues de l'ère de la "digitalisation", accroît davantage la complexité des systèmes de contrôle-commande ferroviaires. Cela élargit le champ d'analyse des risques de ces systèmes critiques et interroge sur la manière d'appréhender les nombreuses interactions supplémentaires engendrées par ces technologies, qu'elles soient de nature technique, fonctionnelle ou dysfonctionnelle.

Pour garantir l'utilisation sûre de technologies sans fil de localisation et de communication dans les systèmes de contrôle-commande ferroviaires avancés, les travaux de recherche présentés dans le mémoire d'HDR visent à contribuer, en termes de sécurité, à différentes phases du processus de développement de ces systèmes. Le but de nos travaux est d'adapter et d'enrichir les processus actuels de gestion des risques pour relever les défis posés par l'emploi en sécurité de ces technologies, tout en respectant le cadre réglementaire européen dans ce domaine. Ainsi, nous avons développé des approches permettant d'allouer des objectifs de sécurité à différents niveaux de décomposition des systèmes de contrôle-commande avancés, ainsi que des approches permettant de démontrer ces objectifs sur les plans technique et opérationnel, malgré les incertitudes liées à l'occurrence de certains dangers, en particulier ceux émanant de la transmission de signaux satellitaires.

Ces approches constituent des moyens méthodologiques originaux d'ingénierie de la sécurité dont peuvent bénéficier les différents acteurs ferroviaires (tels que les exploitants, les constructeurs et les évaluateurs) confrontés à la mise en œuvre de principes opérationnels novateurs utilisant ces technologies, tels que celui fondé sur les cantons mobiles. De plus, les méthodologies développées sont également applicables aux systèmes critiques complexes rencontrés dans d'autres secteurs que le ferroviaire.

ABSTRACT

Contributions to the Safety Activities of Railway Critical Complex Systems – Advanced Control-Command Systems Context

The evolution of railway control-command systems, designed to manage rail traffic in an optimized and safe manner, represents a significant lever for increasing the supply of rail transport, thus contributing to the central challenge of decarbonizing our mobility. The technological changes in these systems enable more efficient train operations. However, they also raise questions about the safety measures and conditions that need to be adapted in response to the envisaged changes. Indeed, the increasing number of interconnected elements, mainly due to the integration of new technologies from the "digitalisation" era, further increases the complexity of railway control-command systems. This broadens the scope of risk analysis for these critical systems, and raises questions about how to handle the numerous additional interactions brought about by these technologies, whether they are technical, functional, or dysfunctional in nature.

To ensure the safe use of wireless localization and communication technologies in advanced railway control-command systems, the research presented in this HDR thesis aims to contribute to various phases of the development process of these systems in terms of safety. The goal of our work is to adapt and enhance the current risk management processes to meet the challenges posed by the safe use of these technologies, while complying with the European regulatory framework in this field. Thus, we have developed approaches to allocate safety targets at different levels of decomposition of advanced control-command systems, as well as approaches to demonstrate these targets on technical and operational levels, despite the uncertainties related to the occurrence of certain hazards, particularly those arising from the transmission of satellite signals.

These approaches represent original methodological means of safety engineering that can benefit various railway stakeholders (such as operators, manufacturers, and assessors) faced with the implementation of innovative operational principles using these technologies, such as those based on moving blocks. Additionally, the developed methodologies are also applicable to complex critical systems encountered in sectors other than railways.