Contribution à l'évaluation de la sécurité de systèmes de localisation ferroviaires basés sur les GNSS par la formalisation des concepts d'intégrité étendue

Cyril Legrand

Thèse de doctorat

De l'Université Lille I

Contribution à l'évaluation de la sécurité de systèmes de localisation ferroviaires basés sur les GNSS par la formalisation des concepts d'intégrité étendue

Présentée par

LEGRAND Cyril

pour obtenir le grade de

Docteur en Automatique, Génie Informatique, Traitement du Signal et de l'Image

soutenue le 16 Décembre 2016 devant le jury composé de

Rapporteurs	
Jean-Marc THIRIET	Professeur, GIPSA-Lab, Université Grenoble-Alpes
Mohamed SALLAK	Maître de conférence HDR, Heudiasyc, Université de Technologie de Compiègne
Examinateurs	
Marion BERBINEAU	Directrice de Recherche, IFSTTAR/LEOST, Villeneuve d'Ascq (Co-directrice de thèse)
Julie BEUGIN	Chargée de Recherche, IFSTTAR/ESTAS, Villeneuve d'Ascq (Encadrante)
Philippe BONNIFAIT	Professeur, Heudiasyc, Université de Technologie de Compiègne
El-Miloudi EL-KOURSI	Directeur de Recherche, IFSTTAR/ESTAS, Villeneuve d'Ascq (Directeur de thèse)
Juliette MARAIS	Chargée de Recherche, IFSTTAR/LEOST, Villeneuve d'Ascq (Co-encadrante)
Nicolas VIANDIER	Chargé d'expertise confirmé en radionavigation, DGA, Rennes
Invités	
David COMBY	Coordinateur interministériel délégué pour les programmes GNSS européens, MEDDE, Paris
Sébastien LEFEBVRE	Chef de projets, IRT Railenium, Valenciennes

N ° d'ordre : 41858 Année 2016

Remerciements

Cette thèse n'aurait pas vu le jour sans le soutien financier de l'IRT Railenium et son partenariat avec l'Institut Français des Sciences et Technologies des Transports, de l'Aménagement et des Réseaux, l'IFSTTAR.

Je souhaiterai remercier Mohamed Sallak du laboratoire Heudiasyc de l'Université Technologie de Compiègne et Jean-Marc Thiriet du laboratoire Grenoble Images Parole Signal Automatique (GIPSA-lab) qui ont accepté de rapporter ce travail de thèse.

Merci à El-Miloudi El-Koursi et Marion Berbineau, directeur(trice) de Recherche de l'IFSTTAR d'avoir dirigé cette thèse et de la confiance qu'ils m'ont accordée durant ces trois années de thèse. Je tiens à remercier tout spécialement Julie Beugin, chargée de recherche de l'unité de recherche ESTAS (Évaluation de la Sécurité des Transports Automatisés et de leur Sécurité) pour ses compétences, ses conseils, sa patience et l'honneur qu'elle m'a fait d'être son premier doctorant. Elle a su m'aider à structurer mes idées et mener à bien cette thèse. Je remercie Juliette Marais, chargée de recherche de l'unité de recherche LEOST (Laboratoire Électronique Ondes et Signaux pour les Transports), pour ses connaissances en matière de systèmes satellitaires. Ses avis et ses remarques constructives m'ont été très utiles au cours de la thèse. Merci également à Blaise Conrard pour son suivi de mes travaux de thèse et ses conseils lors des différentes réunions d'avancement qui ont jalonnées les années de thèse.

Je remercie l'équipe Geoloc de l'IFSTTAR avec Valérie Renaudin et François Peyret pour leur accueil au sein de leur unité. J'adresse un merci tout particulier à Miguel Ortiz, pour m'avoir présenté son équipe et de m'avoir consacré un peu de son temps. Son aide précieuse et éléments ont su enrichir mon travail de thèse avec des données GNSS réelles.

Je tiens à remercier les collègues de bureau qui ont chacun à leur façon rythmé le quotidien. La liste n'est pas exhaustive. Durant 3 ans, j'ai pu rencontrer de belles personnes dont certaines sont devenues des amis. Je vais commencer par mes voisin(e)s de bureau avec Nesrine, Rahma, Pengfei Sun et enfin Abbes. Je poursuis avec les non-permanents (doctorants, stagiaire ou post-doc) : Antoine, Aurélie, Camille, Christophe C, Christophe C-S, Elodie, Julien, Philippe, Olimpia, Wilfried. Concernant les permanents, je remercie Nathalie, Audrey, Lidwine, Bernard, Emmanuel pour les parties administratives et logistiques, Sonia pour son aide LaTeX et autres, Gregory, Paola, Manu avec qui j'ai eu plaisir à discuter.

Enfin, je terminerai par remercier mes proches, en particulier, mes parents pour leur soutien indéfectible qui m'ont continuellement encouragé dans cette voie. Une pensée toute particulière est

réservée à mes grand-mères.

Je dédie cette thèse à mes parents et mes grand-mères

Table des matières

Table des figures

Liste des tableaux

Introduction générale

Contexte et problématiques générales

Les systèmes de navigation par satellites ou GNSS (Global Navigation Satellite Systems), avec notamment le GPS (Global Positioning System) et demain Galileo, sont aujourd'hui largement utilisés dans les systèmes de transport terrestre pour l'aide à la navigation, l'information des voyageurs et le suivi des marchandises. Dans toutes ces applications, la qualité de l'information de localisation n'influe pas sur la sécurité des biens et des personnes (sauf dans le cas particulier du transport de matières dangereuses). En effet, une indisponibilité du service de localisation ou une imprécision sur une courte période peuvent être tolérées car elles n'engendrent aucun risque de dommage matériel ou humain et n'engagent pas la sécurité. Dans le domaine ferroviaire, la localisation par satellites s'intègre progressivement pour ces applications qui ne mettent pas en jeu la sécurité.

En revanche, pour des applications critiques en terme de sécurité, les systèmes GNSS peinent encore à percer. En effet, comme la propagation des signaux satellitaires peut être perturbée par le masquage des infrastructures (ponts, tunnels, tranchées ferroviaires, bâtiments) ou par la végétation aux alentours des voies ferrées, la précision d'un service de positionnement du train reposant sur un système de type GNSS peut vite être dégradée, parfois jusqu'à 500 mètres dans le cas du GPS [ICAO, 2006]. De plus, cette précision est très variable puisque le train évolue dans des configurations environnementales variées le long de son trajet. Le service peut également subir une interruption de quelques secondes à quelques minutes. Cette dernière situation est inacceptable pour une application impliquant la sécurité où la position d'un train, ou plutôt la présence d'un train dans une zone, doit être connue à tout moment. Néanmoins, avec des solutions embarquées qui hybrident et combinent des technologies de localisation actuelles et existantes à bord d'un train, l'apport de la localisation par satellites devient pertinent pour le domaine ferroviaire. En effet, les GNSS peuvent améliorer les systèmes de contrôle-commande des trains notamment en simplifiant les dispositifs actuels situés sur la voie (substitution des balises au sol par une solution embarquée). Depuis les premiers projets nationaux ou européens tels que APOLO (1999-2001) ou LOCOPROL/LOCOLOC (2001-2004), l'intégration des technologies satellitaires est expérimentée pour les applications ferroviaires liées à la sécurité ou non. Aujourd'hui, des projets tels que 3inSat (2012-2014) ou STARS (2016-2018) traitent de la question de l'intégration des systèmes de type GNSS pour des applications de sécurité. Un historique plus complet des différents projets est proposé dans le chapitre 1. Les solutions embarquées présentées dans cette thèse s'inspirent des prototypes utilisés durant les projets cités ci-dessus. Un système de ce type doit intégrer (filtrer, aligner, fusionner, *etc.*) des informations issues de sources hétérogènes (méthodes de mesure et grandeurs physiques différentes) assujetties à des erreurs particulières (propres à la méthode utilisée). À cela, il convient d'ajouter les particularités

de fonctionnement du GNSS et ses sources d'erreurs.

Un sous-système embarqué de localisation devient un élément critique dans un système ferroviaire quand il peut porter atteinte à la sécurité des biens et des personnes. Cette thèse a pour objectif de contribuer à la mise en service d'un tel sous-système critique en proposant une démarche d'évaluation de la sécurité au sein de la démonstration globale de sécurité requise par les textes réglementaires ferroviaires. En effet, le défi actuel porte sur cette démonstration globale de sécurité en tenant compte des spécificités des systèmes GNSS afin de répondre aux exigences de sécurité énoncées dans les normes ferroviaires [EN 50126, 2000], [EN 50128, 2001] et [EN 50129, 2003]. Ces normes requièrent la détermination du degré de confiance que l'utilisateur peut placer dans le service délivré par le nouveau système en analysant et en évaluant ses performances en termes de sûreté de fonctionnement (SdF) c'est à dire la fiabilité, la disponibilité, la maintenabilité et la sécurité. De plus, cette démonstration doit être compatible avec le règlement européen [Réglement 2015/1136, 2015] qui définit une Méthode de Sécurité Commune relative à l'évaluation et à l'appréciation des risques compte tenu de trois principes d'acceptation du risque : l'application des codes de pratique, la comparaison avec des systèmes similaires et l'estimation explicite des risques. La démonstration globale de sécurité apporte les éléments justificatifs nécessaires à l'élaboration du dossier de sécurité qui permettra l'accord des autorités pour la mise en service du système. Afin de tenir compte de ce cadre réglementaire européen et des travaux aujourd'hui réalisés dans le domaine aéronautique sur les risques liés à la localisation GNSS, la thèse se concentrera sur des évaluations de critères liés à la performance de sécurité.

Comme indiqué précédemment, la mise en œuvre d'un système GNSS dans le cadre d'applications de sécurité rend nécessaire l'évaluation de sa sûreté de fonctionnement. Plusieurs verrous doivent être levés pour réaliser cette évaluation. Alors que la modélisation des erreurs liées à la propagation des signaux dans l'atmosphère est bien formalisée, ce n'est pas le cas pour les autres types d'erreurs. Ainsi, en raison de l'influence de l'environnement de propagation sur les performances, il convient de placer le système GNSS dans un nombre de configurations environnementales infini. Dans la pratique, il est donc impossible de couvrir entièrement les conditions d'utilisation du système lors d'une évaluation de sûreté de fonctionnement. L'évaluation par des méthodes opérationnelles de SdF est donc impossible. En effet, ces analyses s'appuient sur la collecte de données brutes de retour d'expérience afin de déterminer quantitativement les attributs de SdF. Or, ce retour d'expérience d'utilisation des GNSS dans le domaine de la sécurité ferroviaire est, pour l'instant, insuffisant. Face à ce constat, de nouvelles méthodes, adaptées aux systèmes de localisation fondés sur les GNSS, doivent être proposées. C'est donc l'objet de ce travail de thèse.

L'Institut de Recherche Technologique Railenium, en soutenant cette thèse, montre l'importance qu'il accorde à la sûreté de fonctionnement des systèmes de localisation ferroviaire embarqués utilisant les systèmes de type GNSS. Cette thèse contribue donc à l'un des objectifs de l'IRT : contribuer à la performance des systèmes ferroviaires. La thèse s'inscrit totalement dans les trois enjeux principaux de l'IRT Railenium : l'amélioration des réseaux ferrés (par l'optimisation de la capacité ferroviaire, la gestion des situations perturbées et l'interopérabilité), l'optimisation des coûts (par la baisse du coût du réseau ferré) et l'enjeu écologique (par la baisse de l'empreinte écologique du réseau).

Organisation du mémoire de thèse

Cette section présente la structure du mémoire ainsi qu'un court aperçu du contenu des différents chapitres. Le mémoire se compose de quatre chapitres. Le premier chapitre propose de répondre aux questions suivantes :

— Quels sont les systèmes/capteurs de localisation ferroviaire existants ?
— Quel est le fonctionnement des systèmes de navigation par satellites (GNSS) ?
— Quels sont les enjeux de leur intégration dans un système ferroviaire et comment les GNSS y répondent ?
— Quels sont les verrous scientifiques relatifs à leur utilisation en milieu ferroviaire et plus spécifiquement à l'évaluation de leur sécurité ?

Un état de l'art sur les différentes techniques et moyens de localisation employés dans des applications ferroviaires ainsi que la présentation des technologies satellitaires répondent aux deux premières questions. Une section est consacrée aux techniques avancées de localisation par satellites avec notamment l'emploi de systèmes et d'algorithmes améliorant les performances des GNSS. La réponse à la troisième question se décline selon plusieurs enjeux à la fois économiques, écologiques et techniques. La dernière question pose les problématiques liées aux risques non maitrisés inhérents à l'utilisation des GNSS (la réflexion des signaux GNSS sur les éléments de l'environnement notamment) et à la différence de classes d'attributs de performances des systèmes de localisation dans les domaines ferroviaires (attributs FDMS) et aéronautiques (attributs Précision, Disponibilité, Continuité et Intégrité). Ces problématiques constituent les principaux freins à l'évaluation de la sécurité des systèmes de localisation ferroviaire fondés sur l'utilisation des satellites.

Le deuxième chapitre est consacré à la sécurité des systèmes de localisation considérés dans cette thèse. Pour cela, ce chapitre pose le cadre réglementaire européen de la gestion des risques dans le domaine ferroviaire. Les moyens et les méthodes de la sûreté de fonctionnement sont décrits d'abord en rappelant les définitions puis en présentant les méthodes d'analyse. Nous montrons que ces méthodes sont inadaptées pour l'évaluation de la sécurité d'un système de localisation de type GNSS au regard des problématiques soulevées dans le chapitre 1. Par conséquent, deux analyses sont proposées pour répondre à l'insuffisance de retours d'expériences et de méthodes adaptées pour les systèmes de localisation de type GNSS : une analyse causale et une analyse de sensibilité. Ces dernières sont menées sur des systèmes multicapteurs avec un récepteur GNSS. La première propose d'identifier les combinaisons d'états de capteurs critiques. Ces états sont analysés par rapport à l'erreur de position fournie par le système de localisation global. La persistance au cours du temps des combinaisons critiques est également analysée. La seconde analyse repose sur des mesures de sensibilité pour identifier les capteurs dont les erreurs affectent le plus la sortie d'un système multicapteurs. Chacune de ces analyses met en avant des paramètres intéressants liés à l'attribut de sécurité (mesures de sensibilité, combinaisons d'états critiques, *etc.*).

Le troisième chapitre de ce mémoire propose d'explorer plus en détails la question de l'évaluation des performances des GNSS dans le domaine de l'aéronautique. L'intégrité est apparue comme l'attribut de performances des GNSS (uniquement) étroitement lié à la sécurité telle que définie dans les normes ferroviaires. Cet attribut n'est pas défini et désigne des concepts différents (intégrité d'un convoi ferroviaire et niveau d'intégrité de sécurité (SIL)) dans le domaine ferroviaire. Ainsi, la contribution de ce chapitre porte sur la définition de l'intégrité de localisation dans le domaine ferroviaire et l'extension à d'autres systèmes de localisation que les systèmes de type GNSS seuls. La

contribution immédiate concerne le lien existant entre l'intégrité et la sécurité, plus précisément, la relation entre la probabilité de défaillances liées à la sécurité et le risque sur l'intégrité. Le concept d'intégrité fait appel à des méthodes d'évaluation particulières : le contrôle d'intégrité. Ainsi, ce troisième chapitre présente ma contribution sur l'adaptation des algorithmes de contrôle d'intégrité aux systèmes de localisation ferroviaire intégrant un récepteur GNSS. Étant donné que l'intégrité est uniquement définie pour les GNSS et non pour les autres systèmes de localisation, une adaptation à la fois sémantique et algorithmique est nécessaire. L'algorithme résultant repose sur la détection des biais instantanés (conséquence des phénomènes de multitrajets) et des erreurs à croissance lente (conséquence de la dérive des centrales inertielles). Afin de quantifier le risque sur l'intégrité, cette seule détection n'est pas suffisante. Il convient d'évaluer si l'erreur de position est supérieure à un seuil donné et si cette erreur persiste au delà d'un intervalle de temps donné. L'erreur de position n'étant pas connue de l'utilisateur, une estimation de celle-ci doit être calculée. Cette estimation est appelée *niveau de protection*. Une mise en relation entre le risque sur l'intégrité de la localisation et la probabilité liée à la sécurité est ensuite proposée.

Le quatrième chapitre traite d'une application concrète de l'évaluation de la sécurité par l'intégrité présentée dans le chapitre 3. Il présente l'architecture du système de localisation choisi dans le chapitre 2 : un système GNSS/INS (INS pour *Inertial Navigation System*). Nous proposons de nous placer dans un cas d'utilisation particulier de ce système : la gestion de l'espacement entre deux trains au sein du système de contrôle-commande ferroviaire européen ERTMS (European Railway Traffic Management System). Le niveau 3 d'intégration d'ERTMS dans une infrastructure ferroviaire repose sur l'utilisation du concept de canton mobile pour lequel le système de contrôle-commande définit une distance de sécurité variable derrière chaque train en fonction des informations de localisation des trains. Le risque majeur dans ce cas d'utilisation est la collision entre deux trains. Dans la section qui suit la description de l'implémentation du système de localisation considéré, nous proposons d'identifier des situations critiques en terme d'intégrité qui conduisent à ce risque. Pour les identifier, il convient de définir des exigences sur l'intégrité de la localisation : une limite d'alerte à comparer avec un niveau de protection calculé à chaque instant, un temps d'alerte et un objectif en terme de risque sur l'intégrité. Ces valeurs sont issues des spécifications ERTMS. Le système présenté dans la première section de ce chapitre est simulé et enrichi par des données réelles GNSS fournies par l'équipe GEOLOC de l'IFSTTAR. La phase de détection des biais instantanés et des erreurs à croissante lente et la phase de calcul du niveau de protection sont mises en œuvre sur les résultats de simulation du système GNSS/INS. L'application numérique du lien entre les attributs d'intégrité et celui de sécurité est effectuée pour conclure sur la valeur effectivement atteinte de la probabilité de défaillance liée à la sécurité lors des simulations.

La conclusion de ce mémoire résume les contributions proposées dans le cadre de l'évaluation de la sécurité des systèmes de localisation avec GNSS. Les travaux de thèse ouvrent des perspectives prometteuses sur différents aspects (systèmes, algorithmes, portée de l'évaluation de l'intégrité, évaluation sur d'autres attributs, *etc.*.)

Chapitre 1

Systèmes de localisation ferroviaires autonomes : enjeux et problématiques de l'utilisation des technologies satellitaires

Sommaire

1.1 Introduction

La fonction de localisation est une fonction importante du système de contrôle-commande ferroviaire. La localisation d'un train est une information essentielle pour permettre au train de se déplacer en toute sécurité. Les systèmes actuels que nous présenterons dans ce chapitre sont coûteux et présentent des contraintes de mise en œuvre, d'exploitation et de maintenance assez élevées. Pour faire évoluer ces systèmes, de nombreux acteurs, industriels de la signalisation ou opérateurs étudient

le potentiel des solutions satellitaires.

Dans ce chapitre, nous abordons les problématiques liées à la localisation ferroviaire réalisée à l'aide de systèmes satellitaires dont l'utilisation est au cœur des enjeux d'évolution des systèmes de contrôle-commande. En Europe, cette évolution s'inscrit dans le processus d'harmonisation des 27 systèmes de contrôle-commande existants via le développement du système ERTMS (*European Railway Trafic Management System*). Le dernier niveau d'intégration de l'ERTMS (niveau 3) dans le paysage ferroviaire européen, toujours à l'étude, permet d'envisager l'usage de nouvelles technologies telles que les technologies satellitaires. Ces solutions peuvent contribuer à l'allègement de l'infrastructure en réduisant le nombre d'équipements au sol. Il reste à démontrer que ces nouvelles techniques de localisation ferroviaire répondent favorablement aux exigences ferroviaires et particulièrement en matière de sécurité.

Ce chapitre d'introduction des travaux de thèse s'organise comme suit. La section 1.2 est consacrée à un état de l'art des différentes techniques de localisation actuellement employées pour des applications de sécurité ferroviaires. Nous distinguons les méthodes dites localisation relative de celles dites positionnement absolu.

La section 1.3 est dédiée aux systèmes de localisation ferroviaire fondés sur les technologies satellitaires avec une présentation des principes de fonctionnement des *Global Navigation Satellite Systems* (GNSS). Les techniques avancées de localisation satellitaire telles que les systèmes d'augmentation et des algorithmes sophistiqués améliorant les services que les GNSS fournissent sont également présentés.

La section 1.4 introduit les enjeux économiques, écologiques et techniques de la localisation satellitaire dans un contexte ferroviaire et les réponses des GNSS face à ces enjeux. L'idée d'utiliser les GNSS pour le domaine ferroviaire a émergé au début des années 90 et a fait l'objet de plusieurs projets et prototypes qui sont présentés à la fin de cette section.

La section 1.5 détaille les problématiques liées à l'évaluation de la sécurité des GNSS. Cela concerne, plus précisément, les risques non maitrisés par les techniques présentées à la section 1.3. Nous expliquerons pourquoi cet aspect est primordial et incontournable dans la conception de nouveaux systèmes pour des applications ferroviaires liées à la sécurité telles que le contrôle-commande (en particulier dans ERTMS).

1.2 Localisation ferroviaire actuelle

Après quelques généralités sur la localisation, cette partie recense les techniques mises en œuvre pour localiser un train. C'est une fonction principale dans tout système de contrôle-commande et de signalisation. Nous distinguons ensuite le type de localisation : relative ou absolue.

1.2.1 Généralités sur la localisation

Avant de présenter les différentes techniques de localisation d'un véhicule, il est nécessaire de bien définir ce qu'est une localisation et à quel moment nous parlons de navigation ou de positionnement. De manière générale, la localisation est la détermination de l'emplacement où se situe une chose, un phénomène ou son origine [CNRTL, 2014b]. On utilise fréquemment les termes **localisation**,

positionnement et **navigation**.

Localisation et **positionnement** sont des termes considérés comme équivalents. En revanche, la navigation désigne toutes les techniques pour calculer non seulement la position, la vitesse et l'accélération de tout mobile mais la trajectoire, le guidage et la commande des organes de direction [Groves, 2013] [Laneurit, 2006]. La localisation est donc un sous-ensemble de la navigation. Dans les applications que nous viserons dans ce mémoire, nous traiterons de localisation et non de navigation.

La **localisation** d'un objet peut se faire de manière relative ou absolue. La localisation **relative** consiste à estimer la position courante relativement à la dernière position connue. La localisation **absolue** est l'estimation de la position par rapport à un repère fixe de l'environnement (amer en navigation maritime, balise ferroviaire). Selon le type de localisation, il existe deux catégories de capteurs qui fournissent une position relative ou absolue :

— Les capteurs **proprioceptifs** : ils déterminent les informations à partir de ce qu'ils perçoivent localement du déplacement du véhicule. Ce sont des capteurs ayant une bonne précision à court terme mais qui souffrent d'un biais cumulatif dans le temps. Celui-ci deviendra grand si aucun recalage n'est effectué.

— Les capteurs **extéroceptifs** : ils mesurent la position absolue d'un véhicule à partir d'un point fixe dans l'environnement (un relief naturel particulier ou un objet artificiel comme un satellite ou une balise) dont les coordonnées dans un référentiel donné sont connues. Ces capteurs sont couramment utilisés pour le recalage du biais des mesures relatives.

Ces groupes de capteurs sont souvent utilisés ensemble pour leur complémentarité. Cette association ou hybridation sera discutée dans la sous-section 1.3.4.1.

1.2.2 Localisation relative et navigation à l'estime

La navigation à l'estime (ou *dead reckoning* en anglais) revient à suivre le déplacement d'un mobile de point en point, grâce aux mesures de distance et de cap effectuées par des capteurs embarqués. L'ensemble de ces dispositifs fournit ce que nous appellerons plus tard une solution de navigation. Les capteurs présentés ici sont de type proprioceptif.

1.2.2.1 Odomètre

Incontournable dans la localisation ferroviaire, l'odométrie est une technique de détermination de la distance parcourue par un mobile depuis une origine. La position est extrapolée par intégration de la vitesse ($x = v \times t$) mesurée au cours du temps par l'odomètre. Les performances d'un odomètre dépendent donc de la précision de la vitesse qu'il mesure et de l'horloge cadençant son fonctionnement.

Classiquement, la distance parcourue fournie par l'odomètre est déterminée par des mesures de vitesse de rotation de la roue. Ces mesures sont effectuées par un encodeur rotatif fixé sur un essieu et couplé à l'axe des roues. L'encodeur est composé d'un disque sur lequel sont disposés des zones opaques et transparentes appelés pistes. Leur nombre détermine notamment la résolution de l'encodeur et, par extension, sa précision. La lecture de ces pistes est réalisée au moyen d'un capteur sans contact (reluctance, à effet Hall, optique, *etc.*) qui génère des impulsions électriques.

Ces impulsions sont fonction de la distance parcourue depuis un point particulier appelé référence [Toledo-Moreo et al., 2007] (balise sur la voie par exemple) avec une imprécision de l'ordre de $\pm 2\%$ (odométrie ferroviaire [Thevenot et al., 2003]). Dans le système de contrôle-commande et de signalisation ERTMS, l'erreur de position permise par l'odométrie est bornée par l'intervalle de confiance $\pm 5 + 5\%d$ [SUBSET-041, 2015] où d est la distance parcourue par le train depuis le dernier point de référence (balise).

La faiblesse de ces systèmes sur essieux résulte des phénomènes de glissement et de patinage. Dans le cas d'un glissement, la roue se bloque et aucune impulsion n'est délivrée par le capteur. Cela se traduit sur l'interface du conducteur par une vitesse qui tend vers zéro. Dans le cas d'un patinage, contrairement au glissement, la roue tourne plus vite. La vitesse affichée est alors anormalement élevée.

Afin de contrer ces phénomènes, il existe plusieurs moyens matériels et logiciels : l'utilisation de capteurs supplémentaires ou des algorithmes de calcul sophistiqués dans le but d'analyser et de filtrer les variations importantes de signaux aberrants [Wilson, 2001].

1.2.2.2 Systèmes inertiels

Les systèmes (ou centrales) inertielles sont des dispositifs complets regroupant gyroscopes et accéléromètres (un couple gyroscope/accéléromètre par axe soit trois gyroscopes/accéléromètres pour une solution de navigation dans un repère (x,y,z)) (cf figure 1.1). Ces derniers mesurent respectivement une position angulaire et une accélération. La vitesse et les angles d'attitude (tangage, lacet et roulis) sont déterminés par un calculateur. Il existe 3 types d'implémentations [Hirwa, 2013] :

— Système avec plateforme stabilisée. Les accéléromètres sont directement reliés à des gyroscopes pour garantir leur alignement sur l'axe considéré.

— Système avec plateforme partiellement stabilisée.

— Système *strap-down*. Les données issues des accéléromètres et des gyroscopes alimentent un processus informatique pour l'alignement.

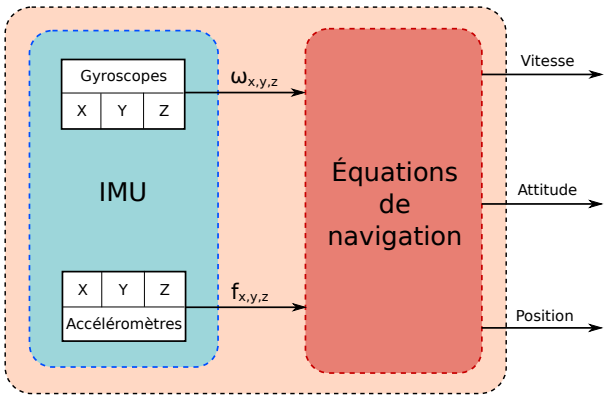


FIGURE 1.1 – *Inertial Navigation System*

Les accéléromètres sont considérés comme des systèmes masse-ressort. L'accélération est direc-

tement déduite de la force exercée sur la masse et mesurée grâce à la déformation du ressort.

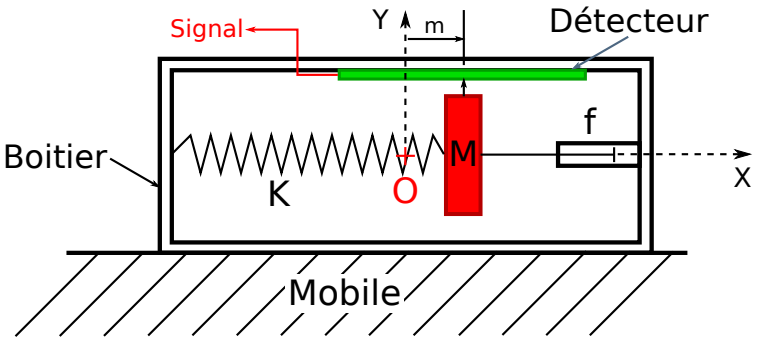


FIGURE 1.2 – Structure de base d'un accéléromètre.

La figure 1.2 montre la structure d'un accéléromètre simple. Lorsqu'une accélération se produit, la masse, retenue par le ressort de constante de raideur K, se déplace. Ce déplacement (m) est alors mesuré via la force spécifique f appliquée sur la masse (sachant l'accélération due à la force gravitationnelle exercée sur la masse M) puis transformé en signal électrique en vue de calculer l'accélération. Le boitier est solidarisé avec le véhicule afin que l'accélération mesurée corresponde bien à celle du véhicule.

Les gyroscopes fournissent une vitesse angulaire et, plus particulièrement, la variation des angles d'attitude (roulis, tangage et lacet).

1.2.3 Localisation absolue

1.2.3.1 Balises

Une balise est un dispositif de signalisation fixe, unique ou jalonnant un trajet, servant de point de repère ou indiquant la voie à suivre, l'obstacle à éviter en mer ou sur terre [CNRTL, 2014a].

Dans le domaine ferroviaire, les balises sont des appareils faisant partie intégrante de l'infrastructure au sol d'un système de contrôle-commande et de signalisation. Dans le système français KVB (contrôle de vitesse par balises), les balises transmettent, au passage d'un train, un message de 172 bits [1].

Ce sont des systèmes passifs : le passage du train active la balise qui émet un message grâce à une antenne embarquée. Ce message (trame) contient des informations de signalisation (distance but, vitesse but, vitesse d'exécution, *etc.*) qui dépend du type de balise. Ces informations sont nécessaires à l'autorisation de mouvement permettant à un train de se déplacer jusqu'à un point cible avec une vitesse donnée. La balise constitue une référence pour la localisation du train et permet le recalage de l'odométrie.

1.2.3.2 RADAR/LIDAR

Les systèmes RADAR (pour *RAdio Detection And Ranging*) utilisent des ondes électromagnétiques pour localiser un objet (présence, position et vitesse). Le principe de base est l'émission d'une

1. Les balises utilisées dans le système ERTMS, les eurobalises, peuvent transmettre un message de 1021 bits [Thouvenot and Pignal, 2007]

onde par un émetteur et la cible réfléchit cette onde indiquant du même coup une information sur sa présence. Le calcul du temps de propagation aller-retour de l'onde permet de mesurer la distance qui sépare l'émetteur de la cible. Dans le cas d'un objet mobile, la fréquence du signal de retour est décalée (Effet Doppler). Ce décalage permet le calcul de la vitesse de la cible.

Les systèmes LIDAR (pour *LIght Detection And Ranging*) utilisent le même principe que le RADAR mais la fréquence des ondes électromagnétiques envoyées diffère. Dans le cas du RADAR, il s'agit d'ondes radio alors que, pour le LIDAR, ce sont des ondes lumineuses qui sont utilisées.

Dans cette section, les principaux capteurs de localisation embarqués existants dans le milieu ferroviaire ont été présentés. Le système de localisation par satellite est décrit dans la section suivante se propose de décrire le fonctionnement.

1.3 Systèmes de localisation ferroviaires autonomes fondés sur les GNSS

1.3.1 GNSS existants et à venir

Le premier système de positionnement par satellite, le GPS (*Global Positioning System*), a été conçu par le DoD (*Department of Defense*) des États-Unis, avant tout pour des utilisations aéronautiques et militaires (notamment pour le suivi de missiles balistiques). Le premier satellite a été lancé en 1979 et la constellation n'est complète et opérationnelle que depuis 1995. Donnant une précision sans égal en comparaison avec les systèmes de positionnement de cette époque, un système satellitaire devient une nécessité d'un point de vue militaire. À la fin des années 80, le président Reagan ouvre progressivement le GPS à des applications civiles à la suite de la catastrophe du vol 007 Korean Air Lines [2] dans le domaine aéronautique puis dans le domaine des transports terrestres (route et transport maritime).

Dans le contexte de la Guerre Froide, la Russie s'est équipée, elle aussi, d'un système équivalent : GLONASS (*Global'naya Navigatsionnaya Sputnikovaya Sistema*). Le premier satellite GLONASS a été lancé en 1980 pour une constellation opérationnelle sur la période 1996 - 2000. Non maintenue après la chute de l'Union Soviétique, la constellation a été remise à jour et est de nouveau complète et opérationnelle depuis 2011.

Face au monopole des États-Unis et dans une période de faiblesse du GLONASS, l'Union Européenne a décidé en 1999 [Conseil de l'Union Européenne, 1999] de créer son propre GNSS, Galileo dont la constellation sera complète à l'horizon 2020. Galileo est une initiative avant tout civile contrairement aux précédentes générations de GNSS. En outre, Galileo fournira des informations d'intégrité des signaux - données très importantes pour l'évaluation des performances des systèmes utilisant ce GNSS, particulièrement en matière de sécurité (cf Chapitre 3).

1.3.2 Architectures et services fournis

Le GPS est constitué de trois parties distinctes appelées segments :

2. Le 1er septembre 1983, ce vol est entré dans l'espace aérien soviétique et a été abattu. L'organisation de l'aviation civile internationale (OACI) a conclu à une erreur de navigation. Cet évènement a motivé l'ouverture du GPS à tous.

— Le segment **spatial** se compose d'un réseau de 24 satellites NAVSTAR évoluant sur 6 orbites autour de 20 000 km d'altitude sur une orbite quasi-circulaire (excentricité proche de 0°) et disposés de façon optimale (six à dix satellites visibles en tout point). L'ensemble des signaux constitue l'interface entre le segment spatial et utilisateur.

— Le segment de **contrôle** assure la partie pilotage et surveillance de l'état des satellites. Des mises à jour transmises aux satellites y sont effectuées depuis des stations au sol.

— Le segment **utilisateur** regroupe les utilisateurs militaires et civils qui en font l'usage et comprend donc l'ensemble des récepteurs.

Le GPS fournit un accès à un service précis (PPS pour *Precise Positioning System*) strictement réservé à des applications militaires et à un service standard (SPS pour *Standard Positioning System*) pour tout utilisateur. Toutefois, la précision du service standard peut être dégradée par un chiffrement appelé SA pour *Selective Availability* passant celle-ci de 10 à 100 m. Ce processus a été désactivé en Mai 2000 pour des raisons politiques. Il est, de plus, rendu obsolète avec les différents systèmes d'augmentation qui existent aujourd'hui (WAAS et EGNOS) présentés dans la sous-section 1.3.4).

Le GNSS européen, Galileo, proposera quatre services (cf [European Commission, 2011] :

— un service tout public (aux performances globalement équivalentes au GPS modernisé),
— un service commercial (crypté et précis au centimètre pour les professionnels),
— un service public mais limité aux utilisateurs autorisés, cryptés et robuste (système anti-brouillage) destiné à des applications sensibles,
— un service de recherche et sauvetage afin de détecter les sinistres, d'alerter les secours et les coordonner sur des zones maritimes, aériennes et terrestres qui contribuera au programme international Cospas-Sarsat.

Les deux principaux GNSS ont été présentés (GPS et Galileo). La sous-section suivante décrit le fonctionnement d'un GNSS (valable aussi bien pour le GPS que pour Galileo).

1.3.3 Fonctionnement des GNSS

La localisation par satellite repose sur le calcul du temps de propagation des signaux émis par les satellites et reçus par un récepteur, et sur le principe de la trilatération [Groves, 2013]. Le temps de propagation est déterminé par la mesure de la différence entre l'instant d'émission du signal et celui d'arrivée au niveau du récepteur. Par multiplication par la vitesse de propagation du signal, la distance satellite-récepteur peut être déduite. En théorie, il faut trois de ces distances pour déterminer une position tridimensionnelle sur Terre. Une quatrième mesure est nécessaire pour lever l'ambiguïté sur le temps que nous verrons plus tard. La position 3D est donnée dans un référentiel géodésique, le WGS 84 (*World Geodetic System*, le système géodésique utilisé par le GPS révisé en 1984), avec une représentation d'un géoïde terrestre particulier. Les distances Satellites-Récepteur forment un système à 3 équations de sphères qui se coupent en deux points. L'un est éliminé car ce point se situe dans l'espace donc non plausible pour le transport terrestre. Seul le deuxième point, sur Terre, est retenu (cf figure 1.4).

Les signaux GNSS sont déviés lors de leur traversée dans l'atmosphère et donc retardés. Ces déviations sont corrigées par l'utilisation de modèles ionosphériques et troposphériques. Des effets relativistes [3] influent sur la précision et l'éloignement satellite-récepteur notamment sur le fait que les horloges des satellites et du récepteur ne sont pas parfaitement synchronisées. Cette désynchronisation est illustrée par la figure 1.3. Côté récepteur, il existe une différence entre l'instant d'arrivée du signal mesuré par rapport à l'instant réel d'arrivée du signal (notée δt_u). Côté satellite, nous trouvons une différence entre l'instant d'émission prévu et l'instant réel d'émission du signal vers le récepteur.

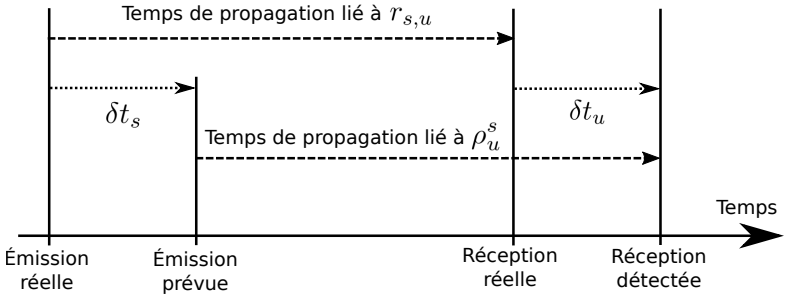


FIGURE 1.3 – Désynchronisation récepteur/satellite (inspiré de Groves [2013]).

Avec :
$\rho_u^s = r_{s,u} + (\delta t_u - \delta t_s)c$, la pseudodistance, mesure de la distance parcourue par un signal envoyé par un satellite s et reçu par un utilisateur u pendant l'intervalle de temps entre l'instant d'émission prévue et l'instant de réception détectée par l'utilisateur,
$r_{s,u}$, la distance réelle entre le satellite s et l'utilisateur u,
δt_u, biais de l'horloge du récepteur d'un utilisateur,
δt_s, biais de l'horloge du satellite, c, la vitesse de la lumière égale à 299 792 458 m/s

Ces différences se chiffrent en nanosecondes par jour, devenant inacceptables si l'exigence de précision est grande. En effet, un biais de 12 nanosecondes [Ashby, 1997] engendre une erreur de position de 3,6 mètres aux fréquences de fonctionnement du GPS (L1 = 1575,42 MHz et L2 = 1227,60 MHz) [CNES, 2011]. Il est donc nécessaire de corriger ce biais d'horloge en resynchronisant les horloges satellites/récepteur. Cela est possible en considérant une variable supplémentaire associée à ce biais d'horloge. Pour résoudre ce problème à 4 inconnues, il faut une quatrième équation c'est à dire une autre distance satellite-récepteur. Ceci signifie la prise en compte d'un quatrième satellite. Si on tient compte du décalage d'horloge satellite/récepteur, on ne parle plus de distance satellite/récepteur (notée $r_{s,u}$) mais de pseudodistances (notée ρ_u^s).

Le GPS, GLONASS et Galileo constituent le paysage présent et futur de la localisation satellitaire globale. Par soucis de concision, nous ne détaillerons pas les autres systèmes (ou projets) de localisation satellitaire. Citons notamment BeiDou (Chine), l'IRNSS (*Indian Regional Navigational Satellite System*) et le QZSS (*Quasi-Zenith Satellite System* (Japon)). Ces derniers ont une couverture régionale donc leurs signaux ne sont pas captés sur la surface complète du globe, mais la vocation de BeiDou est à terme internationale

Bien que ces technologies soient déployées et utilisées depuis plus de 20 ans, elles restent peu utilisées pour le domaine ferroviaire. Le succès de leur utilisation dans le domaine aéronautique,

3. Les théories sur la relativité énoncées par Einstein mettent en évidence un effet de dilatation du temps dû aux vitesses relatives des satellites et d'un utilisateur et l'attraction gravitationnelle de la Terre.

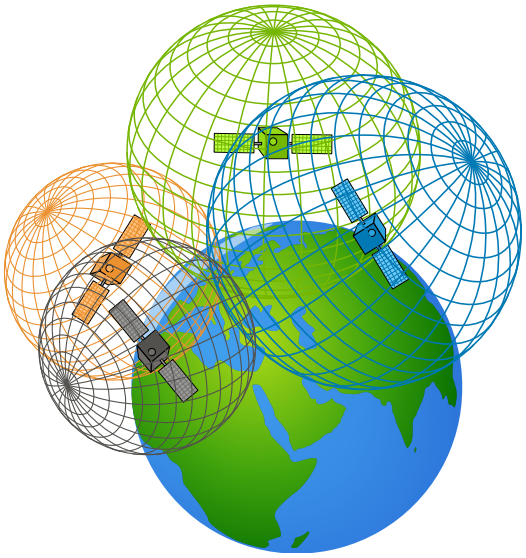


FIGURE 1.4 – Positionnement par satellites.

maritime et automobile motive les acteurs du secteur ferroviaire afin de les intégrer dans les trains en particulier pour des applications de sécurité.

1.3.4 Techniques avancées de localisation satellitaire

Dans cette sous-section, nous décrivons les différents moyens qui permettent, d'une part, d'améliorer les performances de précision et, d'autre part, de contrôler l'apparition de défaillances telles que des biais importants sur la position.

1.3.4.1 Localisation hybride

Les techniques de localisation relative et absolue présentent chacune différents avantages et inconvénients. Les systèmes de localisation relative sont capables de fournir des informations à cadence élevée et précises à court terme. Néanmoins, à chaque intégration successive, des erreurs s'accumulent et deviennent inacceptables à long terme. De l'autre côté, les systèmes de localisation absolue se montrent globalement plus précis mais sont sujets à des indisponibilités (signaux GNSS bloqués par des éléments de l'environnement) ou à des interférences provoquées ou fortuites.

En raison de cette complémentarité, des solutions d'hybridation sont largement développées. Il s'agit de combiner les différentes technologies de positionnement. Il existe différents types d'hybridation selon que l'on utilise les données de pseudodistance à l'entrée du récepteur ou les données de position à la sortie du récepteur [Bhatti et al., 2007] : couplage lâche/serré/très serré (Figure 1.5).

Dans le couplage lâche, les différentes sources sont indépendantes et fournissent 3 solutions de navigation : inertielle, GNSS et hybridée. La solution hybridée est la sortie du système inertiel intégrée par un filtre (filtre de Kalman le plus souvent) et tenant compte de la solution de navigation GNSS. Il existe 2 modes de couplage lâche : en boucle fermée ou ouverte. En boucle fermée, la correction est effectuée en sortie du système inertiel et à l'intérieur de la plateforme. Cette étape permet la validation des hypothèses prises pour la linéarisation (dans le cadre d'une implémentation d'un filtre de Kalman étendu). Cependant, si une erreur apparait sur une source, elle sera difficile à corriger

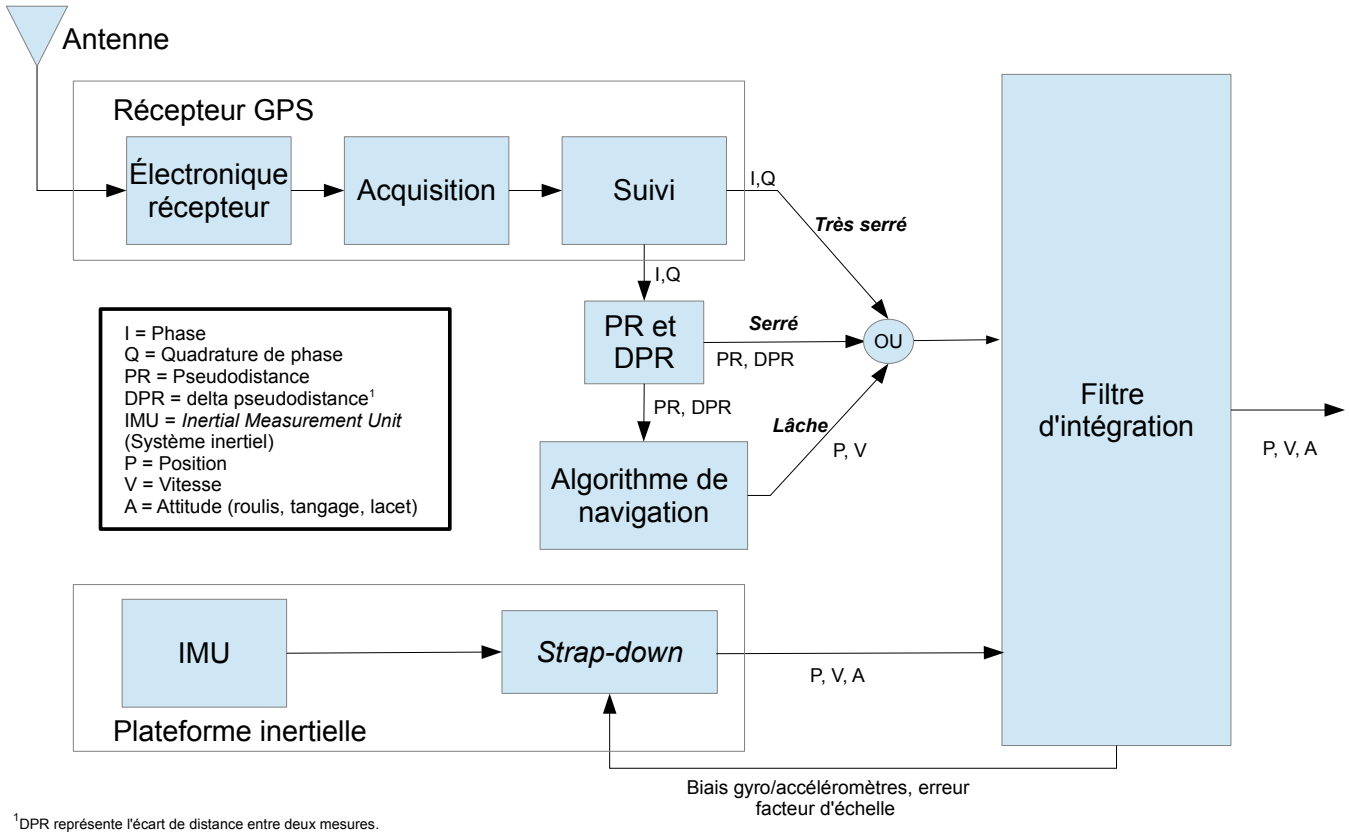


FIGURE 1.5 – Les différents couplages selon les données utilisées : solution de navigation directement (couplage lâche) jusqu'à la phase/quadrature de phase (couplage très serré)[Bhatti et al., 2007].

puisqu'elle se sera propagée sur l'ensemble de la solution de navigation. En boucle ouverte, il n'y a pas d'étape de correction et le système inertiel continue à dériver s'il n'est pas recalé régulièrement.

Dans le couplage serré, les parties GNSS et inertielle sont réduites à de simples fonctions. Cela signifie qu'il n'y a pas 3 solutions comme pour le couplage lâche mais une seule solution, la solution hybridée. Ce sont les pseudodistances qui sont utilisées pour la partie GNSS. Ces dernières peuvent être considérées comme des données brutes c'est à dire les informations fournies par les satellites avant tout traitement. Procéder ainsi a l'avantage de tirer partie des données brutes GNSS même si le nombre de satellites visibles est insuffisant (< 4). La solution apportée par la partie GNSS est supposée exempte d'erreur hormis les erreurs dues à la propagation des signaux GNSS dans l'atmosphère présentées dans la sous-section 1.3.3). Ces dernières sont prises en compte au niveau du récepteur dans l'UERE (*User Equivalent Range Error*) qui peut être assimilée à un écart-type sur les mesures des pseudodistances (cf tableau 1.1).

Le couplage serré n'offrant qu'une seule solution de navigation, la défaillance d'une source d'information aura un impact sur les performances de la solution. Pour assurer une continuité de service, la solution doit être tolérante aux fautes. Plus précisément, le système de localisation doit être capable de détecter et traiter une faute avant qu'elle ne conduise à une défaillance de positionnement (exigence de limite de précision dépassée). Dans le chapitre 3, nous verrons que la tolérance aux fautes pour des systèmes de localisation fondés sur les GNSS peut être garantie par l'utilisation

Tableau 1.1 – Bilan des erreurs sur la mesure de pseudodistance GPS [Faurie, 2011].

Segment	Sources d'erreur	Erreur 1σ (m)
Spatial	Stabilité de l'horloge satellite	3
	Incertitude sur l'accélération du satellite	1
	Autres	0,5
Contrôle	Ephémérides	4,2
	Autres	0,9
Utilisateur	Compensation du retard de propagation ionosphérique	10
	Compensation du retard de propagation troposphérique	2
	Bruit et résolution du récepteur	4,8
	Multi-trajets	1,2
	Autres (interférences)	0,5
	$UERE = \sqrt{\sum \sigma^2_{erreur}}$	12,5

d'algorithmes de contrôle d'intégrité.

Dans le couplage très serré, le système inertiel est une aide à la poursuite des signaux GNSS. Les mesures inertielles et les signaux GNSS entrent dans un filtre d'intégration afin d'estimer des pseudodistances. Cette configuration rend le système inertiel et le récepteur GNSS dépendants. Le phénomène de dérive au niveau de la partie inertielle affecte donc les performances de ce type de couplage. Néanmoins, il reste robuste aux brouillages et interférences. Son implémentation est complexe car les données inertielles doivent être intégrées à l'intérieur du récepteur GNSS.

Coupler un récepteur GNSS avec d'autres systèmes de localisation constitue une des solutions pour la réduction des risques générés par son utilisation. Cependant, les performances de ce récepteur peuvent être également accrues grâce à l'usage de systèmes satellitaires complémentaires et des réseaux de stations au sol appelés systèmes d'augmentations.

1.3.4.2 Systèmes d'augmentation satellitaires

La facilité de mise en œuvre des GNSS a poussé les utilisateurs à les intégrer dans des applications autres que celles pour lesquelles ils ont été conçus à l'origine (navigation d'un aéronef). Les applications nécessitant un haut niveau d'intégrité (concept qui sera abordé plus en détail dans le chapitre 3) et de précision en font partie.

Afin d'améliorer les critères de performances de ces technologies, des systèmes d'augmentation peuvent être utilisés en complément des GNSS. Il en existe trois sortes :

— GBAS pour *Ground Based Augmentation System* s'inspirant du principe du GPS différentiel (cf Figure 1.6). Comme leur nom l'indique l'augmentation se fait respectivement au niveau satellite et au niveau d'installations au sol.

— SBAS pour *Satellite Based Augmentation System* utilisant des satellites géostationnaires pour corriger les erreurs de position.

— ABAS pour *Aircraft Based Augmentation System*. Il s'agit de dispositifs embarqués avec les récepteurs GNSS. Le contrôle de l'intégrité est inclus dans ce type de dispositif centré sur la détermination et l'amélioration de l'intégrité de la localisation d'un véhicule ou aéronef. Le contrôle de l'intégrité fait l'objet d'une présentation détaillée dans la section 3.5 du chapitre 3.

1.3.4.2.1 GBAS

Les GBAS pour *Ground Based Augmentation System* dont le plus courant, le GPS différentiel (cf Figure 1.6), apporte une amélioration venant d'un réseau de stations de référence. Ce réseau transmet à l'utilisateur d'un récepteur GPS l'écart entre la position déterminée par les satellites et la position réelle de la station la plus proche (ou plus précisément ce sont les écarts de pseudodistances qui sont envoyés). Les satellites en vue étant les mêmes pour l'utilisateur et la station de référence, les effets des erreurs sont supposés semblables.

1.3.4.2.2 SBAS

Les SBAS ont une architecture proche d'un GNSS c'est à dire en trois segments (spatial, de contrôle et utilisateur). Le principe des SBAS est d'offrir à l'utilisateur des informations lui permettant d'améliorer sa localisation par GNSS. Ces informations (position, orbite, erreurs liées à la propagation des signaux dans l'atmosphère, *etc.*) sont calculées par un réseau de stations au sol puis transmises à l'utilisateur par l'intermédiaire de satellites géostationnaires [4]. Les SBAS existants couvrent des zones limitées mais sont compatibles entre eux.

Les SBAS réalisent les tâches suivantes :

— Collecter les signaux GNSS.
— Estimer l'intégrité des données reçues (le chapitre 3 traitant plus spécifiquement ce critère).
— Corriger les biais d'horloge et les erreurs iono/troposphériques.
— Transmettre les corrections à l'utilisateur.

Parmi les SBAS existants, nous trouvons le WAAS (pour *Wide Area Augmentation System*), premier SBAS opérationnel depuis 2003. Son principal objectif est d'améliorer les services de localisation offerts par le GPS en terme de précision, de disponibilité de service, de continuité de service et d'intégrité. Il couvre l'Amérique du Nord uniquement. Le segment spatial du WAAS est constitué de 3 satellites géosynchrones [5].

Côté Européen, EGNOS (pour *European Geostationary Navigation Overlay Service*) remplit les mêmes objectifs que le WAAS. Le segment spatial d'EGNOS est constitué de 3 satellites géostationnaires couvrant le territoire européen. Le segment de contrôle est un réseau de stations au sol dont le rôle est de traiter les signaux d'EGNOS, calculer les erreurs précisées plus haut et transmettre les caractéristiques de ces erreurs à tous les utilisateurs sous couverture.

4. L'orbite géostationnaire est une orbite particulière située à 35 786 km d'altitude où tout corps se trouvant sur cette orbite a une période de révolution égale à la période de rotation de la Terre

5. Les satellites géosynchrones ont une période de révolution égale à celle de rotation de la Terre mais, contrairement à l'orbite géostationnaire, leur orbite présente une inclinaison non nulle

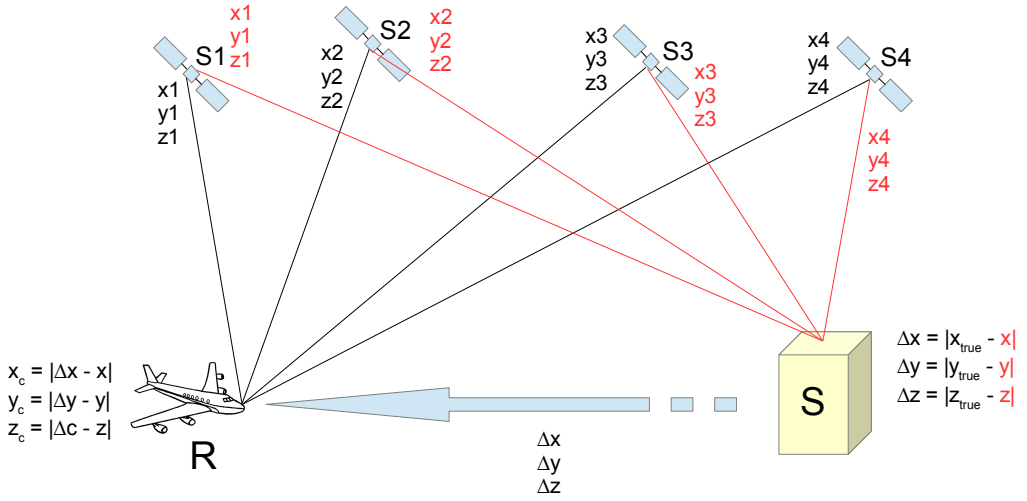


FIGURE 1.6 – Fonctionnement du GPS différentiel.

En outre, EGNOS offre trois services selon les exigences que requiert une application :

— OS (*Open service*) : un service ouvert, gratuit et disponible à tous
— SoL (*Safety of Life*) : il s'agit d'un service qui informe automatiquement l'utilisateur d'une défaillance sur un satellite ou tout autre problème affectant les performances du service ouvert notamment l'intégrité (cf Chapitre 3). Ce service est conçu pour des applications liées à la sécurité tel que le contrôle-commande ferroviaire, le guidage aéronautique, maritime et routier.
— CDDS (*Commercial Data Distribution Service*) : un service réservé aux professionnels mettant à leur disposition les données brutes des stations au sol du segment de contrôle d'EGNOS.

Les deux sous-sections qui suivent sont des systèmes d'augmentation de la famille des ABAS. Nous proposons de présenter les trois plus rencontrés en navigation.

1.3.4.3 Récepteur RTK et *Precise Point Positioning*

Les récepteurs GNSS les plus courants déterminent la position d'un véhicule grâce aux données envoyées par les satellites sous forme d'un code binaire (code C/A pour *coarse acquisition* ou acquisition brute) dont ils comparent l'heure d'émission avec leur horloge interne. Des récepteurs appelés RTK (pour *Real Time Kinematic* ou Cinématique Temps Réel) peuvent non seulement traiter les données des satellites mais aussi exploiter les mesures de la phase des porteuses (L1 et L2) sur lesquelles sont transmises le code C/A [Rietdorf et al., 2006]. Au même titre que le DGPS, les récepteurs RTK utilisent une station ou un réseau de stations de référence fournissant un signal C/A corrigé. L'avantage de travailler ainsi est que la précision de ces récepteurs surclasse celle des récepteurs classiques avec une précision centimétrique. Ce gain de précision vient de la différence des fréquences des porteuses (L1 = 1575,42 MHz et L2 = 1227,60 MHz) par rapport à celle du code C/A (1,023 MHz) utilisés, soit une fréquence 1000 fois plus élevée.

Les processus *Precise Point Positioning* sont des algorithmes sophistiqués travaillant au même niveau que les récepteurs RTK à la différence que les processus PPP ne requièrent pas nécessaire-

ment de stations de référence pour atteindre la même précision [Álvaro Mozo García et al., 2011]. Ces algorithmes intègrent des modèles d'erreur troposphérique et ionosphérique contrairement aux GBAS où les modèles en question sont centralisés dans les stations de référence.

1.3.4.4 *Map-Matching*

Le *Map-Matching*, pouvant se traduire en français par recalage sur une carte, est un processus d'alignement d'une séquence de positions observées avec un réseau routier ou ferroviaire sur une carte numérique.

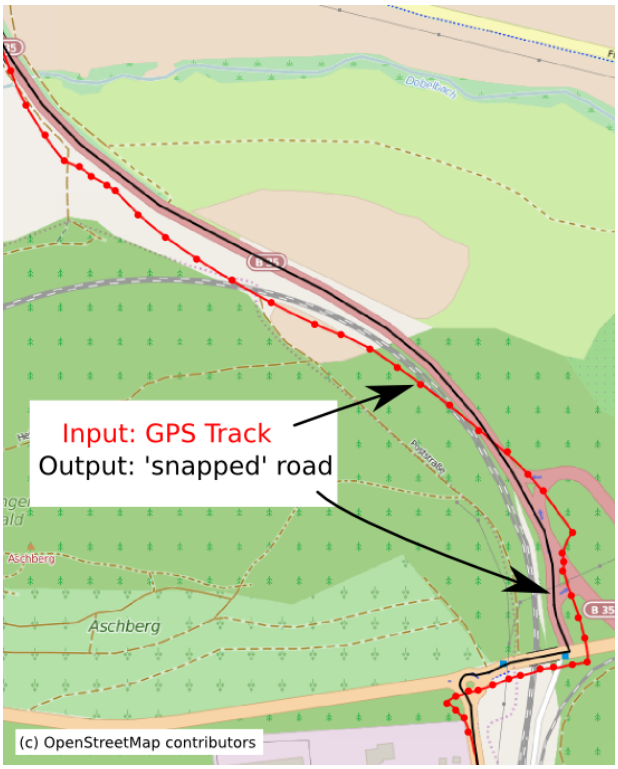


FIGURE 1.7 – Map-Matching de données GPS sur un exemple de route sous le fournisseur de données géographique OpenStreetMap.

Le Map-Matching est souvent utilisé en appui à un récepteur GNSS ou un système multicapteur [Lou et al., 2009] et cette technique est intégrée notamment sur la plateforme DemoOrt ainsi que dans l'architecture du projet GaloROI [Lu et al., 2013] présentées dans la sous-section 1.4.3.

Dans le cadre d'une localisation absolue, cette technique n'est efficace que si l'on dispose d'une carte avec une précision supérieure ou égale aux exigences à garantir (précision $<$ 1 mètre $\rightarrow$ utilisation de carte à une échelle permettant d'atteindre cette exigence de précision).

1.4 Enjeux de la localisation par satellites dans le contexte ferroviaire

Les systèmes GNSS sont aujourd'hui largement utilisés par le grand public, dans les smartphones ou dans les systèmes de navigation routiers. Le domaine ferroviaire s'y intéresse depuis quelques années et de plus en plus fortement. Ces systèmes peuvent être hybridés pour être capables de guider des véhicules routiers autonomes sans infrastructure et à coût relativement faible. Par conséquent, il est important d'étudier leurs apports pour le rail.

Les principes de fonctionnement des GNSS ont été décrits dans la section précédente. Leur utilisation répond à des enjeux cruciaux dans l'avenir pour le domaine ferroviaire. Nous présenterons ces enjeux et nous montrerons comment les GNSS peuvent répondre aux exigences de l'infrastructure de demain.

1.4.1 Des enjeux économiques, écologiques et techniques

La situation économique et écologique d'aujourd'hui pousse les domaines du transport vers une constante évolution. Celle-ci passe par l'innovation dans le but de répondre aux engagements pris par le G20 et la COP21.

Pour l'aspect écologique, la réduction des émissions de gaz à effet de serre fait partie des engagements de la COP21 [6]. L'Union Européenne s'est engagée à réduire d'au moins 40 % d'ici à 2030 ses émissions de gaz à effet de serre par rapport au niveau de 1990 [COP21, 2015]. Afin d'identifier les sources d'émissions de ces gaz sur une infrastructure ferroviaire, un Bilan Carbone® de la construction en 2006 de la branche Est de la Ligne à Grande Vitesse Rhin-Rhône a été effectué [Objectif Carbone, 2009]. Il a démontré que son exploitation et sa maintenance sur 30 ans seraient équivalents à 685 000 teCO2 (tonnes équivalents CO2) dont 19 900 pour la maintenance de l'infrastructure (soit l'équivalent de l'émission de CO2 d'une petite ville de 3 500 habitants durant une année).

Pour l'aspect économique, les coûts d'installation, d'exploitation et de maintenance des infrastructures ferroviaires doivent être revus à la baisse. Un des leviers pour le secteur ferroviaire français est d'alléger l'infrastructure du réseau ferré représentant 30013 km de lignes (chiffre 2012 [Groupe banque mondiale, 2015]). Cet allègement peut passer par la réduction du nombre d'équipements au sol et/ou embarqués. Les balises, équipements au sol très répandus sur les infrastructures ferroviaires, semblent être un bon poste de réduction des coûts. En effet, l'équipement de sécurité ferroviaire français KVB (pour contrôle de vitesse par balises) représente plus de 120 000 balises (chiffre 2008 [SNCF Réseau, 2008]) disposées le long des lignes équipées. De plus, le transport ferroviaire européen doit faire face à une augmentation importante du trafic voyageurs et fret. En effet, le volume de marchandises ainsi que le nombre des passagers seront triplés à l'horizon 2020 (cf projections 2002 [ERRAC, 2002]). L'infrastructure et le matériel roulant doivent pouvoir absorber ces augmentations en optimisant l'usage de ses voies et diminuant les coûts de maintenance.

Les problématiques de l'interopérabilité et de l'ouverture à la concurrence, constituent un autre enjeu, celui de permettre la circulation sûre et sans interruption de trains d'un pays à un autre en garantissant les performances requises pour ces lignes [Parlement Européen et du Conseil, 2008]. Pour pouvoir circuler sans entraves dans plusieurs pays, un train doit disposer à bord des systèmes

6. Conférence de Paris sur le changement climatique du 30 Novembre au 12 Décembre 2015

de contrôle-commande des pays traversés pour gérer les différents écartements de voie, électrification ou signalisations. ERTMS, le nouveau système de contrôle-commande européen, fait partie des réponses à l'enjeu d'interopérabilité ferroviaire en Europe.

Le secteur ferroviaire doit être compétitif vis-à-vis des autres types de transport et des solutions qu'ils apportent (vols *low-cost* moyens et longs courriers, covoiturage, *etc.*). L'augmentation de la compétitivité peut venir de l'intégration de nouvelles technologies afin d'améliorer les performances et les capacités du matériel roulant et de l'infrastructure. Les GNSS font partie des technologies qui peuvent répondre à ces nouvelles exigences et enjeux en faisant baisser les coûts.

1.4.2 Réponses apportées par les GNSS à ces enjeux

Les GNSS, d'après l'European Railway Agency (ERA) [European Railway Agency, 2012], peuvent jouer un rôle majeur dans la sécurité ferroviaire notamment le contrôle-commande et la signalisation mais ce rôle va plus loin que la sécurité. D'abord, la fonction de localisation, aujourd'hui réalisée par les balises peut être remplie par un système satellitaire entrainant de fait la réduction des équipements au sol et du coût inhérent à leur exploitation et à leur maintenance. Attention toutefois, dans les systèmes ferroviaires existants, le rôle des balises n'est pas réduit à la simple transmission de localisation au train. Le remplacement total des balises par les GNSS n'est pas immédiat. Dans ERTMS/ETCS niveau 3 (pour *European Train Control System* niveau 3), celles-ci sont reléguées au rôle de recalage de l'odométrie, fonction tout à fait réalisable par les GNSS sous réserve d'atteindre des performances suffisantes.

Pour atteindre les objectifs d'augmentation du trafic dans les années à venir, l'espacement entre les convois doit être optimisé. Le cantonnement garantit un espacement suffisant entre les convois circulant sur une même voie ferrée et permet aussi d'éviter les rattrapages et les collisions. Un canton est une portion de voie fixe dont il faut assurer qu'un seul et même train occupe un canton donné. Afin d'optimiser leur taille, ce canton doit être déformable et sa taille doit être déterminée en temps réel à bord. Ainsi, la circulation des trains n'est plus dépendante d'équipement au sol et cela permet de faire circuler plus de trains.

Les GNSS peuvent également être utiles pour l'interopérabilité des systèmes ferroviaires. En effet, un GNSS peut fournir une position partout sur Terre donc localiser un train quel que soit le pays et le système ferroviaire utilisé.

Ces réponses apportées par les GNSS aux enjeux de la localisation ferroviaire de demain ont motivé l'émergence de plusieurs projets collaboratifs au niveau européen, dont les premiers ont débuté dès les années 2000.

1.4.3 Projets d'intégration des GNSS dans le contrôle-commande ferroviaire

Ces dernières années, plusieurs projets ont été menés afin d'évaluer l'apport des technologies satellitaires pour le positionnement ferroviaire. Le tableau 1.2 liste de manière non exhaustive différents projets ayant pour objectif des utilisations possibles des GNSS pour des applications ferroviaires. APOLO a été l'un des premiers projets à s'intéresser à la question, une décennie après l'ouverture du GPS pour des applications civiles. L'architecture utilisée dans le cadre des tests durant ce projet était constituée de plusieurs capteurs inertiels (odomètre, gyroscope, accéléromètre et radar Doppler). Ces capteurs servaient de référence pour valider la solution en terme de précision. C'est aussi

la première fois que l'on affirme qu'un récepteur GNSS n'est pas suffisant pour des applications liées à la sécurité notamment sur les lignes où peu (voire aucun) de satellites sont visibles (zone urbaine, boisée ou tunnels). La mise en œuvre d'une méthode de *map-matching* a été suggérée comme une solution d'amélioration.

L'idée d'appliquer les GNSS sur des lignes à faible trafic a été proposée dans les projets LOCOPROL et LOCOLOC. En effet, les conséquences d'une localisation imprécise fournie par un système fondé sur les GNSS ou d'une indisponibilité de celui-ci ont moins d'impact sur la sécurité que dans un contexte de trafic dense. Une des idées prometteuses proposées dans les projets LOCOPROL/LOCOLOC était d'utiliser des paires de satellites. Il a été montré que 2 satellites sont suffisants pour calculer une position dans un contexte 1D en connaissant la trajectoire d'un train. Ceci permet au système de localisation de fournir 3 mesures de position indépendantes. Cette redondance permet au système d'atteindre les exigences ferroviaires en matière de sécurité (SIL4) mais au détriment de la précision (200 à 400 mètres). L'une des perspectives a été l'emploi de systèmes d'augmentation satellitaire pour améliorer les performances du récepteur GNSS.

Ainsi, le projet InteGRail a suggéré l'utilisation des signaux EGNOS afin de corriger les éventuelles erreurs liées aux signaux GPS. Les tests sur le prototype, dont l'architecture est indiquée dans le tableau 1.2, ont montré que la précision de la localisation fournie est suffisante pour les applications de type contrôle-commande sur des lignes à faible trafic. C'est également durant ce projet que les premiers travaux sur l'intégrité de la localisation ont été menés notamment les spécifications des exigences sur des temps d'alertes (TTA). Un des inconvénients soulevés dans le projet InteGRail est le nombre limité de services fournis par le GPS [7]. Offrant une palette de services plus conséquente, l'usage de Galileo a été cité comme une perspective encourageante.

Le projet GADEROS proposa d'ailleurs l'utilisation de Galileo en l'intégrant au système ERTMS. L'intégration des GNSS dans le système de contrôle-commande ERTMS/ETCS était une des perspectives du projet LOCOPROL. L'utilité du GNSS dans des applications ferroviaires est multiple notamment le rôle du GNSS dans la mise en place de passage à niveau automatique (projet ECORAIL). Le projet RUNE implémente le concept de balise virtuelle où la solution de navigation fournie par le récepteur GPS est vue comme une balise sur la voie. Une deuxième approche du projet RUNE visa à utiliser les signaux GNSS avec des systèmes inertiels et de l'odométrie. Le projet GIRASOLE s'est concentré dans le développement d'un récepteur GNSS gérant les différentes constellations GNSS existantes ou amenées à exister : GPS, GLONASS et Galileo.

Le projet GRAIL [GRAIL, 2007] (et son extension GRAIL2 [Marradi et al., 2012]) avait pour objectifs de développer et de valider un système de signalisation, l'ETCS, fondé sur un GNSS. Il s'agit d'une composante de ERTMS. Le projet GRAIL vise les lignes à grande vitesse. Dans la suite de GRAIL, GRAIL-2 se concentre sur de l'odométrie améliorée avec l'utilisation du GNSS pour compenser les problèmes d'odométrie (phénomènes de glissement). Le projet a étudié les performances de ce type de système de localisation dans un environnement réel avec les contraintes inhérentes aux zones urbaines.

Le projet LOCASYS s'appuyait sur les précédents projets dans le but d'intégrer un système de localisation fondé sur les GNSS dans le système de contrôle-commande britannique.

7. Ces services sont décrits dans la sous-section 1.3

Tableau 1.2: Liste de projets européens concernant l'usage des GNSS pour la localisation ferroviaire.

Nom du projet	Période	Système	But
APOLO [Barbu, 1999]	1999-2001	Récepteur GPS + Odomètre + Gyroscope + Accéléromètre + Radar Doppler	Premiers tests de la faisabilité du GPS pour des applications ferroviaires
LOCOPROL / LOCOLOC [Wynants, 2001]	2001-2004	Récepteur GPS + Balise + Odomètre	Développement d'une solution sûre et complète de navigation ferroviaire fondée sur les GNSS pour des lignes à faible trafic et extension à ERTMS/ETCS
InteGRail [Bedrich and Gu, 2004]	2001-2004	Récepteur GPS (+ EGNOS) + Odomètre + Gyroscope + Accéléromètre + Cartes	Utilisation des signaux EGNOS pour des applications liées à la sécurité dans des conditions opérationnelles variées
Gaderos [Bustamante and De Miguel, 2003]	2001-2004	Galileo + Odomètre	Tests de prototypes sur une ligne à faible trafic équipée de ERTMS/ETCS
Ecorail [Wasle and Ringert, 2003]	2001-2005	Récepteur GPS (+ EGNOS) + Odomètre + Carte	Intégration du GPS pour passage à niveau automatique
RUNE [Albanese and Marradi, 2005]	2001-2006	Récepteur GPS (+ EGNOS) + Odomètre + IMU	Utilisation du récepteur GPS (+ EGNOS) comme une balise virtuelle
GIRASOLE [Marradi et al., 2008]	2005-2007	Récepteur GNSS multi-constellation (GPS + GLONASS + Galileo)	Utilisation de prototype de récepteur multi-constellation
GRAIL-1 [GRAIL, 2007]	2005-2008	Récepteur GNSS + Odomètre + balise + IMU	Spécification d'un sous-système GNSS sur différents niveaux d'intégration d'ERTMS/ETCS
LOCASYS [Thomas et al., 2008]	2006-2009	Récepteur GNSS + IMU + capteur de vitesse	Intégration des GNSS dans le système de signalisation britannique
GRAIL-2 [Marradi et al., 2012]	2010-2012	Idem que pour le projet GRAIL-1	Développement d'une application d'odométrie améliorée par GNSS pour ERTMS/ETCS et sur lignes à grandes vitesses

Tableau 1.2: Liste de projets européens concernant l'usage des GNSS pour la localisation ferroviaire.

Nom du projet	Période	Système	But
GaloROI [Manz et al., 2014]	2012-2013	Récepteur GNSS + capteur à courant de Foucault + Carte	Développement d'un système de localisation innovant pour des applications impliquant la sécurité et sur des lignes à faible trafic
3InSat [Rispoli et al., 2013]	2012-2014	Récepteur GNSS (+ EGNOS + multi-constellations GPS + GLONASS + Galileo) + Odomètre + IMU	Application d'un système de localisation basée sur les GNSS utilisant plusieurs constellations de satellites et des technologies existantes compatibles avec ERTMS/ETCS
EATS [Goya et al., 2015]	2012-2016	Récepteur GNSS + Localisation par GSM-R et UMTS	Application des systèmes de télécommunications intelligents basés sur GSM-R et UMTS avec un récepteur GNSS dans un contexte ERTMS/ETCS niveau 3

Chaque projet a apporté des éléments nouveaux pour une intégration future des GNSS dans les systèmes de contrôle-commande ferroviaire. La valeur ajoutée est de différente nature : application des GNSS dans un système de contrôle-commande existant (APOLO, Gaderos) ou en cours de déploiement (GRAIL 1 et 2, 3InSat), application sur des lignes à faible trafic (LOCOPROL/LOCOLOC, GaloROI), des combinaisons de technologies innovantes (GaloROI) ou de technologies bas-coût. Quelques projets se sont concentrés sur la validation de systèmes fondés sur les GNSS seuls. Tous les projets ont montré que, technologiquement parlant, la localisation par satellite apporte de nombreux avantages pour les acteurs du milieu ferroviaire quel que soit le type d'application, mode d'exploitation, *etc.* Cependant, les projets qui ont étudié l'intégration des GNSS dans des applications impliquant la sécurité ont conclu qu'un récepteur GNSS seul n'est pas suffisamment précis, disponible et, finalement, n'est pas suffisamment sûr surtout dans des configurations d'environnement contraignantes (zones urbaines, boisées, *etc.*). Les projets présentés proposent des solutions (hybridation, utilisation de systèmes d'augmentation satellitaire, *etc.*) pour améliorer ces performances cruciales pour la fonction de localisation au sein d'un système de contrôle-commande ferroviaire.

1.5 Problématiques liées à la gestion de la sécurité

Les projets présentés précédemment ont permis d'apporter des réponses aux enjeux de l'utilisation des GNSS dans le domaine ferroviaire. Dans les architectures et les prototypes proposés, différents types de solutions permettant d'assurer les conditions de sécurité dans les applications de contrôle-commande ont été envisagés. En effet, les erreurs de localisation dans ces applications de sécurité sont sources de risques aux conséquences catastrophiques comme, par exemple, la collision entre trains en cas d'erreur de localisation importante.

Cette section présente, dans un premier temps, les risques non maitrisés c'est à dire les risques ne pouvant pas être atténués par les techniques présentées dans la sous-section 1.3.4). Néanmoins, il se pose toujours la question de comment démontrer que ces risques peuvent être réduits de manière acceptable. C'est ce que la sous-section 1.5.2 introduira en présentant les critères d'évaluations des performances des GNSS.

1.5.1 Risques non maitrisés induits par l'usage des GNSS dans le domaine ferroviaire

La sous-section 1.4.3 a montré la faisabilité de l'intégration des technologies satellitaires dans le domaine ferroviaire au travers de plusieurs projets européens. Des solutions existent pour améliorer la précision et la disponibilité des GNSS (cf sous-section 1.3.4). Cependant, il demeure des risques liés à leur utilisation dans le domaine ferroviaire que ces solutions ne permettent pas d'atténuer. Dans le transport ferroviaire (comme dans le transport routier), il existe des risques que l'on ne rencontre pas en aéronautique. Ces risques sont liés à l'environnement dans lequel évolue le train. Celui-ci traverse un nombre de configurations environnementales très variées (zone urbaine, boisée ou dégagée) rendant une modélisation de l'environnement très difficile et complexe. Les signaux GNSS sont réfléchis voire obstrués par divers obstacles rencontrés tout au long d'un trajet (bâtiment, tunnel, arbre, *etc.*). On parle de phénomène de multitrajets (réflexion de signaux) et de masquages (obstruction de signaux).

Dans ce mémoire, nous ne considérons pas les erreurs liées aux interférences radio car il s'agit de sources d'erreur fortuites ou délibérées. Ces phénomènes, illustrés par la figure 1.8, génèrent des erreurs sur la localisation du train. Du fait de la complexité de créer un modèle générique d'environnement, ces erreurs ne peuvent être modélisées de façon statistique [Nahimana, 2009] et *a fortiori* présentent des risques non maitrisés. Toutefois, notons qu'il existe des techniques de "tracé de rayon" (ou *ray tracing* en anglais) pour la modélisation des phénomènes de multitrajet [Lau and Cross, 2007]. Dans les chapitres 3 et 4, nous proposons d'assimiler les erreurs dues au phénomène de multitrajets comme des biais instantanés du fait de leur nature rapide et avec un impact important sur la localisation.

L'évaluation de la sécurité d'un système de localisation fondé sur un GNSS passe par l'évaluation des risques présentés dans cette sous-section. Cependant, nous sommes confrontés à des cultures de

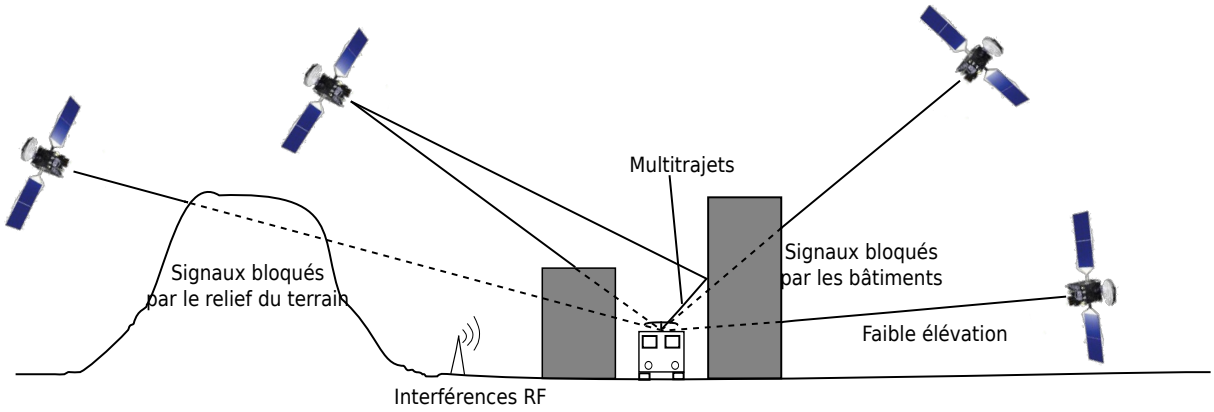


FIGURE 1.8 – Phénomènes locaux rencontrés par un train.

la sécurité (ou plus précisément à l'évaluation des performances des systèmes) différentes : celle du domaine ferroviaire et du domaine aéronautique.

1.5.2 Critères de quantification actuels des performances fournies par les GNSS

L'évaluation des risques résiduels est requise en vue d'une autorisation de mise en service d'un système basé sur les GNSS. Il en va de même pour l'évaluation des performances opérationnelles que le système peut fournir à l'utilisateur compte tenu de ce risque résiduel (cf norme [EN 50126, 2000]. La norme décrit la gestion de la sûreté de fonctionnement de systèmes de signalisation ferroviaires, c'est à dire la gestion et l'évaluation des critères de performances FDMS (Fiabilité, Disponibilité, Maintenabilité, Sécurité). À l'image de cette classe de critères, il en existe une autre propre aux GNSS pour évaluer leurs performances [Duquenne et al., 2005] et des liens sont mis en évidence dans [Beugin and Marais, 2008] :

— La **précision** désigne le degré de conformité entre la position estimée et la position réelle. Ce degré de conformité s'exprime par un intervalle assujetti d'un degré de confiance. À titre d'exemple, le tableau 1.3 montre comment est exprimée la précision du service de positionnement que fournit le GPS dans les normes aéronautiques [ICAO, 2006].

Tableau 1.3 – Erreurs de position limites du GPS horizontales et verticales.

	95 % du temps	99,99 % du temps
Erreur de position horizontale	100 m	300 m
Erreur de position verticale	156 m	500 m

— La **continuité de service** se réfère à la probabilité que le système, supposé fonctionner à l'instant où débute une opération donnée, continue de fonctionner pendant la durée de l'opération considérée.

— La **disponibilité de service** est la proportion de temps pendant lequel les services fournis (donner une localisation par exemple) par le système sont utilisables par l'utilisateur dans une zone de couverture spécifiée.

— L'**intégrité** est définie par l'aptitude d'un système à alerter en temps utile l'utilisateur de son impossibilité à fournir le service de positionnement dans les conditions attendues. Cet attribut est décrit en détail dans le chapitre 3.

Ces critères soulèvent deux questions importantes :

— Peut-on considérer une classe de critères de performance étendue à un système de localisation utilisant d'autres capteurs qu'un récepteur GNSS ?

— Comment évaluer quantitativement et/ou qualitativement ces paramètres dans un contexte de faible retour d'expérience, de données imparfaites et par l'utilisation des technologies GNSS ?

Finalement, il s'agit ici d'exprimer une confiance qu'un utilisateur peut placer en de tels systèmes. Ce mémoire va apporter une partie des réponses à ces interrogations.

1.6 Synthèse et objectifs ciblés dans la thèse

Au cours de ce chapitre, nous avons introduit différentes techniques de localisation (navigation à l'estime, localisation absolue et hybride) existantes ou en cours de développement dans le domaine ferroviaire. Les technologies satellitaires ont été décrites et des projets sur la faisabilité de l'intégration des GNSS dans un système de contrôle-commande ferroviaire ont été présentés.

Avant d'utiliser un nouveau système de localisation dans ce domaine, il est nécessaire d'apporter des preuves montrant que de tels systèmes sont sûrs, c'est à dire qu'ils sont capables de fournir une position digne de confiance et dont les caractéristiques répondent aux exigences. Cette confiance se détermine au travers d'une analyse de sûreté de fonctionnement. Des problématiques au niveau capteurs et architectures de capteurs se dégagent. Tout d'abord, une position sûre est fonction de la qualité des données issues des différents capteurs embarqués. Pour la garantir, les démonstrations de sécurité doivent être apportées notamment sur l'usage des GNSS dans des applications ferroviaires.

De plus, ces justifications doivent être exprimées selon les critères ferroviaires. Il est aujourd'hui difficile d'estimer ces critères faute de retour d'expérience sur l'usage de ces technologies dans le domaine ferroviaire. Une autre difficulté réside dans le fait que les GNSS disposent de leur propre classe de critères de performances comme expliqué dans la sous-section 1.5.2 qui diffèrent considérablement des attributs FDMS, classiques en sûreté de fonctionnement des systèmes ferroviaires.

Les chapitres suivants vont détailler les contributions de la thèse. Le chapitre 2 débute par une section introductive sur le cadre européen de la gestion des risques dans le domaine ferroviaire et sur les concepts généraux de la sûreté de fonctionnement. L'objectif principal du chapitre 2 vise à analyser plusieurs types d'architecture de systèmes de localisation avec GNSS dans le but de déterminer la mieux adaptée aux exigences ferroviaires.

Le diagramme 1.9 illustre les différents sous-systèmes d'un système de localisation générique sur lesquels il est aujourd'hui possible d'agir pour assurer la sécurité. Parmi les sous-systèmes présentés dans le chapitre 1, nous traitons le cas de l'augmentation du degré de liberté par fusion multi-capteur. Dans un premier temps, l'analyse causale permet d'identifier les combinaisons d'états de capteurs conduisant à un état inacceptable de la sortie des systèmes considérés. Cette analyse a été publiée dans les actes de la conférence internationale Railways 2014 [Legrand et al., 2014]. Dans un second temps, nous menons une analyse de sensibilité. Pour cela, nous étudions l'impact des erreurs au niveau des différents capteurs pour déterminer la qualité de la position en fonction des besoins utilisateurs (incertitude, précision, *etc.*). Cette analyse a fait l'objet d'une communication à la conférence internationale avec actes IEEE-ITST [Legrand et al., 2013]. Ces deux analyses nous permettent d'expliciter de nouveaux indicateurs de sécurité autres que ceux cités dans la norme EN50126. Ces nouveaux indicateurs constituent une de nos contributions.

Le chapitre 3 proposera une méthodologie pour évaluer la sécurité d'un système de localisation fondé sur les GNSS. Pour cela, notre contribution majeure a consisté à adapter les concepts et algorithmes liés à l'intégrité GNSS aux systèmes de localisation autres qu'un récepteur GNSS. Ce chapitre 3 a fait l'objet d'un article publié dans la revue *Reliability Engineering and System Safety*

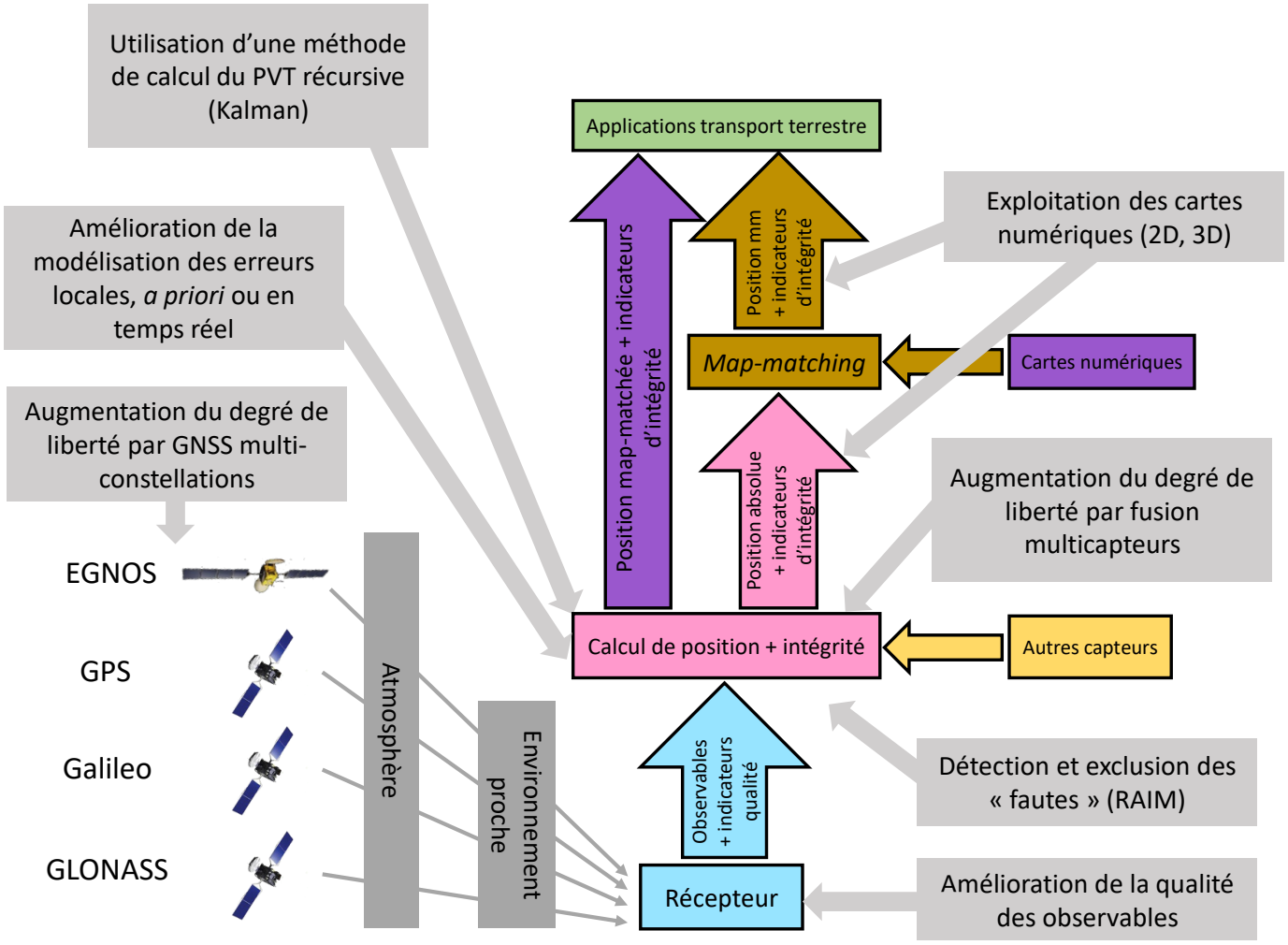


FIGURE 1.9 – Sous-systèmes d'une architecture de systèmes de localisation générique et leviers pour assurer sa sécurité [Bétaille, 2012].

[Legrand et al., 2015].

Enfin, le chapitre 4 appliquera l'évaluation de la sécurité présentée dans le chapitre 3 au contexte ferroviaire et dans un cas d'utilisation précis à savoir la gestion de l'espacement entre trains.

Chapitre 2

Gestion de la sécurité de systèmes embarqués ferroviaires utilisant de nouvelles technologies : application aux systèmes de localisation avec GNSS

Sommaire

2.1 Introduction

Dans le chapitre précédent, différentes techniques de localisation ont été présentées : des techniques existantes dans le milieu ferroviaire (odométrie, systèmes inertiels, balises, *etc.*.) jusqu'à l'intégration de technologies innovantes telles que les GNSS. Les différentes sources d'erreurs de localisation par satellites ont été présentées tout comme les moyens déployés aujourd'hui pour réduire ces risques d'erreurs à un niveau acceptable. Malheureusement, les signaux satellitaires ne peuvent

pas être utilisés seuls pour localiser un train de manière sûre ou, plus exactement, pour fournir une position en laquelle l'utilisateur peut avoir confiance dans l'environnement ferroviaire. De plus, une localisation ne peut pas être garantie tout au long d'un trajet compte tenu de l'indisponibilité des signaux GNSS en tunnel (problème de continuité de service) et des erreurs de propagation qu'ils subissent en environnement contraint (problème de précision). C'est pourquoi, les prototypes de systèmes de localisation ferroviaires utilisant les GNSS s'orientent aujourd'hui fortement vers des solutions de navigation hybride (récepteurs GNSS associés à d'autres capteurs).

Afin de répondre à la principale problématique soulevée au premier chapitre, qui est de déterminer si les risques liés à ces systèmes sont réduits de manière suffisante ou non, nous commençons, dans ce second chapitre, par définir les notions de qualité et de sécurité du service, c'est à dire à leur sûreté de fonctionnement (SdF). Il s'agit d'abord d'identifier quelles approches peuvent être mises en place pour répondre à l'évaluation des performances. Ces approches doivent être compatibles avec les différents étapes du processus harmonisé de gestion des risques utilisé dans la communauté ferroviaire européenne.

La première partie de ce chapitre décrit le processus de gestion des risques utilisé par la communauté ferroviaire.

Dans la seconde partie, les concepts, méthodes et moyens de la sûreté de fonctionnement dédiés à l'analyse des fautes/erreurs/défaillances d'un système (identification, combinaisons et impacts de celles-ci) et à l'évaluation des performances FDMS seront présentés.

Dans la troisième partie, deux approches s'appuyant sur les méthodes de SdF existantes seront proposées pour identifier et évaluer les impacts d'erreurs présentes dans les données des systèmes avec GNSS (les erreurs et défaillances matérielles étant supposées maitrisées). La première repose sur une analyse causale et la deuxième repose sur une analyse de sensibilité. Ces deux approches permettent d'évaluer la qualité et la sécurité de la localisation fournie par quatre exemples d'architectures de systèmes avec GNSS au travers de nouveaux indicateurs propres à ces systèmes. **Dans le cadre de ces analyses, nous injectons de manière aléatoire des pannes au niveau des capteurs pour dégrader volontairement leur signal de sortie. Ces analyses ne s'appuient pas sur la détection de panne. Leur principe est uniquement d'utiliser la trajectoire de référence connue *a priori* pour évaluer l'impact de ces pannes.**

Le chapitre 3 s'intéressera ensuite plus spécifiquement à une méthodologie d'évaluation de la sécurité au travers de l'un des attributs de performance des GNSS, l'intégrité.

2.2 Cadre européen de la gestion des risques dans le domaine ferroviaire

Les nouveaux systèmes ferroviaires (ou les systèmes existants évoluant techniquement) engendrant des **changements significatifs** requièrent obligatoirement l'application du règlement européen numéro 2015/1136 concernant l'adoption d'une Méthode de Sécurité Commune (MSC) [Règlement 2015/1136, 2015]. La question qui se pose ici est la suivante : à quel moment qualifie-t-on un changement comme significatif ? Un changement est dit **significatif** dès que l'une de ces affirmations est vraie :

— le changement peut entrainer une défaillance aux conséquences importantes sur le système à modifier,
— le changement implique une innovation importante, par exemple, une technologie immature dans le domaine ferroviaire,
— le changement engendre une modification complexe,
— le changement est irréversible,
— le suivi du changement est compliqué tout au long du cycle de vie,
— ou des changements récents jugés comme étant non significatifs s'accumulent (additionnalité).

Chaque pays-membre de l'Union Européenne a sa propre culture de la sécurité ferroviaire. Ceci conduit à différents règlements ou d'autres référentiels normatifs pouvant engendrer des incompréhensions entre les autorités de sécurité ferroviaire de chaque pays. Une Méthode de Sécurité Commune mise en œuvre par ces autorités vise à harmoniser le processus d'évaluation et à d'appréciation des risques. Ce processus s'articule autour de trois grandes étapes (cf figure 2.1) :

— l'**appréciation des risques** regroupant leur analyse (identification et caractérisation des dangers) ainsi qu'une estimation du risque pour chaque danger identifié,
— l'**évaluation des risques** par la démonstration de la conformité avec les exigences de sécurité,
— l'**emploi de mesures de sécurité** pour gérer tous les dangers identifiés.

L'analyse des risques s'appuie sur des principes d'acceptation du risque pour conclure sur l'emploi ou non de mesures de sécurité face aux risques identifiés. Il existe trois principes :

— l'**application de règles de l'art** ou **codes de pratiques** (spécification technique d'interopérabilité (STI), règles nationales, normes européennes),
— la **comparaison avec des systèmes similaires de référence**,
— l'**estimation explicite des risques et des critères d'acceptation des risques**.

Il est possible d'en appliquer plusieurs et il n'y a pas de priorité sur ces principes. Un ou plusieurs principes sont choisis en fonction du contexte ou de la nature du changement à opérer sur le système ferroviaire. Par exemple, pour des systèmes totalement nouveaux, il n'est pas possible d'appliquer les règles de l'art. En effet, cela suppose la mise à disposition de retours d'expérience, inexistants pour ce type de systèmes. En France, le principe de comparaison est le GAME (Globalement Au Moins Équivalent), applicable pour les nouveaux systèmes dont les fonctions sont déjà réalisées par un système équivalent. Enfin, le troisième principe réclame la détermination qualitative ou quantitative de critères de sécurité. L'utilisation d'un ou plusieurs principes permet de conclure sur l'acceptabilité du risque. Les risques induits par le changement doivent être également confrontés aux exigences de sécurité stipulées dans les référentiels normatifs ferroviaires issus de la norme [IEC 61508, 2010]. La figure 2.2 montre les déclinaisons de cette norme selon le secteur industriel visé.

Les exigences de sécurité sont ensuite définies à l'aide d'un niveau d'intégrité de sécurité, le SIL (pour *Safety Integrity Level*) (cf tableau 2.1). L'intégrité de sécurité est définie comme étant "la probabilité pour qu'un système Électrique, Électronique et Électronique Programmable (systèmes E/E/PE) relatif à la sécurité, exécute de manière satisfaisante les fonctions de sécurité spécifiées dans toutes les conditions énoncées et dans une période de temps spécifiée". Les niveaux d'intégrité de sécurité sont utilisés pour traduire l'aptitude d'un système E/E/PE à remplir ses fonctions de sécurité. Par exemple, une fonction de sécurité peut être une action pour éviter une situation dangereuse

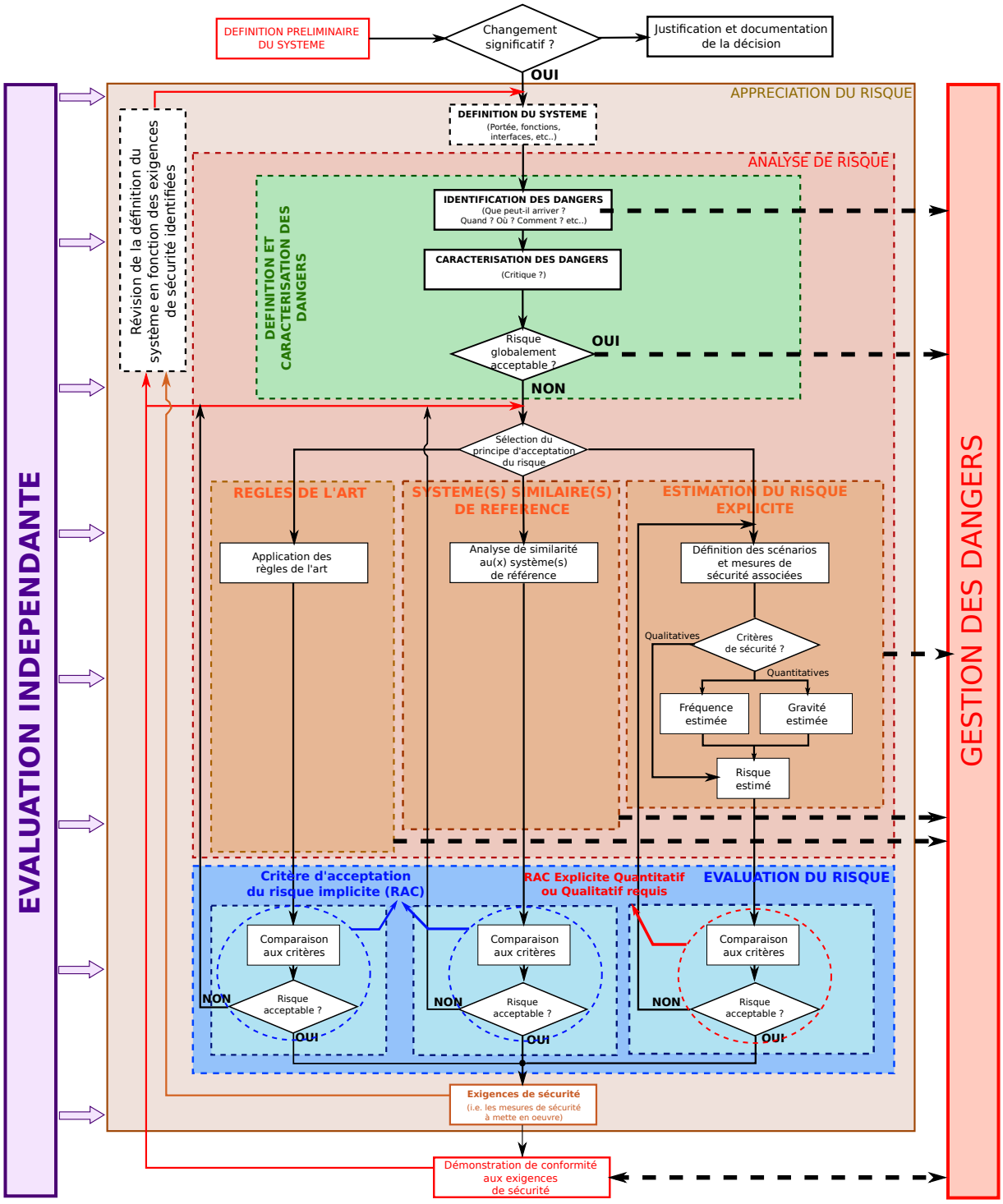


FIGURE 2.1 – Cadre de gestion des risques du règlement MSC.

telle qu'un freinage d'urgence pour éviter une collision. Quatre niveaux, SIL1 à SIL4, permettent de spécifier des exigences de sécurité qualitatives ou quantitatives pour un système selon l'impact de ses défaillances. Le SIL4 est le niveau associé aux exigences de sécurité les plus contraignantes. Les exigences quantitatives (encadrées par une limite minimale et maximale) pour chaque SIL sont

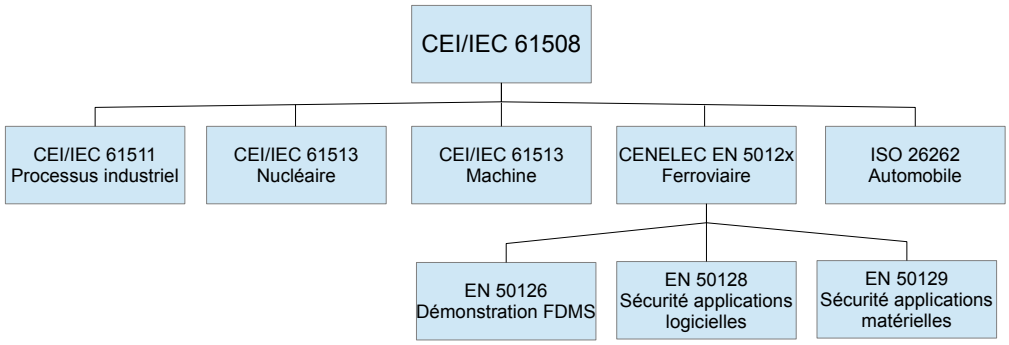


FIGURE 2.2 – Norme IEC 61508 et ses déclinaisons.

définies selon le mode de fonctionnement du système : le PFD_{avg} pour *Average Probability of Failure on Demand* et le PFH pour *Probability of a dangerous Failure per Hour* (cf tableau 2.1). PFD_{avg} est définie par la fréquence moyenne d'une défaillance dangereuse d'un système E/E/PE relatif à la sécurité pour réaliser la fonction de sécurité spécifiée pendant une période de temps donnée. PFH est la probabilité moyenne, par heure, qu'un système/sous-système relatif à la sécurité présente une défaillance dangereuse l'empêchant de réaliser la fonction de sécurité spécifiée pendant une période de temps donnée. Ces définitions sont celles données dans la norme [IEC 61508-4, 2010].

Tableau 2.1 – SIL définis par la norme [IEC 61508-4, 2010] et leurs exigences quantitatives associées.

Niveaux d'intégrité de sécurité	Faible sollicitation	Demande continue / Forte sollicitation
	Probabilité moyenne de défaillance à la demande (PFD_{avg})	Probabilité de défaillance dangereuse par heure (PFH)
SIL 4	$10^{-5} \leq PFD_{avg} \leq 10^{-4}$	$10^{-9} \leq PFH \leq 10^{-8}$
SIL 3	$10^{-4} \leq PFD_{avg} \leq 10^{-3}$	$10^{-8} \leq PFH \leq 10^{-7}$
SIL 2	$10^{-3} \leq PFD_{avg} \leq 10^{-2}$	$10^{-7} \leq PFH \leq 10^{-6}$
SIL 1	$10^{-2} \leq PFD_{avg} \leq 10^{-1}$	$10^{-6} \leq PFH \leq 10^{-5}$

Le secteur ferroviaire se démarque des autres domaines industriels par l'existence de trois normes ([EN 50126, 2000], [EN 50128, 2001] et [EN 50129, 2003]) (cf figure 2.3), utilisées selon le sous-système considéré et par l'utilisation du THR (*Tolerable Hazard Rate*)) pour spécifier les exigences quantitatives liées aux SIL (cf tableau 2.2).

Tableau 2.2 – SIL définis par la norme [EN 50126, 2000] et leur taux d'occurrence maximal acceptable de danger (THR) requis.

Niveaux d'intégrité	Taux d'occurrence maximal acceptable de danger (THR)
SIL 4	$10^{-9} \leq THR \leq 10^{-8}$
SIL 3	$10^{-8} \leq THR \leq 10^{-7}$
SIL 2	$10^{-7} \leq THR \leq 10^{-6}$
SIL 1	$10^{-6} \leq THR \leq 10^{-5}$

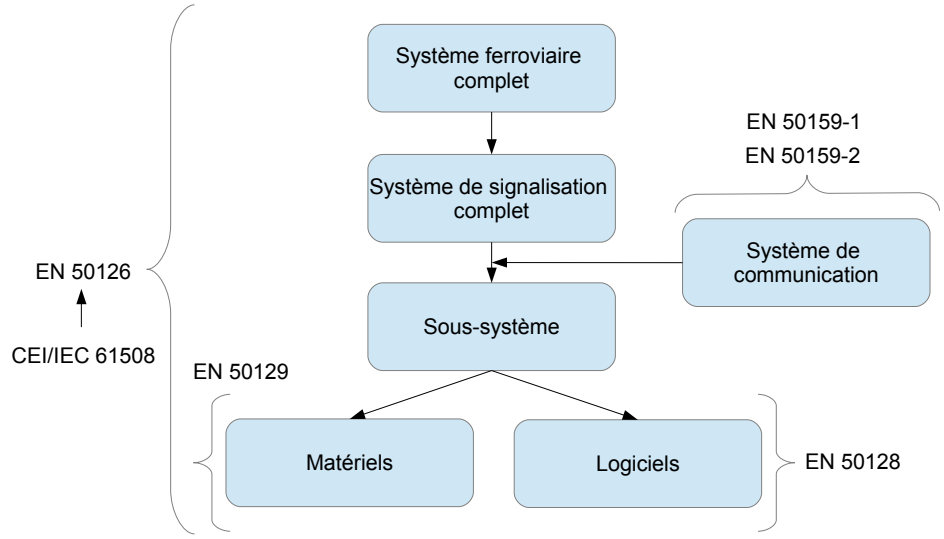


FIGURE 2.3 – Normes ferroviaires EN5012x [Boulanger, 2011].

Tout au long du processus de gestion des risques, des méthodes sont utilisées afin de répondre aux objectifs des différentes étapes de ce processus. La section suivante présente ces différentes méthodes de la sûreté de fonctionnement après avoir présenté les concepts liés à cette discipline.

2.3 Moyens et méthodes d'analyse de la sûreté de fonctionnement de systèmes automatisés

2.3.1 Concepts liés à la sûreté de fonctionnement

Cette section introduit les différents concepts usuels et définit le vocabulaire utilisé dans ce mémoire. La **sûreté de fonctionnement** (SdF) est la science des défaillances : de leur connaissance en passant par leur évaluation, leur prévision, leur mesure jusqu'à leur maîtrise. Plus précisément, elle est l'aptitude d'une entité à satisfaire une ou plusieurs fonctions requises dans des conditions données [Villemeur, 1988]. Selon Laprie, la SdF d'un système définit la propriété qui permet de placer une confiance justifiée dans le service qu'il délivre [Arlat and Laprie, 1995].

Selon Villemeur, une **défaillance** est une cessation de l'aptitude d'une entité représentable, par exemple une organisation, un système ou un produit, à accomplir une fonction requise pour une mission donnée. Cette définition est reprise dans la norme internationale [IEC 60050, 2015a]. Quant à Laprie, il définit la défaillance comme une déviation du service délivré non acceptable par rapport à la fonction attendue du système. La cause d'une **défaillance** est l'activation d'une **erreur** conséquence interne d'une **faute**[1] (cf Figure 2.4). Les défaillances, les erreurs et les fautes sont appelées entraves. La figure 2.6 montre la propagation des erreurs au sein d'un système.

La SdF se mesure au travers de plusieurs paramètres ou attributs. Le sigle FDM (pour Fiabilité, Disponibilité, Maintenabilité) se retrouve souvent dans la littérature au même titre que FDMS (en anglais RAMS pour *Reliability*, *Availability*, *Maintainability and Safety*) avec S pour Sécurité.

1. Le terme anglais *Fault* peut désigner une faute [Arlat and Laprie, 1995] ou une panne [IEC 60050, 2015a]. Or, une panne est inaptitude à fonctionner tel que requis et est toujours la résultante d'une défaillance [Villemeur, 1988]

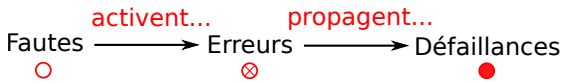


FIGURE 2.4 – Enchainement des évènements liés à la SdF selon Laprie [Arlat and Laprie, 1995].

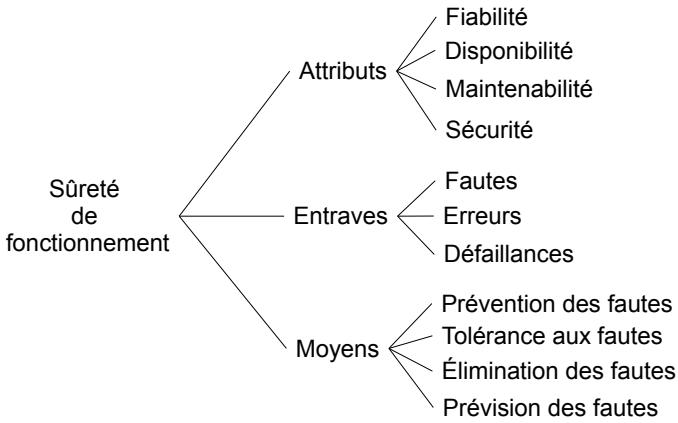


FIGURE 2.5 – La sûreté de fonctionnement du point de vue de Laprie [Arlat and Laprie, 1995].

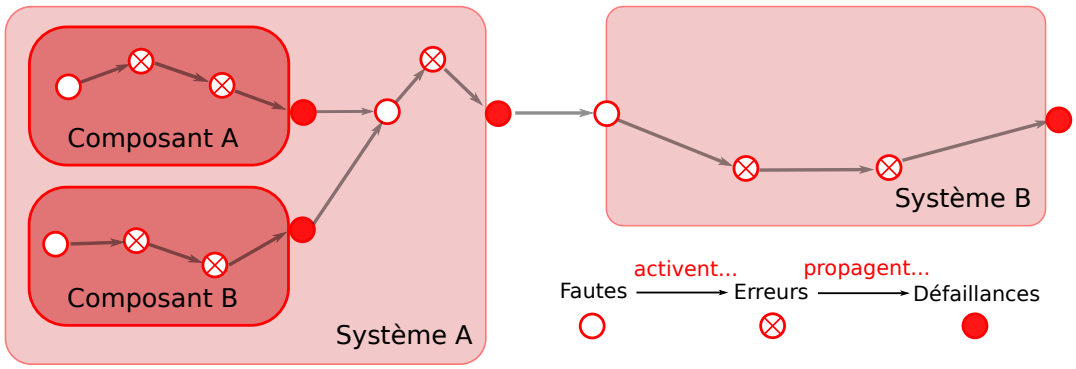


FIGURE 2.6 – Enchainement des fautes, des erreurs et des défaillances au sein d'un système inspiré de [Boulanger, 2011].

La **fiabilité** est l'aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné. Dans cette définition, le terme d'entité est utilisé pour désigner un composant, un sous-système ou un système. Une fonction requise peut être aussi bien une simple fonction ou plusieurs fonctions fournissant un service donné [Rausand and Høyland, 2003]. Ici, la fiabilité d'un système est représentée par une probabilité de bon fonctionnement c'est à dire la probabilité qu'aucune défaillance n'apparaisse durant l'intervalle de temps considéré $[0, t]$ (cf équation 2.1).

$$R(t) = p(\text{E non défaillante sur } [0, t]) \tag{2.1}$$

avec, E une entité quelconque et $p(A)$, la probabilité d'un évènement A.

Dans le cadre de l'étude de la fiabilité d'une entité, on définit également un taux de défaillance. Le **taux de défaillance** $\lambda(t)$ est lié à une probabilité d'apparition de la première défaillance sur un

intervalle de temps donné Δt (cf équation 2.2).

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{1}{\Delta t} \cdot [p(\text{E défaillante entre } t \text{ et } t + \Delta t \text{ sachant pas de défaillance sur } [0,\, t])] \tag{2.2}$$

L'évolution du taux de défaillance peut être décrite par une loi statistique, on parle alors de loi de fiabilité. Ce taux peut être considéré constant ($\lambda(t) = \lambda$ pour une loi exponentielle) ou non. Le tableau 2.3 liste les lois usuelles utilisées en fiabilité.

Tableau 2.3 – Lois usuelles utilisées en fiabilité.

Grandeur statistique	Grandeur fiabiliste	Loi exp	Loi normale	Loi de Weibull
$f(t)$	$U(t)$	$\lambda e^{-\lambda t}$	$\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{t-\mu}{\sigma})^2}$	$\frac{\beta(t-\gamma)^{\beta-1}}{\sigma^\beta} e^{-(\frac{t-\gamma}{\sigma})^\beta}$
$F(t)$	$1 - R(t)$	$1 - e^{-\lambda t}$	$\frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\frac{1}{2}(\frac{t-\mu}{\sigma})^2} dt$	$1 - e^{-(\frac{t-\gamma}{\sigma})^\beta}$
-	$\lambda(t)$	λ	$\frac{U(t)}{R(t)}$	$\frac{\beta(t-\gamma)^{\beta-1}}{\sigma^\beta}$

$f(t)$, Densité de probabilité
$U(t)$, Densité de défaillance
$F(t)$, Fonction de répartition
$1 - R(t)$, Défiabilité
$\lambda(t)$, Taux de défaillance variable
λ, σ, μ, β, γ, paramètres, respectivement, de la loi exponentielle, normale et de Weibull

Malheureusement, il n'est pas toujours réaliste d'utiliser ces lois pour modéliser la fiabilité d'un système complexe. Par exemple, associer un taux de défaillance sur des entités immatérielles comme des signaux de transmission n'est pas possible *a priori*.

La **disponibilité** est l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné. Il ne faut pas confondre disponibilité instantanée et disponibilité moyenne. La disponibilité instantanée à un instant t s'exprime par la probabilité décrite par l'équation 2.3.

$$A(t) = p(\text{entité fonctionnant à l'instant } t) \tag{2.3}$$

La **disponibilité moyenne** est, par définition, le ratio entre le temps de bon fonctionnement et le temps total (équation 2.4).

$$A_{moy} = \frac{\text{Temps de bon fonctionnement}}{\text{Temps de fonctionnement total}} \tag{2.4}$$

Plusieurs variables temporelles sont introduites selon la phase disponibilité/indisponibilité du système. Le schéma de la figure 2.7 montre la succession de ces variables de temps avec :

— *MTTR* (*Mean Time To Repair*) : le temps moyen de réparation dans le cas de systèmes réparables.
— *MUT* (*Mean Up Time*) : le temps moyen de fonctionnement après réparation de la panne.
— *MDT* (*Mean Dowm Time*) : le temps d'indisponibilité du système.

— $MTTF$ (*Mean Time To Failure*) : le temps moyen de fonctionnement avant une première panne. Il existe un lien entre le taux de défaillance λ et $MTTF$ lorsque λ est constant ($MTTF = \frac{1}{\lambda}$). Si λ est variable ($\lambda(t)$), $MTTF$ est de la forme [Kumamoto and Henley, 1996] :

$$MTTF = \int_0^\infty t \cdot f(t)\mathrm{d}t \tag{2.5}$$

avec $f(t)$, une densité de défaillance.

— $MTBF$ (*Mean Time Between Failure*) : le temps moyen entre deux pannes.

En considérant ces temps, la disponibilité moyenne s'exprime selon l'équation 2.6.

$$A_{moy} = \frac{MUT}{MDT + MUT} \tag{2.6}$$

Dans le cas où $MTTR = MDT$ (le temps de réparation correspond alors exactement au temps d'indisponibilité), $MTBF = MTTF + MTTR$. De plus, si $MTTR \ll MTTF$, $MTBF \approx MTTF$. Ces hypothèses permettant d'exprimer la disponibilité moyenne selon l'équation 2.7.

$$A_{moy} \approx \frac{MTBF}{MTBF + MDT} \tag{2.7}$$

La notion inverse de la disponibilité, l'indisponibilité, est également utilisée :

$$\overline{A} = 1 - \frac{MTBF}{MTBF + MDT} \tag{2.8}$$

La **maintenabilité** est l'aptitude d'une entité (système réparable) à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise [Villemeur, 1988]. La maintenabilité s'évalue de manière quantitative grâce au facteur MTTR, le temps de réparation vu plus haut. Cependant, il s'agit d'une maintenance corrective. Il existe des maintenances préventives (systématiques, conditionnelles ou prévisionnelles).

La notion de **sécurité** est ambiguë en français. En anglais, il existe deux termes : *safety* et *security* qui ne désignent pas la même chose. Pour lever l'ambiguïté, la sécurité globale est associée aux termes suivants [Arlat and Laprie, 1995] :

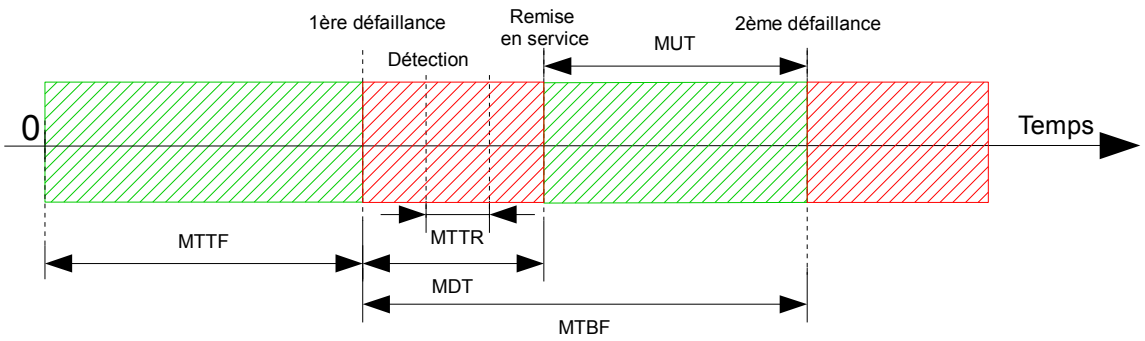


FIGURE 2.7 – Les différents intervalles de temps dans la vie d'un composant.

— La **sécurité-innocuité** (*safety*) qui désigne l'absence de risque inacceptable à l'extérieur des unités fonctionnelles et physiques considérées.

— La **sécurité-immunité** (*security*) pouvant se définir comme la robustesse en matière de prévention d'action hostile délibérée. Cet aspect de la sécurité n'est pas abordé dans cette thèse.

Il existe des mécanismes, appelés **moyens**, permettant d'améliorer la sûreté de fonctionnement d'un système (cf figure 2.5). Ils constituent des stratégies de gestion (prévention, prévision, tolérance voire élimination) des fautes, causes des défaillances pour interrompre l'enchaînement vu à la figure 2.4.

La **prévention des fautes** intervient au niveau de la conception d'un système en introduisant des techniques (règles de construction) pour éviter l'apparition de fautes. La **tolérance aux fautes** est l'aptitude d'une entité à accomplir sa fonction malgré la présence ou l'occurrence de faute. Elle passe par des étapes de détection d'erreur dans le but de rétablir le système dans des conditions normales de fonctionnement. L'**élimination des fautes** est simplement la réduction de la présence des fautes en termes de nombre et de gravité. Quant à la **prévision des fautes**, il s'agit de l'estimation de la présence de fautes, des conditions d'apparition et de leur conséquence. Ces moyens doivent être combinés puisque la sûreté ne peut être garantie si un seul moyen est mis en œuvre. Par exemple, une faute peut être prédite mais ne pas être traitée si aucun moyen n'est disponible.

2.3.2 Catégories de méthodes d'analyse

Il existe de nombreuses méthodes de SdF. La méthode qui sera utilisée dépend du type d'analyse choisie. Le processus d'analyse commence par le recueil d'informations sur le système considéré dans un périmètre bien délimité. Ces informations, une fois traitées, permettent l'établissement d'une première analyse qui peut être enrichie par la suite. Les différents modes de fonctionnement/dysfonctionnement du système (service délivré/non délivré par rapport à ce qui est attendu par l'utilisateur) ainsi que les interactions avec l'environnement dans lequel il évolue sont alors décrits. Les méthodes peuvent s'appuyer sur des analyses prévisionnelles, opérationnelles ou formelles que nous allons présenter.

2.3.2.1 Analyses prévisionnelles

Les analyses prévisionnelles sont des démarches qui consistent à obtenir un modèle du système considéré pour un paramètre de SdF à évaluer (FDMS). Ici, les conditions (une faute d'un composant par exemple) menant aux défaillances sont recherchées et leurs conséquences sont prévues. Parmi les méthodes permettant de faire ce genre d'analyse, deux raisonnements peuvent être effectués : descendant (méthode déductive) et ascendant (méthode inductive). Le raisonnement descendant part du plus général vers le particulier. Un système est supposé en défaillance et ses causes sont recherchées. Le raisonnement ascendant, quant à lui, part du particulier vers le plus général. Les effets et les conséquences d'une défaillance sur le système lui-même ou sur son environnement sont étudiés.

Une analyse prévisionnelle se résume en quatre grandes étapes (cf figure 2.8) :

1. Une analyse technique et fonctionnelle recueille les informations du système et de son environnement afin de définir le périmètre de l'étude. Ces informations concernent l'architecture du système : quelle est sa structure (nature et nombre de composants) ? Quelle est sa nature

(électronique, mécanique, *etc.*) ? Quelles sont ses fonctions principales et secondaires ? Quels sont ses modes de fonctionnement et de défaillance ?

2. Une analyse qualitative applique une ou plusieurs méthodes. Le tableau 2.4 en propose une liste.

3. Une analyse quantitative conduit à une évaluation probabiliste des paramètres FDMS.

4. Conclusion. Il s'agit alors de faire la synthèse des analyses qualitative et quantitative et d'émettre quelques propositions d'amélioration ou de modification.

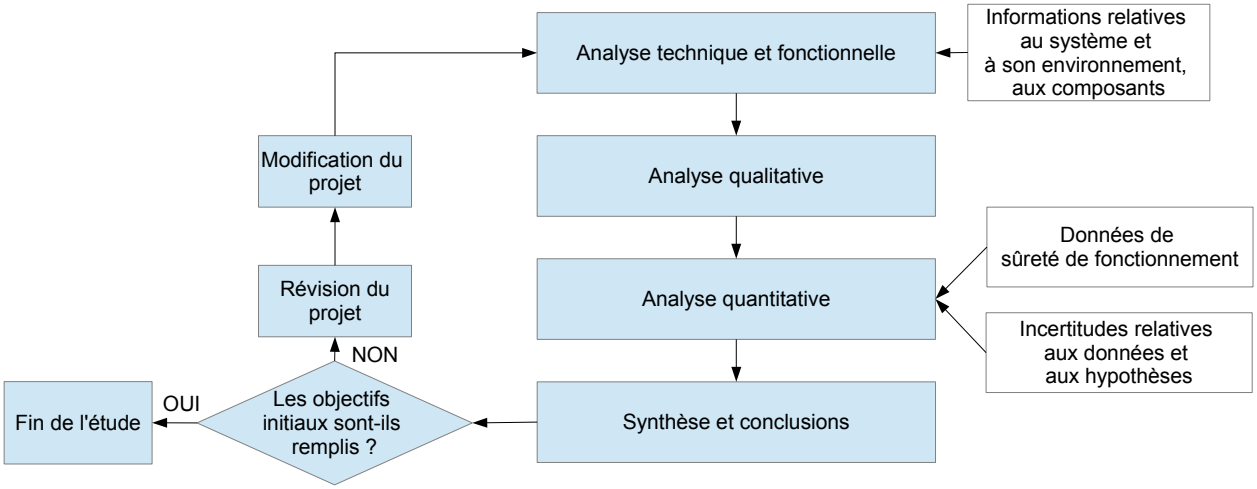


FIGURE 2.8 – Les étapes d'une analyse prévisionnelle.

La première étape, l'analyse technique et fonctionnelle, consiste à décrire le besoin d'un utilisateur sous forme de fonctions hiérarchisées et associées à des critères d'appréciation. Les résultats d'une telle analyse se présentent sous la forme de Cahier des Charges Fonctionnel (CdCF), de diagrammes ou de tableaux fonctionnels.

Différentes méthodes d'analyse fonctionnelle existent. La méthode FAST (pour *Function Analysis System Technique*) est une méthode statique permettant d'ordonner les fonctions identifiées au travers d'une logique fonctionnelle en répondant aux questions : pourquoi une fonction donnée existe-elle ? Comment et quand est-elle réalisée ? La méthode SADT (pour *Structured Analysis and Design Technique*) est une méthode statique de décomposition fonctionnelle, hiérarchisée avec différents niveaux de détails. Les réseaux de Petri permettent de modéliser le comportement dynamique d'un système sous forme de places et transitions reliées par des arcs orientés. L'aspect dynamique d'un réseau de Petri est géré par des jetons (symbolisant des ressources disponibles), retirés ou déposés dans les places selon des conditions de franchissement des transitions.

Pour pouvoir mener à bien les analyses qualitatives et quantitatives (étape 2 et 3), il faut au préalable bien connaitre les objectifs de l'analyse de SdF c'est à dire est-ce que l'étude vise à caractériser un critère FDMS en particulier ? Quelles sont les fonctions concernées ? Ces étapes exigent également de définir le périmètre de l'analyse, c'est à dire est-ce qu'elle concerne un composant d'un

système, un de ses sous-systèmes ou le système dans son intégralité ? Ce n'est qu'en répondant à ces différentes questions que le choix d'une ou de plusieurs analyses prévisionnelles de SdF est possible.

Dans un premier temps, une ou plusieurs analyses qualitatives sont réalisées. Elles ont pour objectifs de lister les différents modes de défaillance qui affectent la SdF du système considéré. Il en résulte une modélisation de la SdF du système en considérant des hypothèses telles que les interactions avec l'environnement, celles avec d'autres systèmes, le comportement de l'opérateur, *etc.*). Des enseignements sont tirés de cette analyse : Quelles sont les défaillances pertinentes ? Quelles sont les défaillances ou combinaisons de défaillances menant à une situation indésirable ? Une de nos contributions, l'**analyse causale**, présentée dans la section 2.4.3 a pour but l'identification de ce genre de combinaisons.

Dans un second temps, il s'agit d'effectuer une ou plusieurs analyses quantitatives permettant de caractériser notamment les données de sûreté telles que des taux d'occurrence, probabilités, *etc...* C'est ici que l'on s'intéresse aux incertitudes sur ces données ainsi que celles générées avec les hypothèses de modélisation. On parle alors d'**études de sensibilité**. Nous en proposons une dans la sous-section 2.4.4. Les conclusions découlant d'une analyse quantitative permettent, d'une part, de nous renseigner sur le niveau de sûreté atteint et, d'autre part, d'identifier et d'évaluer les points faibles du système (les sous-systèmes ou composants les plus critiques en terme de sûreté) et leurs conséquences.

L'ensemble des conclusions des analyses qualitatives et quantitatives sont synthétisées afin de déterminer si les objectifs stipulés en début d'analyse sont remplis ou non. Dans l'affirmative, l'étude de SdF est terminée. Dans le cas contraire, une révision suivie d'une modification du projet est nécessaire avant de réitérer le processus d'analyse. Les conclusions permettent également d'émettre des propositions de différentes natures : application de redondance, plans d'exploitation ou de maintenance, mises en place de barrières, *etc..*

2.3.2.2 Analyses opérationnelles

Une analyse opérationnelle se base essentiellement sur le recueil de données issues de retour d'expérience afin d'évaluer statistiquement les paramètres FDMS [Lannoy, 2003]. La figure 2.9 montre la procédure de collecte et de traitement des données. Les objectifs des bases de données de retour d'expérience doivent être connus avant la création de la base de données et la collection. La sélection des données utiles pour l'analyse permet la création d'un fichier sur lequel vont s'appuyer des analyses quantitatives afin de conclure en termes de paramètres FDMS.

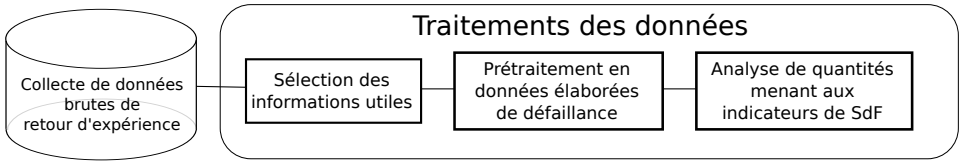


FIGURE 2.9 – Procédure d'une analyse opérationnelle.

Ce type d'analyse n'est pas adapté pour une évaluation FDMS de systèmes totalement nouveaux puisque le retour d'expérience sur leur utilisation n'existe pas.

Tableau 2.4 – Méthodes prévisionnelles classiques (liste non exhaustive) en SdF issues de la norme [EN 60300-3-1, 2005].

Méthodes d'analyse	Démarche	Caractère	Dynamique ?	Objectifs
Tables de vérité (fonction de structure)	-	QL	Non	Identifier des combinaisons logiques d'évènements ou d'états
Prévision du taux de défaillance	I	QT	Non	Estimation des taux de défaillance des équipements
Arbre d'évènement	I	QL-QT	Non	Évaluer les conséquences d'un évènement ou d'une défaillance
Graphe de Markov	D	QL-QT	Oui	Modéliser statistiquement les états d'un système
Réseaux de Pétri	D	QL-QT	Oui	Modéliser le comportement dynamique d'un système
Études HAZOP (*HAZard and OPerability studies*)	I	QL	Non	Identifier les risques et les problèmes de fonctionnement
Diagramme de fiabilité	D	QL-QT	Non	Modéliser un système en fonction élémentaires (série ou parallèle)
Réseaux Bayésiens	D	QT	Oui	Modéliser un système en fonction de probabilité conditionnelle
AMDEC (Analyse des Modes de Défaillance, de leur Effets et de leur Criticité)	I	QL-QT	Non	Identifier les défaillances et évaluer leurs conséquences
APR	I/D	QL	Non	Identifier les évènements redoutés à étudier
Arbre de Défaillance	D	QL	Non	Évaluer les conditions qui ont conduit vers une défaillance

D : Déductive. I : Inductive. QL : Qualitative. QT : Quantitative

2.3.2.3 Analyses formelles

Les analyses formelles utilisent des techniques développées en génie logiciel permettant de raisonner de manière rigoureuse sur un problème avec la logique mathématique [Lindsay, 1998]. Elles permettent de donner une spécification à un système c'est à dire une description dans un langage explicite, non-ambiguë contrairement au langage naturel.

Cette spécification est utilisée en particulier dans le but de vérifier de manière formelle des propriétés requises (preuves formelles), par exemple, des propriétés de sûreté de fonctionnement (pas de panne simple amenant à une conséquence catastrophique par exemple). Le *model-checking* est une des techniques utilisées par la vérification automatique de ces propriétés. Il s'appuie sur des

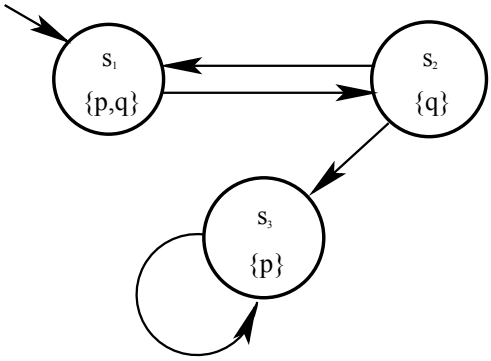


FIGURE 2.10 – Exemple de structure de Kripke [Kripke, 1963] avec s_1, s_2 et s_3, les états d'un système et p, q, des propriétés booléennes quelconques.

structures de Kripke (cf figure 2.10) pour modéliser un système ainsi que les propriétés à prouver. Une propriété est vraie si le produit cartésien entre la structure de Kripke du système et celle de la propriété à prouver est nul. Le produit cartésien de deux structures de Kripke est la combinaison de tous les éléments de ces structures entre eux.

Le cadre ferroviaire de la gestion des risques et ses différents concepts de sûreté de fonctionnement étant posés, nous proposons d'appliquer une **analyse prévisionnelle** de SdF sur les systèmes considérés dans ce chapitre, les systèmes de localisation fondés sur les GNSS. En effet, mettant en œuvre de nouvelles technologies de localisation dans le domaine ferroviaire, une analyse opérationnelle n'est pas envisageable pour un tel système de localisation faute de retour d'expérience suffisant dans ce secteur. De plus, les analyses formelles sont initialement destinées pour la vérification de preuves (de sécurité, de disponibilité, *etc.*) de systèmes logiciels et l'interprétation de spécifications exprimés en langage naturel. Les méthodes formelles commencent à émerger dans la spécification des attributs FDM des systèmes de navigation par satellite [Peng et al., 2014] [Lu et al., 2015] mais elles ne sont pas encore éprouvées pour ces systèmes. Par conséquent, nous nous orientons vers une analyse prévisionnelle (illustrée par la figure 2.8) qui semble la plus adaptée pour des systèmes avec GNSS. Des méthodes reposant sur une démarche prévisionnelle ont déjà été utilisées depuis plusieurs années, notamment les arbres de défaillances dans le domaine aéronautique [ICAO, 2006] et des formalismes innovants à base d'arbres de défaillance dans le domaine ferroviaire [Filip et al., 2001] [Nguyen et al., 2014]. Pour mener à bien une telle analyse, il faut clairement définir l'objet de cette analyse. Dans notre cas, il s'agit d'identifier les scénarios risqués (sous la forme de **combinaisons d'état de capteurs**) grâce à une **analyse causale**. Enfin, il s'agira d'étudier l'impact des données imparfaites et erronées (sous la forme de **mesures de sensibilité** de paramètre) au sein d'un système avec un récepteur GNSS grâce à une **analyse de sensibilité**.

2.4 Identification de scénarios risqués et impacts des données imparfaites/erronées au sein d'architectures centrées sur un récepteur GNSS

Dans ce paragraphe, nous considérons 4 architectures de systèmes de localisation multicapteurs issues des projets ferroviaires présentés au chapitre 1. Dans un premier temps, nous appliquons une analyse causale pour identifier les combinaisons d'état de capteurs risquées sur ces 4 architectures. Dans un second temps, nous choisirons l'architecture la plus simple d'un système multicapteur avec

GNSS (Accéléromètre + Odomètre + Récepteur GPS + fusion par moyenne pondérée) afin de présenter un cas d'école pour l'analyse de sensibilité *i.e.* pour l'identification des paramètres les plus influents sur la sortie de ce système.

Le premier objectif vise à identifier les combinaisons d'erreurs conduisant à une situation indésirable et risquée. Dans notre cas, cela correspond à la situation "le système fournit une position inacceptable". Le terme "inacceptable" signifie que l'erreur de position dépasse un seuil donné (exigence). L'**analyse causale** permet l'identification de combinaisons logiques d'état de composants. Nous considérons non pas uniquement des combinaisons d'états booléens ("0" entité en panne, "1" entité en fonctionnement normal) mais des combinaisons multi-états (Nominal, Dégradé mais Acceptable, Inacceptable) de capteurs (récepteur GNSS + autres capteurs), avec une dépendance temporelle entre ces combinaisons et l'état du système complet.

Le second objectif que nous nous fixons est de déterminer l'impact des erreurs et des incertitudes prises une à une au sein d'une architecture d'un système avec GNSS. Pour répondre à cet objectif, il existe la notion de facteurs d'importance [Vesely and Rasmuson, 1984]. Ils permettent de mesurer l'impact de l'indisponibilité d'un composant dans un système [Mercurio and Thornsbury, 2015]. Cependant, les facteurs d'importance se basent sur la connaissance *a priori* de la disponibilité du système (plus précisément sur son indisponibilité), inconnue pour les systèmes GNSS pour des applications ferroviaires. En l'absence de connaissances sur l'indisponibilité de composant, il existe une autre manière de déterminer l'impact des erreurs sur les données grâce à une **analyse de sensibilité**. Les mesures de sensibilité sont des variantes des facteurs d'importance puisqu'elles peuvent être également déterminées par des dérivées partielles. Nous proposons d'utiliser ce type d'analyse dans la sous-section 2.4.4.

2.4.1 Hypothèses de travail simplificatrices pour les analyses causale et de sensibilité

Avant de décrire les principes des analyses causale et de sensibilité, certaines hypothèses relatives aux systèmes avec GNSS considérées, doivent être présentées.

La première hypothèse simplificatrice consiste à considérer une trajectoire rectiligne connue en contexte 1D pour le train. En effet, nos analyses se concentrent uniquement sur l'impact des différents constituants de l'architecture. La prise en compte d'une trajectoire du train plus complexe telle que présentée dans la thèse de [Zhu, 2014] pourra faire l'objet d'une étude complémentaire. Nous connaissons *a priori* la position réelle du train. Ainsi, l'écart entre la position réelle x et la position estimée $\hat{x}$ est connu et se définit par à l'aide de la norme euclidienne de l'équation 2.9 [Tartakovsky et al., 2014].

$$\|x - \hat{x}\| \tag{2.9}$$

La seconde hypothèse simplificatrice est relative au système multicapteurs. Ce dernier est associé à un processus de fusion de données qui s'appuie sur différents algorithmes de filtrage. Les plus connus dans la littérature sont : moyenne pondérée, moindres carrés [Kuusniemi, 2005], filtres de Kalman [Groves, 2013], filtres particulaires [Doucet et al., 2000]. Ces différentes techniques sont présentées en détails dans la thèse de [Viandier, 2011]. Pour notre démonstration, nous avons choisi de ne considérer que les techniques classiques les plus simples : moyenne pondérée et filtre de Kalman. Les architectures proposées dans la section suivante sont constituées uniquement d'un système

multicapteur avec un récepteur GPS et d'un filtre parmi ceux cités.

La troisième hypothèse simplificatrice est que nous ne considérons pas de système de détection de pannes fondé sur le calcul et la comparaison de résidus. Il s'agit d'indicateurs de panne (ou d'autres défauts) basés sur la **différence entre des mesures et des résultats de calculs à partir d'équations de modèle** [Le Marchand, 2010]. Dans le chapitre 2, ce ne sont pas les résidus qui sont utilisés comme indicateur de panne mais l'**écart de position réel** formulé par l'équation 2.9 sachant que la position réelle est connue. Les résidus sont présentés et utilisés à partir du chapitre 3.

2.4.2 Préalables sur les techniques d'estimation par filtrage statistique

Cette partie rappelle brièvement les principales techniques de filtrage pour les systèmes qui nous intéressent *i.e.* les systèmes de navigation hybrides (GNSS et autres capteurs). Pour ces systèmes, l'état x_t doit être estimé à partir des observations z_t qui sont les mesures de pseudo-distances GNSS et les autres mesures issues des capteurs. Le système est dynamique et les mesures sont bruitées. Il existe différentes méthodes de filtrage qui permettent d'estimer le vecteur d'état. Leurs hypothèses de départ et leurs spécificités les diffèrent :

— La **moyenne pondérée** est la moyenne d'un nombre de valeurs (val) multipliées par des coefficients appelés poids α_i (cf équation 2.10). La moyenne arithmétique est un cas particulier où les poids sont égaux à 1.

$$val_{moy} = \frac{\sum_{i=1}^{n} \alpha_i \cdot val_i}{\sum_{i=1}^{n} \alpha_i} \tag{2.10}$$

— Les **méthodes des Moindres Carrés** et **Moindres Carrés Pondérés** sont des méthodes d'ajustement statistique. Elles cherchent à résoudre une équation du type "$A \cdot x = b$" qui n'a pas de solution exacte. En effet, la matrice d'état A est une matrice $m \times n$ où $m \geq n$. Le nombre d'observations, m, doit être supérieur ou égal au nombre d'inconnues, n. L'estimation de la position par la méthode des Moindres Carrés est donnée par l'équation 2.11.

$$\Delta\hat{X} = (H^t \cdot H)^{-1} \cdot H^t \cdot \Delta Y \tag{2.11}$$

Où $\Delta\hat{X}$ est la mise à jour de l'estimation de la position, H la matrice d'observation et ΔY la mise à jour de la mesure. L'inconvénient de cette méthode est qu'elle ne prend pas en compte d'informations sur les bruits pour corriger son estimation. La méthode des moindres carrés pondérés permet de pondérer la confiance dans les mesures en introduisant un poids sous la forme d'une matrice P. En théorie, P est l'inverse de la matrice de variance-covariance des observations. En pratique, cette matrice est inconnue. Il faut donc soit l'estimer en fonction des mesures (plus exactement, en fonction de la variance de ces mesures) ou en fonction d'un critère de confiance sur la mesure, soit la remplacer par un modèle. L'équation 2.12 s'obtient en introduisant P dans l'équation 2.11.

$$\Delta\hat{X} = (H^t \cdot P \cdot H)^{-1} \cdot H^t \cdot P \cdot \Delta Y \tag{2.12}$$

où, $P = \begin{bmatrix} w_1 & \dots & 0 \\ \vdots & w_i & \vdots \\ 0 & \dots & w_n \end{bmatrix}$. Le poids w_i est fixé dans la littérature comme une fonction de

l'élévation [Wieser et al., 2005] ou du rapport signal à bruit $\frac{C}{N_0}$ [Li and Wu, 2009].

— Le **filtrage bayésien** est plus souvent retenu. Contrairement aux méthodes précédentes, il utilise des informations *a priori*. Le filtre le plus connu est le **filtre de Kalman**. Il repose sur les hypothèses que : le modèle d'état est linéaire et que les bruits d'états et d'observation sont blancs et Gaussiens. Sous ces hypothèses, le filtre de Kalman donne la solution optimale en minimisant le critère MMSE (*Minimum Mean Square Error*). Le filtre de Kalman est une méthode d'estimation bayésienne récursive, qui se compose de deux étapes : une étape de prédiction et une étape de correction. Le système est défini par deux équations : l'équation d'état (cf équation 2.13) et l'équation de mesure (cf équation 2.14) présentées sous leur forme matricielle.

$$X_k = F_{k-1}.X_{k-1} + v_{k-1} \tag{2.13}$$

$$Z_k = H_k.X_k + w_k \tag{2.14}$$

où H et F sont respectivement les matrices d'observation et d'évolution, X_k le vecteur d'état et Z_k le vecteur de mesure. v_k est le bruit du système, w_k est le bruit d'observation à l'instant k. On note que l'équation d'évolution utilise l'information à l'instant $k-1$ pour définir le vecteur d'état à l'instant k.

Pour les équations de navigation, l'expression de la pseudodistance étant faiblement non linéaire, le filtre de Kalman Étendu (EKF) doit être utilisé. Il consiste à ajouter une étape de linéarisation des fonctions d'état et d'observation par un développement de Taylor au 1^{er} ordre. Après cette approximation, la solution de l'EKF est non optimale. Les hypothèses sur les bruits sont les mêmes que pour le filtre de Kalman.

— Lorsque les hypothèses ne sont pas respectées (bruits non blancs ou forte non-linéarité), les performances sont fortement dégradées. Le **filtre particulaire** (FP) peut alors être envisagé. Le filtre particulaire ne fait pas ces hypothèses de départ. Il s'agit d'une méthode de Monte Carlo qui consiste à représenter la densité de probabilité *a posteriori* par un ensemble d'échantillons. Ces échantillons, appelés particules, sont associés à un poids, qui varie dans le temps. L'estimation de l'état repose sur la convergence des échantillons vers la solution. Les principes généraux du FP et ses déclinaisons sont décrites dans [Viandier, 2011] et [Arulampalam et al., 2002]. Plus le nombre d'échantillons est important, plus la solution s'approche de la solution optimale. Les inconvénients du FP sont son coût en temps de calcul et la nécessité de bien choisir la densité d'importance (utilisée dans le calcul des poids).

Maintenant que toutes les hypothèses de travail et préalables sont présentées, l'approche fondée sur l'analyse causale d'architectures de systèmes avec GNSS peut être abordée.

2.4.3 Approche pour l'analyse causale d'architecture de systèmes avec GNSS

Cette approche a pour but d'identifier les combinaisons d'états des capteurs qui conduisent à une défaillance du système de localisation [Legrand et al., 2014]. Elle sera appliquée ensuite sur quelques architectures utilisées dans les projets cités chapitre 1 section 1.4 pour déterminer quelles architectures seront associées à la meilleure qualité de service selon les critères visés. Ces critères sont les indicateurs identifiés au cours de cette analyse c'est à dire le nombre de combinaisons d'états inacceptables, le nombre de combinaisons d'états critiques et leur temps de persistance. La sous-section suivante présente les modèles en fonctionnement nominal et en présence de panne des capteurs

considérés dans les différentes architectures puis le modèle probabiliste associé à une architecture générique.

2.4.3.1 Modélisation des capteurs

Nous modélisons chaque capteur mathématiquement à partir de paramètres de fonctionnement et dans un contexte 1D. Ces capteurs sont simulés grâce au logiciel Matlab®. Les expressions 2.15 pour l'accéléromètre, 2.21 pour l'odomètre et 2.22 pour le récepteur GPS modélisent de manière simplifiée l'occurrence des états nominaux et en présence de panne de ces capteurs (signal de sortie dégradé). L'objectif n'est pas de développer un modèle d'erreur lié aux différentes données mais de voir comment considérer l'impact de ces erreurs.

2.4.3.1.1 Trajectoire de référence

Comme il a été dit dans les hypothèses de travail, la trajectoire est connue *a priori*. Par conséquent, l'accélération, la vitesse et la position réelles sont connues. Nous considérons un profil d'accélération ($\pm$ 2 m/s^2). Il s'appuie sur un profil de vitesse s'inspirant des valeurs de l'existant (ligne Paris-Nord à Lille). Les changements brusques d'accélération et de vitesse ne sont pas réalistes (cf figure 2.11) mais le but est d'avoir une accélération non constante.

2.4.3.1.2 Accéléromètre

État nominal Le modèle choisi pour décrire le fonctionnement nominal de l'accéléromètre (cf équation 2.15) est celui de la thèse de [Kubrak, 2007] :

$$a_{out}(t) = K(t) \cdot fs(t) + b_a(t) + n_a(t) \tag{2.15}$$

fs est la mesure de la force spécifique à l'instant t. L'accéléromètre est considéré comme un système masse-ressort et l'accélération est directement déduite de la force exercée sur la masse et mesurée grâce à la déformation du ressort.

K est le gain de l'accéléromètre reliant la grandeur physique mesurée *i.e* la force spécifique $fs(t)$ à l'accélération déduite par l'accéléromètre $a_{out}(t)$. Dans ce gain, un facteur d'échelle (*Scale Factor* en anglais) est pris en compte ($K = 1 + SF$). Nous pouvons estimer un SF (cf équation 2.16) selon la moyenne μ_{SF} et l'écart-type σ_{SF} mesurés lors d'expérimentations réalisées par [Kubrak, 2007] sur un accéléromètre réel.

$$SF \sim \mathcal{N}(\mu_{SF}, \sigma_{SF}^2) \tag{2.16}$$

avec, μ_{SF} = -0,096 (sans unité),
σ_{SF} = 0,028 (sans unité).

b_a est le biais de l'accéléromètre déterminé par l'équation 2.17 selon les données de [Kubrak, 2007].

$$b_a \sim \mathcal{N}(\mu_{b_a}, \sigma_{b_a}^2) \tag{2.17}$$

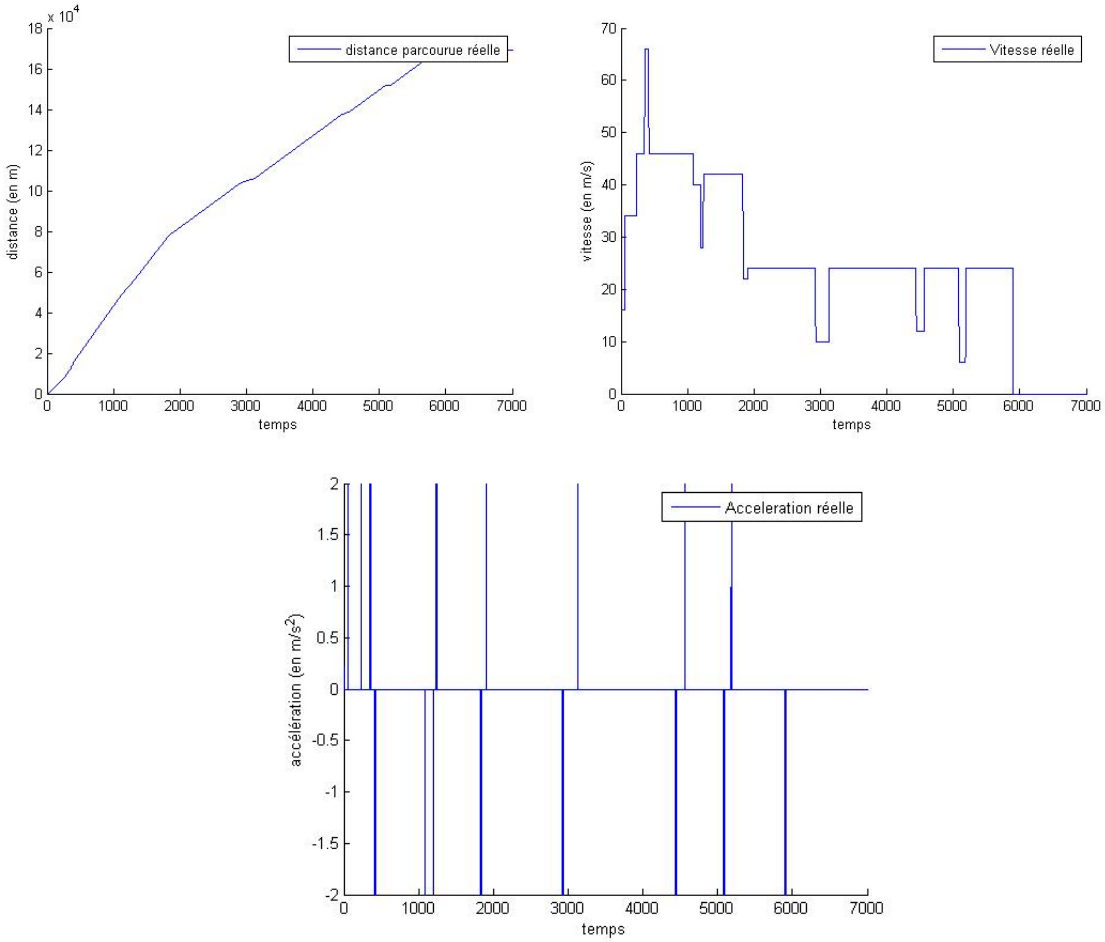


FIGURE 2.11 – Valeurs réelles pour l'accélération, la vitesse et la position pour une simulation de 7000 secondes.

avec, μ_{b_a}, la moyenne des biais mesurés de l'accéléromètre estimée à -0,061 m/s^2,
σ_{b_a}, l'écart-type des biais mesurés de l'accéléromètre estimé à 0,003 m/s^2.

n_a est le bruit sur la sortie de l'accéléromètre supposé blanc gaussien (cf équation 2.18).

$$n_a \sim \mathcal{N}(0, \sigma_{n_a}^2) \tag{2.18}$$

avec, σ_{n_a}, l'écart-type des bruits blanc gaussiens estimé à 0,03 m/s^2.

Il faut aligner les mesures de l'accéléromètre avec les mesures des autres capteurs de position présentés ci-dessous pour pouvoir fusionner par moyenne pondérée. La position (notée x_{acc}) est déduite par double intégration.

Enfin, nous générons en plus d'une mesure d'accélération (a_{out}) une mesure $a_{out_{min}}$ et $a_{out_{max}}$ (par extension, $x_{acc_{min}}$ et $x_{acc_{max}}$ pour les positions minimales et maximales déduites calculées à partir de $a_{out_{min}}$ et $a_{out_{max}}$) en supposant que les valeurs de paramètres K, SF, b_a et n_a sont uniquement dans l'intervalle de confiance à 95 %. Par exemple, les valeurs pour le paramètre SF sont comprises entre $\mu_{SF} \pm 2 \cdot \sigma_{SF}$. Les valeurs minimales et maximales des paramètres K, SF, b_a et n_a permettent de

déterminer $x_{acc_{min}}$ et $x_{acc_{max}}$ valeurs utilisées dans le modèle probabiliste de la sous-section suivante.

État en présence de panne Nous considérons comme "panne" sur le capteur le fait que celui-ci ne nous fournit pas de mesures. Cette panne génère une dégradation sur le signal de sortie qui est un écart de mesure plus important que dans le cas nominal et qui augmente dans le temps. Cet écart peut être acceptable (état dégradé mais acceptable "DA") ou inacceptable (état inacceptable "I") selon les exigences décrites par la suite. Dès lors que le capteur ne fournit pas de mesure, la dernière mesure connue est utilisée. Nous considérons également l'accéléromètre comme un composant ayant un taux de panne beaucoup plus élevé que ce que l'on peut trouver dans les bases de données de fiabilité classiques pour les composants non-électroniques tels que les *Non Electronic Parts Reliability Data* [Reliability Analysis Center, 1995]. En effet, dans cette base de données, nous trouvons un taux de pannes de $2{,}48\times10^{-6}\ h^{-1}$ pour un accéléromètre classique. Ces remarques sont valables pour les autres capteurs présentés plus bas. En augmentant le taux de panne, ceci permet d'ajouter arbitrairement les phénomènes de glissement et de patinage (pour les capteurs proprioceptifs) aux taux de pannes considérés dans les bases de données de fiabilité. La durée jusqu'à la panne est une variable aléatoire notée T qui suit une loi exponentielle de paramètre λ_{acc} (cf équation 2.19).

$$T \sim exp(\lambda_{acc}) \tag{2.19}$$

avec, T durée jusqu'à la panne et $\lambda_{acc} = 10^{-3}\ s^{-1}$ sachant que l'accéléromètre est en fonctionnement normal à $t = 0$. Les pannes introduites dans la simulation de l'accéléromètre sont des pannes transitoires dont la durée est fixée arbitrairement à 10 secondes. Cette remarque est identique pour la simulation de l'odomètre et du récepteur GPS.

2.4.3.1.3 Odomètre

État nominal Dans un référentiel cartésien (x, y), nous définissons R, n, α respectivement le rayon de la roue (0,5 mètre) sur laquelle est fixé l'odomètre, le nombre d'impulsions fournies par l'encodeur pendant un intervalle de temps Δ_t et la résolution de cet odomètre α fixée à 0,2. La distance parcourue Δd est alors donnée par l'équation 2.20. À l'image de l'accéléromètre, l'odomètre est sujet à un bruit blanc Gaussien n_o et un biais b_o (c'est à dire un glissement considéré par un nombre incorrect d'impulsions fournies par l'encodeur). Ces deux paramètres sont déterminés de la même manière que les équations 2.17 et 2.18 en remplaçant μ_{b_a}, σ_{b_a} et σ_{n_a} par $\mu_{b_o} = 0$, $\sigma_{b_o} = 0{,}5$ et $\sigma_{n_o} = 0{,}001$ mètre (sachant que b_o est exprimé en nombre d'impulsions, nous arrondissons à l'entier supérieur).

$$\Delta d = R \cdot (n + b_o) \cdot \alpha + n_o \tag{2.20}$$

Pour la fusion, la position à l'instant $t+1$ est déduite de la distance parcourue Δd par l'équation 2.21 :

$$x_{odo_{t+1}} = x_t + \Delta d_t \cdot cos(\theta_t + \frac{\Delta\theta_t}{2}) \tag{2.21}$$

La trajectoire est considérée comme rectiligne (donc $\theta_t = 0$).

De la même manière que pour l'accéléromètre, nous générons en plus d'une mesure de position (x_{odo}) une mesure $x_{odo_{min}}$ et $x_{odo_{max}}$ grâce aux valeurs minimales et maximales des paramètres b_o et n_o *i.e.* dans un intervalle de confiance à 95 % à l'exception de α et R qui restent constants.

État en présence de panne L'état en présence de panne est déterminé de la même manière que l'accéléromètre en considérant un T avec un $\lambda_o = 10^{-3}\ s^{-1}$.

2.4.3.1.4 Récepteur GPS

État nominal La position (x, y, z) estimée par GPS est déterminée par résolution d'un système d'équations à 4 inconnues qui sont les 3 composantes spatiales et la composante temporelle. Cependant, dans un contexte ferroviaire, deux satellites peuvent suffire avec l'utilisation d'équations représentant le tracé de la voie [Nikiforov and Choquette, 2003]. Pour le moment, nous considérons que le train est sur sa voie et que la position peut être définie uniquement par sa composante longitudinale soit x (contexte 1D) (cf équation 2.22) :

$$x_{gps} = x_{true} + n_{gps} \tag{2.22}$$

avec x_{true}, la position réelle et n_{gps}, l'erreur sur la position fournie par le récepteur. Les valeurs de n_{gps} sont déterminées de manière aléatoire et uniforme à partir de l'intervalle $[-10; +10]$ qui fait un intervalle de longueur 20 mètres, valeur de l'exigence trouvée dans [Barbu, 2000]. L'hypothèse sur les bruits dans la modélisation du récepteur GPS (loi uniforme) sera levée au chapitre 3 et discutée dans le chapitre 4.

De la même manière que pour les capteurs précédents, nous générons en plus d'une mesure de position (x_{gps}), une mesure $x_{gps_{min}}$ et $x_{gps_{max}}$ grâce aux valeurs maximales et minimales de l'intervalle ci-dessus.

État en présence de panne L'état en présence de panne est déterminé de la même manière que l'accéléromètre en considérant un T avec un $\lambda_{gps} = 10^{-3}\ s^{-1}$ afin d'ajouter arbitrairement les phénomènes de masquage (signaux GPS bloqués par l'environnement). De plus, nous y avons introduit des phénomènes de multitrajets. Ces phénomènes sont simulés simplement par l'ajout d'un biais supplémentaire d'amplitude aberrante, constant sur plusieurs centaines de mètres et sur des plages de temps choisies arbitrairement sur les mesures du récepteurs GPS.

Dans le cadre de l'analyse causale, nous proposons de détailler davantage les états des capteurs en introduisant les notions d'états nominal, dégradé mais acceptable et inacceptable.

2.4.3.2 Modèle probabiliste simplifié d'un système multicapteurs

Afin de décrire le modèle probabiliste associé à une architecture générique, il est nécessaire de bien définir l'état nominal et l'état de panne d'un système avec GNSS à travers un modèle probabiliste. Pour l'établir de manière formelle, il nous faut définir [Bérard, 2001] :

— un ensemble noté Ω représentant toutes les situations possibles,
— une application notée $P : \Omega \to [0, 1]$, appelée probabilité sur Ω vérifiant la condition $\sum_{w \subset \Omega} P(w) = 1$ où les éléments w sont des sous-ensembles de Ω.

Pour construire l'ensemble Ω, il est nécessaire de savoir quand la sortie du système est dans un état "N", "DA" ou "I". Considérons que l'écart entre la sortie mesurée du système multicapteur et la réalité est représentée par l'intervalle $[\underline{S}; \overline{S}]$. Les écarts entre les mesures fournies par les capteurs

et la réalité sont représentées par les intervalles $[\underline{M_i}; \overline{M_i}]$ (équation 2.23).

$$[\underline{S}; \overline{S}] = [f(\underline{M_1}, ..., \underline{M_i}); f(\overline{M_1}, ..., \overline{M_i})] \tag{2.23}$$

Avec,
$\underline{M_1}, ..., \underline{M_i}$ et $\overline{M_1}, ..., \overline{M_i}$, respectivement les bornes inférieures et supérieures des écarts avec la réalité des mesures des capteurs $1, ..., i$ simulées,
f, la fonction qui relie les mesures des capteurs à la sortie du système multicapteur. f représente alors la technique de fusion ou de filtrage utilisée.

Pour différencier les états "N", "DA" ou "I", il faut définir deux seuils semblables à ceux utilisés pour séparer des niveaux de précision GNSS [Lu and Schnieder, 2015]. Soit β, l'écart en valeur absolue (cf équation 2.9) désignant l'erreur de position (fixé à 2,5 mètres) et la variable $AlertLimit$, le maximum d'erreur permise sur la position mesurée (cf. [Barbu, 2000]) (fixée à 20 mètres dans [Lu and Schnieder, 2015]). Sachant $\beta < AlertLimit$, la sortie du système est considérée comme :

— *Nominale (état "N_{sys}")* **si** $[\underline{S}; \overline{S}] \subset]0; \beta]$
— *Dégradée mais Acceptable (état "DA_{sys}")* **si** $[\underline{S}; \overline{S}] \subset]\beta; AlertLimit]$ **où** $\beta \leq \frac{\underline{S}+\overline{S}}{2}$
— *Inacceptable (état "I_{sys}")* **si** $[\underline{S}; \overline{S}] \subset]AlertLimit; +\infty[$ **où** $AlertLimit \leq \frac{\underline{S}+\overline{S}}{2}$

La sortie des capteurs est considérée de la même manière c'est à dire :

— *Nominale (état "N_{C_i}")* **si** $[\underline{M_i}; \overline{M_i}] \subset]0; \beta]$
— *Dégradée mais Acceptable (état "DA_{C_i}")* **si** $[\underline{M_i}; \overline{M_i}] \subset]\beta; AlertLimit]$ **où** $\beta \leq \frac{M_i+\overline{M_i}}{2}$
— *Inacceptable (état "I_{C_i}")* **si** $[\underline{M_i}; \overline{M_i}] \subset]AlertLimit; +\infty[$ **où** $AlertLimit \leq \frac{M_i+\overline{M_i}}{2}$

En absence de valeur de référence pour β, nous l'avons fixé arbitrairement à 2,5 mètres. Il faut vérifier qu'à l'état nominal des capteurs (absence de panne) la valeur maximale des sorties des capteurs ($x_{acc_{max}}$, $x_{odo_{max}}$ et $x_{gps_{max}}$) reste en dessous de β. Dans le cas contraire, β doit être réévalué.

Ces états sont illustrés par la figure 2.12. Elle montre notamment comment sont gérées les situations où les intervalles $[\underline{M_i}; \overline{M_i}]$ et $[\underline{S}; \overline{S}]$ sont à cheval entre deux états possibles. Si plus de la moitié de l'intervalle est dans un état, le système ou le capteur est considéré dans cet état. La figure 2.12 représente différents cas possibles d'intervalles associés à une entité donnée.

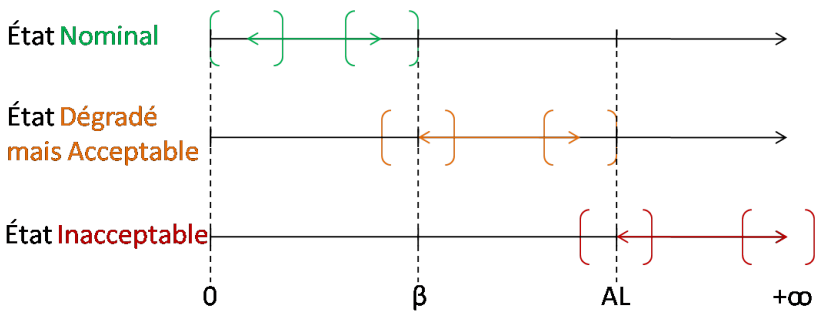


FIGURE 2.12 – États possibles d'un système multicapteurs.

Il faut noter que le système dont la sortie est dans un état "I" devra basculer dans un mode de sécurité *i.e.* le train devra s'arrêter. L'arrêt est l'état du train dans lequel la sécurité est privilégiée quitte à sacrifier la disponibilité.

Maintenant que les états "N", "DA" et "I" sont bien définis, nous pouvons construire l'ensemble Ω que l'on notera par la suite Ω_{sys}. La taille de cet ensemble, *i.e.* le nombre de combinaisons d'états possibles pour le système, est déterminée par l'équation 2.24.

$$card(\Omega_{sys}) = card(\Omega_{N_{sys}}) + card(\Omega_{DA_{sys}}) + card(\Omega_{I_{sys}}) \tag{2.24}$$

avec, $card(\Omega_{N_{sys}})$ est le nombre de combinaison d'états menant à N_{sys} (idem pour $card(\Omega_{DA_{sys}})$ et $card(\Omega_{I_{sys}})$).

Nous rappelons que l'objectif est d'identifier les scénarios risqués c'est à dire identifier tous les scénarios menant à l'évènement risqué "I_{sys}". L'écart entre la position réelle (connue) et la position estimée (mesurée par les capteurs) est inacceptable. Pour évaluer "I_{sys}", nous fixons un risque acceptable d'erreur de position noté pr à 1×10^{-6} par heure (ordre de grandeur du risque d'intégrité utilisé dans la section 4.2.4 du chapitre 3). Ainsi, il y a défaillance de positionnement si le risque acceptable pr est dépassé [Tartakovsky et al., 2014] (équation 2.25).

$$(1 - p_f) \cdot P_\infty(I_{sys}) + p_f \cdot P(I_{sys}) > pr \tag{2.25}$$

Où, p_f est la probabilité qu'une panne de capteur se produise par unité de temps,
$P_\infty(I_{sys})$ est la probabilité que le système soit dans un état inacceptable sachant qu'il n'y a pas de panne au niveau capteur (plusieurs petites erreurs qui se combinent),
$P(I_{sys})$ est la probabilité que le système soit dans un état inacceptable sachant la présence de panne au niveau capteur.

L'analyse causale déterminera empiriquement les probabilités $P_\infty(I_{sys})$ et $P(I_{sys})$ selon l'occurrence de l'évènement I_{sys} par l'équation 2.26.

$$P(I_{sys}) = \frac{card(I_{sys})}{card(\Omega_{sys})} \tag{2.26}$$

La probabilité $P(I_{sys})$ sera estimée après avoir ajusté la distribution des écarts de position fournis par le système par une loi de probabilité connue (loi normale). Sachant la valeur de *AlertLimit*, on peut déterminer $P(I_{sys})$. Ceci est illustré par la figure 2.13 pour l'architecture 1 avec, à gauche, la distribution des écarts de position sous la forme d'un histogramme et, à droite, la densité de probabilité.

Les expressions des probabilités $P_\infty(I_{sys})$ et $P(I_{sys})$ ne seront pas identiques d'une architecture à l'autre (différents capteurs mis en jeu ou fusion/filtrage différent).

2.4.3.3 Identification des combinaisons à risque

Lors des simulations des architectures, les combinaisons d'état de capteurs se succèdent à chaque instant. La situation où une même combinaison d'état apparait plusieurs fois durant une période donnée est possible. Durant cette période l'état de la sortie du système peut changer de DA à I.

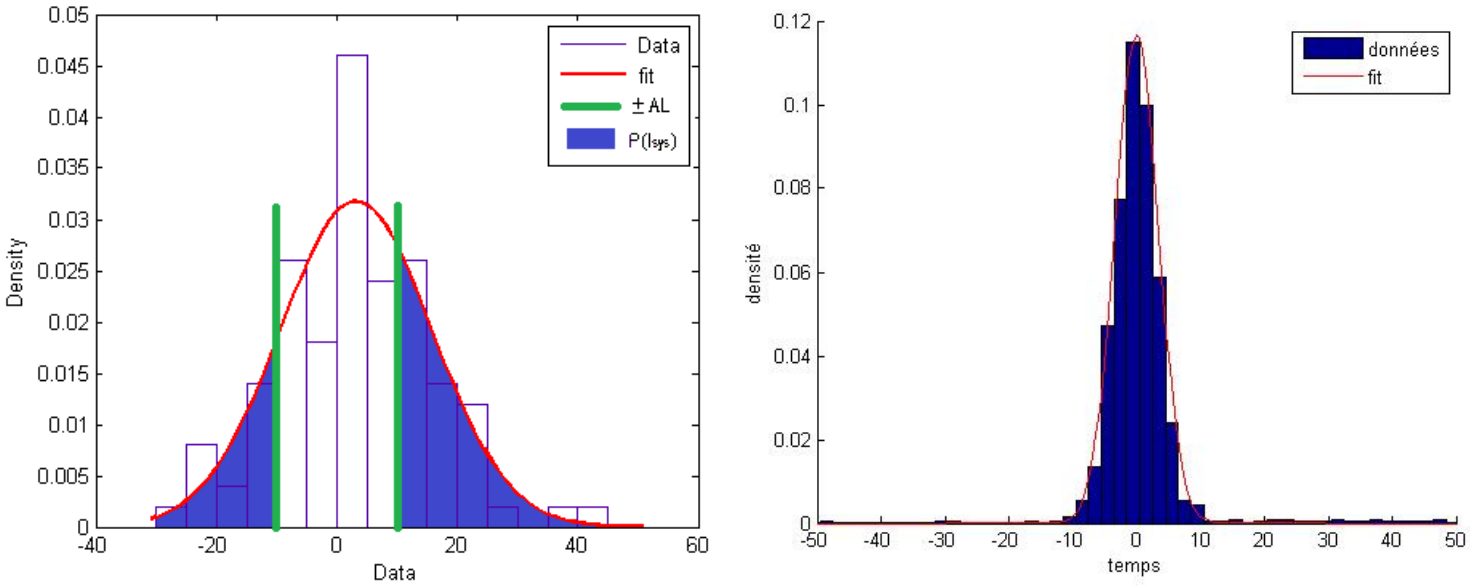


FIGURE 2.13 – Distribution et densité de probabilité des écarts de position fournis par le système (architecture 1) ajustée par une loi normale

Dans ce cas, la persistance dans le temps de ce genre de combinaison peut être étudiée. En effet, pour une même combinaison d'état et au-delà d'une période (notée t_c pour temps "critique"), l'état de la sortie du système peut changer. Ces combinaisons sont appelés "combinaisons d'état critiques" et sont à différencier des combinaisons d'états inacceptables. Pour cette analyse, une fenêtre de 10 secondes nous suffit pour comparer les architectures même si un t_c peut avoir une valeur plus élevée.

Tableau 2.5 – Explication de la persistance.

	Ét(C1)	Ét(C2)	Ét(C3)	Ét(Sys)
	I	DA	DA	DA
	I	DA	DA	DA
	I	DA	DA	I

Temps

Le tableau 2.5 montre un exemple d'enchainement de combinaisons d'état de 3 capteurs notés C1, C2 et C3. La combinaison "(I,DA,DA)" persiste 2 secondes après que celle-ci ait fait passer l'état de la sortie du système de "DA" à "I". L'occurrence de ces combinaisons à risque doit être prise en compte pour l'estimation de $P(I_{sys})$.

Par la suite, une autre approche est abordée pour analyser l'impact des erreurs au niveau des différents capteurs. Le but est de déterminer la qualité de la position en fonction des besoins utilisateurs (incertitude, précision, *etc.*.) ou en phase de conception (choix des capteurs qui contribuent le moins aux erreurs au niveau système multicapteurs).

2.4.4 Approche pour l'analyse de la sensibilité des erreurs de données unitaires sur les données fusionnées

2.4.4.1 Concepts liés à l'analyse de la sensibilité

Une *analyse de sensibilité* consiste à étudier et à quantifier les effets des variations des entrées sur les sorties d'un système. Cette analyse est centrée sur les paramètres spécifiques du système, plus précisément sur des caractéristiques des composants dont les variations affectent le comportement du système. Le but principal est l'étude des conséquences de l'incertitude sur les paramètres du système dans son ensemble. Dans l'analyse de sensibilité, il existe 2 approches [Saltelli et al., 2004] :

— Approche qualitative. Un classement est effectué entre différents paramètres intrinsèques et extrinsèques d'un système et leurs effets sur ses sorties. L'objectif est d'identifier rapidement l'entrée dont l'influence sur les sorties est la plus forte (Méthode de Morris [Campolongo et al., 2003]).

— Approche quantitative qui se décline en deux catégories :

  — une méthode locale : le système est approximé par un modèle mathématique et une dérivée partielle pour chaque paramètre est calculée. Plus l'amplitude de la dérivée d'un paramètre donné est élevée plus le paramètre est influent et *vice versa*.

  — une méthode globale : chaque paramètre est décrit par une distribution de probabilité obtenue en utilisant des observations ou des avis d'experts. Les entrées varient suivant leur distribution de probabilité et l'amplitude de la dérivée partielle est calculée.

Les méthodes quantitatives sont privilégiées car elles apportent des informations non-ambigües sur les sensibilités notamment leur amplitude. Nous adopterons ce principe.

2.4.4.2 Mesure de la sensibilité

Une mesure de sensibilité est une valeur (ou un ensemble de valeurs) quantifiant l'influence d'un paramètre. Elle représente comment des perturbations sur cette variable peuvent avoir une influence sur une sortie autour d'un point de fonctionnement. Soit le modèle d'un système physique défini par l'équation 2.27 :

$$y = f(par_1, ..., par_j) = f(Par) \tag{2.27}$$

où, y est la sortie du modèle et Par est le vecteur des paramètres $par_{1,...,j}$ du modèle de taille j.

La sensibilité d'un paramètre par_j sur la sortie peut être calculée comme suivant l'équation 2.28 :

$$\frac{\partial f(Par)}{\partial par_j} \tag{2.28}$$

où, $\frac{\partial f(Par)}{\partial par_j}$ est la dérivée partielle de $f(Par)$ par rapport à par_j.

Une précaution est ici nécessaire : les différentes variables ne sont pas exprimées dans les mêmes grandeurs. Par conséquent, il faut normaliser les mesures de sensibilité autour du point de fonctionnement. Cette mesure normalisée est donnée par l'équation 2.29 :

$$\frac{par_j^0}{f(Par_0)} \cdot \frac{\partial f(Par)}{\partial par_j} \tag{2.29}$$

où, Par_0 est un vecteur contenant la valeur initiale des paramètres $par_{1..j}^0$ des composants du système, $f(Par_0)$ est la sortie du modèle avec comme entrée le vecteur Par_0.

Dans la pratique, f est une fonction non-linéaire mais elle peut être linéarisée grâce au théorème de Taylor rappelé par l'équation 2.30.

$$f(Par) = f(Par_0) + \sum_{i=1}^{j} \frac{\partial f}{\partial par_i}(Par - Par_0) \tag{2.30}$$

où, $\frac{\partial f}{\partial par_i}$ est appelé sensibilité du premier ordre. Il faut noter que le terme $\frac{\partial f}{\partial par_i}(Par - Par_0)$ est divisé par 1! mais l'équation 2.30 est simplifiée (1! = 1). Cet ordre représente aussi le degré de connaissance du système modélisé. Plus cette expression a de termes, plus fine est la modélisation.

Pour chaque composant et pour chaque paramètre d'un modèle, une mesure de sensibilité est calculée et est représentée dans une matrice, proche d'une matrice Jacobienne, qui sera appelée *matrice de sensibilité* $S_{meas}(y)$ (cf équation 2.31). Cette forme matricielle peut intervenir lors de la mise à jour de la matrice P sein d'un filtre de Kalman (cf sous-section 2.4.2 et annexe B).

$$\boldsymbol{S_{meas}(y)} = \begin{bmatrix} \frac{\partial \Delta y}{\partial par_{11}} & \cdot & \cdot & \frac{\partial \Delta y}{\partial par_{1j}} \\ \cdot & \cdot & & \cdot \\ \cdot & & \cdot & \cdot \\ \frac{\partial \Delta y}{\partial par_{i1}} & \cdot & \cdot & \cdot \frac{\partial \Delta y}{\partial par_{ij}} \end{bmatrix} \tag{2.31}$$

où, Δy représente la différence entre la sortie du système et la réalité (en ayant connaissance de la valeur réelle), par_{ij} est la valeur du paramètre j du composant i.

Dans la sous-section 2.4.5, nous avons choisi un nombre limité de paramètres internes. Dans la pratique, il existe des paramètres intrinsèques mais aussi extrinsèques qui peuvent affecter la sortie des modèles tels que la température ambiante. Par conséquent, plus le nombre de paramètres considérés augmente, plus la matrice de sensibilité sera grande rendant son calcul lourd.

La théorie autour des analyses causales et de sensibilité a été donnée. Il s'agit maintenant d'appliquer cette théorie sur des exemples d'architectures de capteurs avec récepteur GPS.

2.4.5 Applications de l'analyse de causale et de l'analyse de sensibilité sur quelques architectures de systèmes fondés sur les GNSS

2.4.5.1 Analyse causale sur différentes architectures choisies

L'analyse causale, comme présentée ci-dessus, a été appliquée sur plusieurs architectures de capteurs inspirées de projets d'intégration des GNSS dans un système de contrôle-commande ferroviaire

(cf chapitre 1).

2.4.5.1.1 Architecture 1 : Accéléromètre + Odomètre + récepteur GPS + fusion par moyenne pondérée

L'architecture de base considérée ici est présentée figure 2.14. Elle est composée d'un accéléromètre, d'un odomètre et d'un récepteur GPS dont la modélisation est présentée dans la sous-section 2.4.3.1. Le bloc T représente la transformation du déplacement réel du train $depl_{rel}$ en nombre d'impulsions n. En pratique, T est l'encodeur de l'odomètre (cf sous-section 1.2.2.1 du chapitre 1). Les positions déduites de ces capteurs sont fusionnées par moyenne pondérée (cf équation 2.32).

$$x_f = poids_{x_{acc}} \cdot x_{acc} + poids_{x_{odo}} \cdot x_{odo} + poids_{x_{gps}} \cdot x_{gps} \tag{2.32}$$

avec,
x_f, la position fusionnée en sortie du système,
$poids_{acc}$, le poids associé à la position déduite de la mesure de l'accéléromètre $poids_{acc} = \frac{\sigma_{acc}^{-2}}{(\sigma_{acc}^{-2}+\sigma_{odo}^{-2}+\sigma_{gps}^{-2})}$,
$poids_{odo}$, le poids associé à la position mesurée par l'odomètre $poids_{odo} = \frac{\sigma_{odo}^{-2}}{(\sigma_{acc}^{-2}+\sigma_{odo}^{-2}+\sigma_{gps}^{-2})}$,
$poids_{gps}$, le poids associé à la position mesurée par le récepteur GPS $poids_{gps} = \frac{\sigma_{gps}^{-2}}{\sigma_{acc}^{-2}+\sigma_{odo}^{-2}+\sigma_{gps}^{-2}}$.

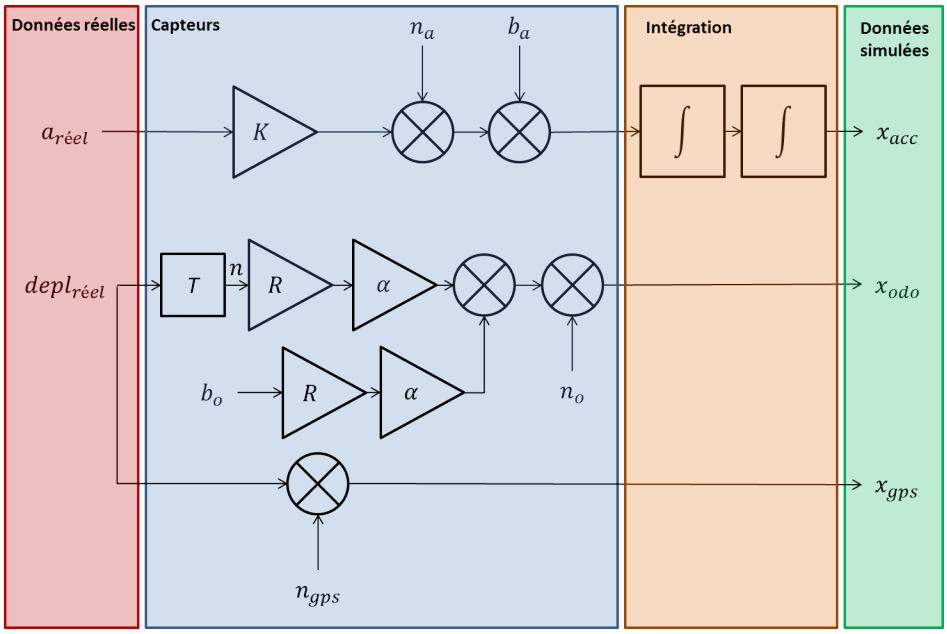


FIGURE 2.14 – Architecture 1.

Tableau 2.6 – Nombre de combinaisons N, DA et I pour l'architecture 1.

État	Sans panne sur capteurs	Avec pannes sur capteurs
N	5 615	4 962
DA	1 385	1 475
I	0	563

Le tableau 2.6 recense le nombre de combinaison d'état du système N, DA et I sans et avec panne sur les capteurs. On rappelle que les pannes sont générées de manière aléatoire suivant une loi exponentielle de paramètre λ donné dans la sous-section 2.4.3.1. D'après le tableau 2.6, on remarque que la présence de panne affecte les performances du système par le biais d'un nombre important (563) d'états inacceptables. Sans panne, la sortie du système reste dans un état nominal (80 % du temps) ou dégradé mais acceptable (les 20 % restants).

Pour estimer la probabilité de $P_\infty(I_{Sys})$ et $P(I_{Sys})$, nous comptabilisons respectivement le nombre de combinaisons d'état du système menant à un état inacceptable en l'absence de panne et en présence de panne. Étant donné que la simulation a une durée limitée (7000 secondes), nous exprimons des estimations de probabilités moyennes de $P_\infty(I_{Sys})$ et $P(I_{Sys})$ (cf tableau 2.7).

Tableau 2.7 – Probabilités moyennes de $P_\infty(I_{Sys})$ et $P(I_{Sys})$ pour l'architecture 1.

Probabilité moyenne	Résultat
$P_\infty(I_{Sys})$	0
$P(I_{Sys})$	$8{,}04 \times 10^{-2}$

La probabilité $P_\infty(I_{Sys})$ est nulle. La combinaison (N,N,$N \rightarrow I$) n'apparait jamais dans la simulation de cette architecture. Concrètement, cela signifie que lorsque l'accéléromètre, l'odomètre et le récepteur GPS sont dans l'état nominal, le système n'est jamais dans l'état Inacceptable. Il en va de même pour la combinaison (N,N,$N \rightarrow DA$). Par conséquent, le valeur du seuil β délimitant l'état nominal est correcte.

Pour l'estimation de la probabilité $P(I_{Sys})$, il s'agit du nombre de combinaison (x,x,$x \rightarrow I$). Reportée sur le nombre d'échantillons, l'estimation de la probabilité moyenne $P(I_{Sys})$ pour l'architecture 1 est de 8×10^{-2}.

En simulation, 158 combinaisons (cf tableau 2.9) ont été identifiées comme "critiques" c'est à dire que leur persistance dans le temps (après t_c seconde(s)) peut changer l'état de la sortie du système de "DA" à "I". Ces combinaisons ont des temps de persistance qui varient de 1 à 7 secondes. Une précaution doit être prise : pour les combinaisons les plus critiques (*i.e.* dont le temps t_c est faible ($t_c \leq 1$)), le pas de mesure doit être réglé de manière adéquate pour une plus grande précision (pas = 1 s => $t_c > 1$ s).

En plus des combinaisons menant directement à un état inacceptable I, les combinaisons critiques sont à surveiller. Par exemple, dans l'architecture 1, la combinaison d'états des capteurs (DA,DA,I) (c'est à dire l'odomètre et l'accéléromètre retournent une position jugée dégradée mais acceptable et le récepteur GPS, une sortie inacceptable) persiste après un temps t_c de 2 secondes (cf tableau 2.8). À la troisième seconde, l'état de la sortie passe de "DA" à "I".

2.4.5.1.2 Architecture 2 : Accéléromètre + 2 Odomètres + récepteur GPS

Ici, l'odomètre est dupliqué pour implémenter une redondance active. Les deux odomètres ont les mêmes caractéristiques (résolution, bruits, *etc.* (cf [Legrand et al., 2013])).

Tableau 2.8 – Extrait d'une succession de combinaisons d'état pour l'architecture 1 où la combinaison (DA,DA,I) apparaît comme "critique" avec un temps de persistance de 2 secondes (une ligne = 1 seconde). La fonction Ét(capteur) retourne l'état d'un capteur.

Ét(Odo)	Ét(Acc)	Ét(GPS)	Ét(Sys)
N	DA	DA	DA
N	DA	DA	DA
DA	DA	I	DA
DA	DA	I	DA
DA	DA	I	I

Temps

Tableau 2.9 – Combinaisons "critiques" pour l'architecture 1 (la fonction Ét(capteur) retourne l'état d'un capteur).

Format des combinaisons (Ét(Odo),Ét(Acc),Ét(GPS))	Temps de persistance t_c (en seconde)	Occurrences
(DA,DA,I)	1	24
(DA,N,I)	1 à 2	2
(I,N,I)	3 à 7	111
(DA,DA,I)	2	21

Tableau 2.10 – Nombre de combinaisons N, DA et I pour l'architecture 2.

État	Sans panne sur capteurs	Avec pannes sur capteurs
N	6045	5520
DA	955	1074
I	0	490

Tableau 2.11 – Probabilités moyennes de $P_\infty(I_{Sys})$ et $P_(I_{Sys})$ pour l'architecture 2.

Probabilité moyenne	Résultat
$P_\infty(I_{Sys})$	0
$P_{I_{Sys}}$	$7 \cdot 10^{-2}$

Le tableau 2.10 montre le nombre de combinaisons apparues lors de la simulation de l'architecture 2. Nous constatons qu'en l'absence de panne, les performances du système sont meilleures que la première architecture. En effet, il y a 6 045 états nominaux contre 5 615 pour l'architecture 1 (27 % de plus). De même, nous trouvons moins d'états dégradés mais acceptables (955 contre 1 385 soit 31 % de moins). En présence de panne, de meilleures performances y sont constatées notamment au vu du nombre de états inacceptables (490 contre 563 soit 13 % de moins). Ceci montre le gain apporté par la redondance d'un capteur. Les estimations des probabilités $P_\infty(I_{Sys})$ et $P(I_{Sys})$ pour l'architecture 2 sont données dans le tableau 2.11.

Cependant, nous trouvons plus de combinaisons critiques (290 contre 158 pour l'architecture 1)

à l'image de la combinaison (N,DA,DA,I) avec un temps de persistance allant de 1 à 10 secondes. Il apparait que la combinaison (DA,N,N,I) est une combinaison critique malgré le fait que les odomètres fournissent une position acceptable.

Tableau 2.12 – Extrait d'une succession de combinaisons d'état pour l'architecture 2 où la combinaison (N,DA,DA, I) est critique.

	Ét(Acc)	Ét(Odo)	Ét(Odo2)	Ét(GPS)	Ét(Sys)
	N	N	N	I	I
	N	DA	DA	I	DA
	N	DA	DA	I	DA
	N	DA	DA	I	I

Temps

Tableau 2.13 – Combinaisons "critiques" pour l'architecture 2.

Format des combinaisons (Ét(Acc),Ét(Odo),Ét(Odo2),Ét(GPS))	Temps de persistance t_c (en seconde)	Occurrence
(N,DA,DA,I)	1 à 10	42
(N,DA,N,I)	1	1
(DA,N,N,I)	1 à 10	205
(DA,DA,N,DA)	1 à 10	4
(DA,DA,DA,I)	1 à 10	38

2.4.5.1.3 Architecture 3 : Accéléromètres + Odomètre + Récepteur GPS associés à un filtre de Kalman (KF)

Dans cette architecture, la fusion par moyenne pondérée est remplacée par un filtre de Kalman. La modélisation des capteurs reste la même que les autres architectures. Une particularité est mise en place sur cette architecture. Dans les architectures 1 et 2, dès lors que le capteur ne fournit pas de mesure, la dernière mesure connue est utilisée. Ici, lorsqu'une panne sur l'odomètre apparait, c'est la dernière mesure connue du **récepteur GPS** qui est utilisée.

Tableau 2.14 – Nombre de combinaisons N, DA et I pour l'architecture 3.

État	Sans panne sur capteurs	Avec pannes sur capteurs
N	5 913	5 320
DA	1 087	1 218
I	0	462

L'architecture 3 est légèrement moins performante que l'architecture 2 vis-à-vis des états nominaux et inacceptables en absence de panne. Toutefois, le tableau 2.14 indique que 462 états

inacceptables contre, respectivement, 563 et 490 pour les architectures 1 et 2 sont apparus au cours de la simulation de l'architecture 3.

Tableau 2.15 – Probabilités moyennes de $P_\infty(I_{Sys})$ et $P(I_{Sys})$ pour l'architecture 1 bis.

Probabilité moyenne	Résultat
$P_\infty(I_{Sys})$	0
$P_{I_{Sys}}$	$6{,}6 \times 10^{-2}$

Nous retrouvons toujours le même ordre de grandeur pour $P_{I_{Sys}}$ $(6.4 \cdot 10^{-2})$ et $P_\infty(I_{Sys})$ est toujours nulle (cf tableau 2.15).

Concernant les combinaisons d'état critiques, nous en trouvons 195 lors de la simulation de l'architecture 3 ce qui la place entre l'architecture 1 et 2.

Tableau 2.16 – Extrait d'une succession de combinaisons d'état pour l'architecture 3 où la combinaisons (DA,N,I) fait passer l'état du système de DA à I au bout d'une seconde.

	Ét(Odo)	Ét(Acc)	Ét(GPS)	Ét(Sys)
	N	DA	I	I
	DA	I	I	I
	DA	DA	I	I
	DA	N	I	DA
	DA	N	I	I

Temps

Tableau 2.17 – Combinaisons "critiques" pour l'architecture 3.

Format des combinaisons (Ét(Odo),Ét(Acc),Ét(GPS))	Temps de persistance t_c (en seconde)	Occurrence
(N,N,I)	1 à 9	19
(N,DA,I)	1 à 3	5
(DA,N,I)	1 à 9	158
(DA,DA,I)	1 à 9	13

Dans cette architecture, les combinaisons critiques sont celles où l'état du récepteur GPS est "I". Par conséquent, cela concerne les combinaisons (ϕ,ϕ,I) où $\phi = \{N,DA,I\}$. En effet, si le réajustement est fortement dégradé, l'étape de mise à jour du filtre de Kalman sera biaisée. Le temps t_c est de 1 à 3 secondes selon l'importance de la dégradation.

En conclusion, cette architecture est très dépendante des performances du récepteur GPS. Dans la réalité, les dégradations des signaux GPS (vues dans le chapitre 1) sont liées à la configuration de l'environnement traversé par le train comme une zone urbaine ou boisée [Marais et al., 2000].

2.4.5.1.4 Architecture 4 : 3 Accéléromètres + 2 Odomètres + récepteur GPS + fusion par moyenne pondérée

L'architecture 2 a proposé une redondance en ajoutant un deuxième odomètre. L'architecture 4 va plus loin en proposant d'ajouter 2 accéléromètres toujours suivant la même modélisation.

Tableau 2.18 – Nombre de combinaisons N, DA et I pour l'architecture 4.

État	Sans panne sur capteurs	Avec pannes sur capteurs
N	5576	5383
DA	1424	1243
I	0	374

Tableau 2.19 – Probabilités moyennes de $P_\infty(I_{Sys})$ et $P(I_{Sys})$ pour l'architecture 2.

Probabilité moyenne	Résultat
$P_\infty(I_{Sys})$	0
$P_{I_{Sys}}$	$5{,}34 \cdot 10^{-2}$

Avec 374 états inacceptables, l'architecture 4 est meilleure que les autres sur cet aspect. $P_{I_{Sys}}$ est, par conséquent, le plus bas parmi les 4 architectures. Le nombre de combinaisons critiques est important (297), le plus important de toutes les architectures simulées.

Tableau 2.20 – Extrait d'une succession de combinaisons d'état pour l'architecture 4 où la combinaison (DA,DA,N,DA,DA,I) est critique.

	Ét(Acc1)	Ét(Acc2)	Ét(Acc3)	Ét(Odo1)	Ét(Odo2)	Ét(GPS)	Ét(Sys)
	N	N	N	N	N	DA	N
	N	N	N	DA	DA	I	DA
	DA	DA	N	DA	DA	I	DA
	DA	DA	N	DA	DA	I	I

Temps

Les tableaux 2.20 et 2.21 recensent les combinaisons d'états critiques pour l'architecture 4. Nous remarquons que les combinaisons critiques suggérant le moins de dégradation sur les capteurs comme la combinaison (N,N,N,N,N,I) ont un taux d'occurrence élevé (76 fois pour la combinaison prise en exemple).

2.4.5.2 Conclusions sur les architectures

L'analyse causale réalisée ici met en évidence des indicateurs qui nous renseignent sur les performances des architectures considérées.

Le premier est le nombre de combinaisons d'état inacceptable en absence ou en présence de panne sur les capteurs. Il faut préciser ici que l'état de la sortie du système ne peut être que dans un seul

Tableau 2.21 – Combinaisons critiques pour l'architectures 4.

Format des combinaisons (Ét(Acc1),Ét(Acc2),Ét(Acc3), Ét(Odo1),Ét(Odo2),Ét(GPS))	Temps de persistance t_c (en seconde)	Occurrences
(N,N,N,N,N,I)	1 à 9	76
(N,N,N,N,DA,DA)	1 à 4	5
(DA,DA,I,N,N,DA)	1 à 9	117
(DA,DA,N,DA,N,I)	1 à 7	2
(DA,DA,N,DA,DA,I)	1 à 8	22
(DA,DA,DA,N,N,I)	1 à 6	62
(DA,DA,DA,DA,N,I)	1 à 9	5
(DA,DA,DA,DA,DA,DA)	1 à 9	8

état à la fois. Il faut aussi préciser qu'une même combinaison d'états de capteur peut se retrouver dans des ensembles d'états de système différents. Ceci se traduit par l'équation 2.33.

$$\Omega_{N_{sys}} \cap \Omega_{DA_{sys}} \; ET \; \Omega_{N_{sys}} \cap \Omega_{I_{sys}} \; ET \; \Omega_{DA_{sys}} \cap \Omega_{I_{sys}} \neq \emptyset \tag{2.33}$$

Le nombre de combinaisons d'état inacceptable nous a permis d'estimer les probabilités $P_\infty(I_{Sys})$ et $P(I_{Sys})$. Pour toutes les architectures, $P_\infty(I_{Sys})$ s'est avérée être nulle. En effet, dans le modèle probabiliste présenté dans la sous-section 2.4.3.2, nous avons fixé arbitrairement un β à 2.5 mètres. Pour rappel, ce seuil délimite l'état nominal d'un capteur (la même valeur est prise pour délimiter l'état nominal du système complet). Si, lors des simulations des architectures, une combinaison d'état (N,N,N) avait donné I à la sortie du système multicapteurs, le seuil β aurait été sous-évalué.

Du fait que $P_\infty(I_{Sys}) = 0$, l'équation 2.25 devient alors :

$$p_f \cdot P(I_{Sys}) > pr \tag{2.34}$$

Le tableau 2.22 rappelle les estimations de la probabilité moyenne $P(I_{Sys})$ pour chaque architecture. Il indique également l'estimation de la probabilité p_f, calculée grâce au nombre de pannes apparues lors des simulations des architectures. Nous rappelons que $P(I_{Sys})$ est donnée sur un intervalle de temps équivalent au temps de simulation soit 7000 secondes. Celui doit être ramené sur une heure pour la comparaison avec la probabilité de risque acceptable pr (fixée à $1 \cdot 10^{-6}\ h^{-1}$).

Le produit $p_f \cdot P(I_{Sys})$ est supérieur au pr fixé pour les quatre architectures. Avec cette valeur de pr, les systèmes ne satisfont pas cette exigence. Plusieurs enseignements peuvent être tirés de ces conclusions :

— La modélisation des capteurs choisie ne tient pas compte de certains paramètres extérieurs comme la température qui ont une influence sur la sortie de celui-ci. Une analyse de sensibilité comme proposée dans ce chapitre montre l'influence de paramètres sur les performances des capteurs.

— Les pannes sont générées de manière aléatoire suivant une loi exponentielle. D'autres lois peuvent se montrer plus adaptées à modéliser le comportement d'un capteur en présence de

Tableau 2.22 – Application numérique du modèle probabiliste pour les architectures considérées (t_{simu} = 7000 secondes).

Architecture	Période	$P(I_{Sys})$	p_f	Produit	Risque acceptable ?
Architecture 1 : Accéléromètre, Odomètre et Récepteur GPS en fusion pondérée	sur t_{simu}	$4 \cdot 10^{-2}$	$8 \cdot 10^{-2}$	$3{,}2 \cdot 10^{-3}$	Non
	sur 1 h	$2{,}06 \cdot 10^{-2}$	$4{,}11 \cdot 10^{-2}$	$8{,}47 \cdot 10^{-4}$	
Architecture 2 : Accéléromètre, 2 Odomètres et Récepteur GPS en fusion pondérée	sur t_{simu}	$4{,}51 \cdot 10^{-2}$	$7 \cdot 10^{-2}$	$3{,}16 \cdot 10^{-3}$	Non
	sur 1 h	$2{,}32 \cdot 10^{-2}$	$3{,}6 \cdot 10^{-2}$	$8{,}35 \cdot 10^{-4}$	
Architecture 3 : Accéléromètre, Odomètre et Récepteur GPS et filtre de Kalman	sur t_{simu}	$5{,}14 \cdot 10^{-2}$	$6{,}6 \cdot 10^{-2}$	$3{,}39 \cdot 10^{-3}$	Non
	sur 1 h	$2{,}64 \cdot 10^{-2}$	$3{,}39 \cdot 10^{-2}$	$8{,}95 \cdot 10^{-4}$	
Architecture 4 : 3 Accéléromètres, 2 Odomètres et Récepteur GPS en fusion pondérée	sur t_{simu}	$6{,}54 \cdot 10^{-2}$	$5{,}3 \cdot 10^{-2}$	$3{,}47 \cdot 10^{-3}$	Non
	sur 1 h	$3{,}36 \cdot 10^{-2}$	$2{,}73 \cdot 10^{-2}$	$9{,}17 \cdot 10^{-4}$	

panne telles que la loi de Weibull (cf section 2.3). Côté récepteur GNSS, il est encore moins aisé de modéliser des pannes sur les signaux satellitaires étant donné qu'on ne peut pas les considérer comme un composant avec un taux de panne donné. [Viandier, 2011] suggère l'utilisation de modélisations par un processus de Dirichlet pour les erreurs de pseudodistances notamment.

— La durée de simulation est limitée à 7000 secondes et constitue un échantillon d'instant restreint. En effet, moins l'échantillon est grand, moins les estimations des probabilités (p_f et $P(I_{Sys})$ notamment) sont pertinentes. C'est la raison pour laquelle nous suggérons de concaténer plusieurs scénarios d'utilisation d'un système multicapteurs dans le chapitre 4 afin d'obtenir un nombre d'échantillons plus important.

Malgré ces résultats, $P(I_{Sys})$ reste un bon indicateur pour évaluer la sécurité de système multicapteur puisque cette probabilité se réfère à un évènement dangereux (une position inacceptable ici).

Le second indicateur est le nombre de combinaisons critiques. Une telle combinaison peut changer l'état de la sortie du système de DA à I au bout d'une certaine durée. Nous avons constaté qu'une architecture peut avoir un nombre de combinaisons d'états inacceptables faible (suggérant une architecture performante) sans pour autant avoir un nombre de combinaisons critiques faible. Ces deux paramètres ne sont donc pas corrélés. Les combinaisons critiques n'entrent pas dans le calcul d'une estimation de probabilité d'évènements dangereux mais elles doivent être à surveiller pour anticiper ces évènements dangereux.

Le troisième indicateur est le temps de persistance des combinaisons critiques. Cet indicateur

montre combien de temps le système continue de fournir une position correcte (mais dégradée) malgré l'état I d'un ou de plusieurs capteurs. Ce temps pourra quantifier un temps d'intervention pour réparer un capteur.

La sous-section suivante conclut la partie applicative de ce chapitre en réalisant une analyse de sensibilité sur l'architecture 1.

2.4.5.3 Analyse de sensibilité

À partir de ces modèles de capteurs, nous réalisons une étude de sensibilité présentée en sous-section 2.4.4. Les mesures de sensibilité sont donc déterminées par les dérivées partielles des paramètres sur la mesure en sortie du système. L'étude de sensibilité sur cet exemple de système avec GNSS montre les deux aspects suivants :

— l'influence déterminée quantitativement ou qualitativement des paramètres du système sur sa sortie. Des résultats sur l'architecture 1 (Accéléromètre + Odomètre + récepteur GPS + fusion par moyenne pondérée) montre que les paramètres les plus influents (ici, le gain de l'accéléromètre et la résolution de l'odomètre en bleu sur l'histogramme de la figure 2.15) sont ceux qui sont directement liés à la grandeur mesurée.

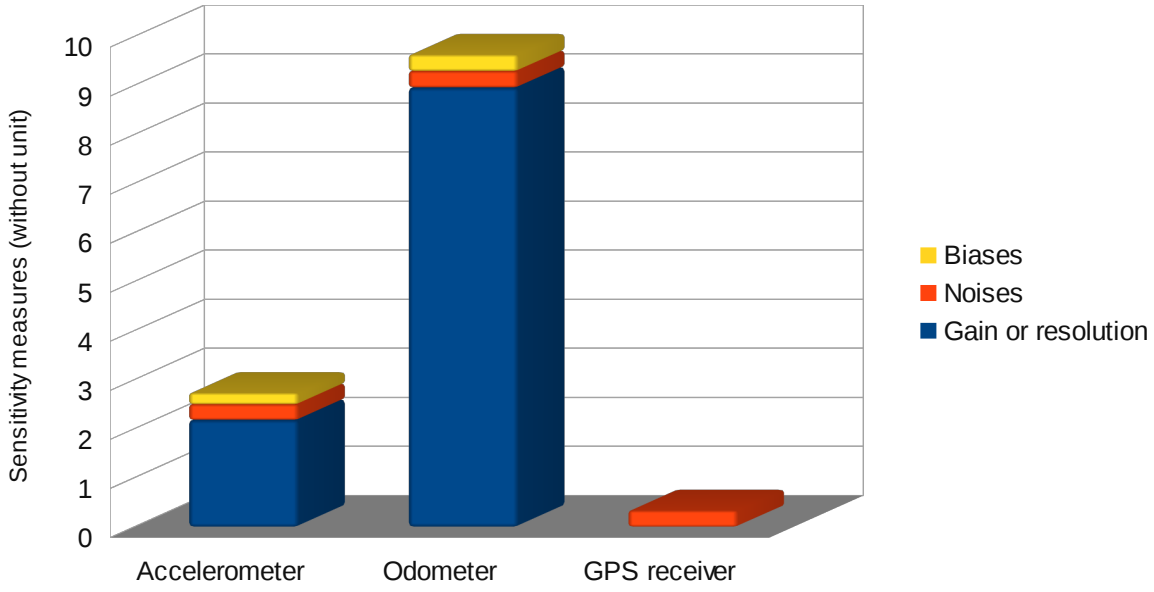


FIGURE 2.15 – Histogramme des sensibilités des paramètres pour une architecture (Accéléromètre + Odomètre + récepteur GPS).

— cette influence peut évoluer à l'occurrence d'une panne d'un des capteurs. La courbe suivante (cf figure 2.16) montre l'évolution de la sensibilité d'un des paramètres du capteur défaillant (ici, le paramètre n_{GPS} du récepteur GPS dont la précision est progressivement dégradée simulant les conséquences d'une faute). De plus, il est possible de déterminer une

valeur "critique", SM_{worst}, au delà de laquelle la position retournée par le récepteur devient inacceptable (faute considérée au niveau du récepteur). SM_{worst} devient alors un critère intéressant à mesurer dans le cadre de l'analyse des risques.

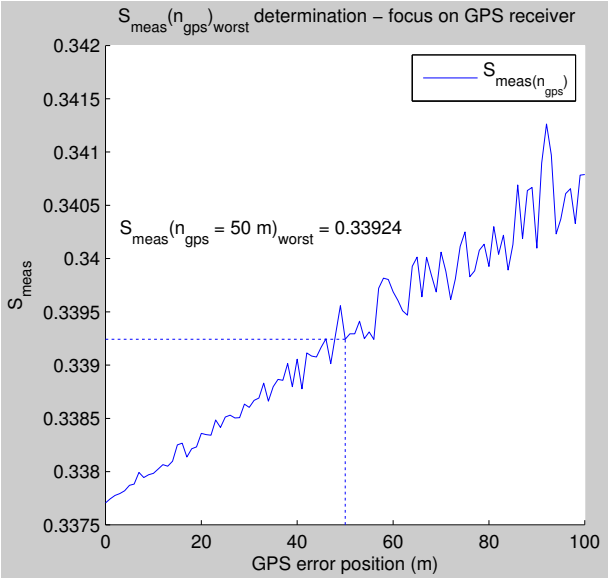


FIGURE 2.16 – Évolution de la sensibilité à l'occurrence d'une défaillance sur le récepteur GPS et détermination d'une valeur "critique" SM_{worst}.

2.5 Conclusions du chapitre

Les systèmes qui s'appuient sur le GNSS induisent des changements dits "significatifs" selon le règlement [Réglement 2015/1136, 2015] lors de leur intégration dans un système de contrôle-commande et de signalisation ferroviaire. En raison de l'innovation importante introduite par les GNSS, l'emploi du processus harmonisé de gestion des risques défini dans le domaine ferroviaire [Réglement 2015/1136, 2015] est primordial en vue d'apporter les justifications pour une future mise en service.

Après avoir rappelé les différents concepts, moyens et méthodes de la sûreté de fonctionnement, nous avons choisi d'appliquer une méthode prévisionnelle adaptée aux systèmes avec GNSS. Elle consiste en deux approches complémentaires.

La première approche vise à identifier les scénarios de risque sous la forme de combinaisons d'états des capteurs. Le nombre de combinaisons dites "critiques" et leur persistance temporelle sont de bons indicateurs dans le cadre d'une analyse explicite des risques, un des trois principes d'acceptation du risque du règlement EU/2015/1136. L'analyse causale vise à déterminer des indicateurs de performances à l'image de ceux proposés pour évaluer la sécurité des systèmes ferroviaires dans l'annexe C de la norme [EN 50126, 2000] (cf annexe A). L'application concrète de ces analyses est présentée en sous-section 2.4.5. L'analyse causale est ensuite réalisée sur 4 architectures de systèmes avec GNSS inspirées de projets d'intégration du GNSS dans le contrôle-commande ferroviaire (cf sous-section 1.4.3).

Dans une seconde approche, nous considérons qu'un système multicapteurs intègre des capteurs hétérogènes, avec des imperfections hétérogènes. Afin d'évaluer l'impact de ces imperfections sur la solution de localisation, nous avons mené une analyse de sensibilité. Cette approche fournit des mesures de sensibilité sur chaque paramètre des capteurs considérés. Un cas d'école utilisant une architecture simple a été proposé pour mettre en œuvre cette analyse. Ainsi, cette section a donné les fondations d'une méthode de conception sûre de systèmes de localisation.

Un des objectifs de cette thèse est de caractériser la confiance attribuée au système de localisation. Cette confiance peut être évaluée au moyen des indicateurs mis en évidence dans ce chapitre. Dans les normes aéronautiques [ICAO, 2006], où les critères de performances des GNSS sont clairement définis, le concept d'intégrité peut apporter les éléments de justification. Dans le chapitre suivant, nous proposons de présenter et d'adapter ce concept d'intégrité ainsi que ses mécanismes pour le domaine ferroviaire et pour des systèmes avec GNSS. Parmi ces mécanismes, nous trouvons le contrôle d'intégrité GNSS dont la première étape est la détection des pannes, aspect qui n'a pas été abordé dans ce chapitre. Cette détection est essentielle puisque elle constitue un moyen pour améliorer la sûreté de tout système. Il s'agit d'un solide argument pour s'intéresser à l'intégrité de la localisation basée sur les GNSS.

Chapitre 3

Contribution à l'évaluation de la sécurité des systèmes de localisation avec GNSS ferroviaires au travers de la formalisation du concept d'intégrité étendu

Sommaire

3.1 Introduction

Dans le chapitre précédent, nous avons montré que les procédures ferroviaires en matière de sécurité nécessitent l'évaluation des performances des systèmes GNSS. Nous avons cherché à quantifier la confiance qui peut être placée dans le service que délivre un système de type GNSS au travers d'indicateurs. Parmi les différentes méthodes utilisées, nous avons montré que la recherche de nouveaux indicateurs pour évaluer la sécurité des systèmes avec GNSS est nécessaire compte tenu du faible retour d'expérience de ces technologies et du changement significatif qu'elles occasionnent sur un système de contrôle-commande ferroviaire. En effet, l'intégration des GNSS dans un système de positionnement ferroviaire constitue une rupture technologique importante. Par conséquent, une démonstration de conformité aux exigences de sécurité ferroviaire est nécessaire. C'est pourquoi, nous avons proposé une analyse causale et une analyse de sensibilité. L'analyse causale a mis en évidence le nombre de combinaisons d'états inacceptables ou critiques et la persistance temporelle de ces combinaisons. Les mesures de sensibilité de paramètres de capteurs ont également été réalisées au cours d'une analyse de sensibilité.

Dans le domaine aéronautique (domaine d'origine des GNSS), d'autres types d'indicateurs existent. Dans la sous-section 1.5.2 du chapitre 1, nous avons vu que les normes aéronautiques utilisent des critères liés aux performances des GNSS : la précision, la disponibilité de service, la continuité de service et l'intégrité. L'intégrité retient notre attention puisqu'elle est liée à la sécurité des GNSS et notamment au fait d'alerter un utilisateur qu'une localisation n'est pas suffisamment sûre pour être utilisée. Dans ce troisième chapitre, nous traitons donc de la détermination de l'intégrité de systèmes avec GNSS dans un contexte ferroviaire.

Dans la première partie, les différentes notions d'intégrité seront synthétisées en partant de la définition générale jusqu'à celle choisie dans ce chapitre. Après ces précisions terminologiques, la notion d'intégrité initialement définie pour l'aéronautique et pour le GNSS sera développée, avec en particulier, les critères qui permettent de l'évaluer [ICAO, 2006]. Un effort d'adaptation pour le domaine ferroviaire est nécessaire. En effet, d'un point de vue sémantique, le concept d'intégrité est déjà utilisé dans ce domaine. En sécurité ferroviaire, on parle de niveau d'intégrité de sécurité, les SIL (*Safety Integrity Level*), abordés au chapitre 2 et de l'intégrité d'un convoi ferroviaire (le fait que le train reste entier) du matériel roulant tracté (rames/wagons/voitures) avec le matériel roulant moteur (locomotive, véhicules automoteurs). Ces deux aspects de l'intégrité peuvent générer des ambigüités. Puisque les problématiques ferroviaires liées à la localisation se distinguent de celles liées à l'aéronautique, les formulations des critères caractérisant l'intégrité diffèrent.

Dans la seconde partie, les mécanismes de contrôle de l'intégrité d'une solution de navigation embarquée seront présentés. Il s'agit d'algorithmes capables de détecter, d'isoler et/ou d'exclure des sources de localisation erronées au sein d'un système de navigation. Par la suite, ils déterminent si la solution de navigation (position, vitesse, accélération) est sûre. Incontournable dans le contrôle d'intégrité, le processus de détection repose sur le calcul de seuils liés à des erreurs données au sein du système. Ce calcul s'appuie sur des tests statistiques effectués sur les mesures à l'instant courant ou sur un historique de mesures fournies par l'ensemble des capteurs du système de localisation. Par conséquent, il s'agit d'un processus en temps réel qui, toutefois, requiert des données d'entrées prédéterminées. Ces données sont issues d'objectifs quantitatifs sur des erreurs maximales tolérables et de probabilités sur le risque d'intégrité venant de référentiels normatifs [ICAO, 2006] ou de groupes de travail [Barbu, 2000]. Dans un cadre d'applications liées à la sécurité, il est nécessaire de concevoir des systèmes de localisation tolérants aux pannes qui garantissent le compromis entre sécurité et

disponibilité. Par conséquent, l'architecture du système de navigation assurant ce compromis est une combinaison de plusieurs technologies de localisation associées à un récepteur GNSS (cf chapitre 1) puis, associées à un processus de diagnostic : le contrôle d'intégrité.

Dans un troisième temps, un algorithme de contrôle d'intégrité adapté à un système de localisation GNSS/INS est proposé pour tenir compte du fait que la partie inertielle est susceptible d'être en panne. Cette proposition permet de considérer également l'intégrité de la localisation fournie par cette partie de l'architecture et ainsi, de proposer une extension de la définition de l'intégrité englobant l'intégrité des systèmes autres que les GNSS.

La dernière contribution de ce chapitre établit le lien probabiliste entre ce critère d'intégrité étendue et la sécurité, attribut classique de SdF, pour répondre à la problématique de l'évaluation de la sécurité d'un système de localisation utilisant les GNSS. Un cas d'étude présenté dans le chapitre 4 permettra de discuter les résultats de cette évaluation au regard des objectifs de sécurité ferroviaires à atteindre.

3.2 Intégrité : de multiples définitions

Dans la norme [IEC 60050, 2015b] du Vocabulaire Électrotechnique International, l'intégrité se rapporte, pour un système technique, à un service (ex. un service de télécommunication) ou à une suite d'éléments numériques. L'intégrité d'une suite d'éléments numériques est définie par "la propriété d'une voie de transmission, d'un circuit de télécommunication ou d'une chaîne de connexion numérique, qui permet de transmettre un signal sans modification de la succession des éléments de signal". De manière plus concise, cela fait référence au fait qu'une information, un message ou une trame est reçu(e) sans altération. Cette définition doit être affinée pour les particularités du service concerné, ici le service de localisation. La section ci-dessous traite le cas de l'intégrité d'un service de localisation fourni par un GNSS. Il convient de prendre des précautions sur le terme "integrity" dans l'acronyme SIL (notion abordée dans le chapitre 2) qui n'a pas le même sens que l'intégrité traitée dans ce chapitre. Il s'agit d'une définition générale puisque l'intégrité d'une solution de navigation vise une fonction de sécurité spécifique : la localisation. La définition du SIL est liée à celle du taux d'occurrence maximal acceptable du danger ou THR (pour *Tolerable Hazard Rate*) [EN 50129, 2003]. Ce danger est généré par la défaillance de la fonction de localisation. En effet, la mesure d'un THR permet d'allouer un SIL pour des systèmes Électriques, Électroniques ou Électroniques programmables. Une probabilité de défaillance dangereuse par heure (PFH) est définie dans la norme générique de sécurité fonctionnelle [IEC 61508, 2010]. Cette norme présente également comment allouer un SIL avec la mesure de PFH. Cette probabilité sera préférée au THR ferroviaire. En effet, nous sommes confrontés ici à deux secteurs industriels différents : le secteur ferroviaire et le secteur aéronautique. Il est donc préférable de s'appuyer sur une norme générique telle que la norme [IEC 61508, 2010] et *a fortiori* sur l'estimation de PFH. Cette estimation est faite à la fin de ce chapitre.

3.3 Intégrité sur la localisation

La notion d'intégrité pour les GNSS a été définie par l'[ICAO, 2006] dans ses SARPs (*Standards and Recommended Practices*) comme étant "la mesure de la confiance qui peut être placée dans l'exactitude de l'information fournie par un système de navigation". Ce critère de performance est associé à un (ou plusieurs) processus de contrôle de l'intégrité qui inclut la capacité du système

à fournir en temps utile un avertissement à l'utilisateur quand le système ne doit pas être utilisé pour le fonctionnement prévu. Les exigences sur l'intégrité sont exprimées pour chaque opération (ou phase de mission) en terme de *niveaux d'alerte horizontaux et verticaux*, de *temps d'alerte* et de *risque sur l'intégrité*. Ce triplet d'exigences, exprimé par l'ICAO pour chaque phase de vol d'un aéronef, est défini en détail comme suit :

— Limite d'alerte

La limite (ou niveau) d'alerte horizontale ou verticale (HAL ou VAL) correspond à une erreur de position tolérable qui ne doit pas être dépassée sans émettre une alerte. Pour des applications terrestres, seul un niveau d'alerte horizontal est pertinent.

— Temps d'alerte

Le temps d'alerte (désigné par la variable TTA pour *Time To Alert*) est la deuxième exigence à formuler. Elle correspond au temps maximal autorisé, écoulé depuis que le système de navigation est hors des limites de tolérance jusqu'à ce que l'équipement énonce l'alerte. En d'autres termes, il s'agit d'un temps prescrit après l'apparition de l'évènement "l'erreur de position dépasse la limite d'alerte". En aéronautique, le TTA est subdivisé en plusieurs TTA alloués aux différents segments d'un système de positionnement satellitaire (cf figure 3.1). Dans la section 3.6, nous nous concentrons sur des processus de contrôle d'intégrité embarqués. Par conséquent, nous considérons uniquement l'équivalent ferroviaire du "TTA aéronef".

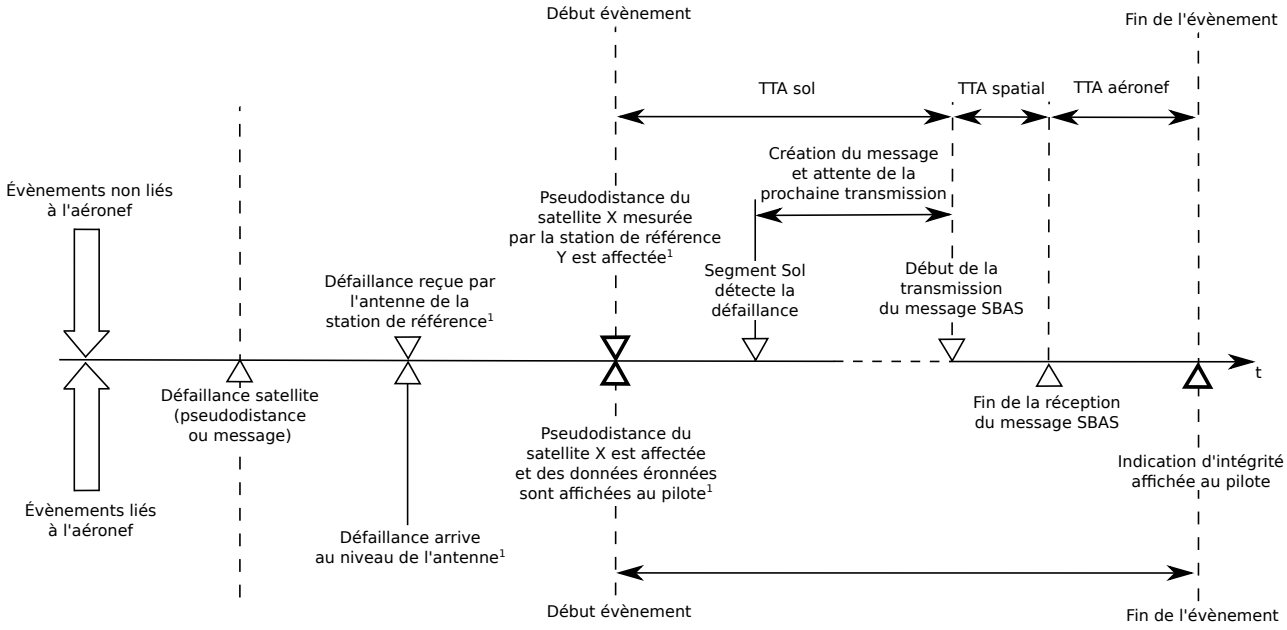


FIGURE 3.1 – Allocation des TTA aux différents segments GNSS dans une application aéronautique [ICAO, 2006].

[1]Ces évènements sont considérés comme simultanés. Ceci n'est pas tout à fait le cas car cela dépend des performances des récepteurs GNSS impliqués. Il existe une légère différence due au traitement des données au sein des récepteurs au moment où la pseudodistance est affectée d'une erreur et le moment où les données erronées sont affichées à l'utilisateur. Pour des raisons pratiques, ceci n'est pas reporté sur la figure.

— Risque sur l'intégrité

La dernière exigence concerne le risque sur l'intégrité (désigné par la variable IR pour *Integrity Risk*). Ce risque est défini par la probabilité qu'un système de navigation GNSS fournisse des informations ayant pour résultat une erreur de position relative en dehors des tolérances ($> AL$) pour une période supérieure à TTA. La position d'un véhicule est dite défaillante dans le cas où l'erreur de position (PE) est supérieure au niveau d'alerte (AL). En d'autres termes, elle exprime une probabilité d'*alerte manquée*. Dans ce cas, l'algorithme de contrôle d'intégrité est à remettre en question.

En opération, l'erreur vraie PE n'est jamais connue. Par conséquent, il faut pouvoir estimer cette erreur, suffisamment précisément, pour pouvoir assurer qu'elle est inférieure à AL. C'est pourquoi, le niveau de protection horizontal ou vertical (HPL, VPL) est également défini dans [ICAO, 2006]. Il correspond à l'erreur de position maximale garantie par le contrôle de l'intégrité. Cette grandeur peut être prédite (*i.e.* calculée) et peut s'exprimer en fonction des éphémérides des satellites [1] et en fonction de la trajectoire du véhicule. La sous-section 3.6.3 montrera comment le calculer.

Grâce à ces niveaux, quatre cas sont considérés (représentés en contexte 1D et pour le domaine aéronautique, automobile et ferroviaire dans la figure 3.2) :

— Le cas "a" représente la **situation normale** où tous les niveaux (PL et PE) sont en dessous de la limite d'alerte AL donnée pour une application/phase de mission particulière.
— Le cas "b" est le cas où le contrôle d'intégrité fournit un PL dépassant AL. Cela se réfère à une **indisponibilité** liée à ce mécanisme. Le système est incapable de garantir l'intégrité de la localisation (soit $PE < AL$).
— Le cas "c" représente la situation où PE dépasse PL mais reste en dessous de AL. Cela signifie que l'erreur de position dépasse les estimations fournies par le contrôle d'intégrité. Cependant, cette situation n'est pas critique puisque PE ne dépasse pas la limite d'alerte. Ce cas ne requiert pas de mise en sécurité du véhicule (arrêt, basculement sur un système de localisation auxiliaire, *etc...*). On parle de **défaillance non critique**.
— Le cas "d" est le cas de **défaillance critique**. En effet, PE dépasse PL ainsi que AL. Si l'utilisateur n'en est pas averti au bout d'un temps d'alerte TTA prescrit selon l'application, le véhicule doit être mis en sécurité.

Par ailleurs, l'université de Stanford propose un diagramme (cf Figure 3.3) pour présenter d'une autre manière les niveaux AL, PL et l'erreur de position PE . Il s'agit d'un graphique ayant comme abscisse PE et comme ordonnée PL. Il permet d'identifier les quatre cas précédents. Ce diagramme est très utilisé pour valider la qualité du contrôle d'intégrité fournie par les systèmes d'augmentations tels que les SBAS [Tossaint et al., 2007].

Après avoir bien posé les différents critères sous-jacents du concept d'intégrité de la localisation, dans la section suivante, nous proposons de les appliquer au contexte ferroviaire.

1. Les éphémérides font parties des données envoyées par les satellites vers un utilisateur. Elles contiennent notamment la position de ces satellites

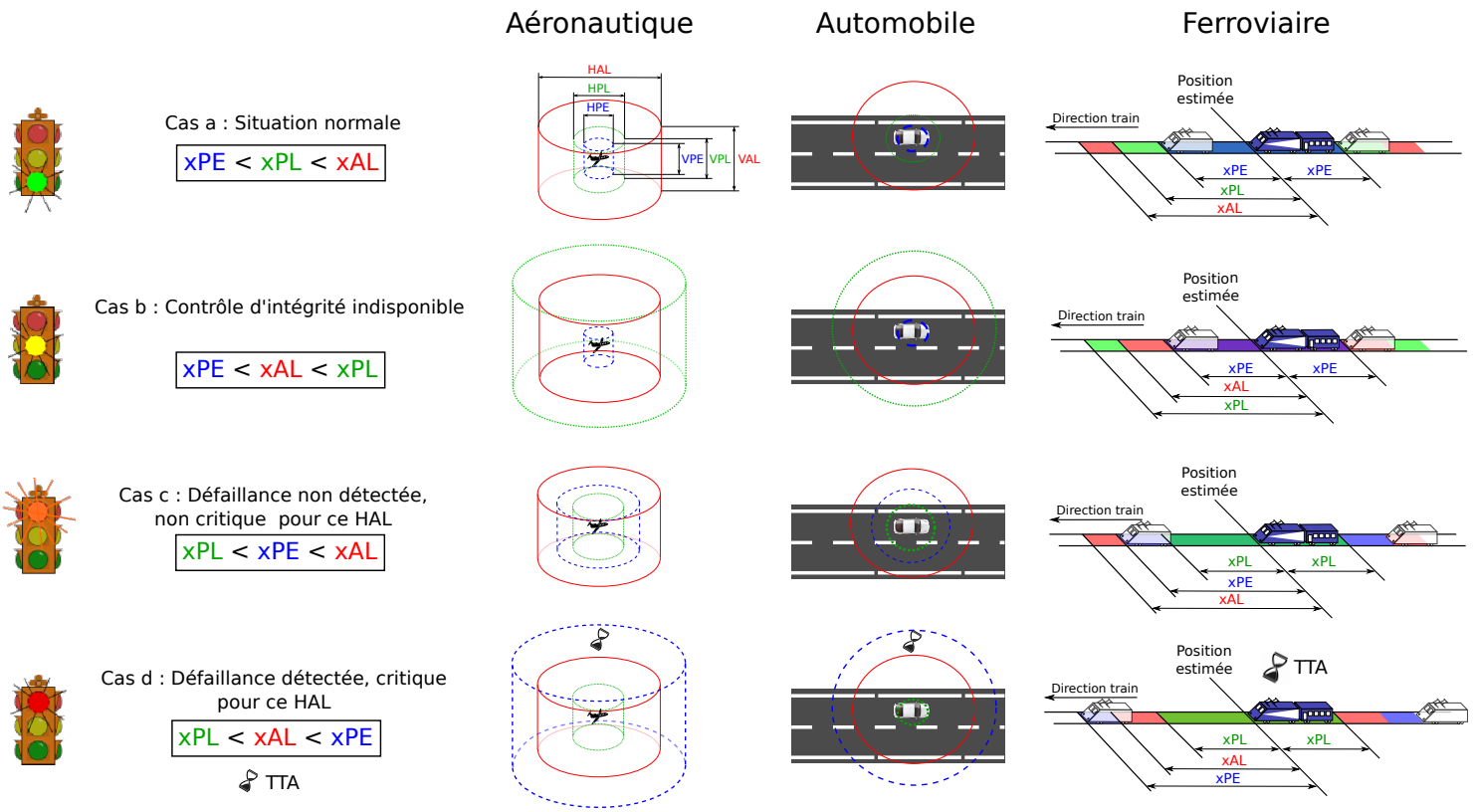


FIGURE 3.2 – Relations entre xPE, xPL et xAL (avec x pour vertical ou horizontal) dans différents cas et dans différents domaines (inspiré de [Le Marchand, 2010]).

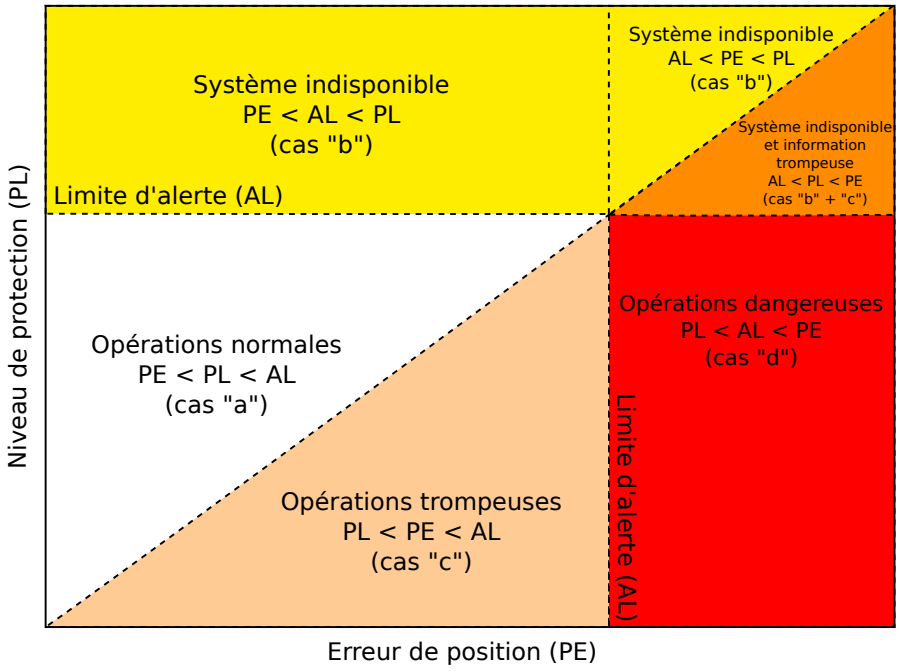


FIGURE 3.3 – Diagramme de Stanford.

3.4 Application au contexte ferroviaire

Le concept d'intégrité a été défini dans un contexte aéronautique et les besoins d'intégrité de la localisation sont clairement posés selon la phase de la mission (décollage, phase de vol, atterrissage, *etc.*) [ICAO, 2006] puisque les GNSS ont été conçus pour répondre aux besoins exprimés dans ce domaine. La volonté d'intégration des technologies satellitaires dans le domaine ferroviaire est relativement récente (le premier en date est le projet Advanced POsition LOcator - APOLO (1998-2001) [Filip et al., 2001]). L'intégrité d'une solution de navigation et les outils associés pour l'évaluer sont peu connus dans le domaine ferroviaire. De plus, dans le domaine aéronautique, il n'existe pas ou peu de phénomènes de masquage ou de signaux de type NLOS (ce sont des signaux GNSS reçus indirectement par le récepteur). Un transport aérien évolue en effet constamment dans un environnement ouvert et sans contrainte à l'exception des interférences électromagnétiques et du brouillage intentionnel. L'automobile partage les mêmes problématiques que le secteur ferroviaire à l'exception du matériel roulant qui est guidé. En effet, ces deux types de transports évoluent dans des milieux très souvent contraints par l'environnement (tunnels, zones urbaines ou boisées, *etc.*). Il est donc intéressant de se rapprocher des travaux menés sur l'intégrité des GNSS pour l'automobile [Le Marchand, 2010] en plus des quelques travaux menés sur le sujet pour le domaine ferroviaire [Liu et al., 2011] [Nikiforov and Choquette, 2003].

Les exigences sur l'intégrité de l'information de localisation, telles que définies dans ce chapitre, sont encore mal spécifiées dans le domaine ferroviaire. Les besoins en termes d'intégrité pour ce domaine ne sont pas exprimés clairement. En revanche, en aéronautique, un pilote ou un pilote automatique a besoin d'avoir une confiance élevée sur sa position pour mener à bien la phase d'atterrissage. Ceci est d'autant plus vrai qu'il dépend exclusivement des instruments de bord. Cette confiance élevée se traduit par une forte exigence sur l'intégrité (cf "Category I precision approach" dans le tableau 3.1).

Le tableau 3.1 donne un aperçu des exigences sur l'intégrité définies par l'ICAO pour quelques phases remarquables de vol. Dans le domaine ferroviaire, des tableaux de ce type n'existent pas. Seul le *GNSS-Rail User Group* a rédigé un rapport [Barbu, 2000] qui donne des recommandations relatives à l'utilisation des GNSS pour des applications ferroviaires. Il fournit notamment un tableau de valeurs pour les critères d'intégrité (cf tableau 3.2). Il est bien stipulé que ces valeurs sont recommandées par le groupe et ne sont pas des exigences adoptées dans un cadre réglementaire et à respecter rigoureusement.

Il manque une donnée cruciale qui rend l'évaluation de l'intégrité incomplète, la probabilité du risque sur l'intégrité. D'après le *GNSS-Rail User Group*, pour des applications liées à la sécurité, cette valeur doit être déduite d'un THR déterminé au cours d'une analyse des risques. De plus, les valeurs de TTA, quelle que soit l'application, nous semblent difficilement atteignables. En effet, elles sont plus drastiques (inférieure à 1 seconde pour le TTA) que celles associées à une phase d'approche précise d'un aéronef alors que celle-ci est la phase de vol la plus critique en terme d'intégrité (6 secondes pour le TTA). Le *GNSS-Rail User Group* stipule que ces valeurs de TTA sont recommandées notamment pour les distances de sécurité lors de l'approche de points critiques (passages à niveau, aiguillages, *etc.*). Dans le chapitre 4, nous proposerons d'autres valeurs, que nous avons jugées plus réalistes pour un cas d'utilisation spécifique du système de contrôle-commande ERTMS. Ces valeurs trouvent une justification dans les SRS (*System Requirement Specifications*) [SUBSET-041, 2015]. Ces valeurs de TTA ainsi que celles de AL et de IR sont des données d'entrées pour les algorithmes de contrôle d'intégrité abordés ci-après.

Tableau 3.1 – Exigences sur l'intégrité, TTA et xAL pour différentes phases de vol [ICAO, 2006].

Phases de vol[1]	Intégrité[2]	TTA	HAL	VAL
En-route	$1 - 10^{-7}/h$	$5\,min$	$3.7\,km$	-
En-route, Terminal	$1 - 10^{-7}/h$	$15\ s$	$1.85\ km$	-
Initial approach, Intermediate approach, Non-precise approach (NPA), Departure	$1 - 10^{-7}/h$	$10\ s$	$556\ m$	-
Approach operations with vertical guidance (APV-I)	$1 - 2 \times 10^{-7}$ par approche	$10\ s$	$556\,m$	$50\ m$
Approach operations with vertical guidance (APV-II)	$1 - 2 \times 10^{-7}$ par approche	$6\ s$	$40\ m$	$20\ m$
Category I[3] precision approach	$1 - 2 \times 10^{-7}$ par approche	$6\ s$	$40\ m$	15 à 10 m

[1]Les phases de vols ne sont pas traduites en français car elles sont soumises à des intitulés exacts.
[2]L'exigence sur l'intégrité est exprimée en $1 - 10^{-x}$ $(1 - IR)$ où 10^{-x} représente le risque d'intégrité.
[3]Il existe des phases Category II/III precision approach mais les exigences pour ces phases sont en révision et seront incluses à une date ultérieure dans les SARPs de l'ICAO

Tableau 3.2 – Extrait des recommandations sur la limite d'alerte AL et sur le délai d'alerte TTA pour des applications ferroviaires de sécurité [Barbu, 2000].

Applications liées à la sécurité	TTA (en secondes)	AL (en mètres)
Contrôle/commande sur lignes à trafic dense	< 1	$2,5$
Contrôle/commande sur lignes à trafic moyen	< 1	20
Contrôle/commande sur lignes à faible trafic	< 1	50

3.5 Algorithmes de contrôle d'intégrité actifs

Outre le service de localisation, les technologies satellitaires doivent apporter des garanties d'intégrité aux utilisateurs quel que soit le domaine de transport ou l'application. Le contrôle d'intégrité est inclus dans les systèmes d'augmentation, présentés dans la sous-section 1.3.4.2 du chapitre 1. Les ABAS (*Aircraft-Based Augmentation System*), notamment, visent l'amélioration de l'intégrité d'une localisation. La figure 3.4 résume toutes les déclinaisons possibles des algorithmes de contrôle

d'intégrité pour les ABAS selon le contexte, le moyen, la méthode employée et le type. Ces quatre catégories seront détaillées dans cette section.

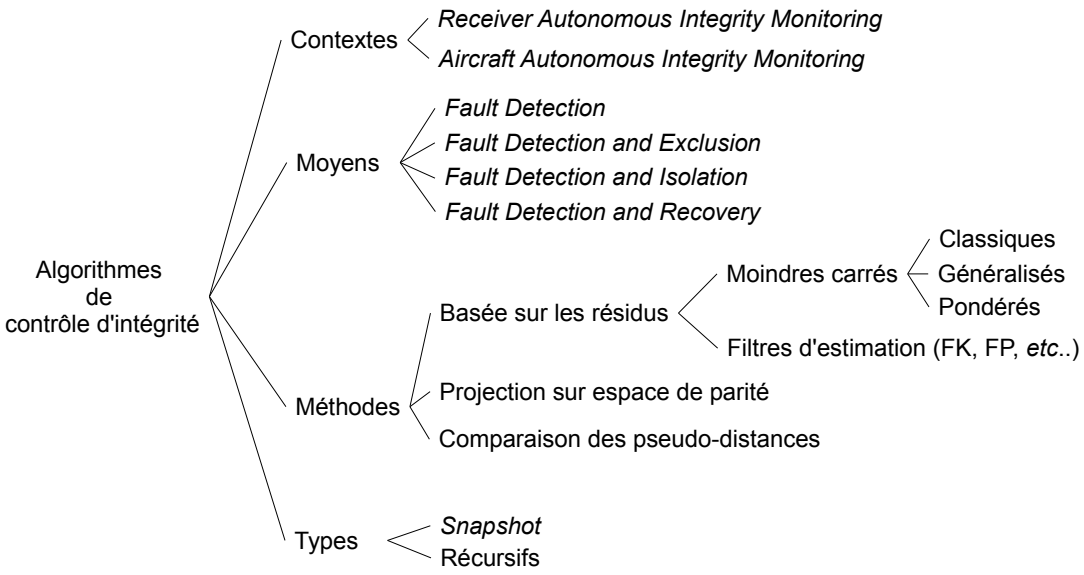


FIGURE 3.4 – Déclinaison des algorithmes de contrôles d'intégrité [Martineau et al., 2008][Le Marchand, 2010][Faurie, 2011] (FK : Filtre de Kalman. FP : Filtre Particulaire).

3.5.1 Contextes d'utilisation

Les processus de contrôle d'intégrité utilisent, si nécessaire, les autres moyens de navigation disponibles à bord. Ces outils se déclinent en deux grandes catégories selon leur contexte d'utilisation (sources et types de données de positionnement disponibles) : les algorithmes RAIM et les algorithmes AAIM.

— Pour un contrôle d'intégrité utilisant uniquement des données GNSS, on parle de contexte RAIM (*Receiver Autonomous Integrity Monitoring* ou contrôle autonome de l'intégrité par le récepteur). Les algorithmes de cette catégorie sont inclus dans le système de navigation GNSS embarqué. Ils constituent la première solution pour garantir l'intégrité. Le principe de redondance utilisé nécessite la réception de cinq satellites en vue, au minimum, pour fournir une solution de navigation et une information d'intégrité sur celle-ci. La sollicitation de davantage de satellites est recommandée pour bénéficier d'une redondance.

— Dans le cas d'utilisation de données GNSS associées à des données issues d'autres systèmes de navigation (par exemple, des systèmes inertiels), on parle de contexte AAIM (*Aircraft Autonomous Integrity Monitoring* ou contrôle autonome de l'intégrité par l'aéronef). Les algorithmes de ce type utilisent la redondance entre plusieurs capteurs (dont un récepteur GNSS) afin de fournir une performance d'intégrité au moins équivalente aux processus RAIM. L'exemple le plus connu de système de localisation combiné avec un récepteur GNSS est la centrale inertielle fournissant une solution de navigation proprioceptive donc obtenue indépendamment du satellite. Lorsque les données GNSS sont insuffisantes pour fournir une information d'in-

tégrité (cas où un algorithme RAIM serait indisponible), les données issues, comme dans cet exemple, de la centrale inertielle viennent compenser ce manque d'information sur l'intégrité de la solution de navigation.

Quel que soit le contexte, les algorithmes de contrôle de l'intégrité ont trois fonctions principales :

— Détecter les pannes,
— Atténuer les pannes (par exclusion ou isolation),
— Estimer un niveau de protection.

Les deux premiers points sont présentés dans la sous-section suivante. Le troisième constitue est présenté dans la sous-section 3.5.5.

3.5.2 Moyens utilisés pour le contrôle d'intégrité

Parmi les trois fonctions listées ci-dessus, la fonction de détection d'une source de localisation erronée reste incontournable quel que soit l'algorithme choisi. Tous les types de contrôles d'intégrité sont donc munis au minimum du moyen "*Fault Detection*".

Les étapes qui suivent sont optionnelles mais elles passent obligatoirement par une étape d'identification de la source erronée. Il s'agit de trouver quelle mesure est responsable de la détection d'une erreur avec l'hypothèse qu'il n'y a qu'une défaillance à la fois. La mesure incriminée est associée à un élément précis du vecteur d'état du système qui correspond à la coordonnée de la position fournie par une des sources disponibles. Une fois cette source identifiée, il faut la traiter. C'est à ce niveau que nous pouvons parler de tolérance aux pannes. Une source a été identifiée comme étant *en panne* et il s'agit de prendre une décision sur la marche à suivre.

Le moyen "*Fault Detection and Recovery*" détecte une panne et tente de faire revenir le système de localisation dans un état précédant la panne. Le moyen "*Fault Detection and Isolation*" détecte et isole la panne avant qu'elle contamine toute la solution de navigation. Le moyen "*Fault Detection and Exclusion*" détecte et exclut la source de localisation erronée [Yu, 1998]. Ces actions optionnelles peuvent être menées tant qu'il y a assez de sources pour déterminer une position. Cela signifie que, par exemple, l'exclusion est impossible si le nombre de sources encore disponibles n'est plus suffisant [2].

Par souci de concision et comme un algorithme *FD* est utilisé par la suite, nous ne nous attarderons pas sur ces étapes facultatives mais sur l'étape de détection. La détection repose essentiellement sur des tests statistiques nécessitant de déterminer un seuil pour la détection. Classiquement, un test statistique se déroule de la manière suivante :

1. Vérification des conditions de validité du test.
2. Choix de la statistique du test (variable aléatoire).
3. Choix des hypothèses nulle et alternative (H0 et H1).
4. Choix d'un risque α.

2. Dans un algorithme FDE appliqué à une architecture en hybridation serrée, une pseudodistance est considérée comme une source. Cependant, quatre pseudodistances sont nécessaires pour la détermination d'une position voire deux dans le cas ferroviaire [Wynants, 2001]. En dessous de ces valeurs, l'exclusion d'une pseudodistance est impossible à moins d'exclure toute la solution GNSS.

5. Détermination du seuil de décision.
6. Conclusion.

Le test classique utilisé dans la plupart des algorithmes de contrôle d'intégrité est le test du χ^2 [Groves, 2013] dont la variable aléatoire testée diffère selon la méthode choisie pour le contrôle d'intégrité (cf sous-section 3.5.3). Ce test n'est valable que si les bruits considérés au sein du système à modéliser sont gaussiens (cf représentation d'état dans la section 3.6). Ce test du χ^2 est un test dit d'adéquation à une loi, c'est à dire qu'il permet de déterminer si la distribution des valeurs prises par la statistique choisie suit la loi du χ^2 centrée (hypothèse H0) ou pas (hypothèse H1). L'étape suivante consiste à renseigner une probabilité liée au risque de se tromper au cours de ce test (notée α) notamment la probabilité de rejeter l'hypothèse nulle H0 alors qu'elle est vraie (risque de première espèce). Elle correspond à la probabilité de fausse alarme.

3.5.3 Méthodes statistiques employées

Le choix de la statistique la plus adéquate à première vue pour le test statistique est l'erreur de position. En effet, pour déterminer l'intégrité de la position, l'erreur de position est comparée à un niveau d'alerte (cf section 3.3). Néanmoins, l'erreur de position n'est pas connue puisqu'elle suppose la connaissance de la position réelle du train. Cet obstacle peut être levé par l'utilisation d'un système de positionnement très précis dont la position sert de référence et est assimilée à la position réelle. Le problème peut aussi être contourné par l'utilisation de cartes centimétriques (cf la méthode de *Map-Matching* expliquée dans la sous-section 1.3.4 du chapitre 1). Ces solutions présentent quelques inconvénients non négligeables. D'une part, les systèmes de positionnement suffisamment précis pour fournir une position de référence ont des coûts prohibitifs ($> 100k€$) pour une centrale inertielle répondant à ces critères de précision. Ils peuvent être utilisés dans des conditions de tests mais pas généralisés en opération. Les cartes centimétriques ne couvrent pas le réseau ferroviaire complet d'un pays tel que la France. De plus, le stockage et la manipulation de telles cartes nécessitent d'importantes ressources informatiques, ressources limitées par la contrainte d'utilisation d'un système embarqué. Par conséquent, la considération de l'erreur de position comme variable aléatoire pour les tests n'est pas envisageable.

Pour lever l'hypothèse de la position réelle connue faite dans le chapitre 2, il faut se tourner vers d'autres variables aléatoires. Les 3 méthodes ci-dessous sont les méthodes les plus répandues et définissent trois variables aléatoires différentes :

— La méthode de comparaison ou *Range-Comparison* [Brown, 1992],
— Les méthodes utilisant les résidus,
— La méthode de projection sur l'espace de parité [Maquin et al., 1997],

que nous allons comparer.

3.5.3.1 Approche comparative de solutions de navigation ou *Range-Comparison*

La méthode de comparaison, appelée *Range-Comparison* [Brown, 1992], consiste à confronter deux solutions de navigation calculées en fonction du nombre de sources de localisation disponibles. Il s'agit de la méthode la plus simple pour détecter une panne sur une source de localisation. Par exemple, 4 pseudodistances sont nécessaires pour déterminer une solution de navigation. Les $n-4$ pseudodistances disponibles servent à calculer une seconde solution de navigation. La différence des

mesures de celles-ci est comparée à un seuil donné. En dessous de ce seuil, le système de détection déclare qu'il n'y a aucune défaillance de positionnement. Initialement, cette méthode est utilisée uniquement avec des pseudodistances (contexte RAIM) mais peut être exploitée dans un contexte type AAIM (sources autres que satellitaires).

3.5.3.2 Approche fondée sur les résidus

Les résidus peuvent être définis comme la **différence entre les mesures et les estimations obtenues à partir d'équations de modèle**. Le terme *innovation* est parfois assimilé aux résidus. Or, une nuance existe entre innovation et résidus. Selon [Groves, 2013], l'innovation, dont le vecteur est noté δz^-, est la différence entre le vecteur de mesure réel z et celui calculé à partir du vecteur d'état précédant la mise à jour de la mesure $h(\hat{x}^-)$. Le résidu, selon une définition plus précise, est la différence entre le vecteur de mesure réel z et celui calculé à partir du vecteur d'état mis à jour $h(\hat{x}^+)$. Par conséquent, cela dépend à quel instant (avant, symbolisé par le "-", ou après la mise à jour, symbolisé par le "+") nous récupérons les informations de résidus sur les mesures. Pour rappel, la mise à jour des mesures est une des étapes du filtrage de Kalman.

Le choix du vecteur de résidus par rapport à celui d'innovation semble judicieux parce que les résidus sont des valeurs moins obsolètes que l'innovation. Les résidus sont d'ailleurs largement utilisés dans les processus de détection. Pour ne pas alourdir les équations, nous utiliserons la notation $\hat{x}$ à la place de $\hat{x}^+$. Le vecteur de résidu δz est ainsi obtenu par l'équation 3.1.

$$\delta z = z - h(\hat{x}) \tag{3.1}$$

Les résidus sont obtenus soit par estimation paramétrique (méthode des moindres carrés classiques, généralisés ou pondérés) soit par estimation d'état par filtrage de Kalman ou filtre particulaire (présentés dans la sous-section 2.4.2 du chapitre 2).

La particularité des résidus est que la distribution de leur somme pondérée normalisée au carré (notée $NSSE$ pour *Normalised Sum of the Squared Errors* dans l'équation 3.2) suit une loi du χ^2 centrée compte tenu de l'hypothèse sur les bruits gaussiens (cf Annexe B équations B.5, B.6 et B.7).

$$NSSE = \frac{\|\delta z\|^2}{\sigma_{\delta z}^2} \tag{3.2}$$

où, δz est le vecteur de résidus (cf équation 3.1) et $\sigma_{\delta z}^2$ est la variance des résidus. Chaque élément du vecteur de résidus δz_i a une variance $\sigma_{\delta z_i}^2$ supposée identique et constante soit $\sigma_{\delta z_1}^2 = \sigma_{\delta z_2}^2 = ... = \sigma_{\delta z_n}^2$ (avec n la taille du vecteur de résidus). Nous notons que cette hypothèse est parfois levée [Nikiforov, 2015].

Il est communément admis que la distribution des résidus suit une loi normale de moyenne $\mu_{\delta z}$ et de variance $Q_{\delta z}$.

$$\delta z \sim \mathcal{N}(\mu_{\delta z}, Q_{\delta z}) \tag{3.3}$$

$\mu_{\delta z}$ est considérée comme nulle en l'absence d'erreur sur les mesures des capteurs [Le Marchand, 2010] et $Q_{\delta z} = \sigma_{\delta z}^2 I_m$ où I_m est une matrice identité d'ordre m (δz est un vecteur de taille $(1 \times m)$).

En présence d'une erreur, la distribution de $NSSE$ est décalée vers la droite et suit alors une loi du χ^2 décentrée. Le choix de $NSSE$ comme statistique de test plutôt que le résidu directement est justifié par le fait que, à chaque instant, nous avons plusieurs résidus (regroupés dans un vecteur) et non pas un seul. $NSSE$ permet de conserver une seule variable. Le test est ainsi simplifié. Par conséquent, nous ne pouvons pas différencier les sources de mesures si l'on souhaite isoler ou exclure une source erronée.

Connaissant une probabilité de fausse alarme pfa et la distribution de $NSSE$ en temps normal (selon une loi du χ^2 centrée), un seuil de détection est calculé (cf sous-sections 3.6.1.3 et 3.6.1.3). La conclusion de ce test permet de rejeter ou d'accepter H0. Notons que si H0 est acceptée alors qu'elle devrait être rejetée, on parle de risque de seconde espèce. Dans le cadre de ce chapitre, il s'agit de la probabilité de détection manquée, probabilité importante en terme de sécurité.

Cette approche basée sur les résidus est utilisée dans l'algorithme de contrôle d'intégrité proposé dans la section 3.6.

3.5.3.3 Approche par projection sur l'espace de parité

Le but de la méthode de projection sur l'espace de parité est d'obtenir une variable de décision qui soit indépendante de l'estimation d'état $\hat{X}$ [Maquin et al., 1997] [Nikiforov, 2005]. Pour cela, nous définissons p, appelé espace de parité, orthogonal à $\hat{X}$ (cf équation 3.4) [3].

$$\begin{bmatrix} \hat{X} \\ \hline p \end{bmatrix} = \begin{bmatrix} (H^t H)^{-1} H^t \\ \hline W \end{bmatrix} z \tag{3.4}$$

où z est le vecteur de mesures et W est la matrice de transformation (ou matrice de parité) de z à p.

Cette matrice W est déterminée par la décomposition en valeur singulière [4] de la matrice H et possède les propriétés suivantes :

$$W \cdot W^t = I \tag{3.5}$$
$$W \cdot H = 0 \tag{3.6}$$
$$W^t \cdot W = (I - H^t H)^{-1} H^t \tag{3.7}$$

Une fois le vecteur de parité p calculé à partir du vecteur de mesure et de la matrice W (soit $p = W \cdot z$), on peut calculer un $NSSE$ selon l'équation 3.8.

$$NSSE = \frac{\|p\|^2}{\sigma_p^2} \tag{3.8}$$

où σ_p^2 est la variance des éléments du vecteur de parité et déterminé de la même manière que $\sigma_{\delta z}^2$ c'est à dire $\sigma_{p1}^2 = \sigma_{p2}^2 = ... = \sigma_{pn}^2$ (n est la taille du vecteur de parité).

3. Les tirets signifient que le vecteur p et la matrice W sont calculés respectivement à partir de $\hat{X}$ et de la matrice H

4. Les détails calculatoires de cette décomposition sont disponibles dans l'annexe B de la thèse de [Le Marchand, 2010]

Ce $NSSE$ est déterminé par le vecteur de parité p et le test statistique est le même que celui pour les résidus. Ainsi, l'approche utilisant les résidus et par projection sur l'espace de parité sont équivalentes.

Ces trois méthodes représentent le cœur des algorithmes de contrôle d'intégrité. Cependant, celles-ci ont quelques points faibles. En effet, les deux dernières méthodes prennent pour hypothèse que les bruits de mesures peuvent être représentés par des gaussiennes. Ceci qui n'est pas conforme à la réalité [Viandier, 2011] car les environnements terrestres ont une incidence sur les résidus. [Panagiotakopoulos, 2009] propose d'améliorer la représentation de ces bruits par la théorie des valeurs extrêmes utilisée dans le secteur financier [Embrechts et al., 2013]. [Hewitson, 2003] enrichit les algorithmes de contrôle d'intégrité par des modèles de déplacement. La prise en compte du type d'environnement est possible également au travers d'un filtrage de Kalman en couplage serré [Feng and Ochieng, 2007] présenté dans la sous-section 1.3.4.1 du chapitre 1. Autre hypothèse importante, toutes les méthodes sont incapables de mettre en évidence les pannes multiples. La thèse de [Faurie, 2011] s'attache à lever ce verrou.

3.5.4 Types d'algorithmes de contrôle d'intégrité

Les algorithmes RAIM ou AAIM se distinguent également selon qu'ils utilisent des mesures à l'instant actuel (*snapshot*) (c'est le cas des méthodes des Moindres Carrés et de la projection sur un espace de parité) ou des mesures passées (récursifs) typiques des filtres d'estimation d'état.

L'ultime étape réalisée par tout contrôle d'intégrité est de déterminer un niveau de protection PL. Le niveau de protection est confronté au niveau d'alarme stipulé dans les exigences sur l'intégrité dans le but de vérifier si le système de localisation atteint ses objectifs.

3.5.5 Calculs du niveau de protection lors du contrôle d'intégrité

Dans tous les algorithmes de contrôle d'intégrité, le niveau de protection est calculé à partir de la géométrie des satellites (matrice S décrite ci-après), d'une erreur minimale détectable P_{biais} et d'hypothèses sur les bruits. [Le Marchand, 2010] considère que la position et la pseudodistance sont chacune entachées d'un bruit et d'un biais. [Le Marchand, 2010] distingue 2 hypothèses :

— H_{err} : l'impact du bruit de mesure sur l'erreur de position est négligeable par rapport à celui de la panne,
— H_{res} : l'impact du bruit de mesure sur les résidus est négligeable par rapport à celui de la panne.

Par conséquent, quatre cas sont possibles. Le détail des calculs est disponible dans la thèse de [Le Marchand, 2010].

Cas 1 : H_{err} et H_{res} sont vraies

Dans ce cas, le bruit de mesure n'a pas d'impact significatif ni sur l'erreur de position ni sur les résidus. Il n'intervient donc pas dans le calcul de PL (cf équation 3.9).

$$PL = \max_j \sqrt{\frac{(H_{aj}^+)^2 + (H_{bj}^+)^2}{S_{jj}}} \cdot \sigma_{\delta z} \sqrt{NSSE} \tag{3.9}$$

où, $\sigma_{\delta z}$ est l'écart-type des résidus.
S est une matrice idempotente qui lie les résidus à l'erreur de mesure (l'erreur de mesure ne peut être déduite des résidus car S est non-inversible) avec $S = I - HH^+$ (I, matrice identité, H, matrice Jacobienne de la fonction d'observation h et H^+, sa pseudo-inverse),
Les éléments aj et bj de H^+ sont reliés aux composantes a et b du vecteur d'état choisi selon le modèle d'évolution d'un système GNSS/INS (cf équation 3.13). Le PL est ici un HPL (niveau de protection horizontal).

La quantité $\sqrt{\frac{(H_{aj}^+)^2+(H_{bj}^+)^2}{S_{jj}}}$ est aussi appelée dans la littérature $SLOPE$. Elle correspond au coefficient directeur des droites illustrées par la figure 3.5). Ces droites permettent, à partir d'un seuil de décision T (ou d'une erreur minimale détectable P_{biais} (cf équation 3.24)), de déterminer une valeur particulière (notée PR) de l'erreur de position PE. La valeur maximale de PR correspond à la valeur de PL. Pour alléger l'écriture des équations, nous remplacerons cette quantité par $SLOPE_j$.

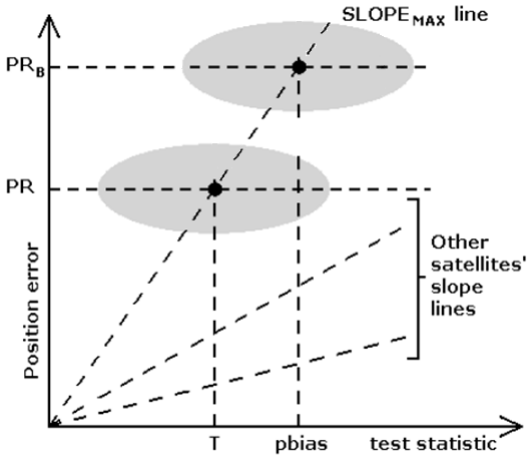


FIGURE 3.5 – Droites de coefficient directeur $SLOPE$ permettant d'un seuil de décision de déterminer PL (figure simplifiée issue de Brown [1992]).

Cas 2 : H_{err} fausse et H_{res} vraie

Dans ce cas, l'impact du bruit n'est pas négligeable sur l'erreur de position mais l'est sur les résidus. Cela se traduit par l'ajout un terme supplémentaire qui dépend du bruit considéré (cf équation B.5 de l'annexe B) noté λ dans [Walter and Enge, 1995] et d'un facteur k (rayon d'un cercle englobant l'erreur) calculé à partir de la loi statistique utilisée pour représenter ce bruit (cf équation 3.10).

$$PL = \max_j \; SLOPE_j \cdot \sigma_{\delta z} \sqrt{NSSE} + k \cdot \lambda \tag{3.10}$$

Cas 3 : H_{err} vraie et H_{res} fausse

L'impact du bruit de mesure est négligeable sur l'erreur de position mais pas sur les résidus. S'il y a impact sur les résidus, $NSSE$ ne suit plus une loi du χ^2 centrée mais décentrée avec un paramètre de non-centralité c dont il faut tenir compte dans le calcul de PL. D'après [Feng et al., 2005] et [Le Marchand, 2010], l'équation 3.9 devient :

$$PL = \max_j \ SLOPE_j \cdot \sigma_{\delta z}\sqrt{c} \tag{3.11}$$

Cas 4 : H_{err} et H_{res} fausses

Le cas 4 est simplement la combinaison des cas 2 et 3 où, d'une part, $NSSE$ ne suit plus une loi du χ^2 centrée (donc c doit intégrer le calcul de PL) et, d'autre part, un terme $k \cdot \lambda$ dépendant du bruit de mesure s'ajoute.

$$PL = \max_j \ SLOPE_j \cdot \sigma_{\delta z}\sqrt{c} + k \cdot \lambda \tag{3.12}$$

Cette sous-section a synthétisé les techniques existantes des algorithmes de contrôle d'intégrité. La sous-section qui suit liste les algorithmes de contrôle d'intégrité les plus connus.

3.5.6 Algorithmes existants

Le tableau suivant 3.5.6 propose une liste non-exhaustive des algorithmes existants et classés selon leur contexte d'utilisation (RAIM ou AAIM), la méthode employée (*Range-comparison*/Moindres Carrés/Espace de parité/filtre d'estimation), selon si les mesures actuelles ou un historique de mesures sont utilisés (*Snapshot*/récursifs). Les références proposées dans ce tableau (une seule par algorithme) pointent vers les publications originales où sont décrits pour la première fois ces algorithmes.

Tableau 3.3 – Liste d'algorithmes de contrôles d'intégrité existant

Algorithmes	Contexte	Méthodes	Type	Références
RAIM-LS	RAIM	Moindres Carrés	*Snapshot*	[Parkinson and Axelrad, 1988]
Weighted RAIM-LS	RAIM	Moindres Carrés Pondérés	*Snapshot*	[Walter and Enge, 1995]
RAIM-SS	RAIM	Filtres d'estimation	Récursif	[Brown and McBurney, 1988]
NIORAIM	RAIM	Moindres Carrés Pondérés et espace de parité	*Snapshot*	[Hwang and Brown, 2006]
MSS	AAIM	Filtres d'estimation	Récursif	[Brenner, 1998]
AIME	AAIM	Filtres d'estimation	Récursif	[Diesel and Luu, 1995]
CGLR	RAIM	Espace de parité	*Snapshot*	[Nikiforov, 2005]
GEV-RAIM	RAIM	Filtres d'estimation	Récursif	[Panagiotakopoulos, 2009]
RANCO	RAIM	Filtres d'estimation	Récursif	[Schroth et al., 2008]
Forward Backward FDE	RAIM	Moindres Carrés Pondérés	*Snapshot*	[Kuusniemi, 2005]

L'algorithme RAIM-LS (pour RAIM - *Least Squares*) est le plus simple car il utilise la méthode des Moindres Carrés classique. Le RAIM-SS (pour RAIM - *Separate Solution*) utilise les résidus issus de plusieurs filtres d'estimation pour déterminer au moins 2 estimations d'état. En l'absence de panne, ces deux estimations sont proches mais en présence de panne, elles s'éloignent l'une de l'autre. La différence ou "séparation" (d'où le nom de l'algorithme) engendrée est utilisée lors des tests statistiques pour la détection de panne. Le NIORAIM (pour *Novel Integrity-Optimized RAIM*) se distingue par l'utilisation conjointe de la méthode de projection sur l'espace de parité et de celle des Moindres Carrés Pondérés pour la détection de panne. Le AIME (pour *Autonomous Integrity Monitoring and Extrapolation*) est un algorithme AAIM utilisant les résidus d'un filtre intégrant un système GNSS/INS en hybridation serrée. Il fait l'objet d'une documentation technique [RTCA, 2006] dans la *Radio Technical Commission for Aeronautics*, société privée américaine délivrant ce genre de document à l'ICAO notamment. Le GEV-RAIM (pour *Generalized Extreme Value*) s'appuie sur la théorie des valeurs extrêmes et utilise les résidus issus d'un filtre d'estimation de manière classique. Le fondement statistique y est plus réaliste. Enfin, le RANCO (pour *RANge COnsensus*) est le premier algorithme RAIM à prendre en compte des pannes multiples issues des satellites. [Faurie, 2011] propose un algorithme de ce type.

Il faut noter que les contextes précisés dans ce tableau sont les contextes dans lesquels sont initialement conçus les algorithmes. Il est tout à fait possible qu'un algorithme RAIM puisse être adapté à un contexte AAIM comme c'est le cas entre les algorithmes RAIM-SS et MSS (pour *Multiple Separate Solution*). Dans ce même contexte, [Bhatti and Ochieng, 2009] et [Liu et al., 2010] ont proposé des algorithmes de contrôle d'intégrité dans le cas d'utilisation de systèmes GNSS/INS.

Dans la thèse, l'intégrité d'un système GNSS/INS est également évalué. Cependant, l'originalité de l'algorithme proposé dans ce chapitre réside sur la détection de deux types d'erreurs : les biais instantanés et les erreurs à croissance lente. La détection des biais instantanés s'appuie sur des tests statistiques classiques tandis que la détection des erreurs à croissance lente s'inspire d'une méthode de détection d'erreurs sur les résidus de pseudodistances [Ochieng et al., 2008]. D'après l'état de l'art sur les techniques de localisation effectué dans le chapitre 1, ce sont les deux catégories d'erreurs qui sont mises en évidence respectivement pour les GNSS et les capteurs proprioceptifs tels que l'INS. Selon [Faurie, 2011], "le contrôle d'intégrité AAIM souffre classiquement du problème d'accommodation aux pannes lentes". Pour tenir compte des pannes lentes, des algorithmes ont été proposés : l'AIME, RANCO (cf tableau 3.5.6) et une variante du RANCO proposée par [Faurie, 2011]. Néanmoins, ces solutions sont complexes à mettre en œuvre notamment par l'utilisation de plusieurs bancs de filtres (en plus du filtre d'estimation fournissant la solution de navigation).

L'algorithme proposé est, selon des catégories vues dans cette section, un algorithme de type AAIM *FD* qui s'appuie sur la détermination des résidus par un filtre de Kalman étendu et issus d'un système GNSS/INS. L'utilisation d'un système GNSS/INS a été discutée dans le chapitre 1. Par conséquent, nous sommes bien dans un contexte AAIM où d'autres données que celles issues d'un récepteur GNSS sont utilisées. Un moyen de type "*FD*" suffit à évaluer un risque sur l'intégrité pour la mise en relation avec l'attribut de sécurité (cf section 3.7). La détermination des résidus par un filtre d'estimation est la méthode la plus classique dans le contrôle d'intégrité. Enfin, le filtre de Kalman est le filtre d'estimation le plus utilisé en navigation.

3.6 Algorithme de contrôle de l'intégrité particulier pour un système avec GNSS

Nous avons vu dans la section précédente que les méthodes de détection classiques s'appuient sur des probabilités de fausse alarme et de détection manquée et les tests d'hypothèses (elles font l'objet d'un brevet dans le cadre d'une localisation par GPS [Yu, 1998]). Ces dernières prennent des hypothèses sur la modélisation du système de localisation, notamment sur les bruits du système et de mesure ($w_s(t)$ et $w_m(t)$) considérés comme des bruits gaussiens. La représentation d'état d'un système avec GNSS en hybridation serrée est donnée sous sa forme continue par les équations 3.13 et 3.14.

$$\dot{x}(t) = f(x(t), t) + w_s(t) \tag{3.13}$$

$$z(t) = h(x(t), t) + w_m(t) \tag{3.14}$$

où,
$x(t)$ est le vecteur d'état de dimension n sachant que, pour un système GNSS/INS, $x(t) = [\delta\Psi\ \delta v\ \delta r\ b_a\ b_g\ \delta\rho\ \delta\dot{\rho}]^T$,
$\dot{x}(t)$, sa dérivée,
Ψ les angles (roulis ψ, tangage θ et lacet ψ),
v et r, respectivement, la vitesse (Vx, Vy, Vz) et la position (x, y, z) dans le repère cartésien,
b_a et b_g, vecteur de biais constants liés à la température et aux vibrations, respectivement sur les accéléromètres et les gyroscopes au sein de la centrale inertielle (dimensionnés au chapitre 4 sous-section 4.3.2.2),
ρ, vecteur de pseudodistances, $\dot{\rho}$, quantité (appelée *pseudorange rate*) en fonction des mesures Doppler où $\dot{\rho} = \frac{cD}{f}$ avec c, célérité de la lumière, D, fréquence Doppler mesurée et f, fréquence de la porteuse,
$z(t)$ est le vecteur de mesure de dimension m,
$w_s(t) \in \mathbb{R}^q$ et $w_m(t) \in \mathbb{R}^m$ sont des vecteurs, respectivement, liés au bruit du système (lié aux erreurs de modélisation et des perturbations) et à celui de mesure (lié à l'imperfection des capteurs) considérés comme gaussiens (cf annexe B),
f et h sont, respectivement, la fonction du système et celle d'observation (F et H étant leurs matrices Jacobiennes respectives).

Cette représentation d'état est à la base des filtres de navigation classiques [Groves, 2013] : le filtre de Kalman et ses extensions (discret, étendu et sans parfum). Le filtre, pour un vecteur d'état $x(t)$, donne une estimation de cet état notée $\hat{x}(t)$. Le vecteur d'état présenté ci-dessus correspond à un vecteur utilisé dans une hybridation serrée. La connaissance de ce vecteur ainsi que de la fonction h permet la détermination des résidus δz, à extraire du filtre de Kalman (cf équation 3.1).

Nous pouvons mettre en œuvre le contrôle d'intégrité suivant la représentation d'état présentée ci-dessus (le système complet sera décrit au chapitre 4). Les tests statistiques qui vont suivre permettent la mise en œuvre de la phase de détection du contrôle d'intégrité. Face à la conjugaison des erreurs liées aux GNSS, de celles des capteurs proprioceptifs (type centrales inertielles) et face également aux faiblesses des algorithmes de contrôle d'intégrité existants, nous proposons une solution basée sur une double détection (cf figure 3.6) issue de techniques classiques liées à des techniques innovantes [Ochieng et al., 2008]. La figure 3.6 montre en détail l'algorithme de contrôle d'intégrité que nous proposons. Les résidus sont extraits des mesures fournies par un système GNSS/INS ainsi

que la matrice d'observation H. D'une part, ces résidus viennent directement alimenter le test du χ^2. D'autre part, ils viennent enrichir une base de données constituant un historique. La matrice d'observation H est utilisée pour le calcul de PL. Avec les hypothèses sur la forme des distributions des résidus (loi du χ^2 et loi normale), des seuils de détection sont déterminés. En parallèle, les niveaux de protection (GNSS et INS) seront calculés.

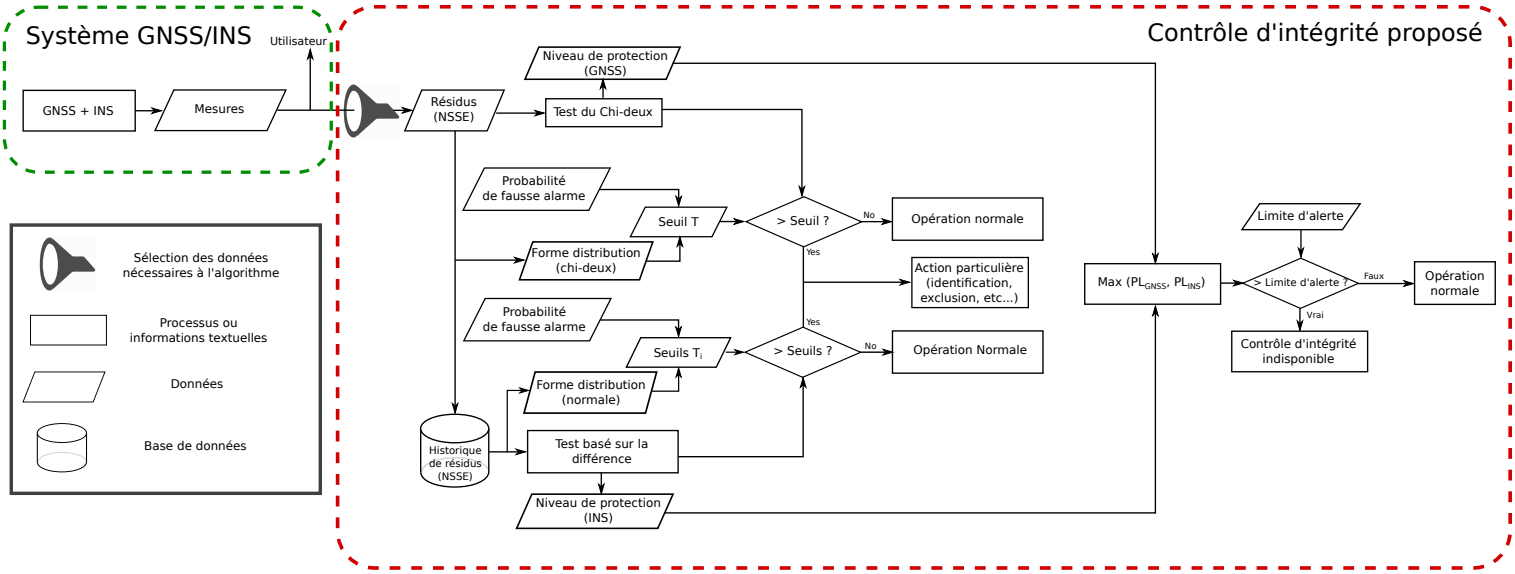


FIGURE 3.6 – Schéma de l'algorithme de contrôle d'intégrité proposé [Legrand et al., 2015].

Dans la sous-section suivante, nous présentons le premier type de détection, celui des biais instantanés. Ces biais sont assimilés aux erreurs aberrantes générées par le phénomène de multitrajet.

3.6.1 Détection des biais instantanés

L'erreur de position aberrante liée à une erreur aberrante sur une mesure des capteurs dont l'allure présente une pente qui tend vers l'infini est considérée comme un *biais instantané*. L'amplitude de ces erreurs peut aller jusqu'à des centaines voire des milliers de mètres. Ces erreurs proviennent alors essentiellement d'erreurs aberrantes sur les pseudodistances engendrées par des phénomènes de multitrajets, une des premières sources d'erreur GNSS liée à l'environnement proche [Bhatti and Ochieng, 2007]. En pratique, nous considérons une pente importante (cf figure 3.7).

Pour une possible vérification de la qualité de cette détection, il faut distinguer un biais instantané d'une rampe à évolution dite "rapide" (cf sous-section 3.6.2). Pour cela, il faut dimensionner un coefficient directeur limite décrit par l'équation 3.15. Cette équation s'exprime dans le domaine de calcul des positions et non dans celui des mesures puisqu'il s'agit d'une étape de vérification de la détection. Pour éviter de prendre une valeur arbitraire, nous proposons d'utiliser l'exigence AL pour quantifier ce coefficient directeur. Le dépassement de l'exigence au cours d'un seul pas d'échantillonnage Te peut être considéré comme un biais instantané. Le processus de détection se réalisant à chaque pas d'échantillonnage, il n'a aucune visibilité sur l'erreur de position entre deux pas.

$$\text{biais instantané} \equiv \delta PE(t_i) = \frac{PE(t_i + Te) - PE(t_i)}{Te} \geq \frac{AL}{Te}\ m/s \tag{3.15}$$

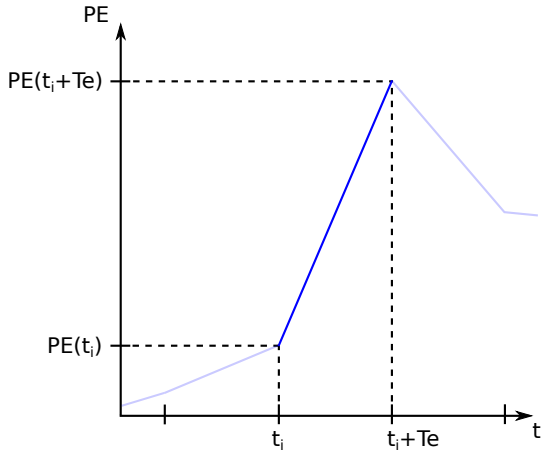


FIGURE 3.7 – Biais instantané.

avec,
PE, l'erreur de position obtenue par un système de référence,
$\delta PE(t_i)$, la dérivée de PE à t_i,
Te, un temps d'échantillonnage.

À présent que les biais instantanés sont caractérisés, le test statistique lié à leur détection peut être présenté. La première étape est le choix des hypothèses nulle et alternative.

3.6.1.1 Énoncé des hypothèses nulle et alternative

Lors du test du χ^2, il s'agit de tester si $NSSE$ suit la loi du χ^2 (hypothèse H0 - équation 3.16) ou une loi du χ^2 décentrée avec un paramètre de non-centralité c (hypothèse H1 - équation 3.17).

$$H0 \quad : \quad NSSE \sim \chi^2_{ddl} \tag{3.16}$$
$$H1 \quad : \quad NSSE \sim \chi^2_{ddl,c} \tag{3.17}$$

où,
ddl est le degré de liberté, paramètre de la loi du χ^2, dépendant du nombre de paramètres considérés pour le système (taille du vecteur d'état soit n) et du nombre d'observations (taille du vecteur de mesure soit m) tel que $ddl = m - n$ ($ddl > 0$). Au cours d'une mission, le nombre de satellites en vue peut varier, ce qui signifie que m n'est pas constant mais évolue au cours du temps. Quant à n, il reste constant puisqu'il dépend de la modélisation du système. c est le coefficient de non-centralité de la distribution.

Dans le cadre de l'utilisation d'un système de localisation fondé sur les GNSS, H_0 représente le comportement normal, sans multitrajet, du système de positionnement et H_1 représente son comportement avec multitrajets. La figure 3.8 montre graphiquement l'évolution de la densité de probabilité de la variable aléatoire selon les hypothèses posées précédemment. Les hypothèses sur la distribution normale des bruits (système et mesure) induisent que la norme du vecteur de résidus au carré (cf équation 3.1), $NSSE$ (cf équation 3.2) suit une loi du χ^2 (cf équation 3.16) avec un degré de liberté ddl.

Sur la figure 3.8, la probabilité de détection manquée pmd (*probability of missed detection*) correspondant à la zone signalée en rouge, représente la distribution des $NSSE$ avec des biais

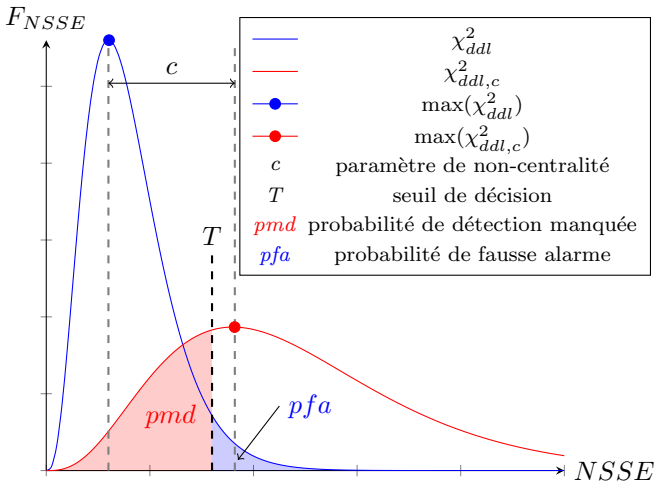


FIGURE 3.8 – Densités de probabilité relatives à l'hypothèse H0 (courbe bleue) et H1 (courbe rouge).

instantanés présents mais non détectés (en dessous d'un seuil T). La probabilité de fausse alerte pfa (*probability of false alarm*) correspondant à la zone signalée en bleue, représente la distribution des $NSSE$ sans biais instantané mais détectés comme présents (au dessus d'un seuil T). On rappelle que la loi du χ^2 possède une densité de probabilité donnée par l'équation 3.18.

$$f(x) = \frac{1}{2^{ddl/2}\Gamma(ddl/2)} x^{(ddl/2)-1} e^{-x/2} \tag{3.18}$$

où,
x est la variable aléatoire suivant la loi du χ^2 (ici $x = NSSE$),
$\Gamma(a) = \int_0^\infty t^{a-1}e^{-t}d\tau$ est une fonction Gamma.

La figure 3.8 montre que pfa et pmd sont des portions de densité de probabilité d'une loi du χ^2 respectivement de 0 à T (zone rouge) et de T à $+\infty$ (zone bleue) (cf équations 3.19 et 3.20). Pour une lecture plus aisée, nous conservons $x = NSSE$.

$$pfa = \int_T^{+\infty} \frac{1}{2^{ddl/2}\Gamma(ddl/2)} x^{ddl/2-1} e^{-x/2} dx \tag{3.19}$$

$$pmd = \int_0^T \frac{e^{-(x+c)/2}}{2^{ddl/2}} \sum_{i=0}^{+\infty} \frac{c^i x^{(i-1+ddl/2)}}{2^{2i} i! \Gamma(i + ddl/2)} dx \tag{3.20}$$

Afin de déterminer le paramètre de non-centralité c et le seuil T, nous avons besoin de fixer pfa et pmd. Cela revient à quantifier le risque que l'on prend en acceptant ou rejetant les hypothèses H0 ou H1 durant ce test.

3.6.1.2 Prise de risque durant le test

Lors d'un test statistique, nous prenons le risque de conclure de manière erronée. Nous pouvons rejeter $H0$ (et donc accepter $H1$) alors que $H0$ est vraie, on parle de faux positif. Ce risque est appelé risque de première espèce. À l'inverse, nous pouvons rejeter $H1$ (et donc accepter $H0$) alors que $H0$ est fausse, il s'agit d'un faux négatif. Ce risque est appelé risque de seconde espèce (1- β est

appelé puissance de test) (cf équation 3.21).

$$\begin{aligned} p(\text{résultat} = H0|\text{Vrai} = H0) = &\quad 1-\alpha \\ p(\text{résultat} = H1|\text{Vrai} = H1) = &\quad 1-\beta \end{aligned} \tag{3.21}$$

Dans notre contexte, le risque de première espèce correspond à la probabilité de fausse alarme (pfa) et le risque de seconde espèce à la probabilité de détection manquée (pmd) (cf équation 3.22).

$$\begin{aligned} p(\text{résultat} = H1|\text{Vrai} = H0) = &\quad \alpha = \quad pfa \\ p(\text{résultat} = H0|\text{Vrai} = H1) = &\quad \beta = \quad pmd \end{aligned} \tag{3.22}$$

Ces probabilités doivent être minimisées pour une détection plus performante (moins de faux positifs ou plus de vrais positifs). Cependant, en pratique, il n'est pas possible de minimiser les deux à la fois. En effet, en diminuant α, le risque β augmente. D'une manière générale, un statisticien recherchera le bon compromis entre les deux en commençant par minimiser α c'est à dire la probabilité de fausse alarme. Quantifier β est plus délicat car cela nécessite la connaissance de la distribution liée à $H1$. Or, pour un test de détection de pannes dans une application liée à la sécurité, il est plus important de minimiser β soit la probabilité de détection manquée. En termes de SdF, cela se réfère au compromis entre la sécurité et la disponibilité. Par conséquent, il faut accepter de prendre un seuil α plus large pour avoir le plus petit β possible. De plus, β décroît lorsque la taille de l'échantillon (nombre de mesures) augmente.

3.6.1.3 Seuil de décision

Pour définir un seuil (cf équation 3.23), une probabilité de fausse alarme doit être choisie en fonction du compromis que l'on est prêt à accepter.

$$NSSE < T = \chi^2_{ddl,(1-pfa)} \tag{3.23}$$

La figure 3.8 montre un seuil T déterminé pour un pfa donné. La différence entre le sommet de la distribution liée à $H0$ et celui de la distribution liée à $H1$ correspond au coefficient de non-centralité. Ce paramètre, c, permet le calcul de l'erreur de mesure minimale détectable par cette méthode de détection, P_{biais} (cf équation 3.24).

$$P_{biais} = \sigma\sqrt{c} \tag{3.24}$$

où, σ, écart-type des erreurs de mesures,
c, le paramètre de non-centralité dont la valeur est donnée par inversion de l'équation 3.20 sachant le seuil de détection T et la probabilité de fausse alarme connus.

Toutes les étapes du test statistique lié à la détection des biais instantanés ont été présentées. Cette détection a une faiblesse. Elle détecte trop tardivement les erreurs à croissance lente. Une solution existe mais suggère de changer de variable aléatoire lors du test statistique. Le déroulement de cette méthode de détection est présenté dans la sous-section suivante.

3.6.2 Détection des erreurs à croissance lente

Les erreurs à croissance lente sont typiques des systèmes inertiels non recalés par une source de localisation complémentaire. Elles sont reconnaissables à leur évolution en forme de rampe dont les

caractéristiques dépendent du biais initial et de la vitesse du véhicule. La figure 3.9 montre l'allure de ces erreurs ou plus exactement d'une variable de test associée à ces erreurs. Il est question, ici, de détecter au plus tôt ces erreurs à croissance lente afin d'anticiper l'instant où elles deviennent inacceptables. En effet, la méthode de détection classique est capable de détecter ces erreurs mais de manière très tardive (plusieurs minutes selon le degré de la pente de la rampe). Ceci n'est pas envisageable pour des applications liées à la sécurité où l'on cherche à avertir l'utilisateur au plus tôt de la présence d'une erreur de position, ici, une erreur à croissance lente d'une mesure de capteur.

Nous proposons d'utiliser une méthode de détection de SGE (pour *Slowly Growing Error*) qui s'appuie sur la différence entre deux variables, fonction de $NSSE$ [Ochieng et al., 2008]. Cette technique s'apparente à celle que nous avons employée pour la détection des biais instantanés à l'exception de la variable aléatoire qui ne dépend plus d'un seul vecteur de résidus mais de deux vecteurs choisis à des instants différents. Pour caractériser une droite relative à une rampe, deux points sont nécessaires. Le cas est identique pour les erreurs à croissance lente. Tenir compte des résidus à différents instants suppose donc de disposer d'un historique de tous les résidus calculés lors d'une mission afin de détecter les erreurs à croissance lente. Ce type de détection permet également de déterminer plusieurs évolutions de rampes. Pour cela, plusieurs tests statistiques peuvent être réalisés en fonction du nombre de vecteurs de résidus présents dans l'historique et de la puissance de calcul disponible à bord du véhicule.

3.6.2.1 Énoncé des hypothèses nulle et alternative

Les hypothèses $H0$ et $H1$ sont de même nature que pour les biais instantanés. En effet, il est toujours question de savoir si la variable aléatoire choisie suit une loi connue et centrée ($H0$) ou si elle suit cette même loi mais décentrée ($H1$). Le changement réside dans la variable considérée. En introduction à cette méthode, l'idée de choisir une statistique calculée à partir de la différence entre variables calculées en fonction de $NSSE$ a été abordée. Au même titre qu'il est nécessaire de connaitre au moins deux points d'une courbe pour déterminer sa dérivée en un point, il faut définir une variable aléatoire qui dépend de deux $NSSE$ de distributions liées à la loi du χ^2 pour déterminer une croissance des résidus de mesure (cf équation 3.25) dans un intervalle de temps Δt.

$$V_{test} = NSSE_t - NSSE_{t-\Delta t} \sim \chi^2_{ddl_B} - \chi^2_{ddl_A} \tag{3.25}$$

Par ailleurs, d'après une analyse sur la moyenne, la variance, le coefficient de dissymétrie (propriété de toute distribution déformée vers la droite ou la gauche) et le coefficient d'aplatissement des différentes distributions mises en jeu [Ochieng et al., 2008], il a été montré que la différence entre les distributions de $\sqrt{NSSE_t}$ et celle de $\sqrt{NSSE_{t-\Delta t}}$ peut être approximée par une loi normale de moyenne μ_D et de variance σ_D déterminées en fonction des caractéristiques des deux distributions. Si $NSSE$ suit une loi du χ^2 alors sa racine carrée suit une loi du χ. La figure 3.10 montre comment

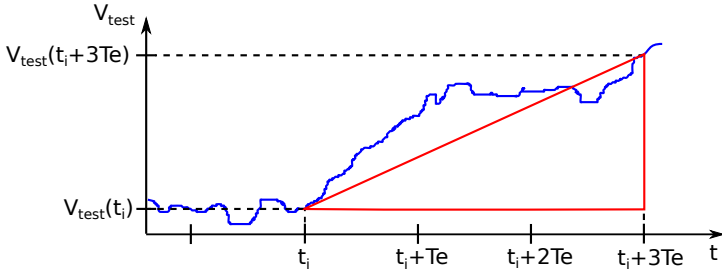


FIGURE 3.9 – Profil d'une erreur à croissance lente.

sont déterminées, à un instant t, les variables aléatoires notées $T_{\Delta t}$ dans un intervalle de temps Δt donné.

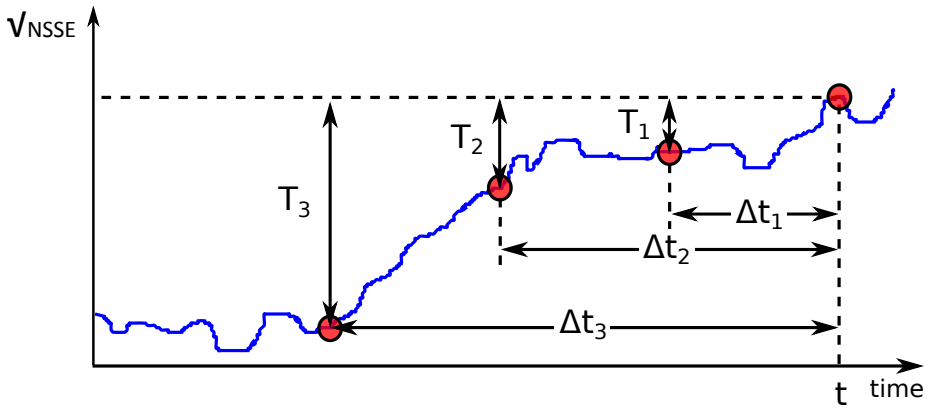


FIGURE 3.10 – Tests statistiques basés sur la différence entre $\sqrt{NSSE}$ avec différents intervalles de temps Δt_i.

Les hypothèses ainsi que la variable aléatoire choisies pour ce test sont exprimées dans les équations 3.26 et 3.27.

$$H0 \quad : \quad T_{\Delta t} \sim \chi_{ddl_B} - \chi_{ddl_A} = \sqrt{NSSE_t} - \sqrt{NSSE_{t-\Delta t}} \leq \mathcal{N}(0, \sigma_D) \tag{3.26}$$

$$H1 \quad : \quad T_{\Delta t} \sim \chi_{ddl_B} - \chi_{ddl_A} = \sqrt{NSSE_t} - \sqrt{NSSE_{t-\Delta t}} \leq \mathcal{N}(\mu_D, \sigma_D) \tag{3.27}$$

où, H_0 représente le comportement normal sans erreur à croissance lente du système de positionnement [5] ,
H_1 représente le comportement en présence d'une erreur à croissance lente,
ddl_A et ddl_B sont les degrés de liberté des deux distributions du χ notée A et B,
$\mu_D = \mu_d - \gamma_{1d}$, la moyenne de la différence entre les distributions A et B notée D,
$\mu_d = \mu_B - \mu_A$ est la moyenne théorique déterminée au travers de celles des deux lois du χ (A et B),
μ_A et μ_B sont les moyennes de A et B ($\mu = \frac{\sqrt{2}\Gamma(\frac{1}{2}(ddl+1))}{\Gamma(\frac{1}{2}ddl)}$),
$\Gamma(ddl)$ est la fonction Gamma de paramètre ddl,
$\gamma_{1d} = \frac{((\gamma_{1B})^{\frac{1}{3}} - (\gamma_{1A})^{\frac{1}{3}})\sigma_d}{2}$ est l'asymétrie globale (*skewness* en anglais) due à l'asymétrie de A et B (γ_{11} et γ_{12}),
$\gamma_1 = \frac{\mu}{\sigma^3}(1 - 2\sigma^2)$ est l'asymétrie d'une distribution du *chi*,
$\sigma_d^2 = \sigma_A^2 + \sigma_B^2$ est la variance de D,
$\sigma_{A,B}^2 = ddl_{A,B} - \mu^2$ est la variance de A ou B,
Δt, un intervalle de temps fonction d'un temps d'échantillonnage Te. Plusieurs $T_{\Delta t}$ peuvent être calculés en fonction des $NSSE$ disponibles dans l'historique. Ils seront à comparer en fonction de leurs seuils de décision respectifs décrits plus loin.

3.6.2.2 Prise de risque durant le test

De la même manière que pour les biais instantanés, les probabilités pfa et pmd (cf équation 3.22) permettent de quantifier les risques pris lors des tests statistiques. Toutefois, les particularités

5. La moyenne d'un résidu étant nulle en l'absence d'erreur [Le Marchand, 2010], la moyenne de la loi normale associée à $H0$ est nulle.

du test statistique fondé sur la différence entre $\sqrt{NSSE}$ poussent à considérer non seulement ces probabilités à un instant t mais également à des instants antérieurs pris pour le test. En choisissant, trois intervalles de temps Δt_1, Δt_2 et Δt_3, il faut considérer trois pfa, par exemple, $pfa(\Delta t_1)$, $pfa(\Delta t_2)$ et $pfa(\Delta t_3)$.

La méthode de détection des SGE que l'on utilise pour les erreurs à croissance lente est celle de [Ochieng et al., 2008]. Dans cet article, les trois probabilités $pfa(\Delta t_i)$ sont supposées être égales *i.e.* $pfa(\Delta t_1) = pfa(\Delta t_2) = pfa(\Delta t_3) = 1 \times 10^{-2}$. Le choix de prendre trois intervalles de temps permet non seulement de caractériser une erreur à croissance lente (un intervalle de temps suffit à détecter une erreur de ce type) mais aussi plusieurs types de rampe avec des coefficients directeurs différents. La sous-section suivante présentera le seuil de décision et explicitera les trois intervalles de temps choisis.

3.6.2.3 Seuil de décision

Il a été dit précédemment que si $NSSE$ suit une loi du χ^2, *a fortiori* $\sqrt{NSSE}$ suit une loi du χ. La différence de deux variables aléatoires suivant une loi du χ suit approximativement une loi normale. Cela permet de majorer $T_{\Delta t}$ (cf équation 3.28) comme étant une variable qui suit une loi normale de paramètres μ_D et σ_D. De la même manière que pour le test précédent, le seuil de décision est déterminé par une exigence en terme de probabilité de fausse alarme pfa.

$$T_{\Delta t} < seuil_{\Delta t} = \mathcal{N}(\mu_D, 1)_{1-pfa(\Delta t)} \tag{3.28}$$

On notera que, à la différence des biais instantanés, cette détection d'erreurs à croissance lente n'est pas seulement un test mais n (avec $n = \{1, 2, 3, ...\}$) tests réalisés de manière séquentielle où des couples ($T_{\Delta t}$, $seuil_{\Delta t}$) sont définis. De plus, pour avoir n tests différents, il faut donc n valeurs de pfa (cf équation 3.28). Cette multiplication de tests permet l'identification de plusieurs types de rampes correspondants à des évolutions plus ou moins rapides de ces erreurs (pour simplifier la lecture, nous proposons de remplacer $T_{\Delta t}$ et $seuil_{\Delta t}$ par T_i et $seuil_i$). Pour un cas avec trois tests successifs ($n = 3$), nous avons les scénarios suivants :

- si $T_3 > seuil_3$ tant que $T_2 < seuil_2$ et $T_1 < seuil_1$, une rampe à évolution dite "très lente" [6] est détectée,
- si $T_3 > seuil_3$ tant que $T_2 > seuil_2$ et $T_1 < seuil_1$, une rampe à évolution dite "lente" est détectée,
- si toutes les variables de tests ont franchi leurs seuils respectifs, une rampe à évolution dite "rapide" est détectée,
- si aucune des variables de tests n'ont franchi leurs seuils respectifs, il n'y a aucune détection.

Ceci représente les quatre cas définis dans la méthode originale [Ochieng et al., 2008]. Cependant, dans le cas précédent à trois tests successifs, nous avons 2^3 soit 8 scénarios possibles. Il manque donc les cas suivants :

1. Si $T_3 < seuil_3$ tant que $T_2 < seuil_2$ et $T_1 > seuil_1$,
2. Si $T_3 < seuil_3$ tant que $T_2 > seuil_2$ et $T_1 > seuil_1$,
3. Si $T_3 < seuil_3$ tant que $T_2 < seuil_2$ et $T_1 < seuil_1$,

6. Le chapitre 4 quantifiera les qualificatifs "très lent", "lent" et "rapide" (notamment dans le tableau 4.19) en fonction des simulations du système avec GNSS choisi.

4. Si $T_3 > seuil_3$ tant que $T_2 < seuil_2$ et $T_1 > seuil_1$.

Ces quatre cas considèrent que $\sqrt{NSSE}$ peut croître ou décroître durant les intervalles de temps Δt_i. Il faut donc définir, parmi ces quatre cas, quels sont les cas de détection d'erreur à croissance lente et les types de rampes. Prenons le dernier cas où $T_3 > seuil_3$ tant que $T_2 < seuil_2$ et $T_1 > seuil_1$ (ce cas est illustré par la figure 3.11). L'évolution de $\sqrt{NSSE}$ change entre $t - \Delta_{t3}$ et t. Les cas de détection et non-détection sont fixés grâce à l'état de T_1 uniquement. Cela signifie que les cas (1), (2) et (4) sont des cas de détection à évolution rapide ($T_1 > seuil_1$) et le cas (3) un cas de non-détection ($T_1 > seuil_1$) quel que soit l'état de T_2 et T_3.

De la même manière que le P_{biais} défini dans l'équation 3.24, il existe une erreur de mesure minimale détectable pour les erreurs à croissance lente que l'on note, P_{rampe} (cf équation 3.29).

$$P_{rampe} = \sigma\sqrt{\mu_D} \tag{3.29}$$

où, σ, écart-type des erreurs de mesures,
μ_D, définie dans la sous-section 3.6.2.1. μ_D est à l'image du paramètre de non-centralité c mais concerne la loi normale.

Les deux aspects de la détection des erreurs au sein d'un système GNSS/INS ont été présentés. La figure 3.12 représente une succession de biais instantanés (en rouge) et d'erreurs à croissance lentes (en noir). Elle illustre les différences d'allure des pentes entre ces 2 types d'erreurs.

La détection est la première étape dans le contrôle de l'intégrité de la solution de navigation fournie par ce système. La deuxième étape est l'atténuation des erreurs détectées en excluant la source défaillante. Dans ce chapitre, l'objectif n'est pas de concevoir une architecture robuste mais de conclure sur l'intégrité. Cette deuxième étape n'est pas nécessaire. Par contre, le contrôle d'intégrité doit répondre à la question "Est ce que la solution de navigation est suffisamment sûre pour être utilisée ?" lorsqu'il n'y a pas de détection. Cette réponse est apportée grâce au calcul du niveau de protection.

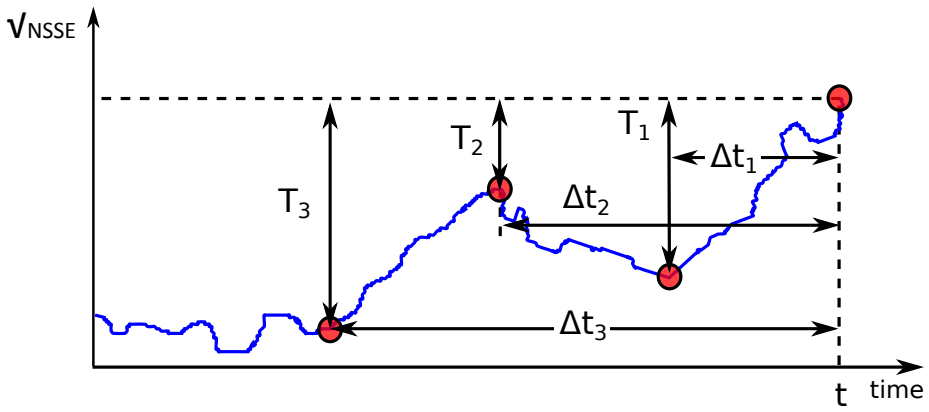


FIGURE 3.11 – Cas particulier où $T_3 > seuil_3$ tant que $T_2 < seuil_2$ et $T_1 > seuil_1$.

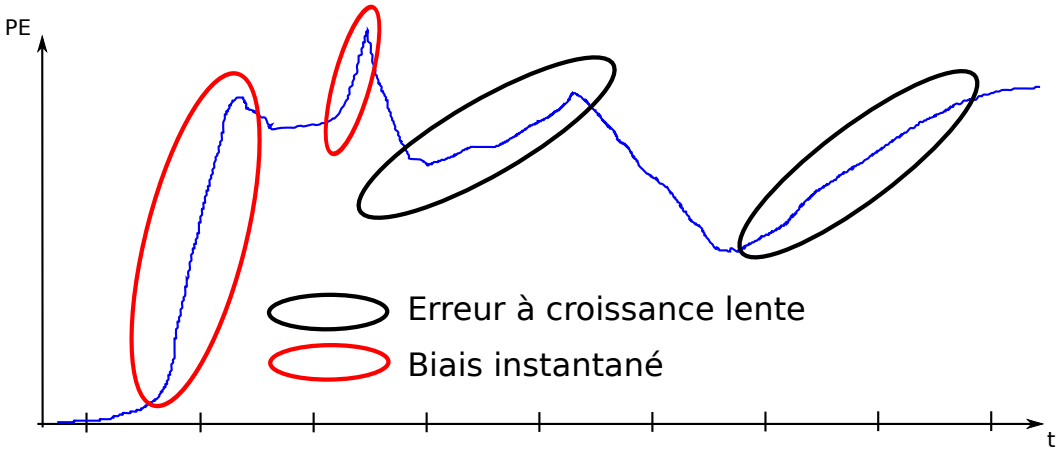


FIGURE 3.12 – Succession de biais instantanés et erreurs à croissance lentes

3.6.3 Calcul de niveaux de protection

Dans la sous-section 3.5.5, nous avons présenté les différents calculs possibles de PL selon des hypothèses sur l'impact de bruit de mesure. Nous nous plaçons dans le cas 3 où nous supposons que l'impact du bruit sur l'erreur de position est négligeable mais qu'il ne l'est pas sur les résidus. En effet, il est plus simple *a priori* de vérifier l'impact du bruit de mesure sur l'erreur de position que de vérifier l'impact du bruit de mesure sur les résidus. Si, au terme de l'exécution de l'algorithme de contrôle d'intégrité, PL ne borne pas de l'erreur de position PE, le calcul de PL du cas 4 où aucun impact n'est négligé sera à privilégier.

La connaissance de la matrice H entre dans le calcul des niveaux de protection PL_{GNSS} et PL_{INS} (cf équation 3.30) [Feng et al., 2005] [Le Marchand, 2010].

$$PL_{GNSS} = \max_j SLOPE_j \times P_{biais} \tag{3.30}$$

$$PL_{INS} = \max_j SLOPE_j \times P_{rampe} \cdot \max \Delta t \tag{3.31}$$

où, P_{biais} et P_{rampe}, sont respectivement l'erreur minimale détectable pour les biais instantanés (cf équation 3.24) et pour les erreurs à croissance lente (cf équation 3.29),
$\max \Delta t$, le plus grand des intervalles de temps utilisés lors de la détection des erreurs à croissance lente (Δt_3 dans le figure 3.10).

Dans la figure 3.13, les comportements des variables de tests sont représentés. La première courbe représente le comportement normal (Il s'agit de l'évolution des $NSSE$ en l'absence d'erreur). Les seuils de détection des tests du χ^2 (biais instantanés) et du test fondé sur la différence (erreurs à croissance lente) sont représentés par les lignes horizontales colorées. La seconde courbe représente le comportement en présence de multitrajets (assimilés à des biais instantanés) simulés à $t = 1000, 2000,$ 4000 et 5000 pour des durées allant de 100 à 500 secondes. La troisième est liée au comportement en présence d'une erreur à croissance lente à partir de la $525^{\text{ème}}$ seconde. Les $NSSE$, représentés sur la figure 3.13, permettent le calcul du P_{biais} lié aux biais instantanés (cf équation 3.24) et celui lié aux erreurs à croissance lente (cf équation 3.24). Ceux-ci permettent le calcul des niveaux de protection relatifs à chaque partie d'un système GNSS/INS.

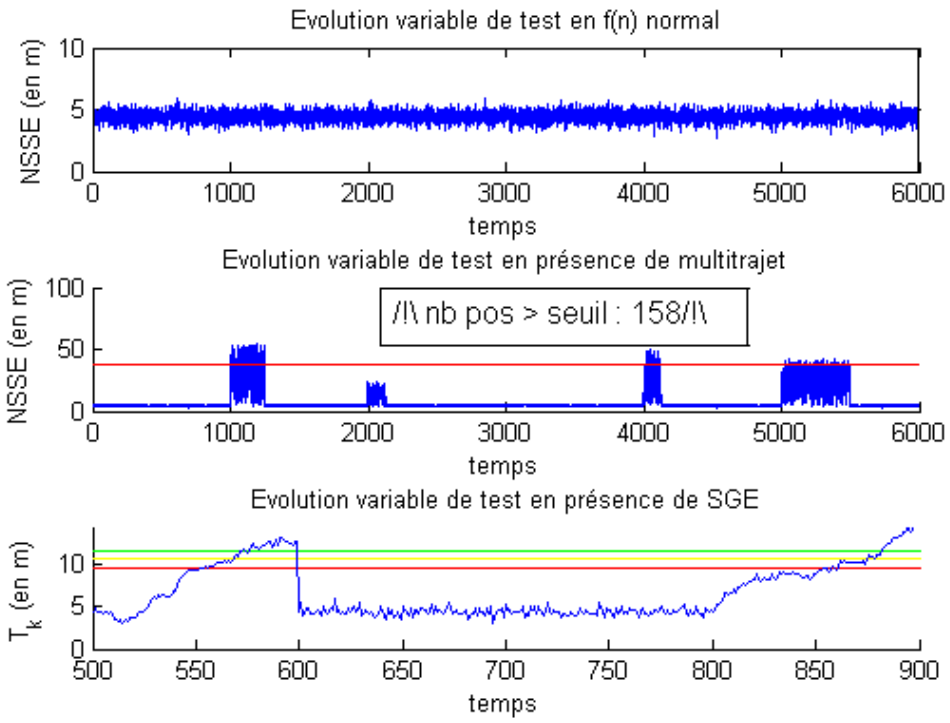


FIGURE 3.13 – Comportements attendus des résidus respectivement en temps normal, en présence de biais instantanés (= multitrajets) et en présence d'une erreur à croissance lente (en anglais, SGE pour *Slowly Growing Error*).

3.6.4 Conclusions sur l'algorithme et remarques

Les parties centrales de l'algorithme de contrôle d'intégrité (détection des biais instantanés, des erreurs à croissance lentes et du calcul de PL) ont été présentées. 2 PL sont obtenus : PL_{GNSS} et PL_{INS}. Par conséquent, il est proposé de prendre la valeur maximale de PL (cf équation 3.32 et tableau 3.4 ligne "Ensemble").

$$PL_{algo} = \max(PL_{GNSS}, PL_{INS}) \tag{3.32}$$

Tableau 3.4 – Exemple de calcul des niveaux de protection au sein d'un système GNSS/INS.

Partie du système	PL (en mètre)
GNSS	$15,60$
INS	$6,61$
Ensemble	$15,60$

Le risque sur l'intégrité étant la probabilité qu'une défaillance du système de positionnement se produise et que l'utilisateur n'en soit pas informé au bout d'un délai supérieur à un temps *Time To Alert*, il faut un échantillon suffisamment grand pour que son estimation soit pertinente.

Les erreurs minimales détectables (P_{biais}) sont exprimées en mètre ou en mètre par seconde selon l'erreur à détecter (biais ou rampe). Il n'est pas *a priori* pertinent de comparer ces deux valeurs puisque le phénomène à détecter n'est pas le même. La qualité de l'algorithme de détection pourra plutôt être évaluée.

L'algorithme d'intégrité est fondé sur un filtre de navigation (filtre de Kalman) sur une architecture en hybridation serrée. Ceci implique qu'il existe une relation étroite entre le filtre de Kalman et le contrôle d'intégrité (nécessité de données utilisées au sein du filtre). Par conséquent, une implémentation sur un système existant est complexe mais réaliste. Un filtre de Kalman est un processus informatique duquel il est possible d'extraire des informations si elles sont accessibles (code ouvert) notamment le vecteur de résidus.

3.7 Intégrité étendue pour évaluer la sécurité des systèmes avec GNSS

Le chapitre 2 a montré que l'utilisation des systèmes avec GNSS engendre un changement significatif dans un système de contrôle-commande ferroviaire. Par conséquent, leur intégration nécessite d'employer la Méthode de Sécurité Commune (MSC) réglementée dans le domaine ferroviaire. La première étape de la MSC est l'identification des dangers, *i.e.* les conditions (techniques/technologiques, opérationnelles, organisationnelles et humaines) pouvant mener à un accident. Ces travaux se sont concentrés sur l'aspect technologique et les causes principales de danger liées à l'application ont été identifiées. Le danger a été défini comme le fait d'obtenir une erreur de position dépassant une tolérance. Ces causes se rapportent, d'une part, aux phénomènes de multitrajet et de masquage (pour la partie GNSS) et, d'autre part, à la dérive des capteurs (pour la partie proprioceptive). Les biais instantanés et les erreurs à croissance lente, présentés dans le chapitre 3, caractérisent ces 2 causes de danger.

L'étape suivante de la MSC est d'appliquer un ou plusieurs principes d'acceptation du risque. Dans le chapitre 2, nous avons conclu que seule "l'estimation explicite du risque" est un principe compatible avec les systèmes fondés sur les GNSS. Cette estimation passe par la détermination quantitative de critères liés à la sécurité, ici les probabilités liées à ces deux causes de danger.

Dans le domaine ferroviaire, la sécurité est définie par l'absence de risque inacceptable et peut être caractérisée par une probabilité de défaillance liée à la sécurité $f_S(t)$ [EN 50126, 2000]. Il s'agit plus précisément d'une probabilité de défaillance dangereuse comme expliqué par la suite..

Dans le chapitre 1, nous avons vu que les performances de sécurité des GNSS s'expriment en terme d'intégrité, plus exactement en terme de risque sur l'intégrité. Le but de cette section est de formaliser le lien entre la sécurité et l'intégrité ou plus précisément entre le $f_S(t)$, définie dans les normes ferroviaires et le risque sur l'intégrité IR, défini pour les GNSS. Ce lien a déjà été abordé dans la littérature notamment dans [Beugin and Marais, 2008] [Filip et al., 2008a] et [Lu, 2014]. Nous allons le développer. Les algorithmes de contrôle d'intégrité constituent une barrière de sécurité pour maitriser le risque lié à l'application (par exemple, le risque d'une localisation incorrecte menant à un accident avec décès). Nous en avons proposé une dans la section précédente. Cette barrière n'est pas infaillible, elle est associée au risque IR. Pour déterminer IR, il faut exprimer le niveau de qualité de l'algorithme de contrôle d'intégrité proposé. Cette qualité est en fonction des

probabilités des différents cas de détection (détections vraies/fausses/manquées). Certaines de ces probabilités correspondent aux probabilités des causes de dangers ci-dessus. La section suivante les décrit.

3.7.1 Présentation des états dangereux considérés pour l'utilisation d'un système avec GNSS

Cette partie permet mettre en avant les différents modes de défaillance au sein d'un système de localisation avec GNSS. Ils sont représentés sur la figure 3.14. Pour chaque mode, nous exprimons les probabilités associées aux cas de détection en utilisant les concepts liés à l'intégrité.

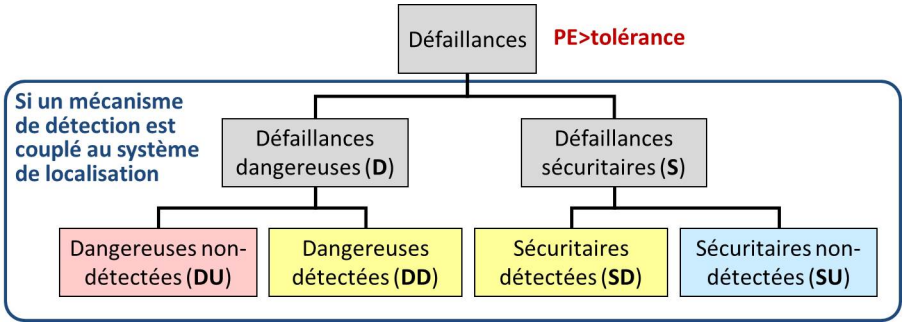


FIGURE 3.14 – Modes de défaillances d'un système de localisation

$f_S(t)$ se réfère à la défaillance dangereuse notée "D" sur l'arbre. La défaillance "l'erreur de position PE dépasse une tolérance" du système peut être décomposée en 4 modes de défaillance possibles : les défaillances **Sécuritaires non-détectées** (SU), **Sécuritaires détectées** (SD), **Dangereuses détectées** (DD) et **Dangereuses non-détectées** (DU).

Les états SD et SU se réfèrent à des défaillances non critiques c'est à dire qu'elles n'ont pas de conséquences majeures sur la sécurité du système. La détection ou non-détection n'a donc *a priori* pas d'importance. Cependant, l'état SU met en évidence un problème dans le processus de détection à ne pas négliger (ceci sera expliqué par la suite).

L'état DD est lié à des défaillances qui sont critiques pour la sécurité. Contrairement aux états SD et SU, la détection des défaillances dans l'état DD est primordiale pour que l'application puisse déclencher un repli en sécurité.

Pour l'état DU, les défaillances critiques associées à cet état ne sont pas détectées. Sans détection, aucune réaction de l'application ne peut intervenir (comme un freinage d'urgence du train). C'est une situation dangereuse qui a de forte probabilité de causer un accident comme une collision entre deux trains par exemple.

Nous avons présenté les différents états ou modes de défaillance d'un système avec GNSS incluant un contrôle d'intégrité. Nous pouvons maintenant détailler ces probabilités avec les concepts liés à l'intégrité. L'objectif est d'exprimer $f_S(t)$ en fonction de $IR(t)$. Cette mise en relation de ces deux probabilités se fait en 3 étapes :

— **Étape 1** : il est nécessaire d'exprimer les probabilités $PF_{SD}(t)$, $PF_{SU}(t)$, $PF_{DD}(t)$ et $PF_{DU}(t)$ (respectivement la probabilité de défaillances sécuritaires détectées, sécuritaires non-détectées, dangereuses détectées et dangereuses non-détectées) avec le niveau de protection PL, le niveau d'alerte AL et les tests statistiques du processus de détection.

— **Étape 2** : $f_S(t)$ doit être exprimée en fonction de $PF_{SD}(t)$, $PF_{SU}(t)$, $PF_{DD}(t)$ et $PF_{DU}(t)$.

— **Étape 3** : Toutes les probabilités citées précédemment sont instantanées. Or, IR est définie sur une durée TTA. La section 3.3 de ce chapitre a montré que le risque sur l'intégrité est critique si les défaillances critiques associées durent pendant TTA. Il faut donc tenir compte de cette durée dans la relation de $f_S(t)$ et de IR.

3.7.2 Mise en relation de l'intégrité et de la sécurité

Cette sous-section détaille les 3 étapes présentées précédemment.

3.7.2.1 Étape 1 : $PF_{SD}(t)$, $PF_{SU}(t)$, $PF_{DD}(t)$ et $PF_{DU}(t)$ exprimées en fonction des concepts d'intégrité (AL, PL et tests de détection)

Pour la première étape, la détection des biais instantanés et celle des erreurs à croissance lente sont notées respectivement $test_{biais}$ et $test_{rampe}$ afin de faciliter la lecture des équations qui suivent. Quand ces tests sont *positifs*, une erreur est détectée. Quand ils sont *négatifs*, aucune erreur n'est détectée. Concrètement, cela signifie que :

— $test_{biais}$ positif $\rightarrow NSSE > T$,
— $test_{rampe}$ positif $\rightarrow T_i > seuil_i$ avec $i = \{1, 2, 3\}$,
— $test_{biais}$ négatif $\rightarrow NSSE \leq T$ et
— $test_{rampe}$ négatif $\rightarrow T_i \leq seuil_i$ avec $i = \{1, 2, 3\}$.

Les variables $NSSE$, T, T_i et $seuil_i$ sont décrites dans la section 3.6.

Les 4 états présentés précédemment sont détaillés comme suit :

— **Sécuritaire détecté** : l'erreur de position PE reste en dessous du niveau d'alerte AL. Deux évènements peuvent se produire :

1. PL dépasse AL, ce qui signifie que PL est surdimensionné et nous sommes dans le cas d'une fausse alerte.
2. Les tests statistiques pour la détection des biais instantanés ou des erreurs à croissance lente sont positifs et ont correctement rempli le rôle de détection.

Cet état SD s'écrit alors selon l'équation 3.33.

$$SD = \text{"}PE < AL\text{"} \text{ ET } [\text{"}AL < PL\text{"} \text{ OU "}test_{biais} \text{ positif"} \text{ OU "}test_{rampe} \text{ positif"}] \quad (3.33)$$

— **Sécuritaire non détecté** : PE est toujours inférieur à AL donc n'a pas de conséquence sur la sécurité. Mais, PL est inférieur à PE. Cela signifie que PE est mal bornée par PL. Côté

détection, $test_{biais}$ et $test_{rampe}$ sont négatifs. Nous sommes en dessous de la sensibilité de la détection (cf équations 3.23 et 3.28). Cet état SU s'écrit alors selon l'équation 3.34.

$$SU = \text{"}PE < AL\text{" ET "}PL < PE\text{" ET "}test_{biais} \text{ négatif" ET "}test_{rampe} \text{ négatif"} \quad (3.34)$$

— **Dangereux détecté** : PE dépasse AL et une alarme est émise. L'alarme est émise soit parce que PL dépasse AL, soit parce que $test_{biais}$ ou $test_{rampe}$ sont positifs. Cet état DD s'écrit alors selon l'équation 3.35.

$$DD = \text{"}PE > AL\text{" ET ["}PL > AL\text{" OU "}test_{biais} \text{ positif" OU "}test_{rampe} \text{ positif"}] \quad (3.35)$$

— **Dangereux non détecté** : PE est supérieur à AL mais aucune alarme n'est émise parce que PL est inférieur à AL et que $test_{biais}$ et $test_{rampe}$ sont négatifs. Cet état DU s'écrit alors selon l'équation 3.36.

$$DU = \text{"}PE > AL\text{" ET "}PL < AL\text{" ET "}test_{biais} \text{ négatif" ET "}test_{rampe} \text{ négatif"} \quad (3.36)$$

Après cette première étape, il s'agit d'exprimer $f_s(t)$ en fonction des probabilités $PF_{SD}(t)$, $PF_{DD}(t)$, $PF_{DU}(t)$ et $PF_{SU}(t)$.

3.7.2.2 Étape 2 : $f_S(t)$ exprimée en fonction $PF_{SD}(t)$, $PF_{DD}(t)$, $PF_{DU}(t)$ et $PF_{SU}(t)$

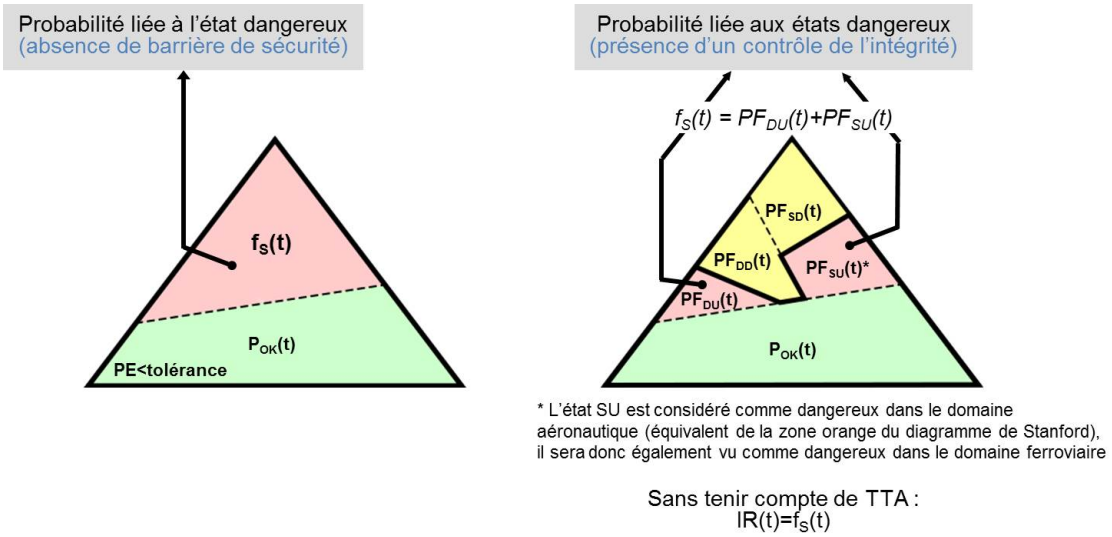


FIGURE 3.15 – Illustration par un diagramme de Venn de la probabilité de défaillance liée à la sécurité $f_S(t)$ inspiré de [Filip et al., 2008b]

Dans [Filip et al., 2008b], le risque sur l'intégrité est directement lié aux défaillances Dangereuses non-détectées. Or, selon [Roturier et al., 2001], les défaillances sécuritaires non-détectées constituent également un danger d'un point de vue aéronautique. L'état SU sera donc vu comme dangereux du point de vue ferroviaire (cf figure 3.15). $f_s(t)$ est donc la somme des probabilités de défaillances dangereuses non-détectées $PF_{DU}(t)$ et de défaillances sécuritaires non-détectées $PF_{SU}(t)$ (cf équation 3.37).

$$f_S(t) = PF_{DU}(t) + PF_{SU}(t) \quad (3.37)$$

3.7.2.3 Étape 3 : $f_S(t)$ exprimée en fonction IR

Enfin, la troisième étape consiste à exprimer $f_S(t)$ en fonction de IR. Comme vu précédemment, la différence entre ces probabilités réside dans l'intervalle de temps considéré. En effet, le délai TTA intervient dans le calcul de IR donc le lien entre l'intégrité et la sécurité sera en fonction de ce paramètre. Pour rappel, TTA est le temps maximal autorisé, écoulé depuis que le système de navigation est hors des limites de tolérance jusqu'à ce que l'équipement énonce l'alerte à l'utilisateur.

Pour une application ferroviaire, considérons un temps de réaction maximal qui permet d'assurer un repli en sécurité. Après ce temps noté $t_{marge\_sécu}$, on ne pourra pas garantir qu'un accident puisse être évité. Considérons également $A_{t_i}, A_{t_i+1}, ..., A_{t_i+t_{marge\_sécu}}$ les situations dangereuses respectivement aux temps t_i, t_i+1, ..., $t_i+t_{marge\_sécu}$. On peut noter que $A_{t_i} = \{SU_{t_i} \cup DU_{t_i}\}$ et $p(A_{ti}) = f_S(t)$. L'ensemble des événements successifs $\{A_{t_i}, A_{t_i+1}, ..., A_{t_i+t_{marge\_sécu}}\}$ constitue une situation critique en terme d'intégrité.

Ces situations critiques en terme d'intégrité, que nous détaillerons sur un cas applicatif dans le chapitre 4, peuvent s'écrire simplement par :

— Situation 1 : DU sur un intervalle de temps $t_{marge\_sécu}$ (fixé au chapitre 4),
— Situation 2 : SU sur $t_{marge\_sécu}$,
— Situation 3 : Succession DU et SU sur $t_{marge\_sécu}$.

Nous définissons un $IR_{étendu}(t_i)$ qui exprime le risque sur l'intégrité à l'instant t_i et qui tient compte des conditions menant aux états DU ou SU sur une période $t_{marge\_sécu}$. Le terme *étendu* désigne le fait que ces conditions à t_i sont étendues jusqu'à $t_i + t_{marge\_sécu}$. Avec un temps d'échantillonnage Te en secondes, $IR_{étendu}(t_i)$ peut être exprimée par l'équation 3.39.

$$\begin{aligned} IR_{étendu}(t_i) &= p(A_{t_i}, A_{t_i+1}, ..., A_{t_i+t_{marge\_sécu}}) \\ &= \prod_{j=i}^{i+int(\frac{i+t_{marge\_sécu}}{Te})} p(A_{t_j}) \\ &= \prod_{j=i}^{i+int(\frac{i+t_{marge\_sécu}}{Te})} f_S(t_j) \end{aligned} \tag{3.38}$$

La fonction $int(x)$ pour un nombre x quelconque est la partie entière de x. En effet, $t_{marge\_sécu}$ n'est pas nécessairement un multiple de Te.

Pour pouvoir conclure en terme de niveau de SIL pour un système avec GNSS, il convient d'estimer la fréquence de défaillance dangereuse par heure PFH issue de la norme [IEC 61508, 2010]. PFH permet d'allouer un niveau de SIL dans le cas d'un système à fortes sollicitations (cf tableau 2.1 dans le chapitre 1). C'est le cas de notre système de localisation.

$IR_{étendu}$ peut être estimé par la moyenne $IR_{étendu\_moy}$ sur une période donnée (Tm, temps de mission). Sur les chronogrammes de la figure 3.16, le "1" représente l'apparition de l'évènement associé. Toutefois, Tm n'est pas nécessairement un multiple de Te et Te peut être différent de 1. Le nombre total d'instants n'est donc plus égal à Tm mais à $int(\frac{Tm}{Te})$ (cf équation 3.39). La fonction $card(E)$ est la fonction qui retourne le cardinal d'un ensemble E.

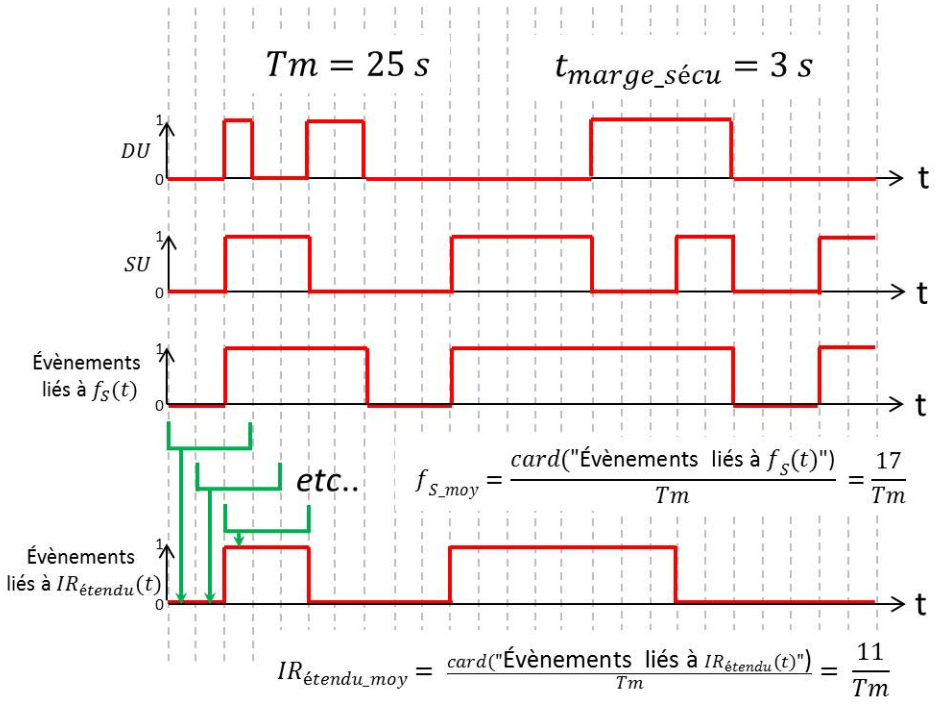


FIGURE 3.16 – Exemple simple du calcul de l'estimation de $IR_{étendu}$ en fonction de $f_S(t)$.

$$IR_{étendu\_moy} = \frac{card(\text{situation 1 OU situation 2 OU situation 3})}{int(\frac{Tm}{Te})} \tag{3.39}$$

PFH est une fréquence moyenne sur une heure. Par conséquent, l'équation 3.40 permet d'estimer PFH en fonction de $IR_{étendu\_moy}$ en considérant que Tm est exprimé en seconde et PFH est en h^{-1}.

$$PFH = \frac{IR_{étendu\_moy}}{3600 \cdot Tm} \tag{3.40}$$

Dans le cas où $IR_{étendu}(t_i)$ (cf équation 3.39) est connu et que l'on cherche à exprimer $f_S(t_i)$, il est possible d'inverser l'équation 3.39 (cf équation 3.41). C'est une notation retrouvée dans [Faurie, 2011] avec TTA utilisé à la place de $t_{marge\_sécu}$. Cependant, ceci n'est valable que si $f_S(t_i)$ est constant soit $f_S(t_i) = f_S$. Soit $a = int(\frac{t_{marge\_sécu}}{Te})$, alors :

$$f_S(t_i) = (IR_{étendu}(t_i))^{\frac{1}{a}} \tag{3.41}$$

Cette mise en relation permet d'exprimer le risque d'intégrité et les probabilités de défaillances dangereuses ($f_S(t)$ et PFH). Il est à présent possible d'évaluer quantitativement la sécurité en passant par l'intégrité (et inversement).

3.8 Conclusion

Dans ce chapitre, les concepts d'intégrité ont été présentés. Ils ont d'abord été introduits dans le domaine aéronautique puis explicités pour le domaine ferroviaire. Dans un premier temps, nous avons décrit les mécanismes de contrôle d'intégrité, qui visent à maintenir ce paramètre de performance des GNSS autour d'une valeur de risque d'intégrité tolérée, selon le contexte d'utilisation,

les moyens utilisés, les méthodes employées et le type *snapshot* ou récursif. Après avoir répertorié les algorithmes les plus connus, nous avons proposé un algorithme de contrôle d'intégrité pour un système avec GNSS en considérant la détection de deux types d'erreur : les biais instantanés pour la partie GNSS et les erreurs à croissance lente pour les capteurs proprioceptifs.

Dans un système multicapteurs, ces capteurs proprioceptifs sont souvent considérés comme exempts de pannes. La validité de leurs données proprioceptives est déjà garantie en amont. Dans des applications automobiles, telles que le système ADAS (*Advanced Driver Assistance Systems*), la panne d'une centrale inertielle n'est pas considérée [Le Marchand, 2010]. Cependant, cette hypothèse n'a jamais été discutée dans le domaine ferroviaire. Dans le système ferroviaire, les capteurs proprioceptifs comme l'odomètre, sont recalés lorsque le train passe sur une balise. Nous avons montré, dans le chapitre 1, que les GNSS pourraient avoir ce rôle et alléger ainsi l'équipement de l'infrastructure. Cependant, l'indisponibilité des solutions satellitaires et leur imprécision dans les environnements contraints restent des obstacles d'importance qui ne permettent pas toujours de garantir le recalage. Les solutions développées reposent donc sur des systèmes multicapteurs, bénéficiant ainsi de la complémentarité des capteurs embarqués.

Par conséquent, afin de se rapprocher d'un cas applicatif, nous avons considéré un algorithme de contrôle d'intégrité applicable à un système composé d'un récepteur GNSS et d'un autre système proprioceptif comme l'INS. Cet algorithme considère les erreurs générées par la partie GNSS (biais instantanés) mais également par la partie proprioceptive (erreurs à croissance lente). Ces algorithmes existent déjà dans le domaine aéronautique et ils sont de plus en plus courants dans les domaines automobile et ferroviaire. Les erreurs à croissance lente sont de type rampe en cas de recalage non fréquent dont le profil peut être détecté au plus tôt par un test statistique particulier [Ochieng et al., 2008]. Ce test particulier, conçu initialement pour des SGEs sur les données GNSS, est adapté pour les données proprioceptives. La détection des erreurs n'est pas l'unique étape du contrôle d'intégrité. Le calcul d'un niveau de protection est indispensable. Différents calculs de PL sont proposés dans ce chapitre selon les hypothèses sur l'impact des bruits de mesure sur l'erreur de position et sur les résidus. Nous avons retenu l'hypothèse que l'impact des bruits de mesure sur l'erreur de position est négligeable par rapport au résidus. Ce choix est expliqué dans le sous-section 3.6.3.

L'objectif de la thèse étant d'apporter un moyen pour évaluer la sécurité des systèmes de localisation, nous avons proposé une passerelle entre le concept d'intégrité et celui de la sécurité. Leurs définitions sont très proches puisqu'elles font référence à un risque inacceptable. Ce risque est associé au danger suivant : "l'utilisateur n'est pas prévenu de l'occurrence d'une erreur dépassant un seuil maximal toléré". Cette passerelle est présentée de manière à évaluer la sécurité d'un système fondé sur les GNSS au travers de l'intégrité de celui-ci, intégrité étendue aux systèmes avec GNSS. La probabilité liée au risque sur l'intégrité IR est mise en relation avec les probabilités de défaillances dangereuses $f_S(t)$ et PFH. PFH nous permet d'allouer un niveau de SIL défini dans la norme générique [IEC 61508, 2010] valable quel que soit le secteur industriel.

Le chapitre suivant propose d'évaluer quantitativement, avec la méthode développée dans ce chapitre 3, la sécurité d'un exemple de système GNSS/INS grâce notamment à des données GNSS réelles issues de compagnes expérimentales sur automobile [Ortiz, 2012] et des données inertielles simulées.

Chapitre 4

Cas d'étude : détermination de la sécurité d'un système ferroviaire GNSS/INS au travers de l'intégrité de la localisation

Sommaire

4.1 Introduction

Dans le chapitre précédent, nous nous sommes concentrés sur l'intégrité de la localisation fournie par un système fondé sur les GNSS pour évaluer quantitativement la sécurité de ce type de système. La relation entre l'intégrité de la localisation, attribut de performances des GNSS, et l'attribut de

sécurité utilisé pour caractériser les équipements ferroviaires a été explicitée. Il s'agit, plus précisément, de la relation qui existe entre la probabilité de risque sur l'intégrité et la probabilité de défaillance dangereuse liée à la sécurité.

Dans ce quatrième chapitre, nous appliquons les principes d'évaluation exposés au chapitre 3 sur un système particulier. L'architecture choisie repose sur la combinaison des deux techniques les plus utilisées en navigation : la localisation à l'estime et le positionnement par satellite. Le mécanisme de contrôle d'intégrité proposé est appliqué sur une architecture GNSS/INS en hybridation serrée (avec quelques adaptations qui seront expliquées). Les résultats d'évaluation s'appuient, plus précisément, sur la détection des biais instantanés induits par le phénomène de multitrajet des signaux GNSS et la détection des erreurs variant lentement liées à l'INS (en anglais *Slowly Growing Errors*).

Dans la première section de ce chapitre, nous proposons des recommandations sur des valeurs d'exigences liées à l'intégrité de la localisation dans une application de contrôle-commande et de signalisation ferroviaire. Un cas d'utilisation particulier du système européen ERTMS est choisi en s'appuyant sur les SRS (*System Requirements Specification*) : la gestion de l'espacement entre deux trains. ERTMS permet, en effet, une utilisation des GNSS dans le cadre de son dernier niveau d'intégration : le niveau 3.

La seconde section présente les résultats, d'une part, de la détection des biais instantanés et des erreurs à croissance lente et, d'autre part, de la détermination de l'intégrité de la localisation. Il s'agit de déterminer l'intégrité et, plus précisément, le risque sur l'intégrité lié à l'occurrence du risque que "l'erreur de position PE dépasse une limite d'alerte AL sans être détectée après un temps d'alerte TTA". Le sous-système bord d'ERTMS s'appuie sur la position délivrée par l'équipement de localisation. Cette position est entachée d'erreurs. La probabilité liée à la sécurité $f_S(t)$ (qui fait partie des paramètres caractérisant la sécurité ferroviaire, cf [EN 50126, 2000] et annexe A) sera évaluée grâce à la probabilité de risque sur l'intégrité IR. La probabilité de défaillance par heure (PFH) (cf norme générique [IEC 61508, 2010]) est aussi intéressante à évaluer car elle mène à un niveau d'intégrité de sécurité (SIL) pour le système de localisation choisi.

Enfin, nous terminons ce chapitre en proposant des perspectives d'amélioration de l'architecture (redondance, systèmes d'augmentation satellitaires, algorithmes de contrôle d'intégrité plus sophistiqués, *etc.*.) au regard des résultats afin de garantir une meilleure intégrité et, *a fortiori*, une meilleure sécurité pour une application de contrôle-commande ferroviaire.

4.2 Justifications des exigences sur l'intégrité de la localisation pour ERTMS

Dans le chapitre 3, nous avons exprimé des réserves sur les recommandations du *GNSS-Rail User Forum* notamment sur les valeurs de TTA et AL. En effet, en comparant ces valeurs avec les exigences sur l'intégrité en aéronautique lors de la phase d'approche précise (cf tableau 3.1), les valeurs proposées par le *GNSS-Rail User Forum* [Barbu, 2000] (un TTA inférieur à une seconde et un AL compris entre 2,5 et 50 mètres selon la densité de trafic (cf tableau 3.2)) paraissent difficiles à atteindre compte tenu de la différence de vitesse entre un train et un aéronef. La phase d'approche précise d'un aéronef, application la plus critique en terme d'intégrité, requiert un TTA égal à 6 secondes, un HAL égal à 40 mètres et un VAL compris entre 10 et 15 mètres. Nous proposons d'uti-

liser des valeurs adaptées au cas d'utilisation choisi : la gestion de l'espacement entre deux trains dans ERTMS. Ce cas d'utilisation est présenté dans la sous-section suivante.

4.2.1 Cas d'utilisation ERTMS : la gestion de l'espacement entre trains

À l'heure actuelle, un ensemble d'équipements répartis sur les trains (sous-système bord) et les voies (sous-système sol) permet le contrôle et la commande des trains tout en assurant la sécurité des circulations. Cette fonction de contrôle-commande des trains s'appuie nécessairement sur la localisation de chacun des véhicules pour gérer, en particulier, l'espacement entre les trains.

Nous nous plaçons dans le niveau 3 d'intégration du système de contrôle-commande d'ERTMS. Dans ce niveau 3, l'occupation des voies en sécurité n'est plus réalisé à l'aide de cantons de tailles fixes mais de tailles variables définis autour de la position du train. Ces cantons mobiles sont déterminés par le train lui-même en fonction d'informations transmises depuis le sous-système sol. Au sol sont calculés : le point cible et la vitesse cible du train à partir de la position que le train aura communiquée au préalable et, à partir également, des positions des autres trains. Le message d'autorisation de mouvement (MA) contient ces données cibles. Il est transmis entre un RBC (*Radio Block Center*) au sol et le train. La MA est mise à jour au fur et à mesure du parcours du train.

La **sécurité** de la gestion de l'espacement entre trains repose donc en priorité sur la localisation sûre des trains. Si le système fournit une localisation **respectant les exigences** (erreur de position $<$ tolérance), il n'y aura pas de problème de sécurité dans le cas limite de gestion d'espacement suivant : si le train 1 est à l'arrêt pour des conditions inconnues, la MA envoyée au train 2 qui le suit pourra être mise à jour en conséquence pour que celui-ci puisse freiner au plus tard dès que la distance train 1 / train 2 est égale à la distance de freinage du train 2 (comme expliqué par la suite, celle-ci doit tenir compte de la distance parcourue par le train 2 durant les transmissions de messages du train 1 vers le RBC et du RBC vers le train 2). Si l'erreur de position de l'un des trains dépasse le seuil de tolérance, il y a un **risque** de collision qui doit être maîtrisé.

Pour **maitriser ce risque**, il convient de réduire l'occurrence du danger associé à l'aide d'une **barrière de sécurité**. Une fonction de détection du franchissement de l'erreur de position dépassant une tolérance associée au système constitue cette barrière de sécurité contrant le danger. En effet, si l'utilisateur est averti du danger existant (danger détecté), l'application ferroviaire réagira en conséquence (avec un freinage d'urgence du train 2 dans l'exemple).

Un laps de temps peut s'écouler avant que les conditions d'éloignement entre les 2 trains deviennent non sécuritaires. Ce temps $t_{marge\_sécu}$ est représenté sur la figure 4.1 ainsi que les deux types de situations critiques et non critiques pour la sécurité et leurs conséquences associées. Les situations critiques ont été détaillées dans la section 3.7 du chapitre 3 en fonction de différents cas de détection d'erreur de localisation. Nous avons vu que ces situations critiques sont liées à des défaillances dangereuses et sécuritaires non-détectées (respectivement les états DU et SU) qui se succèdent sur une période liée à l'application. Sans détection sur cette période $t_{marge\_sécu}$, aucune réaction de l'application ne peut intervenir. Il est donc nécessaire d'évaluer l'occurrence de ces situations critiques et de voir si elle est suffisamment faible pour répondre aux exigences liées au risque sur l'intégrité IR. Dans la section 4.4, nous notons respectivement S1 et S2 ces situations menant à des défaillances dangereuses et sécuritaires non détectées et qui perdurent jusqu'à $t_{marge\_sécu}$. La situation S3 est la succession des deux premières situations jusqu'à $t_{marge\_sécu}$. Pour information,

les situations S4 à S6 sont relatives aux situations non critiques liées aux états DD et SD vus au chapitre 3.

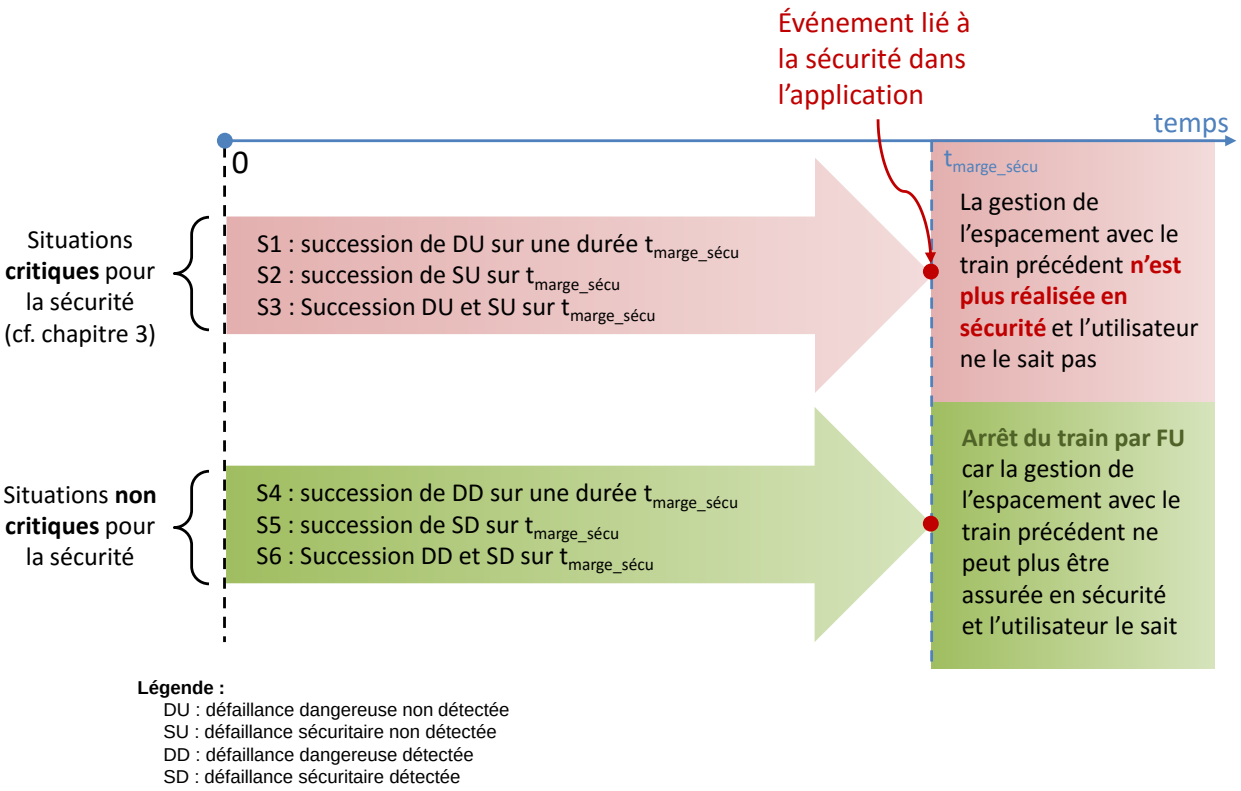


FIGURE 4.1 – Situations liées à la sécurité au regard de l'intégrité de la localisation

La barrière de sécurité doit être dimensionnée de telle sorte qu'elle permette la réduction de l'occurrence des situations critiques de manière à ce qu'elle devienne acceptable (le risque ne pouvant pas être éliminé complètement). Nous avons montré au chapitre 3 que la barrière de sécurité nécessite de quantifier le niveau d'alerte AL pour définir la tolérance sur l'erreur de position, le TTA et le risque d'intégrité IR. Nous verrons par la suite que le TTA est dimensionné en fonction de la distance "minimale" de sécurité entre 2 trains comme c'est le cas pour le temps $t_{marge\_sécu}$.

4.2.2 Dimensionnement de la limite d'alerte AL

Pour affirmer qu'une position est inacceptable en terme d'intégrité de localisation, il convient de dimensionner AL pour pouvoir comparer AL avec l'erreur de position PE. Pour cela, nous nous appuyons sur les exigences d'ERTMS [SUBSET-041, 2015]. Ces exigences définissent la précision attendue de la position mesurée à bord (cf figure 4.2) compte tenu du recalage régulier du sous-système bord au passage de balises. L'erreur maximale permise est bornée par un intervalle de confiance de

$\pm(5+5\%\ d)$ [1] mètres autour de la tête du train (d est la distance parcourue depuis le dernier passage du train sur un groupe de balises [2]). Cette exigence de performance inclut la détection manquée d'un groupe de balises. Cet intervalle de confiance augmente avec la distance parcourue (à hauteur de 5% maximum). Les SRS d'ERTMS considèrent les erreurs de positionnement ferroviaire comme étant cumulatives. AL peut constituer une marge de sécurité sur la position d'un train pendant laquelle le système de contrôle-commande peut réagir afin d'éviter une collision.

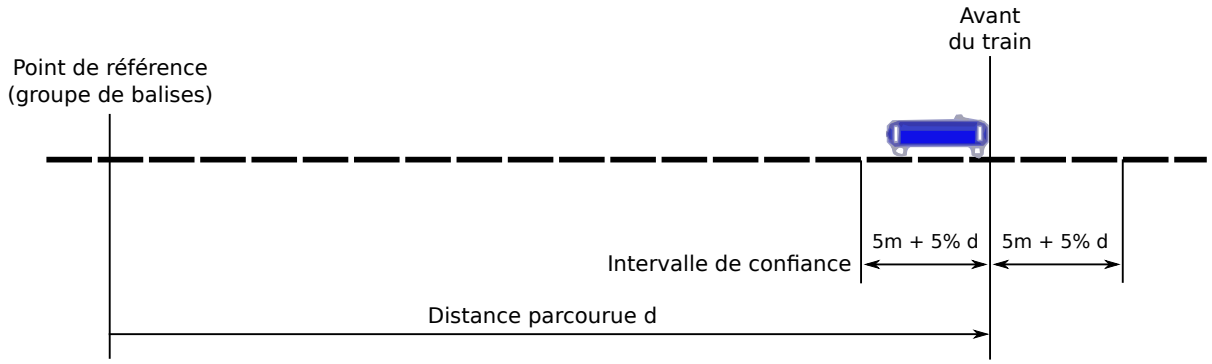


FIGURE 4.2 – Extrait du Subset-041 concernant la précision de la position à bord.

Il n'existe pas de valeur pour AL dans les SRS d'ERTMS. De plus, les erreurs de positionnement prévues dans les SRS sont liées à l'odométrie uniquement. Or, le système de localisation choisi dans la thèse est un système de positionnement GNSS/INS. Dans notre cas d'utilisation pour la gestion de l'espacement entre trains, AL est déterminée en fonction de la distance entre deux trains et des erreurs INS et GNSS. L'odomètre et l'INS sont des dispositifs proprioceptifs soumis à des erreurs cumulatives. Par conséquent, nous prenons $\pm(5 + 5\%\ d)$ comme étant la contribution de l'INS sur l'erreur de position soit, dans le cas de deux trains, $\pm(10 + 10\%\ d)$. Il reste à fixer la contribution de l'erreur GNSS. Dans [Zimmermann and Hommel, 2005], une erreur de position de 20 mètres est liée aux erreurs de localisation du train 1. Cette valeur de 20 mètres est pertinente pour AL pour notre cas d'utilisation. Elle laisse une marge d'erreur de 10 mètres supplémentaires pour la contribution des erreurs des récepteurs GNSS de chaque train. À titre d'information, cette valeur de 10 mètres pour la localisation d'un train se retrouve dans un autre système de contrôle-commande, le CBTC (pour *Communication Based Train Control*) [Rail Transit Vehicle Interface Standards Committee, 2004] pour le contrôle automatique des métros notamment.

AL ainsi fixé, la figure 4.3 montre, pour information, les intervalles qui constituent la distance minimale de sécurité entre deux trains notée s. Pour éviter la collision de l'avant du train 2 avec l'arrière du train 1, ces intervalles sont les suivants :

— la longueur du train 1 notée L,

— la distance de freinage du train 2 lors d'un freinage d'urgence. C'est une distance incompressible (3212 mètres). Elle tient compte des performances des freins ainsi que d'une marge de

1. Dans les SRS, la distance parcourue est notée s. Pour éviter toute ambiguïté avec le s de la figure 4.3, la notation d est privilégiée

2. Typiquement, un groupe est constitué de deux balises (Eurobalise), une balise fixe qui envoie un message de positionnement uniquement et une balise dite "switch" qui envoie des informations sur l'état de la circulation du trafic. Les niveaux d'intégration les plus élevés d'ERTMS (à partir du niveau 2) n'ont besoin que de la balise fixe.

sécurité liée aux courbes de freinage [Hougardy et al., 2012],

— une distance tampon qui tient compte de l'obsolescence des positions des trains 1 et 2 liée à des délais de transmission d'informations entre trains et RBC et à des délais de traitement à bord et au sol. En effet, une position est une valeur figée envoyée par un train à un instant t qui, à son arrivée au RBC après un délai δt, n'est potentiellement plus la position de ce train à l'instant $t + \delta t$, le train ayant *a priori* continué son parcours. L'autorisation de mouvement (MA) pour ce train est obtenue après un délai de traitement de la position (obsolète) par les équipements au sol. Une MA contenant une position cible "biaisée" est alors transmise. La distance tampon considérée ici tient compte de délais de traitement et de transmission de rapports de position (PR) et de messages d'autorisations de mouvement (MA) transitant entre un RBC et 2 trains qui se suivent. Le cumul de ces délais est évalué au plus à 18 secondes d'obsolescence dans [Zimmermann and Hommel, 2005], le pire des cas. Ceci correspond à une distance tampon de 1500 mètres avec une vitesse maximale du train fixée à 300 km/h. Cette distance est considérée comme incompressible puisque la question des performances des systèmes de communication et des calculateurs embarqués n'est pas abordée dans cette thèse.

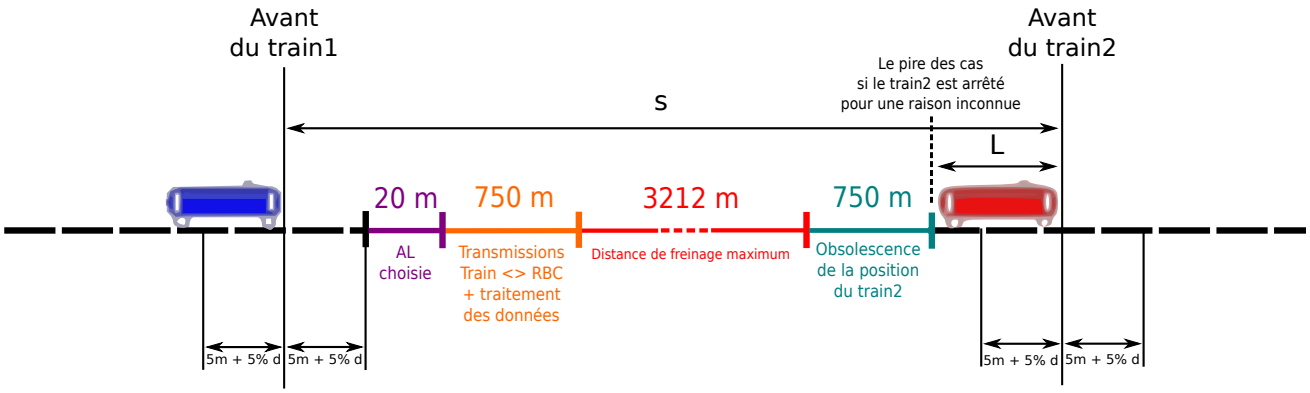


FIGURE 4.3 – Prise en compte de AL dans la gestion de l'espacement entre trains.

À présent que AL est dimensionné, il est nécessaire de fixer l'objectif temporel d'intégrité, TTA.

4.2.3 Dimensionnement du temps d'alerte TTA

Le niveau d'alerte AL ne suffit pas à caractériser entièrement un risque sur l'intégrité. En effet, il convient de dimensionner le temps d'alerte, TTA. Il peut également être déterminé selon le cas d'utilisation grâce aux spécifications de ERTMS/ETCS. La position du train est incluse dans PR et est utilisée pour déterminer des MA. Les informations échangées se présentent sous la forme d'entités de transmission appelées paquets. Le rapport de position correspond au paquet n°0 [SUBSET-041, 2015]. Un des paramètres intéressants pour quantifier TTA est la fréquence d'envoi des rapports de position illustrée par la figure 4.4. Cette fréquence est réglée dans le paquet n°58 dont le contenu est détaillé dans le tableau 4.1.

Les versions actuelles des SRS (version 3.4.0) ne proposent pas de valeurs pour les variables du tableau 4.1. Toutefois, leur longueur (espace de stockage mémoire) et des valeurs particulières sont réservées dans le système ERTMS/ETCS. C'est à l'exploitant de fixer ses propres valeurs. Le

Tableau 4.1 – Extrait des spécifications ERTMS de ERTMS/ETCS [SUBSET-026-7, 2014] concernant les paramètres liés au rapport de position

Description	Le paquet 58 est destiné à spécifier quand et à quelle fréquence la position doit être signalée	
Transmis par	RBC	
Variable	**Longueur (en bits)**	**Commentaire**
NID_PACKET	8	Identifiant du paquet
Q_DIR	2	Qualificatif pour indiquer le sens des données transmises
L_PACKET	13	Longueur du paquet
Q_SCALE	2	Échelle des distances
T_CYCLOC	8	Intervalle de temps entre deux rapports de position envoyés par le train
D_CYCLOC	15	Distance entre deux rapports de position en fonction de Q_SCALE
M_LOC	3	Variable spécifiant à quel moment ou endroit le train doit signaler sa position
N_ITER	5	Nombre d'itérations d'un ensemble de données dans un paquet
D_LOC(k)	15	Distance incrémentale entre les endroits où le train doit signaler sa position.
Q_LGTLOC(k)	1	Ce qualificatif indique si le train doit signaler sa position au moment où l'extrémité avant (ou arrière) du train passe sur l'emplacement défini par D_LOC

document [SUBSET-041, 2015] donne des recommandations pour certains délais. Par exemple, le délai associé au fait que la position d'un train doit être connue 1 seconde avant que le train envoie un rapport de position est important. Il permet de minimiser la propagation d'une erreur dans le prochain rapport de position. Une valeur de 5 secondes (retenue par [Zimmermann and Hommel, 2005] notamment) a été trouvée dans la version 2.1.0 (2012) du SUBSET-041 pour T_CYCLOC et supprimée dans sa dernière version 3.1.0 (2015) pour une raison inconnue au moment de la rédaction de ce mémoire. Ces 5 secondes seront toutefois conservées par la suite. Nous tenons compte également du délai d'1 seconde avant l'envoi d'un nouveau rapport de position. Nous en déduisons qu'un TTA doit être inférieur à 4 secondes (cf figure 4.4).

Dans cette figure, nous avons indiqué les instants d'émission des rapports de position par le train et de réception d'une autorisation de mouvement (MA) envoyée par le RBC. Ces émissions/réceptions ne sont pas systématiques : PR n'est envoyé que s'il est demandé par le RBC. La fréquence d'émission

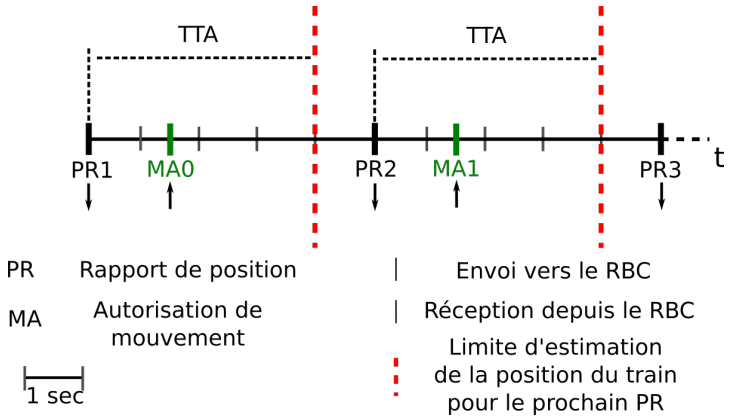


FIGURE 4.4 – Illustration du choix pour TTA par rapport à la fréquence d'envoi de rapports de position (PR) et la réception d'autorisations de mouvement associées (MA)

des MA évolue en fonction de la position et vitesse cible du train et celle des PR est fonction des paramètres réglés dans le paquet décrit dans le tableau 4.1 notamment la variable M_LOC. Cette variable, codée sur 3 bits, peut être réglée de manière à ce que le rapport de position soit envoyé à tout moment sur demande du RBC (000), à chaque passage sur un groupe de balises (001) ou non (010). Dans notre cas d'utilisation, le GNSS remplace les balises qui ne sont donc plus considérées ici. Par conséquent, nous supposons cette variable réglée sur 000 ou 010 pour qu'il n'y ait aucune action au passage sur le groupe de balise. Il reste à présent à quantifier l'objectif probabiliste de l'intégrité de la localisation c'est à dire le risque sur l'intégrité maximal à tolérer.

4.2.4 Exigence sur le risque d'intégrité de la localisation IR

Le *GNSS-Rail User Group* [Barbu, 2000] a indiqué uniquement des recommandations pour AL et TTA (cf section 3.4 du chapitre 3). Pour choisir un objectif de risque sur l'intégrité, nous utilisons la valeur de $2 \times 10^{-7}/150$ secondes proposée dans [Filip et al., 2008b] soit $4{,}8 \times 10^{-6}$ sur un intervalle de temps d'une heure. Il s'agit d'un objectif de risque sur l'intégrité inspiré des exigences aéronautiques de risque sur l'intégrité concernant la phase d'approche précise (cf Tableau 3.1). Le risque atteint par notre application sera déterminé dans la sous-section 4.4.4. La figure 4.5 montre que le risque d'intégrité est lié à une défaillance dangereuse non détectée avec un taux de défaillance $\lambda_{DU} = 4,8 \times 10^{-6}/h$. Cette défaillance dangereuse pour le système de localisation est l'évènement relatif à une erreur de position PE (bornée par PL) inacceptable et non détectée. Dans le chapitre 3, nous avons considéré que les défaillances sécuritaires non détectées sont incluses dans l'estimation de IR. Il n'existe pas de valeur pour un taux de défaillances sécuritaires non détectées. Par conséquent, nous conservons la valeur de $4,8 \times 10^{-6}/h$ pour les états DU et SU.

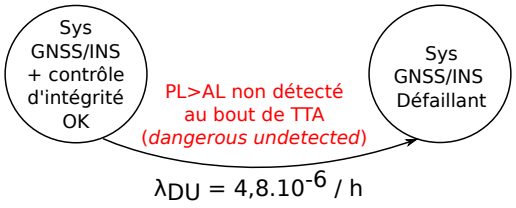


FIGURE 4.5 – Exigence sur IR inspirée de [Filip et al., 2008b].

Tableau 4.2 – SIL définis par la norme [IEC 61508-4, 2010] et la correspondance avec PFH.

Niveaux d'intégrité de sécurité	Probabilité de défaillance dangereuse par heure (PFH)
SIL 4	$10^{-9} \leq PFH \leq 10^{-8}$
SIL 3	$10^{-8} \leq PFH \leq 10^{-7}$
SIL 2	$10^{-7} \leq PFH \leq 10^{-6}$
SIL 1	$10^{-6} \leq PFH \leq 10^{-5}$

À présent que le triplet d'exigence sur l'intégrité (AL, TTA, IR) est fixé, la partie suivante présente les simulations relatives au système GNSS/INS et le contrôle de l'intégrité proposé dans ce travail.

4.3 Simulation de l'architecture GNSS/INS à base de données réelles

4.3.1 Description de l'architecture

L'architecture choisie est illustrée figure 4.6. Elle s'inspire du schéma de Groves [Groves, 2013] auquel le contrôle d'intégrité proposé dans le chapitre 3 est ajouté. Cette architecture se compose d'un récepteur GNSS associé à une centrale inertielle INS composée d'une partie capteur IMU (*Inertial Measurement Unit*) et d'une partie logicielle. L'hybridation choisie est une hybridation serrée (cf sous-section 1.3.4.1 du chapitre 1 présentant les différents types d'hybridation). Le choix d'une hybridation serrée est argumenté au chapitre 3. La fusion des données GNSS (les pseudodistances) avec les données inertielles (issues de la résolution des équations inertielles) est assurée par un filtre de Kalman étendu. Ce dernier fournit une seule et unique solution de navigation à partir des informations fournies par le récepteur GNSS et l'INS. Les flèches en pointillé matérialisent l'aide apportée par la solution de navigation INS et le filtre de Kalman dans le calcul des pseudodistances. Cette aide intervient dans la phase d'acquisition des signaux en réduisant l'espace de recherche lors de la synchronisation des signaux GNSS avec le récepteur. Ce soutien est surtout utile lors des traversées des zones à faible réception GNSS.

Dans le cas d'un filtre de Kalman, comme développé dans l'annexe B, le système est décrit par un vecteur d'état, une équation d'évolution et une équation de mesure. Le vecteur d'état choisi (cf équation 4.1) est

$$x = [x_{INS}\ x_{GNSS}]^T. \tag{4.1}$$

$$\tag{4.2}$$

Dans le domaine discret, x_k et z_k sont le vecteur d'état et le vecteur d'observations à l'instant k. L'équation d'évolution et l'équation de mesure s'écrivent alors :

$$x_k = F_{k-1}.x_{k-1} + w_{s,k-1} \tag{4.3}$$

$$z_k = H_k.x_k + w_{m,k} \tag{4.4}$$

où,
$x_{INS} = [\delta\psi\ \delta v\ \delta r\ b_a\ b_g]^T$,
$x_{GNSS} = [\delta\rho\ \delta\dot{\rho}]^T$.

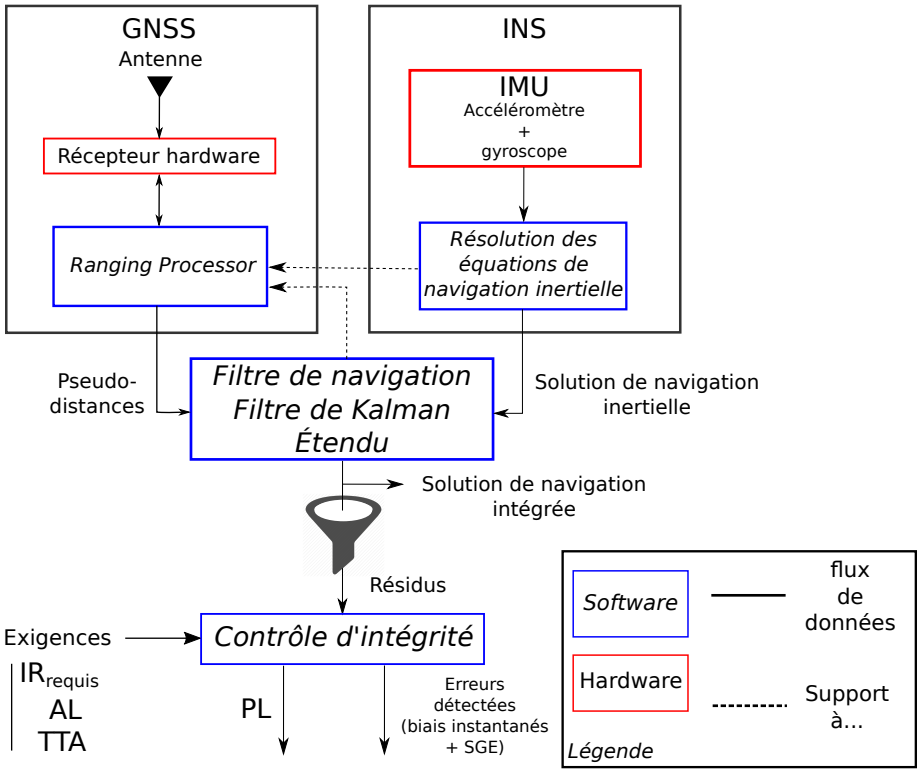


FIGURE 4.6 – Schéma de l'architecture du système choisi.

F, matrice d'évolution modélisant le système GNSS/INS,
H, matrice d'observation,
ψ les angles de roulis, tangage et lacet,
v et r, respectivement, la vitesse et la position dans le repère cartésien,
b_a et b_g biais constants liés à la température et aux vibrations, respectivement sur les accéléromètres et les gyroscopes au sein de la centrale inertielle,
ρ les pseudodistances, $\dot{\rho}$ dérivées des pseudodistances,
$z(t)$ est le vecteur de mesure de dimension m,
$w_s(t) \in \mathbb{R}^q$ et $w_m(t) \in \mathbb{R}^m$ sont des vecteurs, respectivement, liés au bruit du système (lié aux erreurs de modélisation et des perturbations) et à celui de mesure (lié à l'imperfection des capteurs) considérés comme gaussiens (cf Annexe C).

Lorsque le modèle du système n'est pas linéaire, comme c'est le cas avec la navigation GNSS, le filtre de Kalman classique ne peut pas être appliqué et on utilise sa version étendue (EKF).

4.3.1.1 Modèle d'état GNSS/INS choisi

Comme détaillé dans l'annexe B, les différentes étapes du filtre EKF sont :

1. Calcul de la matrice de transition Φ_{k-1}.
2. Calcul de la matrice de covariance du bruit du système Q_{k-1} (variance du bruit d'état $\Gamma_{k-1} w_{s,k-1}$).
3. Propagation de l'estimation du vecteur d'état $\hat{x}_{k-1}^{+}$ vers $\hat{x}_k^{-}$.
4. Propagation de la matrice de covariance de l'erreur P_{k-1}^{+} vers P_k^{-}.

5. Calcul de la matrice d'observation H_k.
6. Calcul de la matrice de covariance du bruit d'observation R_k.
7. Calcul du gain du filtre de Kalman, K_k.
8. Prise en compte des mesures z_k.
9. Mise à jour de l'estimation du vecteur d'état $\hat{x}_k^-$ vers $\hat{x}_k^+$.
10. Mise à jour de la matrice de covariance de l'erreur P_k^- vers P_k^+.

Dans cette sous-section, nous allons décrire les matrices d'entrées nécessaires au système. Quel que soit le type d'hybridation, il n'y a pas d'interaction entre les états de l'INS et les états du GNSS. L'interaction intervient dans le modèle de mesure mais pas dans le modèle d'état. Il est ainsi possible de séparer les deux sous systèmes, ce que nous ferons pour plus de lisibilité dans la suite.

Dans le filtre EKF, la première étape de l'algorithme consiste à linéariser la fonction d'évolution F. Dans la suite, nous appellerons Φ la matrice F linéarisée. Le calcul de Φ nécessite de définir F.

La matrice d'état du système GNSS/INS, F, est définie par l'équation 4.5.

$$F = \begin{bmatrix} F_{INS} & 0 \\ 0 & F_{GNSS} \end{bmatrix} \tag{4.5}$$

avec,

$$F_{INS} = \begin{bmatrix} 0_3 & 0_3 & 0_3 & 0_3 & T_b^n \\ F_{21}^n & 0_3 & F_{23}^n & T_b^n & 0_3 \\ 0_3 & F_{32}^n & 0_3 & 0_3 & 0_3 \\ 0_3 & 0_3 & 0_3 & 0_3 & 0_3 \\ 0_3 & 0_3 & 0_3 & 0_3 & 0_3 \end{bmatrix} \tag{4.6}$$

où,
0_n est la matrice nulle de dimension n × n où n = 3,
T_b^i est la matrice de transformation des coordonnées d'un référentiel centré sur le véhicule (noté b comme *body*) vers un référentiel inertiel (noté i comme *inertial*). Une solution de navigation est, comme son nom l'indique, donnée dans un référentiel de navigation (noté n comme *navigation*). Cependant, les mesures de l'INS sont données dans le référentiel b. Il faut donc exprimer ces mesures dans le référentiel n. L'équation 4.7 montre la forme générale d'une matrice de transformation d'un référentiel α vers un référentiel β.

$$T_\alpha^\beta = \begin{bmatrix} cos\theta_{\alpha\beta}\, cos\psi_{\alpha\beta} & cos\theta_{\alpha\beta}\, sin\psi_{\alpha\beta} & -sin\theta_{\alpha\beta} \\ T_{\alpha\ 21}^{\beta} & T_{\alpha\ 22}^{\beta} & sin\phi_{\alpha\beta}\, cos\theta_{\alpha\beta} \\ T_{\alpha\ 31}^{\beta} & T_{\alpha\ 32}^{\beta} & cos\phi_{\alpha\beta}\, sin\theta_{\alpha\beta} \end{bmatrix} \tag{4.7}$$

où,
$\phi_{\alpha\beta}$, $\psi_{\alpha\beta}$ et $\theta_{\alpha\beta}$ sont les angles d'Euler liés à la rotation du référentiel α vers le référentiel β.
$F_{21}^n = [-(T_b^n f_b^n)\widehat{\ }]$ est une matrice asymétrique (symbolisé par $\widehat{\ }$), fonction de la matrice de transformation T_b^n du référentiel b vers n[3]et de la force spécifique f_b^n (grandeur mesurée par la partie

3. Les angles d'Euler liés à cette transformation (ou ϕ_{bn}, ψ_{bn} et θ_{bn}) sont donnés dans le vecteur $in\_profile$ décrit en Annexe C.

accélérométrique de la centrale inertielle).

$$T^{\beta}_{\alpha\ 21} = \begin{bmatrix} -cos\phi_{\alpha\beta}\ sin\phi_{\alpha\beta} \\ sin\phi_{\alpha\beta}\ sin\theta_{\alpha\beta}\ cos\psi_{\alpha\beta} \end{bmatrix}, T^{\beta}_{\alpha\ 22} = \begin{bmatrix} cos\phi_{\alpha\beta}\ cos\phi_{\alpha\beta} \\ sin\phi_{\alpha\beta}\ sin\theta_{\alpha\beta}\ sin\psi_{\alpha\beta} \end{bmatrix}, T^{\beta}_{\alpha\ 31} = \begin{bmatrix} cos\phi_{\alpha\beta}\ sin\phi_{\alpha\beta} \\ sin\phi_{\alpha\beta}\ sin\theta_{\alpha\beta}\ cos\psi_{\alpha\beta} \end{bmatrix}$$
$$T^{\beta}_{\alpha\ 32} = \begin{bmatrix} -sin\phi_{\alpha\beta}\ cos\phi_{\alpha\beta} \\ cos\phi_{\alpha\beta}\ sin\theta_{\alpha\beta}\ sin\psi_{\alpha\beta} \end{bmatrix}$$

$$F^{n}_{23} = -\frac{2g_0(L_b)}{r_{eS}(L_b)} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{4.8}$$

avec,
$r_{eS}(L_b) = R_E(L_b)\sqrt{cos^2L_b + (1-e^2)^2 sin^2L_b}$, rayon géocentrique ou distance entre le centre de la Terre et un point sur la surface S à la latitude L_b,
e, l'excentricité de l'ellipsoïde de référence (WGS84) soit e = 0.0818191908425 (sans unité),
$R_E(L_b) = \frac{R_0}{\sqrt{1-e^2 sin^2 L_b}}$, rayon de courbure normal [4] à une surface S,
R_0, rayon équatorial de la Terre (distance entre le centre de la Terre et l'équateur) soit 6378,1370 km,
L_b, latitude du véhicule selon l'ellipsoïde de référence (WGS84),
$g_0(L_b) = 9.7803253359\ \frac{1+0.001931853 sin^2 L_b}{\sqrt{1-e^2 sin^2 L_b}}$, accélération gravitationnelle à la latitude L_b (modèle de gravité utilisé par le système WGS84).

$$F^{n}_{32} = \begin{bmatrix} \frac{1}{R_N(L_b)+h_b} & 0 & 0 \\ 0 & \frac{1}{(R_N(L_b)+h_b)cosL_b} & 0 \\ 0 & 0 & -1 \end{bmatrix} \tag{4.9}$$

avec, $h_b = \frac{z_b}{sinL_b} - (1-e^2)R_E(L_b)$, l'altitude du véhicule (distance entre le véhicule (avec z_b la composante verticale de la position du véhicule) et la surface de l'ellipsoïde de référence (WGS84)).

Pour $x_{GNSS} = [\delta\rho\ \delta\dot{\rho}]^T$, sachant que $\frac{\partial\delta\rho}{\partial t} = \delta\dot{\rho}$, on peut simplement définir F_{GNSS} :

$$F_{GNSS} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \tag{4.10}$$

Dans [Groves, 2013], Φ est la matrice F linéarisée par un développement en série, telle que $\Phi_{k-1} = \exp(F_{k-1}\ \tau_S)$, où τ_S représente l'intervalle de temps de propagation au sein du filtre de Kalman (ici égal à 0,2 s). Le terme $\exp(F_{k-1}\ \tau_S)$ peut être approximé par $I - F_{k-1}\ \tau_S$.

Comme pour la matrice du système, on peut définir la matrice d'évolution Φ selon l'équation 4.11 avec deux sous-matrices Φ_{INS} et Φ_{GNSS} développées juste après.

$$\Phi = \begin{bmatrix} \Phi_{INS} & 0 \\ 0 & \Phi_{GNSS} \end{bmatrix} \tag{4.11}$$

4. Un arc a un seul rayon de courbure tandis que, pour définir la courbure d'une surface, il faut déterminer deux rayons courbures appelés "rayon de courbure méridien" et "rayon de courbure normal".

$$\Phi_{INS} = \begin{bmatrix} I_3 & 0_3 & 0_3 & 0_3 & T_b^n \tau_S \\ F_{21}^n \tau_S & I_3 & F_{23}^n \tau_S & T_b^n \tau_S & 0_3 \\ 0_3 & F_{32}^n \tau_S & I_3 & 0_3 & 0_3 \\ 0_3 & 0_3 & 0_3 & I_3 & 0_3 \\ 0_3 & 0_3 & 0_3 & 0_3 & I_3 \end{bmatrix} \tag{4.12}$$

$$\Phi_{GNSS} = \begin{bmatrix} 1 & 0 \\ \tau_S & 1 \end{bmatrix} \tag{4.13}$$

I_3 est la matrice identité de dimension 3. Les matrices F_{21}^n, F_{23}^n, F_{32}^n et T_b^n sont les mêmes que définies pour la matrice du système F (cf équation 4.5).

La matrice de covariance du bruit du système Q est ensuite définie par les sous-matrices Q_{INS} et Q_{GNSS} (cf équation 4.14).

$$Q = \begin{bmatrix} Q_{INS} & 0 \\ 0 & Q_{GNSS} \end{bmatrix} \tag{4.14}$$

où,

$$Q_{INS} = \begin{bmatrix} S_{rg} I_3 & 0_3 & 0_3 & 0_3 & 0_3 \\ 0_3 & S_{ra} I_3 & 0_3 & 0_3 & 0_3 \\ 0_3 & 0_3 & 0_3 & 0_3 & 0_3 \\ 0_3 & 0_3 & 0_3 & S_{bad} I_3 & 0_3 \\ 0_3 & 0_3 & 0_3 & 0_3 & S_{bgd} I_3 \end{bmatrix} \tau_S \tag{4.15}$$

avec
$S_{rg} = \sigma_{rg}^2 \tau_i$, densité spectrale de puissance du bruit gyroscope,
$S_{ra} = \sigma_{ra}^2 \tau_i$, densité spectrale de puissance du bruit accéléromètre,
τ_i, intervalle de temps entre deux échantillons du bruit gyroscope et accéléromètre (= 0.2 s),
$S_{bad} = \frac{\sigma_{bad}^2}{\tau_{bad}}$, densité spectrale de puissance de la variation du biais d'accéléromètre,
$S_{bgd} = \frac{\sigma_{bgd}^2}{\tau_{bgd}}$, densité spectrale de puissance de la variation du biais gyroscope,
τ_{bad} et τ_{bgd} ; intervalle de temps entre deux échantillons des variations des biais accéléromètre et gyroscope (= 0.2 s),

et

$$Q_{GNSS} = \begin{bmatrix} S_{c\phi}^a \tau_S & 0 \\ 0 & S_{cf}^a \tau_S \end{bmatrix} \tag{4.16}$$

avec,
$S_{c\phi}^a$, densité spectrale de puissance du décalage en fréquence de l'horloge récepteur (fixée à 0.04 m^2 s^{-3}),
S_{cf}^a, densité spectrale de puissance du décalage de phase (fixée à 0.01 m^2 s^{-3}).

Les variations de biais sur ces capteurs sont dues à l'influence de la température. Les densités spectrales de puissance se réfèrent à l'équation B.6. La propagation de l'estimation du vecteur d'état x et de la matrice de covariance de l'erreur P est expliquée dans l'annexe B.

4.3.1.2 Modèle de mesure

L'état du système x et l'erreur d'estimation du filtre P sont à présent propagés de l'instant $k-1$ à k. La deuxième phase du filtrage est la phase de mise à jour. Elle nécessite différentes matrices utilisées dans le modèle de mesure (cf équation 4.4) à commencer par la matrice d'observation H_k.

$$H_k = \begin{bmatrix} 0_{1,3} & 0_{1,3} & (u^e_{as,1})^T & 0_{1,3} & 0_{1,3} & 1 & 0 \\ 0_{1,3} & 0_{1,3} & (u^e_{as,2})^T & 0_{1,3} & 0_{1,3} & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0_{1,3} & 0_{1,3} & (u^e_{as,m})^T & 0_{1,3} & 0_{1,3} & 1 & 0 \\ 0_{1,3} & (u^e_{as,1})^T & 0_{1,3} & 0_{1,3} & 0_{1,3} & 0 & 1 \\ 0_{1,3} & (u^e_{as,2})^T & 0_{1,3} & 0_{1,3} & 0_{1,3} & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0_{1,3} & (u^e_{as,m})^T & 0_{1,3} & 0_{1,3} & 0_{1,3} & 0 & 1 \end{bmatrix} \tag{4.17}$$

où, $u^e_{as,j} = \frac{r^e_{es,j}(t_{st}) - r^e_{ea}(t_{sa})}{|r^e_{es,j}(t_{st}) - r^e_{ea}(t_{sa})|}$ est le vecteur unité d'un j-ème satellite en vue (*line-of-sight unit vector*) avec :

$r^e_{es,j}(t_{st})$, la position du j-ème satellite en vue à l'instant t_{st} (instant de transmission du signal GNSS) exprimée dans un repère centré sur le satellite s dont les coordonnées de l'origine sont exprimées dans le référentiel terrestre (e pour *earth-centred frame*),
$r^e_{ea}(t_{sa})$, la position de l'antenne du récepteur a à l'instant t_{sa} (instant d'arrivée du signal GNSS) exprimée dans le référentiel terrestre.

Il reste à déterminer R_k, la matrice de covariance du bruit de mesure.

$$R_k = \begin{bmatrix} \sigma^2_{\rho 1} & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & \sigma^2_{\rho 2} & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma^2_{\rho m} & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & \sigma^2_{r1} & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \sigma^2_{r2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & \sigma^2_{rm} \end{bmatrix} \tag{4.18}$$

où, $\sigma_{\rho j}$ et σ_{rj} dépendent de l'élévation des satellites en vue à la j-ème mesure, du rapport de la puissance de porteuse c sur la puissance du bruit n_0 à j (c/n_0) et de accélération d'un satellite à j (déduite de la vitesse et de la position fournie dans les éphémérides) et sont fixés respectivement à 2,5 et 0,1 quel que soit j.

Grâce aux matrices H_k et R_k, il est possible de calculer le gain du filtre de Kalman dont le calcul est disponible en Annexe B. Pour mettre en œuvre la phase de mise à jour du vecteur d'état x et de la matrice de covariance de l'erreur P, il est nécessaire d'avoir le vecteur d'observation z. Ce vecteur est constitué des données que la sous-section suivante propose de présenter.

4.3.2 Application

Les données utilisées pour mettre en œuvre l'application sont de deux types : simulées et réelles. Dans un premier paragraphe, nous présentons les données réelles utilisées. Elles concernent la partie GNSS du système. Dans un deuxième paragraphe, nous décrivons les données issues de la simulation de l'INS. Le filtrage sera ensuite effectué avec ces deux ensembles de données (section 4.3.3)

4.3.2.1 Données GNSS réelles du laboratoire Geoloc de l'IFSTTAR

Au chapitre 2, nos analyses ont été conduites avec des données GNSS de type positions fournies dans un repère cartésien par un récepteur GNSS simulé. Pour être davantage en adéquation avec la réalité, nous avons enrichi nos simulations par les acquisitions faites par l'équipe Geoloc, unité de recherche de l'IFSTTAR basée à Nantes. Le véhicule de test dispose d'une centrale inertielle utilisée pour déterminer une trajectoire de référence. Deux types de récepteur GNSS sont utilisés : un bas de gamme (LEA-6T de marque Ublox) et un haut de gamme (DLV3 de marque Novatel). Nous avons eu accès aux données brutes fournies par ces récepteurs. Elles remplacent les données simulées lors de l'analyse causale et l'analyse de sensibilité du chapitre 2. Parmi ces données brutes, nous utilisons les pseudodistances, les mesures Doppler (pour déterminer le taux de variation des pseudodistances entre chaque instant), le nombre et la position/vitesse de chaque satellite en vue (exprimées dans le référentiel terrestre). Ces campagnes de mesures ont été réalisées le 30/01/12 à Nantes et les 21-22-23/02/12 à Paris dans le cadre d'une étude sur l'intégrité de positionnement automobile en environnement urbain. Il s'agit de données de localisation d'un véhicule automobile mais nous avons considéré que la localisation d'un train souffrait des mêmes sources d'erreur que celles d'une voiture dans un même environnement, notamment du phénomène de multitrajet. Le but est de mettre en œuvre l'algorithme de contrôle d'intégrité que nous proposons et l'évaluation de la sécurité proposée avec des données de terrain.

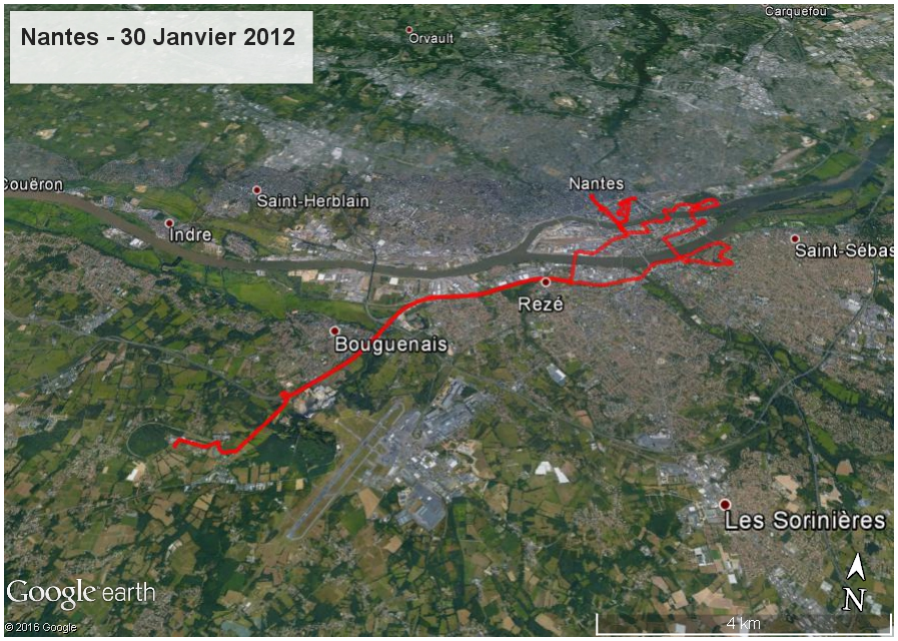


FIGURE 4.7 – Trajet effectué lors d'acquisition à Nantes le 30 Janvier 2012.

5 scénarios sont utilisés (cf exemple de la figure 4.7) représentant 5 trajets effectués avec un

système composé des deux récepteurs GNSS cités précédemment. Dans la suite, ces scénarios sont déroulés les uns à la suite des autres. L'intérêt ici est d'avoir un échantillon de données plus vaste. Chacun des scénarios contient de 134 586 à 490 941 pseudodistances. Nous ne cherchons pas à recréer un scénario à partir de plusieurs (les lieux et les dates étant différents pour chacun) mais à concaténer les données des différents scénarios afin d'obtenir un résultat final (IR notamment) le plus significatif possible. Contrairement aux données GNSS réelles, rares sont les simulations prenant en compte des phénomènes tels que le blocage des signaux (masquage), les interférences, le brouillage, le multitrajet. Ces phénomènes nécessitent des simulations plus lourdes (géométrie des bâtiments à considérer et temps de calcul plus long) et complexes à mettre en œuvre [Nahimana, 2009] compte tenu du nombre très important de configurations environnementales. Notons que le phénomène de multitrajet peut être simulé en augmentant l'écart-type du bruit considéré au niveau récepteur. En pratique, les multitrajets ont des impacts rarement aussi déterministes.

Tableau 4.3 – Données GNSS des 5 jeux de données du récepteur LEA-6T (bas coût).

Date / Lieu	30/01/12 Nantes	21/02/12 Paris (Boulevards)	22/02/12 Paris (Boulevards)	22/02/12 Paris (XIIème)	23/02/12 Paris (XIIème)
Durée du trajet (en sec)	4 832,4	9 825,2	12 154	7 116,4	7 510
Nombre de pseudodistances	204 810	332 676	490 941	288 925	312 841
Nombre de satellite moyen	8,7	6,8	8,1	8,1	8,3
Erreur de position moyenne	4,88	18,09	15,26	11,08	9,91
Nombre de positions indisponibles	1	193	1	154	459
Disponibilité	99,9995	99,9420	99,9998	99,9467	99,8533
Nombre de points aberrants	0	161	0	0	0

Le tableau 4.3 donne les détails de chaque scénario (date, lieu, nombre de pseudodistances, temps de trajet). Pour présenter les différents jeux de données issus de ces scénarios, nous avons déterminé une solution de navigation par moindres carrés uniquement avec les mesures GPS du récepteur LEA-6T. Ainsi, le tableau 4.3 nous renseigne sur :

— la moyenne du nombre de satellites en vue (cf figure 4.9),
— la moyenne de l'erreur de position horizontale par rapport à la référence (cf figure 4.8),
— le nombre d'indisponibilité qui représente le nombre de situations où moins de 4 satellites sont visibles (minimum pour déterminer une solution de navigation GNSS),
— la disponibilité par le complément du nombre de situations d'indisponibilité sur le nombre total de mesures.

Des points aberrants (position avec une erreur supérieure à 20 km) ont été exclus du calcul des différentes moyennes afin qu'elles n'en soient pas affectées. Toutefois, par souci de transparence, nous les avons comptabilisés dans la dernière colonne du tableau 4.3.

Au vu de ces chiffres, quelques remarques peuvent être énoncées :

— Le nombre de satellites en vue est compris entre 1 et 12 (minimum et maximum tous scénarios

confondus) avec une moyenne oscillant entre 5,45 et 8,69 (soit entre 5 et 8 satellites en vue), ce qui est assez classique (cf sous-section 1.3.2 du chapitre 1).

— L'erreur de position moyenne est meilleure dans le scénario de Nantes que dans les scénarios de Paris. Cela peut s'expliquer par la nature de l'environnement de propagation des signaux GNSS. Le trajet de Nantes traverse une zone mixte (semi-urbaine/urbaine) alors que les scénarios de Paris se déroulent exclusivement en zone urbaine dense et sont donc sujets à davantage de multitrajets et de masquages.

— la disponibilité est globalement supérieure à 99 %. Les environnements traversés sont bruités mais ne sont pas fortement masquants.

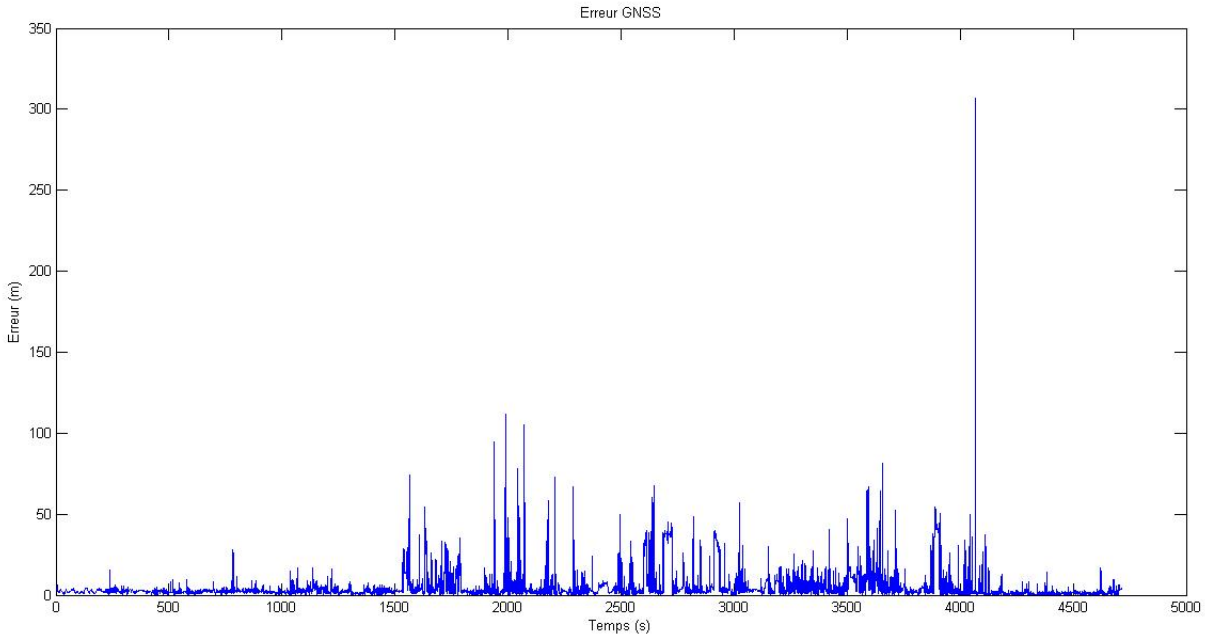


FIGURE 4.8 – Distribution de l'erreur de position (scénario 1).

Dans cette sous-section, les données GNSS ont été présentées. À présent, il est nécessaire de décrire les données issues de l'INS à combiner avec les pseudodistances.

4.3.2.2 Données INS utilisées

Les données INS sont des données simulées comme suit. [Groves, 2013] propose des exemples d'utilisation d'INS et de récepteur GNSS grâce à des routines Matlab® conçues suivant la modélisation présentée figure 4.10. Ces routines sont sous licence BSD (*Berkeley Software Distribution license*) libre d'utilisation. L'avantage de ces modèles est leur finesse par rapport aux modèles des capteurs proposés au chapitre 2.

La figure 4.10 montre comment les données INS sont bruitées puis utilisées pour estimer une position. Le modèle réel est un compromis entre représentation réaliste et simplifiée du monde réel. Il faut tenir compte d'un maximum de phénomènes dans le modèle (dont les conséquences sont

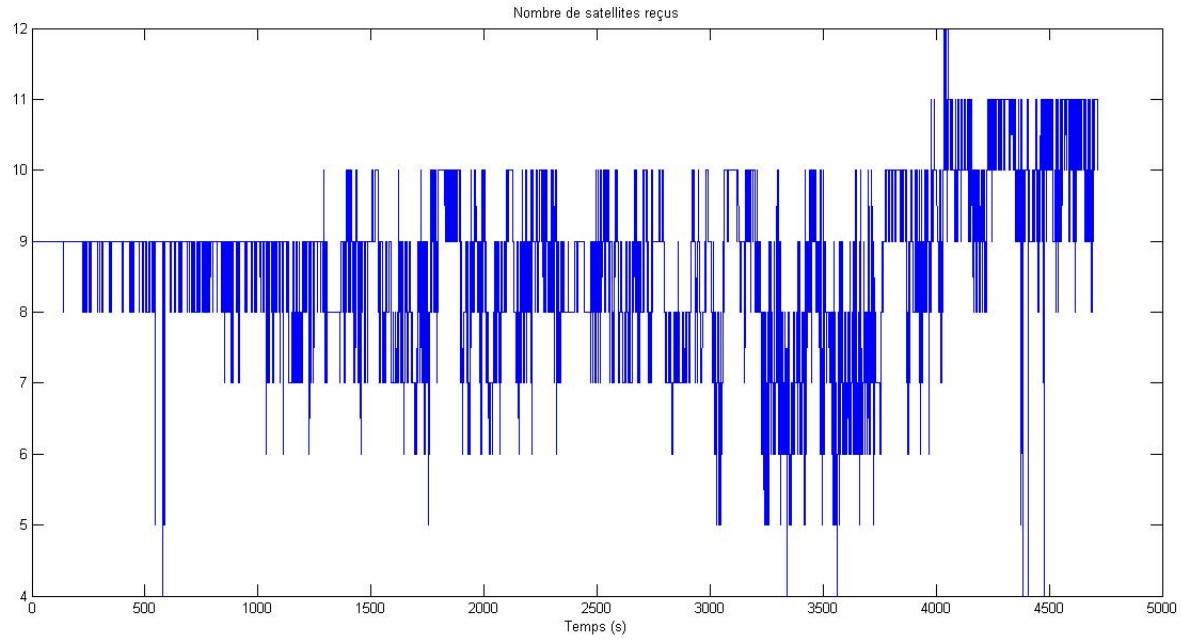


FIGURE 4.9 – Nombre de satellite en vue (scénario 1).

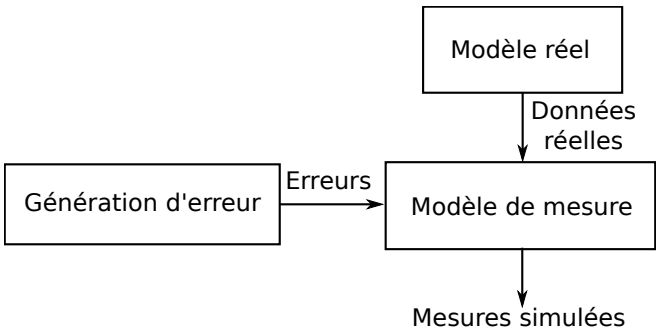


FIGURE 4.10 – Modélisation générique du bruitage des observations.

les plus significatives telles que la dérive de l'INS) tout en étant simulable (nombre raisonnable de paramètres). Le modèle réel fournit des données considérées comme vraies soit par un système de référence (cas des expérimentations de l'équipe Geoloc) soit par un développeur (cas de Groves). Dans le cas de l'INS, nos données réelles sont les positions, vitesses et accélérations réelles. Ces données peuvent être vues comme des mesures venues d'une INS parfaite. Le modèle de mesure injecte des erreurs, générées aléatoirement (bruits de mesure) ou de manière déterministe (biais accélérométrique ou gyroscope) sur les données réelles afin d'obtenir une solution de navigation bruitée. Cette modélisation est identique à celle des analyses causale et de sensibilité du chapitre 2.

La figure 4.11 montre le modèle utilisé pour notre INS. $f_{s,true}$ et w_{true} sont respectivement la force spécifique réelle (force exercée sur la masse au sein de l'accéléromètre (cf section 1.2.2.2 du chapitre 1)) et la vitesse angulaire réelle. $f_{s,true}$ est déterminée par la variation de la vitesse du véhicule sur un intervalle de temps τ_i. Elle est déduite de la vitesse réelle précisée dans les colonnes n°5 à 7 du profil de déplacement (vecteur $in\_profile$ décrit en annexe C) donné en entrée de la

simulation. De la même manière, w_{true} est déterminée par la variation de la position en latitude, longitude et hauteur du véhicule sur un intervalle de temps τ_i. Elle est déduite de la position réelle précisée dans les colonnes n°2 à 4 du profil de déplacement (vecteur $in\_profile$).

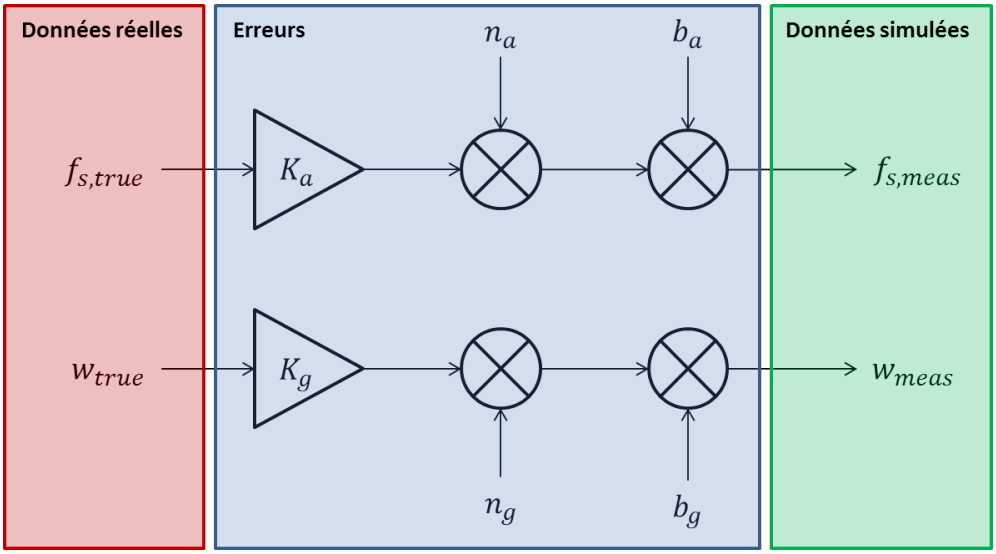


FIGURE 4.11 – Modèle de l'INS simulé.

Les bruits sur l'accéléromètre, n_a et sur le gyroscope, n_g de l'INS sont exprimés par l'équation 4.19.

$$n_{a,g} \sim \mathcal{N}(0, \sigma_{a,g}) \tag{4.19}$$

avec,
$\sigma_a = \sqrt{\frac{S_a}{\tau_i}}$ et $\sigma_g = \sqrt{\frac{S_g}{\tau_i}}$, écart-types des bruits sur accéléromètre et gyroscopes simulés,
S_a et S_g sont les densités spectrales des bruits blancs gaussiens (S_a et S_g sont fixés respectivement à 0.001 et 0.1),
τ_i est l'intervalle de temps entre deux mesures de l'INS (ici, 0.2s).

Les biais accélérométrique b_a et gyroscopique b_g sont des valeurs constantes (cf tableau 4.4). Le tableau 4.4 reprend plusieurs valeurs utilisées par Groves et [Kubrak, 2007]. Les données de [Kubrak, 2007] sont les biais sur chaque axe (x, y et z). Les valeurs de Groves concernent un biais identique sur chaque axe et appliqué dans le domaine automobile. Dans la suite de nos simulations, nous retiendrons les valeurs de [Kubrak, 2007].

K_a et K_g sont des coefficients de proportionnalité entre la valeur réelle et la valeur mesurée de la force spécifique et de la vitesse angulaire. $K_{a,g}$ est fonction du facteur d'échelle $SF_{a,g}$ tel que $K_{a,g} = I_3 + SF_{a,g}$. Le facteur d'échelle est une donnée constructeur dont des valeurs sont également données par [Kubrak, 2007] et [Groves, 2013] dans le tableau 4.5. [Kubrak, 2007] ne donnant pas de valeur pour le facteur d'échelle gyroscopique, nous utilisons celui de [Groves, 2013].

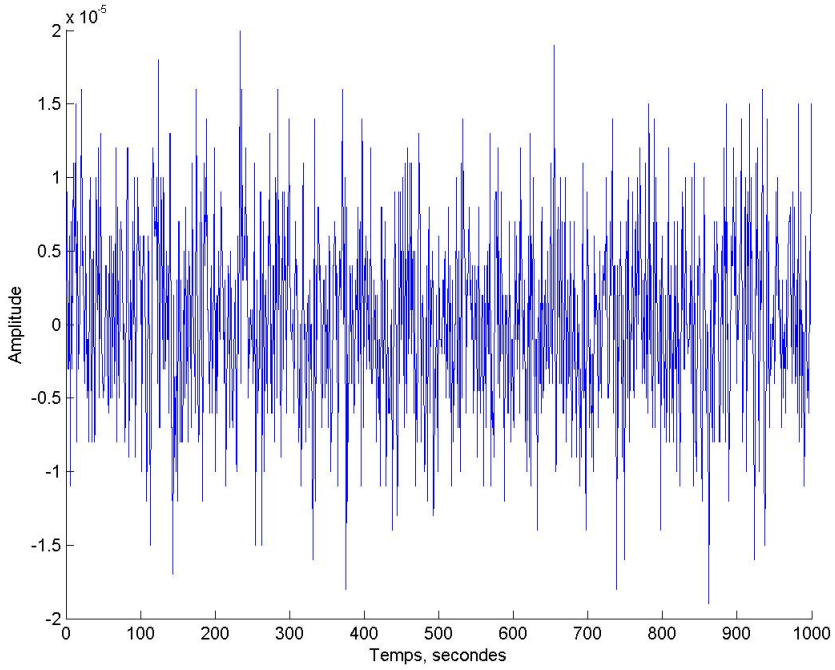


FIGURE 4.12 – Bruit blanc Gaussien simulé (affiché pour de t=0 à 1000 s) pour l'accéléromètre ou gyroscope.

Tableau 4.4 – Biais accélérométrique et gyroscopique.

Source	Biais accéléromètre (en m/s^2)	Biais gyroscopique (en rad/s)
	-6,1 $\times$ 10^{-2} (x)	2,1 $\times$ 10^{-3} (x)
[Kubrak, 2007]	-5 $\times$ 10^{-3} (y)	-6,6 $\times$ 10^{-3} (y)
	1,82 $\times$ 10^{-1} (z)	-1,09 $\times$ 10^{-2} (z)
[Groves, 2013]	$> 10^{-1}$	$> 5\times$ 10^{-4}

Tableau 4.5 – Facteur d'échelle accéléromètre et gyroscope.

Source	Facteur d'échelle accéléromètre (en m/s^2)	Facteur d'échelle gyroscopique (en rad/s)
	-0,096 (x)	- (x)
[Kubrak, 2007]	-0,076 (y)	- (y)
	-0,058 (z)	- (z)
[Groves, 2013]	$> 10^{-3}$	$> 10^{-4}$

Les valeurs de $f_{s,meas}$ et w_{meas} peuvent ainsi s'écrire :

$$f_{s,meas} = K_a \times f_{s,true} + n_a + b_a \tag{4.20}$$

$$w_{meas} = K_g \times w_{true} + n_g + b_g \tag{4.21}$$

D'autres erreurs peuvent être considérées dans ce modèle INS et, plus particulièrement, l'influence de l'accélération gravitationnelle terrestre sur le gyroscope. Pour tenir compte de cette influence, il

suffit d'ajouter un terme supplémentaire à l'équation 4.21, fonction de la force spécifique réelle $f_{s,true}$ et d'une matrice 3x3, notée G_g. Nous considérons ce terme négligeable : chaque élément de la matrice G_g est de l'ordre de 5×10^{-5}. Le modèle INS et celui de ses erreurs sont au cœur des routines disponibles dans le CD de démonstration de [Groves, 2013] qui utilisent plusieurs fonctions liées au fonctionnement de l'INS :

— des fonctions d'initialisation (remise à zéro des erreurs et mise en position initiale),
— des fonctions calculant les erreurs de position, vitesse et attitude (cf "Génération d'erreur" de la figure 4.10),
— plusieurs fonctions de conversion des positions, vitesses et attitudes vers plusieurs repères (repère Nord, Est, Bas (NEB) vers les repères de roulis, tangage, lacet (RTL) et vice versa),
— des fonctions liées à la modélisation des différents capteurs (accéléromètre et gyroscope) et fonctionnement de la partie hardware de l'INS, l'IMU,
— des fonctions résolvant les équations inertielles (partie software de l'INS).

Avec ces routines, les valeurs des biais, bruits et facteur d'échelle choisies et la trajectoire de référence pour le premier jeu de données de Nantes, nous obtenons la solution de navigation inertielle illustrée en bleue sur la figure 4.13 (la courbe rouge représente la trajectoire de référence).

Les données INS et GNSS doivent être traitées par un filtre de navigation : le filtre de Kalman étendu. L'objectif d'un filtre de navigation est d'estimer l'état du système GNSS/INS à partir de toutes les mesures disponibles. Il permet la fusion de ces mesures afin de calculer une seule et même solution de navigation. Nous ne nous concentrons pas sur la solution de navigation finale mais sur les résidus pour leur utilisation dans les tests statistiques décrits dans le chapitre 3. Ces résidus sont calculés et utilisés par le filtre de Kalman mais ne sont pas fournis en sorties des routines. Par conséquent, il est nécessaire de les extraire afin de mener à bien la phase de détection du contrôle d'intégrité.

Dans [Groves, 2013], des exemples simples d'utilisation de ces fonctions en hybridation serrée avec un récepteur GNSS sont proposés pour des applications automobiles, aéronautiques ou maritimes. Les exemples pour automobiles sont privilégiés pour les raisons évoquées en sous-section 4.3.2.1. L'auteur propose également une modélisation du récepteur GNSS mais nous ne l'avons pas utilisée puisque nous avons exploité les données réelles de l'équipe Geoloc décrites précédemment.

Le système et le format des données ont été fixés. Pour présenter le fonctionnement du système GNSS/INS et les résultats, il est nécessaire d'en dimensionner les paramètres. Ces paramètres concernent le profil de déplacement, l'initialisation de l'INS, des erreurs et du filtre de Kalman. Le lecteur trouvera ces informations en annexe C.

4.3.3 Simulation du fonctionnement du système GNSS/INS

La simulation du système GNSS/INS en hybridation serrée nécessite l'utilisation des mesures issues de la centrale inertielle du laboratoire Geoloc pour construire le trajet de référence (vecteur $in\_profile$). La section 4.3.2.2 a montré comment sont simulées les données INS. Dans ce but, il est nécessaire de générer les erreurs INS (bruits, biais ainsi que les facteur d'échelle gyroscopiques et accélérométriques) afin de construire des mesures inertielles à partir de $in\_profile$. Par défaut, les exemples de Groves génèrent les pseudodistances, leur variation entre deux instants, la position et

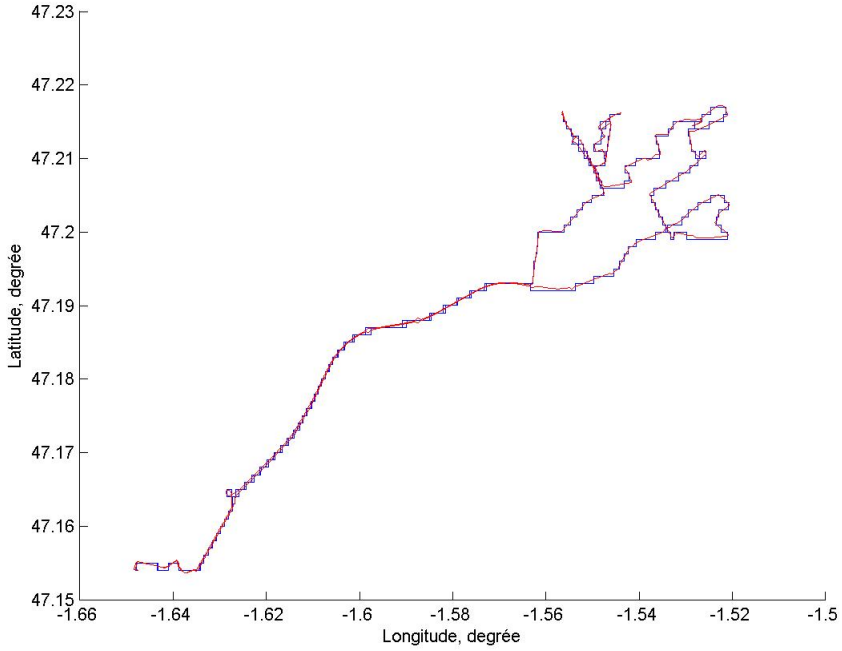


FIGURE 4.13 – Solution de navigation inertielle seule (en rouge, la trajectoire de référence ; en bleu la trajectoire estimée)

la vitesse des satellites en vue. C'est ici que nous insérons les données GNSS du laboratoire Geoloc. Les mesures INS et GNSS sont intégrées par un filtre de Kalman étendu où seront calculés le vecteur de résidus et la matrice d'observation H nécessaires à la phase de détection du contrôle d'intégrité et au calcul du niveau de protection.

La figure 4.14 illustre l'évolution de l'erreur de position entre la solution de navigation GNSS/INS et la trajectoire de référence. Elle correspond à l'erreur de position du scénario présenté figure 4.7. Cette erreur a pour moyenne 5,29 mètres (cf tableau 4.6) mais présente des zones où l'erreur est plus importante témoignant d'un environnement contraignant. Le tableau 4.6 montre également le gain en précision d'une solution GNSS/INS par rapport à la solution GNSS seule et la solution INS seule.

Nous constatons qu'une solution GNSS/INS, pour 5 jeux de données utilisés, est bien globalement meilleure que le GNSS ou l'INS seule. Pour le jeu de Nantes, la précision est de 10,48 mètres dans 95% des cas. Il est à noter que la position pour le jeu de Paris XII du 23/02/12 est précise à 17,49 mètres (sachant que AL a été fixé à 20 mètres) à 95% des cas.

Il s'agit à présent d'appliquer le contrôle d'intégrité sur le système GNSS/INS présenté ici. La première étape de ce processus est la détection des erreurs que nous avons identifiées pour ce type de système : les biais instantanés et les erreurs à croissance lente. Pour cela, nous utilisons les résidus, données calculées au sein du filtre de Kalman. Ces résidus sont les entrées des tests statistiques vus dans la section 3.6 du chapitre 3. Ces tests statistiques représentent l'étape de détection du contrôle d'intégrité. Pour fonctionner, ce processus a besoin de données d'entrée correspondant aux exigences sur l'intégrité quantifiées dans la section 4.2 c'est à dire AL, TTA et IR requis. Dans

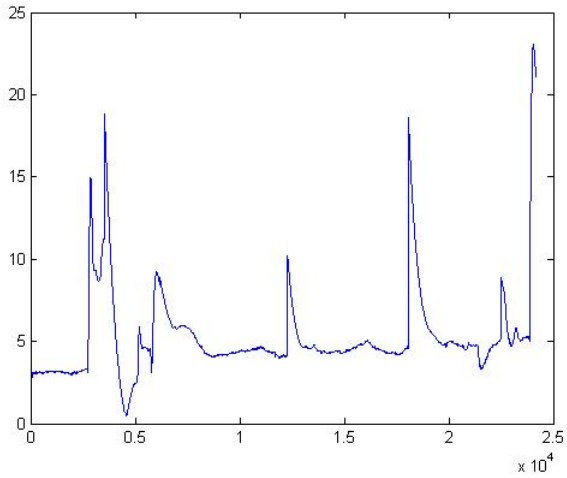


FIGURE 4.14 – Erreur de position horizontale GNSS/INS en mètre et en fonction du temps.

Tableau 4.6 – Erreurs de position du système GNSS/INS.

Date / Lieu	30/01/12 Nantes	21/02/12 Paris (Boulevards)	22/02/12 Paris (Boulevards)	22/02/12 Paris (XIIème)	23/02/12 Paris (XIIème)
Erreur moyenne	5,29	5,61	5,68	5,86	6,66
Précision (95ème centile)	10,48	8,74	8,50	11,10	17,49
Réduction de l'erreur par rapport à l'INS seule	-108,02 %	-101,02 %	-98,15 %	-90,01 %	-75,05 %
Réduction de l'erreur par rapport au GNSS seul	+10,05 %	-69,02%	-62,80%	-47,14%	-32,79%

notre application, le contrôle d'intégrité se résume à la phase de détection de situation à risque en terme d'intégrité et de calcul de niveau de protection PL. L'algorithme relatif à ces étapes a été présenté au chapitre 3. L'évaluation de la sécurité par l'intégrité de la localisation repose sur ces informations. Cette évaluation conclura sur un risque sur l'intégrité atteint et le niveau de sécurité qui en découle.

4.4 Application du contrôle d'intégrité et évaluation quantitative de la sécurité

La figure 4.15 montre de manière complète comment sont déterminées en pratique les situations décrites en section 4.2.1. Le volet opérationnel a été décrit dans la section 3.6 du chapitre 3. La figure se lit de haut en bas. Pour mettre en œuvre le volet évaluation, nous avons besoin :

— des mesures fournies par le système et décrites dans la section précédente,
— des détections des biais instantanés et des erreurs à croissance lente fournies par la partie

détection du contrôle d'intégrité,
— du niveau de protection.

L'erreur de position PE est déterminée grâce à la position réelle du train dans le cadre de l'évaluation de la performance en position du système. La qualité de la détection permet d'évaluer les performances de détection des biais instantanés et des erreurs à croissance lente en terme de détections vraies, fausses et manquées. Les détections fausses et manquées nous renseignent sur la qualité de la détection. La détection manquée est un des critères qui nous permet de déterminer l'occurrence des situations S1 à S3. La pertinence de PL est importante pour ces situations.

D'abord, nous présentons les résultats de cette phase de détection. Ceci nous permet d'identifier les situations décrites dans le chapitre 3 section 3.7. En parallèle, un PL est calculé pour caractériser le problème en bornant l'erreur de position PE. Il est ensuite possible d'identifier les situations à risques en terme d'intégrité (situation S1 à S3). Le nombre d'occurrence de ces évènements permet de quantifier le risque d'intégrité effectivement atteint par le système considéré. Enfin, une fois ce risque connu, le lien entre l'intégrité et la sécurité est appliqué pour conclure sur le niveau de sécurité de ce système.

4.4.1 Détection des erreurs GNSS et INS

Le contrôle d'intégrité se réfère dans ce chapitre à la phase de détection d'erreurs de position (dans la littérature, c'est un algorithme type FD - *Fault Detection*). Les étapes d'identification, d'isolation ou d'exclusion ne sont pas abordées. Néanmoins, ce type d'algorithme est suffisant pour conclure sur l'intégrité. On rappelle que l'objectif ici n'est pas de concevoir un système de localisation intègre avec GNSS mais d'appliquer une méthode d'évaluation de la sécurité d'un système donné grâce à l'évaluation de l'intégrité.

Que l'on se place dans une phase de conception ou d'évaluation des performances, l'étape de détection est importante afin d'identifier les situations à risques énoncées précédemment. Plus précisément, il s'agit de déterminer les situations durant lesquelles l'algorithme de contrôle d'intégrité détecte un problème ou ne détecte rien. À ce niveau du contrôle d'intégrité, nous raisonnons de manière prudente. S'il y a détection, nous faisons confiance au contrôle d'intégrité. Les cas de fausses alarmes (erreur détectée par le contrôle d'intégrité mais non présente sur la solution de navigation) sont prises en compte de manière défavorable d'un point de vue sécurité : la position fournie par le système GNSS/INS est considérée comme non-intègre.

Ici la phase de détection sera appliquée à chaque partie du système : GNSS et INS. Cette phase s'appuie sur les résidus liés aux mesures de capteurs générés par le filtre de Kalman et la solution de navigation illustrée dans la sous-section 4.3.3. On rappelle qu'il s'agit de détecter les biais instantanés induits par le phénomène de multitrajet sur les données GNSS et les erreurs à croissance lente sur les données INS. Les résultats de détection des erreurs considérées sont présentés dans les sous-sections suivantes.

4.4.1.1 Biais instantanés

Dans un premier temps, l'évolution de la variable aléatoire pour le test du χ^2 est présentée sur la figure 4.16. On rappelle que cette variable est $NSSE$ et est calculée avec les résidus (cf section

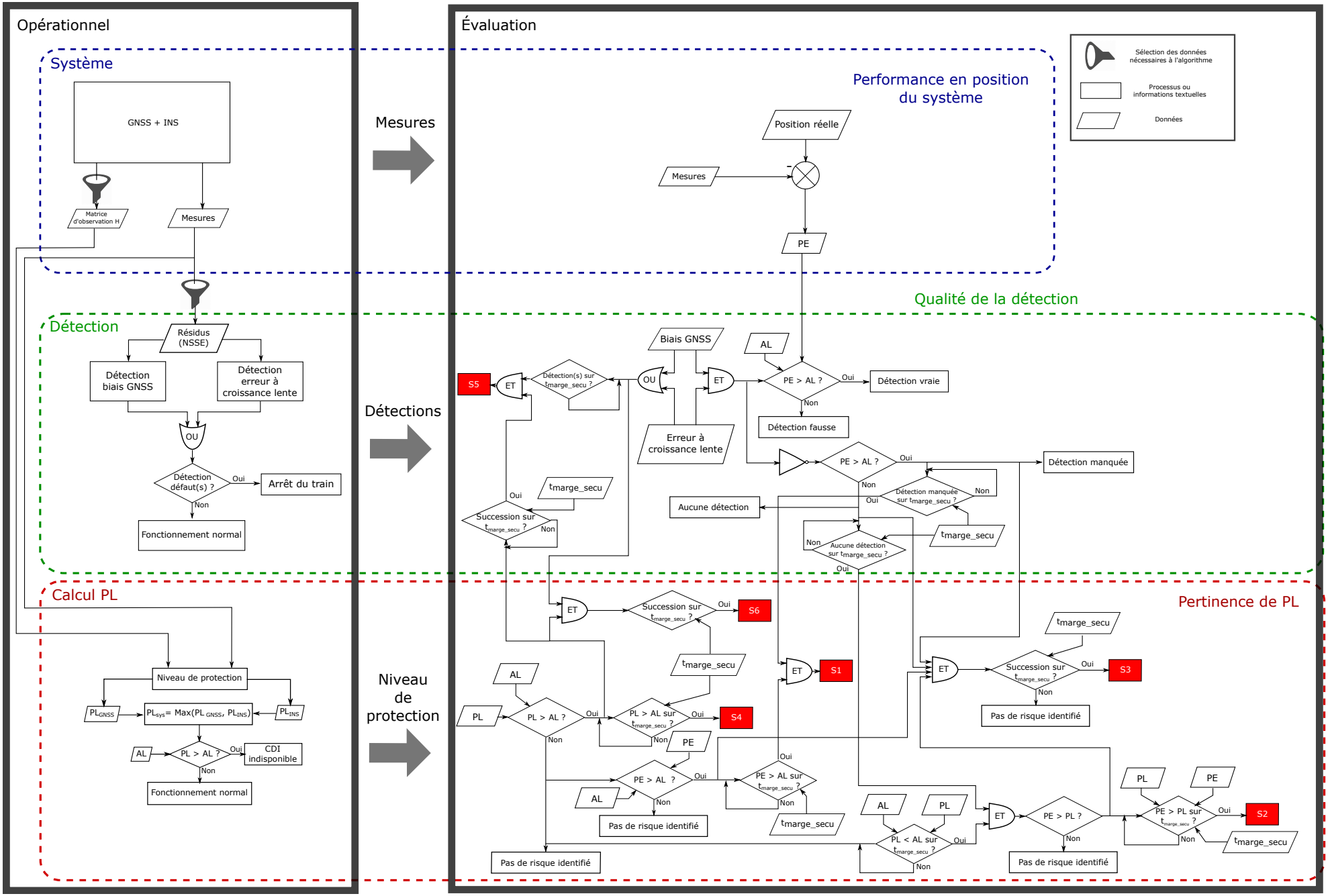


FIGURE 4.15 – Logigramme présentant l'aspect opérationnel et évaluation du système GNSS/INS avec contrôle d'intégrité.

3.6 du chapitre 3). La barre rouge représente le seuil de détection déterminé par la probabilité de fausse alarme fixée selon les normes aéronautiques à 1×10^{-7} pour la durée d'une simulation donnée. Il y a détection lorsque $NSSE$ franchit ce seuil. Au dessous de ce seuil, il n'y a pas de détection. Dans la simulation, cela ne signifie pas qu'il n'y a pas d'erreur de position PE en dehors des limites, seulement que le processus de détection n'a détecté aucun problème. On parle de sensibilité de la détection. Plus précisément, cela provient de P_{biais} dont le calcul a été proposé à la section 3.6 du chapitre 3. Dans le cas présent, l'erreur minimale détectable pour les biais instantanés est de $15,05$ mètres. Cela signifie que tous les biais au dessous de cette valeur ne sont pas détectés.

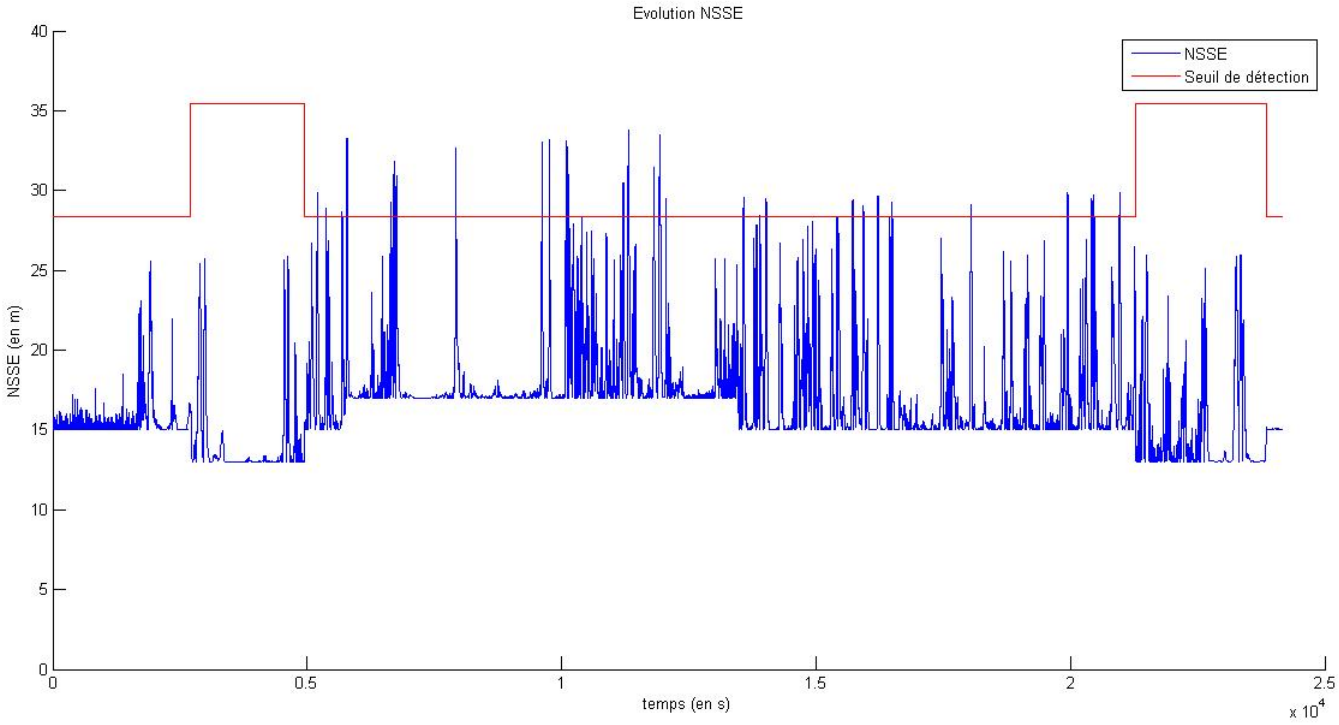


FIGURE 4.16 – Évolution de NSSE sur toute la période de simulation et seuil de détection des biais instantanés.

Dans la simulation illustrée par la figure 4.16, le nombre de biais instantanés détectés s'élève à 284. Attention, ces 284 biais instantanés ne conduisent pas à un risque d'intégrité mais à une indisponibilité de la position. Pour plus de lisibilité, nous nous limitons à une fenêtre intéressante de temps $[t = 9\ 530$ s à $t = 12\ 370$ s$]$ (cf figure 4.17) au cours de laquelle 9 biais instantanés sont identifiés. Cette fenêtre illustre également la nature instantanée de ces biais : il s'agit de pics de $NSSE$ d'amplitudes importantes (supérieures à P_{biais}).

Le tableau 4.7 donne le nombre total de biais instantanés détectés pour chaque scénario. Les performances de la détection des biais instantanés sont données en fonction d'un nombre de détection manquée correspondant au nombre de fois où un biais instantané n'a pas été détecté alors qu'au moins un est présent. Les performances de la détection sont aussi fonction d'un nombre de fausses alarmes correspondant au nombre de fois où un biais instantané a été détecté alors qu'aucun n'est présent. Des précautions peuvent être prises. PE n'est pas représentée sur la figure 4.16 car, comme

le montre le tableau 4.7, la qualité de la détection des biais n'est pas idéale, de ce fait, le lien visuel entre $NSSE$ et PE n'est pas suffisamment représentatif ici. Nous en reparlerons dans la conclusion de ce chapitre (cf sous-section 4.4.6).

Tableau 4.7 – Biais instantanés pour les 5 jeux de données du récepteur LEA-6T (bas coût).

Date / Lieu	30/01/12 Nantes	21/02/12 Paris (Boulevards)	22/02/12 Paris (Boulevards)	22/02/12 Paris (XIIème)	23/02/12 Paris (XIIème)
Taille échantillon	24 162	49 126	60 770	35 583	37 550
Biais instantanés détectés	284	1 071	833	3 891	3 485

Autre remarque : NSSE demeure au-dessus du seuil pendant 10 voire 20 secondes. L'allure laisse à penser qu'il peut s'agir d'erreurs à croissante lente (cf sous-section 4.4.1.2) mais le coefficient directeur à ces endroits de la courbe est trop important pour des erreurs à croissante lente telles que définies au chapitre 3. Nous pouvons remarquer que ces situations sont regroupées (cf figures 4.16) et sont rarement isolées : L'utilisateur traverse une zone contraignante engendrant de fréquents multitrajets et masquages.

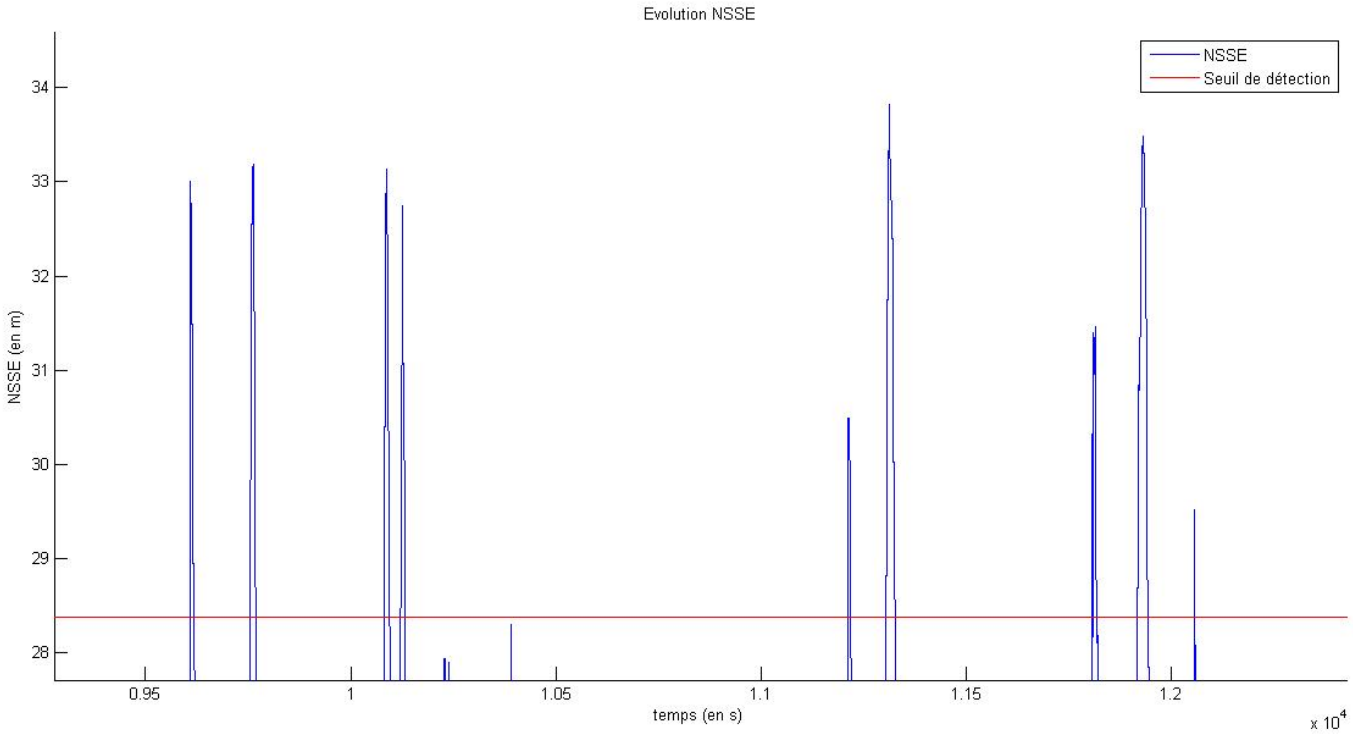


FIGURE 4.17 – Zoom intéressant sur un groupe de biais.

Pour exprimer une probabilité sur le risque d'intégrité, il est nécessaire de calculer le nombre d'occurrences de détections manquées (le contrôle d'intégrité fonctionne selon les exigences *i.e.* $PL > AL$

alors que ce n'est pas le cas *i.e.* $PE > PL$ ou $PE > AL$). Ceci concerne uniquement les biais engendrés par la partie GNSS. Il faut s'intéresser ensuite à la détection de l'autre type de biais lié à l'INS : les erreurs à croissance lente.

4.4.1.2 Erreurs à croissance lente

Comme nous l'avons énoncé dans le chapitre 3, l'INS, comme tout capteur proprioceptif, souffre de biais qui se cumulent avec le temps. Un biais instantané est assimilé à une droite PE en fonction du temps avec un coefficient directeur important. Par conséquent, dans la sous-section 3.6.1 du chapitre 3, nous avons fixé une valeur de coefficient directeur donnée pour distinguer un biais instantané d'une erreur à croissance lente. Cette dernière se présente sous la forme d'une rampe avec un coefficient directeur inférieur à celui d'un biais instantané.

Dans la description du processus de détection des erreurs à croissance lente (cf sous-section 3.6.2 du chapitre 3), la partie statistique de la détection est fondée sur plusieurs variables. Dans notre cas, nous prenons 3 variables T_1, T_2 et T_3 (calculées à partir de $NSSE$) à comparer respectivement à 3 seuils ($seuil_1$, $seuil_2$ et $seuil_3$) soit 3 tests effectués pour déterminer une erreur à croissance lente. Les 3 seuils sont déterminés grâce à des probabilités de fausses alarmes, pfa_1, pfa_2 et pfa_3 (notations simplifiées des pfa présentées dans la sous-section 3.6.2 du chapitre 3). Dans la figure 4.18, pfa_1, pfa_2 et pfa_3 sont fixées à $4,6 \times 10^{-3}$. Cette valeur est choisie selon les normes aéronautiques qui exigent un pfa de l'ordre de 10^{-7} ($pfa_1 = pfa_2 = pfa_3 = (10^{-7})^{1/3}$).

Pour un biais instantané, il suffit d'une seule variable et d'un seul seuil. Pour une rampe, il faut deux variables et deux seuils au minimum (au même titre qu'il faut deux points pour décrire une droite). Un troisième test est effectué pour identifier différentes évolutions de rampe. Pour plus de lisibilité, nous illustrons le résultat de ces trois tests figure 4.18. Nous rappelons que les différentes évolutions d'erreur à croissance lente (sachant toutes les situations possibles (cf sous-section 3.6.2.3)) sont décrites de la manière suivante à un instant t :

- une rampe à évolution "très lente" est détectée si $T_3 > seuil_3$ tant que $T_2 < seuil_2$ et $T_1 < seuil_1$,
- une rampe à évolution "lente" est détectée si $T_3 > seuil_3$ tant que $T_2 > seuil_2$ et $T_1 < seuil_1$,
- une rampe à évolution "rapide" est détectée si tous les seuils sont franchis.

La figure 4.19 montre l'évolution de l'erreur sur la position fournie par le système GNSS/INS dans le temps ainsi que les instants où différentes erreurs à croissance lente sont détectées.

À l'image de l'erreur minimale détectable (P_{biais}) pour les biais instantanés, il existe aussi un P_{rampe} pour les erreurs à croissance lente. Elle correspond à une rampe d'évolution très lente car ce type de rampe n'est détecté que par un seul seuil (T_3) parmi les trois. Étant donné que les rampes de ce type sont comprises entre de 0,8718 à 1,7425 m/s (cf tableau 4.8), le P_{rampe} pour la détection des erreurs à croissance lente vaut 0,8718 m/s. Il est important de signaler dans les cas de non détections indiquées dans le tableau 4.9, ils peuvent contenir des détections manquées (situations dangereuses). La sous-section suivante comptabilise ces situations.

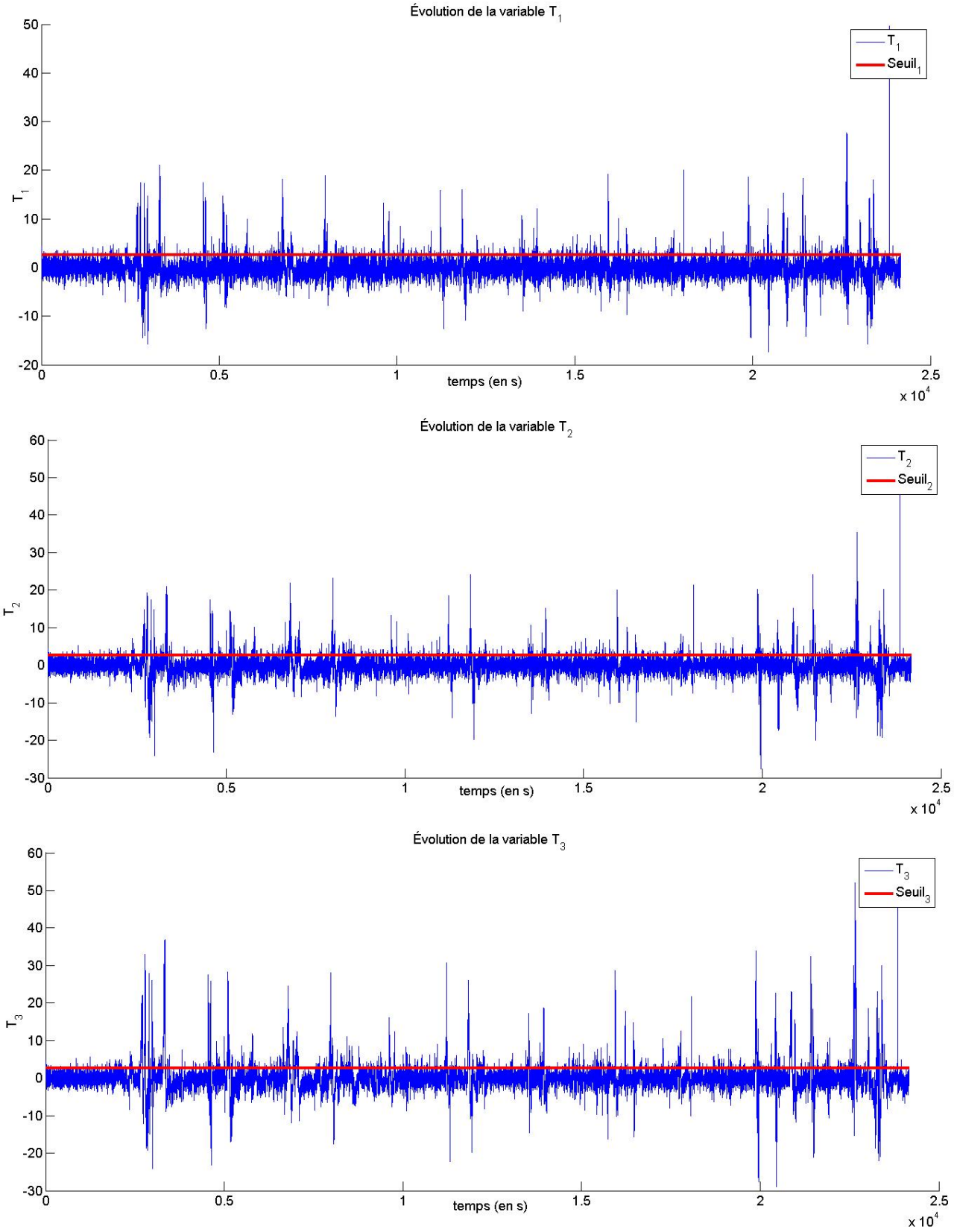
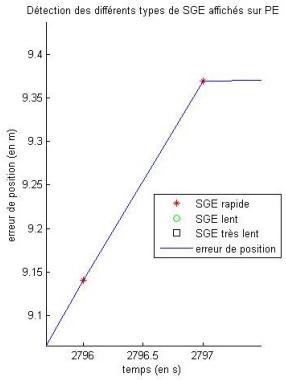
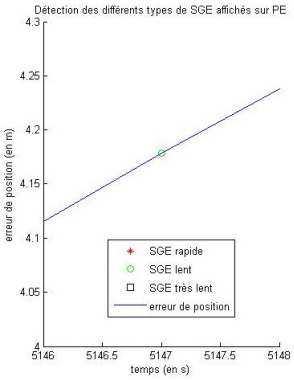
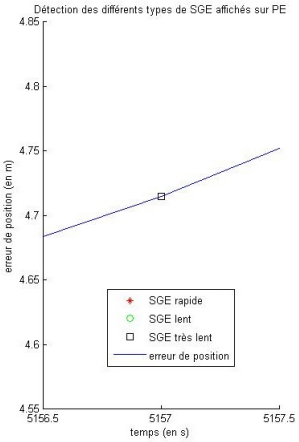


FIGURE 4.18 – Évolution des variables aléatoires de test T_1, T_2 et T_3 et leur seuil respectifs $seuil_1$, $seuil_2$ et $seuil_3$ (égaux à 2,61 - valeur sans unité - pour un pfa de $4,6 \times 10^{-3}$).

Tableau 4.8 – Types, profil, nombre d'erreurs à croissance lente détectées pour le jeux de données de Nantes.

Évolution de la rampe	Minimum-Maximum	Nombre	Erreur à croissance lente sur $\sqrt{(SSE)}$
Rapide	à partir de 2.6187 m/s	1025	
Lente	de 1.7424 à 2.6186 m/s	1045	
Très lente	de 0.8718 à 1.7425 m/s	697	

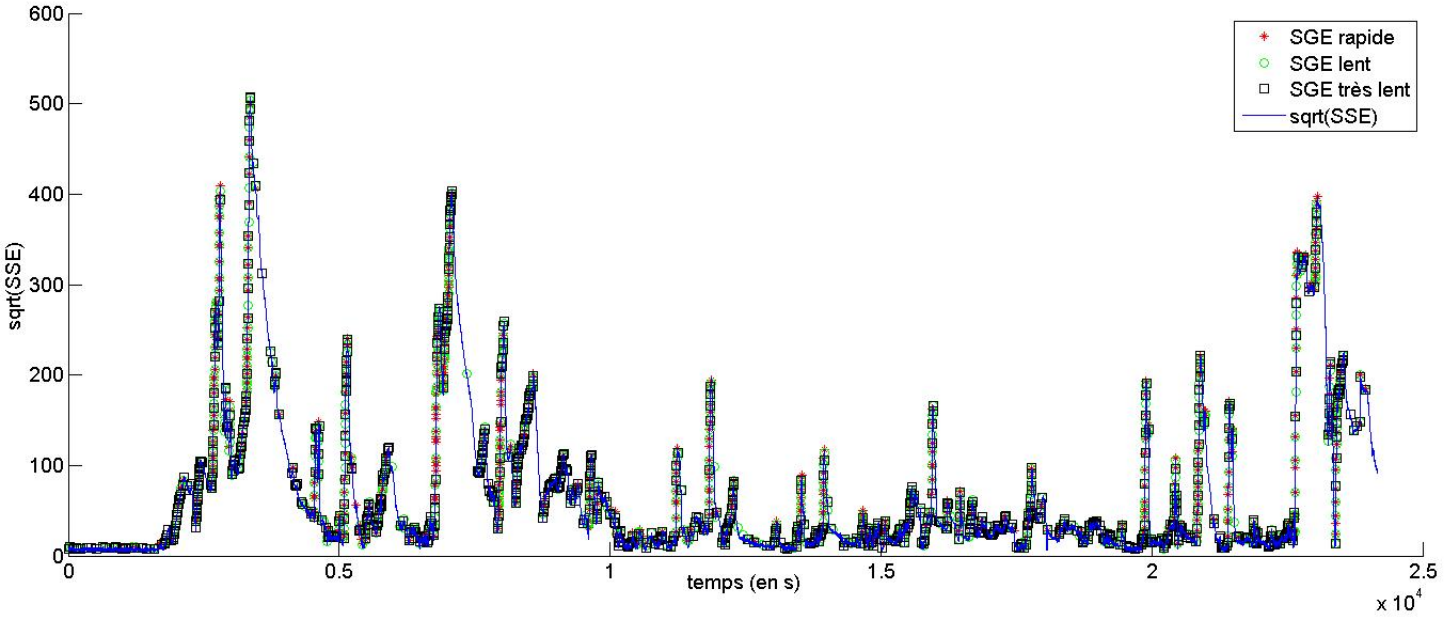


FIGURE 4.19 – Détection des différents types de rampe (rapide, lente et très lente).

Tableau 4.9 – Erreurs à croissance lente des 5 jeux de données du récepteur LEA-6T (bas coût).

Date / Lieu	30/01/12 Nantes	21/02/12 Paris (Boulevards)	22/02/12 Paris (Boulevards)	22/02/12 Paris (XIIème)	23/02/12 Paris (XIIème)
Rampe très lente	697	867	892	1 299	1 247
Rampe lente	1 045	1 661	1 803	1 854	1 948
Rampe rapide	1 025	1 939	2 081	1 531	1 739
Aucune détection	10 671	22 586	29 109	14 420	15 178

4.4.2 Qualité de la détection des erreurs GNSS et INS

Dans cette section, nous présentons les résultats sur la qualité de la détection des biais instantanés et des erreurs à croissance lente. Cette qualité s'exprime en fonction de la probabilité de détection manquée notée pmd et de fausse alarme pfa. Dans les tableaux 4.10 et 4.11 (qui s'appuient sur les tableaux 4.7 et 4.9), les estimations de ces deux probabilités seront données compte tenu de la taille des échantillons limitée (plus l'échantillon est grand, plus l'estimation est représentative de la réalité).

4.4.2.1 Qualité de la détection des biais instantanés

Le tableau 4.10 indique, pour chacun des 5 jeux de données, le nombre de détections manquées et de fausses alarmes dans le cadre de la détection des biais instantanés. Les fausses détections sont au nombre minimal de 86 (sur 37 550 instants) pour le jeu de Paris XIIème et au maximum de 198 (sur 24 162 instants) pour le jeu de Nantes. Ceci nous donne des estimations de probabilité de fausse détection entre 2,29 $\times$ 10^{-3} et 8,19 $\times$ 10^{-3} (données sans unité).

Tableau 4.10 – Nombre de fausses détections et de détections manquées de biais instantanés et leur probabilité estimée associée.

Date / Lieu	30/01/12 Nantes	21/02/12 Paris (Boulevards)	22/02/12 Paris (Boulevards)	22/02/12 Paris (XIIème)	23/02/12 Paris (XIIème)
Taille échantillon	24 162	49 126	60 770	35 583	37 550
Fausses détections	198	98	133	203	86
Détections manquées	469	816	607	2 499	2 156
pfa_{moy}	$8{,}19 \times 10^{-3}$	$1{,}99 \times 10^{-3}$	$2{,}19 \times 10^{-3}$	$5{,}7 \times 10^{-3}$	$2{,}29 \times 10^{-3}$
pmd_{moy}	$1{,}94 \times 10^{-2}$	$1{,}66 \times 10^{-2}$	1×10^{-2}	$7{,}02 \times 10^{-2}$	$4{,}57 \times 10^{-2}$
pfa_{moy} global			$3{,}47 \times 10^{-3}$		
pmd_{moy} global			$3{,}16 \times 10^{-2}$		

Les détections manquées sont au nombre minimal de 469 (sur 24 162 instants) pour le jeu de Nantes et au maximum de 2 499 (sur 35 583 instants). Ceci permet de calculer les estimations de probabilités de détection manquées entre $1{,}94 \times 10^{-2}$ et $7{,}02 \times 10^{-2}$. En concaténant les 5 jeux de données, nous avons les estimations globales de pfa et pmd qui sont respectivement de $3{,}47 \times 10^{-3}$ et $3{,}16 \times 10^{-2}$. Nous pouvons constater qu'il y a plus de biais instantanés dont la présence n'a pas été détectée que de fausses alarmes.

4.4.2.2 Qualité de la détection des erreurs à croissance lente

Le tableau 4.10 donne, pour les 5 jeux de données, le nombre de détections manquées et de fausses alarmes dans le cadre de la détection des erreurs à croissance lente. Les fausses détections sont au nombre minimum de 1 475 (sur 24 162 instants) pour le jeu de Nantes et au maximum de 2 458 (sur 37 550 instants) pour le jeu de Paris XII du 23/02/12. Ceci nous donne des estimations de probabilité de fausse détection entre $6{,}1 \times 10^{-2}$ et $6{,}55 \times 10^{-2}$. Concernant les détections manquées, il n'y en a pas dans le jeu de Paris Boulevards du 21/02/12. Le nombre maximal de détection manquées est de 206 pour le jeu de Paris XII du 23/02/12 soit une estimation de probabilité de détection manquée de $5{,}49 \times 10^{-3}$. Sur les 5 jeux de données concaténés, nous avons des pfa et pmd globaux respectivement égaux à $4{,}72 \times 10^{-2}$ et $1{,}88 \times 10^{-3}$. Nous constatons un très faible nombre de détections manquées comparé au nombre de fausses alarmes.

Tableau 4.11 – Nombre de fausses détections et de détections manquées d'erreurs à croissance lente et leur probabilité estimée associée.

Date / Lieu	30/01/12 Nantes	21/02/12 Paris (Boulevards)	22/02/12 Paris (Boulevards)	22/02/12 Paris (XIIème)	23/02/12 Paris (XIIème)
Taille échantillon	24 162	49 126	60 770	35 583	37 550
Fausses détections	1475	1849	2172	1818	2458
Détections manquées	17	0	76	90	206
pfa_{moy}	$6{,}1 \times 10^{-2}$	$3{,}8 \times 10^{-2}$	$3{,}57 \times 10^{-2}$	$5{,}11 \times 10^{-2}$	$6{,}55 \times 10^{-2}$
pmd_{moy}	$7{,}04 \times 10^{-4}$	0	$1{,}25 \times 10^{-3}$	$2{,}53 \times 10^{-3}$	$5{,}49 \times 10^{-3}$
pfa_{moy} global			$4{,}72 \times 10^{-2}$		
pmd_{moy} global			$1{,}88 \times 10^{-3}$		

Nous avons comptabilisé les fausses alarmes et les détections manquées des deux types de détections. En comparant les deux tableaux, nous pouvons affirmer que la détection des biais instantanés produit peu de fausses détections et un nombre plus important de détections manquées. *A contrario*, la détection des erreurs à croissance lente produit peu de détections manquées et un nombre plus important de fausses alarmes. Une détection optimale répond au meilleur compromis entre pfa et pmd. Un pfa élevé a pour conséquence un problème de disponibilité (freinage d'urgence inutile) et un pmd élevé relève plus d'un problème de sécurité (freinage d'urgence non déclenché à la présence d'une erreur de position inacceptable).

Le nombre de détections manquées et de fausses alarmes des erreurs à croissance lente et des biais instantanés sont utiles pour juger de la qualité de la détection. Cependant, ils ne suffissent pas à identifier totalement un risque sur l'intégrité. Pour le risque d'intégrité, il convient de compléter l'étude en prenant en compte le temps d'alerte TTA, le calcul du niveau de protection PL et de sa comparaison avec l'erreur de position PE. C'est l'objet de la sous-section qui suit.

4.4.3 Détermination du niveau de protection

Grâce à la détermination du nombre d'occurrences des biais instantanés et des erreurs à croissance lente, il est possible d'identifier les évènements liés à la détection. Ceci n'est pas suffisant pour caractériser le risque d'intégrité. Nous rappelons que le niveau de protection est calculé à partir de la matrice d'observation H (plus précisément, les éléments de cette matrice relatifs à la composante horizontale de la position) et de P_{biais} et P_{rampe} (cf sous-section 3.5.5). Le tableau 4.12 donne les valeurs moyennes du niveau de protection pour chaque jeu de données.

Tableau 4.12 – PL moyen pour les 5 jeux de données du récepteur LEA-6T (bas coût).

Date / Lieu	30/01/12 Nantes	21/02/12 Paris (Boulevards)	22/02/12 Paris (Boulevards)	22/02/12 Paris (XIIème)	23/02/12 Paris (XIIème)
PL_{moyen}	17,1052	11,7154	15,8307	37,1690	43,0329

La figure 4.20 montre l'évolution de PL sur la simulation avec le premier jeu de données. On rappelle également que le PL considéré dans ce mémoire a pour but de borner l'erreur de position PE. Il s'agit ici de la manière choisie dans le chapitre 3 pour calculer PL. Il en existe d'autres (cf sous-section 3.5.5 du chapitre 3 et dans [Le Marchand, 2010] ou Faurie [2011]). Nous pouvons voir que PL est globalement supérieur à PE (98, 75 % du temps). Ce qui signifie que PL borne bien PE. La figure 4.20 montre aussi un zoom sur une fenêtre de temps où $PL > PE$. Ces instants représentent 1, 25 % restants et ne désignent pas nécessairement un problème d'intégrité si $PE < AL$. Il faut également intégrer le niveau d'alerte AL pour déterminer les situations liées à un risque sur l'intégrité. Avec ce niveau de protection, nous sommes à présent capable d'identifier le risque sur l'intégrité de la localisation.

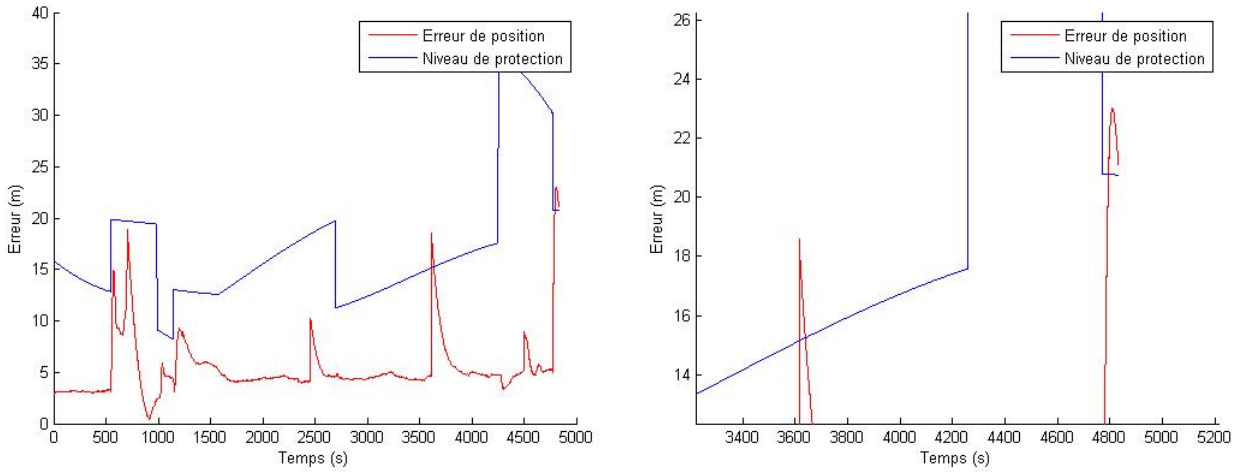


FIGURE 4.20 – Évolution du niveau de protection PL et de l'erreur de position PE au cours de la simulation et zoom sur des phases où $PL > PE$.

4.4.4 Risque sur l'intégrité de la localisation atteint par le système considéré

Reprenons les notations utilisées dans le chapitre 3. Nous avons exprimé le risque sur l'intégrité selon l'équation 4.22.

$$IR_{étendu}(t_i)) = p(A_{t_i}, A_{t_i+1}, ..., A_{t_i+t_{marge\_sécu}}) \tag{4.22}$$

Les évènements $A_{t_i}, A_{t_i+1}, ..., A_{t_i+t_{marge\_sécu}}$ représentent les situations dangereuses à chaque instant t_i jusqu'à $t_i + t_{marge\_sécu}$. L'ensemble des évènements successifs $\{A_{t_i}, A_{t_i+1}, ..., A_{t_i+t_{marge\_sécu}}\}$ représente une situation critique en terme d'intégrité. La période de temps $t_{marge\_sécu}$ est liée à l'application (cf. équation 3.39) correspond au temps TTA comme vu en au début du chapitre 4. Dans la section 3.7 du chapitre 3, nous avons identifié les situations 1, 2 et 3 comme étant critiques en terme d'intégrité. Le risque sur l'intégrité dépend de l'occurrence de chacune de ces situations. Grâce au calcul de PL et la détection des biais instantanés et erreurs à croissance lente, nous sommes en mesure de calculer le nombre d'occurrences de chaque situation. Sachant le nombre de situations au total (par exemple, 24 162 pour la simulation de Nantes), il est possible d'estimer la probabilité liée au risque sur l'intégrité. Néanmoins, une précaution doit être prise : une probabilité est d'autant plus représentative de la réalité (c'est à dire qu'un risque R est bien quantifié) que le nombre de situations possibles n tend vers l'infini. Étant donné qu'il est impossible de générer un nombre infini

de situations, une estimation des probabilités sera déterminée par un échantillon statistique suffisamment grand. Pour construire cet échantillon, nous concaténons les 5 scénarios. Plus précisément, nous additionnons le nombre d'occurrences des situations de risque sur l'intégrité. Ce nombre sera ensuite divisé par le nombre total d'instants des 5 scénarios (soit 207 191 ou la somme des temps de mission Tm de chaque scénario). Pour comptabiliser les différentes situations, nous avons besoin de PL ainsi que de AL et TTA (fixés à 20 mètres et 4 secondes), PE et de la détection des biais instantanés et erreurs à croissance lente et de l'identification des détections manquées. Les trois dernières situations (S4, S5 et S6) sont présentées dans le tableau 4.13 mais il s'agit de situations liées aux défaillances dangereuses détectées et sécuritaires détectées du système. On rappelle que ce sont des situations qui n'entrent pas dans l'estimation de $IR_{étendu}$. En vue d'évaluer la sécurité du système de localisation, nous nous concentrons sur les situations S1, S2 et S3 qui correspondent respectivement aux états : la succession d'états DU sur $t_{marge\_sécu}$, celle des états SU sur $t_{marge\_sécu}$ et à la succession DU et SU sur un intervalle $t_{marge\_sécu}$.

Tableau 4.13 – Fréquences en nombre d'occurrences des situations critiques (S1 à S3) et non critiques (S4 à S6) en terme d'intégrité respectivement sur un temps de mission Tm en secondes puis ramenées à une heure).

Situations	Période	30/01/12 Nantes	21/02/12 Paris (Boulevards)	22/02/12 Paris (Boulevards)	22/02/12 Paris (XIIème)	23/02/12 Paris (XIIème)
S1	sur Tm s	0	0	$3{,}7 \times 10^{-3}$	$3{,}5 \times 10^{-3}$	$4{,}53 \times 10^{-4}$
	sur 1 h	0	0	$2{,}20 \times 10^{-4}$	$3{,}53 \times 10^{-4}$	$4{,}34 \times 10^{-5}$
S2	sur Tm s	$4{,}97 \times 10^{-4}$	$4{,}40 \times 10^{-2}$	$2{,}05 \times 10^{-2}$	$6{,}58 \times 10^{-2}$	$1{,}48 \times 10^{-2}$
	sur 1 h	$7{,}40 \times 10^{-5}$	$3{,}2 \times 10^{-3}$	$1{,}20 \times 10^{-3}$	$6{,}7 \times 10^{-3}$	$1{,}4 \times 10^{-3}$
S3	sur Tm s	$8{,}3 \times 10^{-4}$	$5{,}7 \times 10^{-2}$	$3{,}30 \times 10^{-2}$	$2{,}73 \times 10^{-1}$	$2{,}02 \times 10^{-2}$
	sur 1 h	$1{,}23 \times 10^{-4}$	$4{,}2 \times 10^{-3}$	$2{,}0 \times 10^{-3}$	$8{,}7 \times 10^{-3}$	$1{,}9 \times 10^{-3}$
S4	sur Tm s	$1{,}19 \times 10^{-1}$	6×10^{-3}	$5{,}37 \times 10^{-1}$	$9{,}59 \times 10^{-2}$	$9{,}34 \times 10^{-1}$
	sur 1 h	$1{,}18 \times 10^{-3}$	$4{,}40 \times 10^{-4}$	$3{,}18 \times 10^{-2}$	$9{,}7 \times 10^{-3}$	$8{,}95 \times 10^{-2}$
S5	sur Tm s	$8{,}2 \times 10^{-3}$	$1{,}8 \times 10^{-3}$	$1{,}9 \times 10^{-3}$	$7{,}8 \times 10^{-3}$	$4{,}2 \times 10^{-3}$
	sur 1 h	$1{,}2 \times 10^{-3}$	$1{,}30 \times 10^{-4}$	$1{,}14 \times 10^{-4}$	$7{,}86 \times 10^{-4}$	$4{,}03 \times 10^{-4}$
S6	sur Tm s	$1{,}28 \times 10^{-1}$	$8{,}3 \times 10^{-3}$	$5{,}38 \times 10^{-1}$	$1{,}03 \times 10^{-1}$	$9{,}34 \times 10^{-1}$
	sur 1 h	$1{,}91 \times 10^{-2}$	$6{,}12 \times 10^{-4}$	$3{,}19 \times 10^{-2}$	$1{,}05 \times 10^{-2}$	$8{,}95 \times 10^{-2}$
Total instants		24 162	49 126	60 770	35 583	37 550

La situation S1 représente la situation où PE dépasse AL alors que PL est en dessous de AL et que la détection d'un biais instantané et d'une erreur à croissance lente est manquée. Cet état DU est le cas identifié comme le plus critique en terme d'intégrité. Nous nous apercevons que cette situation n'apparait jamais dans le premier jeu de données (idem pour le deuxième). Cela signifie que PE ne dépasse jamais AL dans le scénario de Nantes et de Paris Boulevard du 21/02/12. Ceci aura une conséquence directe sur le risque sur l'intégrité de ces deux scénarios (cf tableau 4.14).

La situation S2 représente la situation où PE dépasse PL sachant que PE reste en dessous de

AL et qu'aucun biais instantané et erreur à croissance lente n'est détecté ceci sur la durée TTA. Sur la même simulation illustrée sur toute cette section (Nantes 30/01/12), si 284 biais instantanés et 2767 erreurs à croissance lente tous types confondus sont détectés, 469 biais instantanés et 17 erreurs à croissance lente ne sont pas détectés. La situation où ces erreurs se succèdent en même temps sur une durée d'au moins égale à TTA apparait 123 fois. Ce qui donne une estimation de probabilité sur la simulation de 4,97 $\times$ 10^{-4} (sur un Tm de 4 832,4 secondes) et, ramenée à 1 heure, 7,40 $\times$ 10^{-5}. La situation 2 apparait également moins souvent au cours du premier scénario où l'estimation de probabilité (ramenée à l'heure) est de l'ordre de $10^{-5}/h$ alors que les autres scénarios restent cantonnés à $10^{-3}/h$ voire moins.

La situation S3 est la succession de DU et SU durant à un temps $t_{marge\_sécu}$. Cette situation apparait 8,3 $\times$ 10^{-4} soit 1,23 $\times$ 10^{-4} sur un intervalle de temps d'une heure.

Tableau 4.14 – Estimations des probabilités du risque sur l'intégrité IR pour chaque scénario puis ramenées à une heure et IR global avec les scénarios concaténés.

	Période	30/01/12 Nantes	21/02/12 Paris (Boulevards)	22/02/12 Paris (Boulevards)	22/02/12 Paris (XIIème)	23/02/12 Paris (XIIème)
$IR_{étendu}$	sur Tm s	1,3 $\times$ 10^{-3}	1,01 $\times$ 10^{-1}	5,74 $\times$ 10^{-2}	1,55 $\times$ 10^{-1}	3,54 $\times$ 10^{-2}
	sur 1 h	1,94 $\times$ 10^{-4}	7,40 $\times$ 10^{-3}	3,40 $\times$ 10^{-3}	1,57 $\times$ 10^{-2}	3,39 $\times$ 10^{-3}
$IR_{étendu}$ global	sur Tm_{global} s			7,4 $\times$ 10^{-2}		
	sur 1 h			1,29 $\times$ 10^{-3}		

Les nombres d'occurrences liées aux situations critiques en terme d'intégrité (S1, S2 et S3) sont données. Le risque sur l'intégrité estimé ($IR_{étendu}$) est le nombre total d'occurrences des situations S1, S2 et S3 soit 1,94 $\times$ 10^{-4} sur un intervalle de temps d'une heure.

4.4.5 Application de la mise en relation de l'intégrité et de la sécurité

Le risque sur l'intégrité étant quantifié, il est possible de déduire $f_S(t)$ et PFH grâce à la relation entre l'intégrité et la sécurité proposée dans la sous-section 3.7.2 au chapitre 3.

Tableau 4.15 – $f_S(t)$ et PFH pour chaque scénario et pour les scénarios concaténés.

	30/01/12 Nantes	21/02/12 Paris (Boulevards)	22/02/12 Paris (Boulevards)	22/02/12 Paris (XIIème)	23/02/12 Paris (XIIème)
$f_S(t)$	6,62 $\times$ 10^{-5}	5,10 $\times$ 10^{-3}	2,90 $\times$ 10^{-3}	7,80 $\times$ 10^{-3}	1,80 $\times$ 10^{-3}
PFH (en h^{-1})	1,94 $\times$ 10^{-4}	7,40 $\times$ 10^{-3}	3,40 $\times$ 10^{-3}	1,57 $\times$ 10^{-2}	3,39 $\times$ 10^{-3}
$f_S(t)$ global			3,7 $\times$ 10^{-3}		
PFH global (en h^{-1})			1,29 $\times$ 10^{-3}		

Pour une vision globale, nous résumons, dans le tableau 4.15, les valeurs moyennes $f_S(t)$ et PFH pour chaque jeu de données concaténé (GNSS et INS) et calculées à partir de $IR_{étendu}$ (cf tableau 4.14). Ceci permet de retenir une seule valeur à évaluer par paramètre. D'après le tableau 4.14, le système GNSS/INS atteint un risque sur l'intégrité estimé à 1,94 $\times$ $10^{-4}/h$ pour le scénario de Nantes. Dans la sous-section 4.2.4, nous avons choisi un objectif de risque sur l'intégrité égal à 4,8 $\times$ $10^{-6}/h$. Nous remarquons donc que l'objectif de risque sur l'intégrité n'est pas atteint. $f_S(t)$ et PFH, déduits de $IR_{étendu}$, sont estimées respectivement à 6,62 $\times$ 10^{-5} (quantité sans dimension) et 1,94 $\times$ $10^{-4}/h$ toujours pour le scénario de Nantes. Sur l'ensemble des scénarios, $f_S(t)$ et PFH atteignent respectivement 3,7 $\times$ 10^{-3} et 1,29 $\times$ $10^{-3}/h$. PFH nous permet de déterminer un niveau de SIL grâce au tableau de la norme 61508. Le SIL associé à ce PFH est SIL1. Ce résultat doit prendre en considération la précision atteinte par notre application. En effet, d'autres études telles que LOCOPROL/LOCOLOC [Wynants, 2001] ont proposé des architectures de système avec GNSS atteignant le niveau SIL4 mais où la position était estimée dans un intervalle de 200 à 400 mètres de long 98% du temps. Dans le tableau 4.6, la précision atteinte par notre application est, dans le pire des cas (jeu de données de Paris XII du 23/02/12), de 17,49 mètres 95% du temps et 27 mètres 98% sans l'appui de systèmes d'augmentation satellitaires.

La section suivante propose de discuter plus en détail ces résultats et de revenir sur les hypothèses prises lors de la phase de détection.

4.4.6 Discussions sur les résultats et sur la pertinence des hypothèses prises sur l'application

Classiquement, la phase de détection d'un contrôle d'intégrité prend pour hypothèse que les NSSE suivent une loi du χ^2. On rappelle que NSSE est utilisée comme variable aléatoire lors des tests statistiques effectués pour la détection puisque, d'un point de vue opérationnel, l'erreur de position est inconnue. Dire que la distribution de NSSE suit une loi du χ^2 suppose que les résidus (indicateurs de défaut des mesures utilisés à la place des erreurs réelles de mesures de capteurs) suivent une loi normale. Or, dans des environnements sujets au phénomène de multitrajet, cette affirmation n'est pas vérifiable compte tenu de la variabilité de l'environnement.

La figure 4.21 montre que l'évolution des résidus sur une pseudodistance n'est pas un processus aléatoire suivant une loi normale de moyenne et variance données. Il s'agit là de la principale faiblesse de la détection. La qualité de la détection a été clairement évaluée en terme de nombre de détections vraies, fausses et détections manquées. Cette faiblesse implique qu'un biais sur NSSE n'indique pas forcément une erreur de position au même instant comme le montre la figure 4.22. Nous n'avons parlé que de l'aspect GNSS de la détection. La comparaison des résultats sur la qualité de la détection de biais instantanés (GNSS) (cf tableau 4.7) et erreurs à croissance lente (INS) (cf tableau 4.9) montre un nombre de détections manquées plus faible côté INS que côté GNSS. Ceci suppose que l'hypothèse discutée ici demeure valable pour la détection des erreurs à croissance lente. Pour lever cette hypothèse côté GNSS, d'autres lois statistiques peuvent être utilisées pour décrire la distribution de NSSE comme la loi de Rayleigh par exemple [Arnold and Emerson, 2011].

La loi de distribution utilisée a également un impact sur le calcul du niveau de protection. En effet, l'erreur minimale détectable pour les biais instantanés, (P_{biais}), et pour les erreurs à croissance lente (P_{rampe}) utilisées lors de ce calcul, dépend du paramètre de non-centralité c. Celui-ci est déterminé grâce à la densité de probabilité d'une loi du χ^2 sachant une probabilité de détection manquée donnée (cf équation 3.20 dans la section 3.6.1 du chapitre 3). Une précaution doit être prise. Dans la

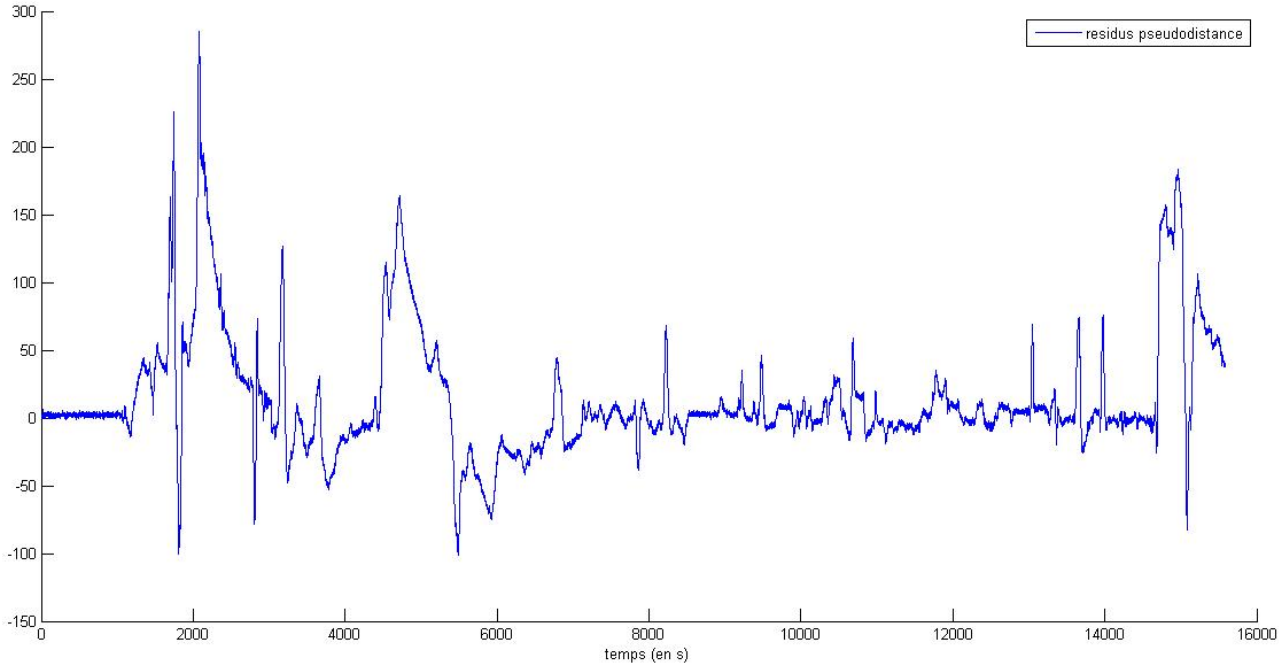


FIGURE 4.21 – Résidus pseudodistance du satellite 1 (scénario de Nantes).

figure 4.20, PL borne bien PE. S'il est décidé de changer de loi statistique pour les raisons invoquées au début de cette sous-section alors PL sera modifié et il n'est pas garanti.

Dans ce chapitre, nous avons considéré un système GNSS/INS en hybridation serrée avec un récepteur GNSS et un INS bas coût uniquement. Du point de vue purement structurel, la redondance est le moyen le plus logique d'améliorer la sécurité du système de localisation avec GNSS. Selon la norme 61508, un système GNSS/INS peut être vu comme une architecture 1oo2D dont le récepteur GNSS et l'INS constituent les deux canaux et le contrôle de l'intégrité, le processus de diagnostic. Un tel système est capable de réaliser sa fonction (fournir une localisation) si au minimum un canal n'est pas dans un état dangereux (lié au risque d'intégrité). De meilleurs résultats peuvent donc être espérés d'une architecture 1ooND [Ding et al., 2014] c'est à dire en couplant d'autres systèmes de localisation au récepteur GNSS et à l'INS. C'est pour cette raison que les projets nationaux et européens (cf sous-section 1.4.3 du chapitre 1) ont opté pour des solutions de localisation de plus en plus complexes en vue d'être appliquées au contrôle-commande ferroviaire.

De plus, nous n'avons pas traité les signaux issus de systèmes d'augmentation satellitaires tels qu'EGNOS (système présenté au chapitre 1). L'utilisation de ce type de système couplé à un récepteur GNSS apporte un gain supplémentaire de performance notamment pour l'intégrité mais ne gère pas les problèmes de masquages et de multitrajets liés à l'environnement proche. D'ailleurs, la redondance entre systèmes d'augmentation satellitaires n'est pas à exclure. D'autres recommandations seront formulées de manière plus détaillée dans les perspectives de ce mémoire.

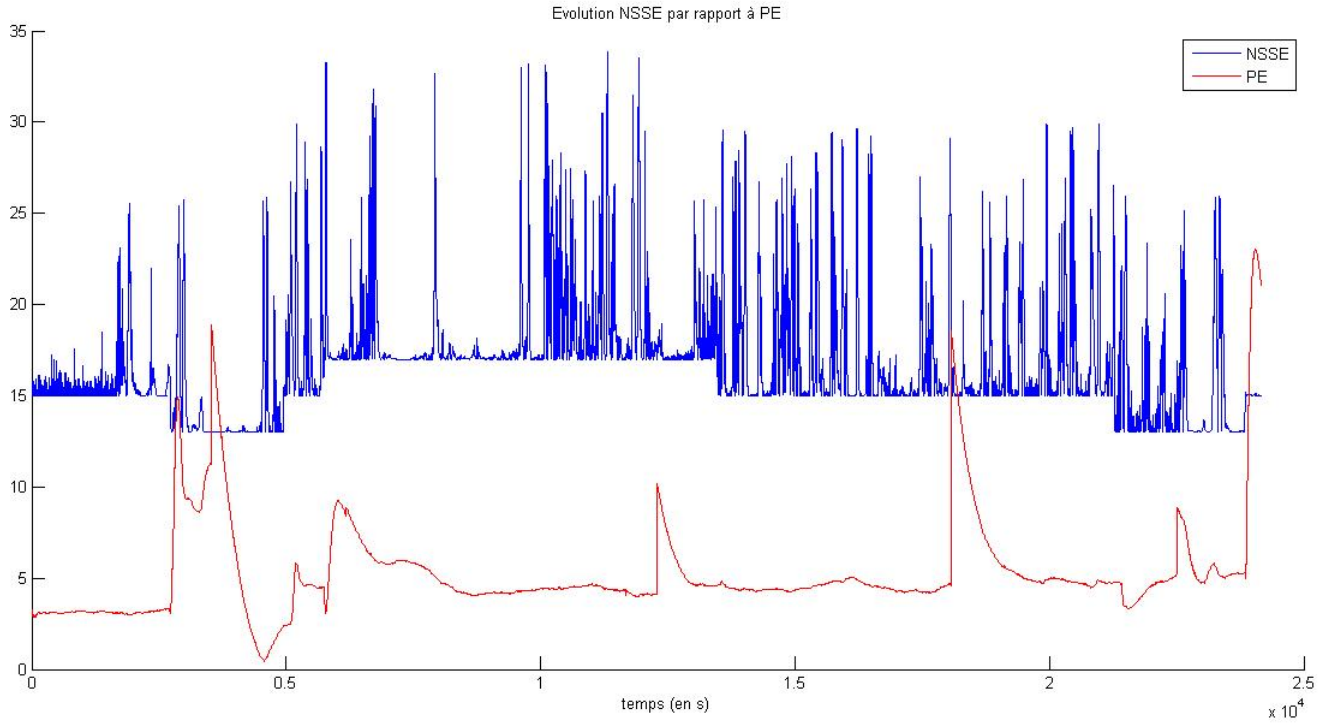


FIGURE 4.22 – Évolution de NSSE par rapport à PE (scénario de Nantes).

4.5 Synthèse

Dans ce chapitre, nous avons appliqué sur un cas d'utilisation les propositions mathématiques du chapitre 3 concernant l'évaluation de la sécurité au travers de l'évaluation de l'intégrité de la localisation ferroviaire. Le chapitre 2 a permis de justifier le choix d'une architecture centrée sur l'utilisation d'un récepteur GNSS. Le choix d'un GNSS/INS en hybridation serrée est motivé de plusieurs manières. D'abord, la centrale inertielle (INS) est un système très connu en navigation, complémentaire à un récepteur GNSS pour pallier les problèmes de disponibilité liés au masquage des satellites. Les projets comme APOLO, InteGRail ou LOCASYS (parmi ceux présentés au chapitre 1) ont d'ailleurs choisi ces technologies de localisation pour leurs systèmes. Enfin, le système GNSS/INS s'est révélé prometteur au regard de nos analyses de sensibilité et causale du chapitre 2.

Pour mettre en œuvre un contrôle d'intégrité sur le système GNSS/INS, nous nous sommes concentrés sur le dimensionnement des différents paramètres d'exigence pour l'intégrité de la localisation (AL, TTA et IR). Le concept d'intégrité considéré dans la thèse étant peu connu dans le milieu ferroviaire, le chapitre 3 a posé clairement les définitions du concept de l'intégrité de la localisation ferroviaire. Dans ce chapitre 4, il était nécessaire de justifier le choix des valeurs d'exigence pour l'intégrité. Bien que des propositions de valeurs aient été faites par le groupe de travail *GNSS-Rail User Forum*, notamment pour des applications liées à la sécurité [Barbu, 2000], ces valeurs nous ont paru difficilement atteignables et très contraignantes en comparaison avec l'une des applications aéronautiques les plus critiques en matière de sécurité et d'intégrité : l'approche précise avant l'atterrissage. Des justifications ont été trouvées au sein de documents de spécifications du système de contrôle-commande et de signalisation ERTMS.

La seconde partie de ce chapitre est consacrée à la présentation de l'architecture choisie ainsi que des données utilisées : les mesures GNSS et les données de simulation INS. Les données GNSS (fournies par l'équipe Geoloc de l'IFSTTAR Nantes) et les données INS ont été fusionnées grâce aux routines Matlab® issues de [Groves, 2013] et adaptées pour le cas d'utilisation. Le protocole de simulation a été posé et l'initialisation des données (positions/vitesses/accélérations initiales) nécessaires au fonctionnement du système GNSS/INS sont disponibles en annexe C.

La troisième partie a montré les résultats de la détection des erreurs considérées (les biais instantanés et les erreurs à croissance lente). Cette phase est une étape importante dans le contrôle de l'intégrité puisqu'elle a permis d'identifier les situations à risque en termes d'intégrité et d'en estimer une probabilité grâce aux échantillons de données mis à notre disposition. Grâce au lien intégrité-sécurité formalisé dans le chapitre 3 section 3.7.2, les probabilités $f_s(t)$ et PFH ont été déduites. Ces probabilités sont des paramètres utilisés en sécurité ferroviaire (cf Annexe A). La détermination de PFH a permis de déduire un niveau d'intégrité de sécurité ou SIL pour le système de localisation considéré grâce au tableau de la norme 61508 (repris dans la section 2.2 du chapitre 2). Nous suggérons d'employer des systèmes d'augmentation de type SBAS tels qu'EGNOS ou de type ABAS autre que le contrôle d'intégrité.

Conclusion générale et perspectives

Ces travaux de thèse ont porté sur l'évaluation de la sécurité des systèmes de localisation ferroviaires s'appuyant sur des systèmes satellitaires. Les verrous scientifiques concernant cette évaluation ont été d'ordre méthodologiques (méthodes de sûreté de fonctionnement reposant sur le retour d'expérience inadaptées) et environnementaux (transport guidé évoluant dans un environnement contraint et varié pour la propagation des signaux). Des problématiques sont apparues au niveau des systèmes (sources d'erreur hétérogènes des systèmes de localisation considérés) et au niveau des référentiels normatifs, cultures de la sécurité différentes entre le domaine ferroviaire (Normes [EN 50126, 2000], [EN 50128, 2001] et [EN 50129, 2003]) et le domaine aéronautique (Normes SARPs [ICAO, 2006]).

Nous avons proposé deux analyses inspirées d'approches classiques de SdF et adaptées aux problématiques citées précédemment : l'analyse causale [Legrand et al., 2014] et l'analyse de sensibilité [Legrand et al., 2013]. Ces analyses ont permis de construire une méthodologie centrée sur l'évaluation de la sécurité des systèmes de localisation ferroviaires de type GNSS et d'autres sources de localisation par la mise en relation de l'intégrité étendue avec la sécurité. Cette méthodologie constitue la contribution majeure de cette thèse.

Bilan de la thèse

Un état de l'art sur les systèmes de localisation et de navigation ferroviaire a été réalisé dans le chapitre 1. Le fonctionnement classique des systèmes de localisation de type GNSS a été décrit de manière détaillée et des techniques satellitaires avancées (localisation hybride, récepteurs RTK, *Precise Point Positioning*) ont également été présentées. Les enjeux économiques, écologiques et techniques des GNSS ont été mis en lumière. Les technologies s'appuyant sur les satellites peuvent, selon l'ERA [European Railway Agency, 2012], jouer un rôle majeur dans la sécurité ferroviaire. Ce rôle va au-delà de la sécurité puisque les GNSS peuvent répondre aux besoins en termes d'augmentation de la capacité des lignes ferroviaires ainsi qu'à des besoins écologiques (cf [COP21, 2015]) en réduisant l'empreinte carbone de l'infrastructure ferroviaire. Une synthèse des projets nationaux et européens (du projet APOLO (1999-2001) jusqu'au projet EATS (2014-2016)) a été réalisée dans le but de positionner les travaux de cette thèse sur la question de l'évaluation de la sécurité des systèmes avec GNSS dans le domaine ferroviaire. Enfin, les problématiques liées à la gestion de la sécurité ont été présentées notamment celles qui traitent des risques non maitrisés que représentent l'usage des récepteurs GNSS dans le domaine ferroviaire et l'évaluation des performances des GNSS dont la formulation diffère des attributs classiques de SdF.

Le chapitre 2 a présenté, dans une première partie, la gestion de la sécurité des systèmes embarqués ferroviaires utilisant les GNSS. Le cadre européen de la gestion des risques dans le domaine ferroviaire a été posé avec l'obligation d'adopter une Méthode de Sécurité Commune [Réglement 2015/1136, 2015] dans le cas de changements significatifs du système ferroviaire. Les GNSS occasionnent ce type de changement puisqu'ils constituent notamment une innovation importante pour la localisation ferroviaire. Ce processus de gestion des risques fait appel aux concepts de SdF dont nous avons rappelé la théorie avec les définitions des concepts de fiabilité, de disponibilité, de maintenabilité et de sécurité et la présentation de plusieurs méthodes d'évaluation quantitatives et/ou qualitatives. Dans une deuxième partie, face aux problématiques relatives à l'utilisation des GNSS dans le domaine ferroviaire, de nouvelles méthodes centrées sur une analyse causale et une analyse de sensibilité ont permis d'apporter de nouveaux indicateurs de SdF (nombre de combinaisons d'états critiques, persistance de ces combinaisons et mesures de sensibilité) et, d'autre part, de comparer plusieurs architectures de capteurs pour un système de localisation ferroviaire avec GNSS. L'analyse causale a mis en évidence deux paramètres [Legrand et al., 2014] : le nombre de combinaisons critiques et leur persistance dans le temps. Dans un système multicapteurs, le premier paramètre est le nombre de combinaisons d'états des capteurs dont la sortie génère une position non acceptable. Ces combinaisons sont susceptibles d'amener la sortie du système dans un état inacceptable si elles persistent dans le temps. Le nombre de combinaisons critiques et leur persistance dans le temps ont également servi de critères de comparaison sur plusieurs architectures de capteurs avec GNSS. L'analyse de sensibilité a mis en évidence des mesures de sensibilité [Legrand et al., 2013]. Pour rappel, ces mesures quantifient l'influence d'un paramètre d'un capteur (facteur d'échelle, biais, résolution, température, *etc.*.) sur sa sortie et sur la sortie d'un système multicapteurs. Des valeurs extrêmes de mesures de sensibilité (calculées en fonction d'une erreur maximale permise sur la position) ont été proposées pour conclure sur l'acceptabilité de la sortie d'un système multicapteurs.

Dans le chapitre 3, nous nous sommes concentrés sur l'évaluation des indicateurs de la sécurité en montrant leur lien avec l'attribut d'intégrité de la localisation. Les notions autour de ce concept d'intégrité ont alors été présentées. Il a été nécessaire d'adapter ce concept initialement défini pour les GNSS seuls et pour des applications aéronautiques, au domaine ferroviaire où des systèmes multicapteurs sont utilisés [Legrand et al., 2015]. C'est ici que se situent les contributions majeures de la thèse à savoir :

— la définition de l'intégrité étendue associée à un algorithme de contrôle d'intégrité particulier,
— la détermination de cette intégrité pour l'évaluation de la sécurité des systèmes avec GNSS.

Cette détermination n'est possible que grâce à la mise en relation de la probabilité de défaillances liées à la sécurité avec la probabilité du risque sur l'intégrité. Nous avons identifié les défaillances dangereuses et sécuritaires non détectées comme des situations critiques en terme d'intégrité. Les simulations du système GNSS/INS et du contrôle d'intégrité proposés ont été utilisées pour appliquer numériquement ce lien et d'estimer les probabilités citées. Nous rappelons que la simulation et l'implémentation d'un contrôle d'intégrité n'est pas l'objectif principal de la thèse. Il s'agit d'évaluer la sécurité de système de localisation ferroviaire avec GNSS compte tenu des problématiques soulevées au début du mémoire. L'évaluation de l'intégrité de la localisation est une réponse cohérente face à ces problématiques. En effet, du point de vue de l'évaluation des performances d'un système, le concept d'intégrité, très proche de la sécurité telle que définie dans la norme [IEC 61508-4, 2010], donne accès à des processus d'évaluation (contrôle d'intégrité ou RAIM) répondant au manque de méthodes SdF adaptées pour les systèmes avec GNSS.

Dans le chapitre 4, un cas d'utilisation a été mené afin d'évaluer l'intégrité étendue pour les systèmes de localisation ferroviaire avec GNSS tel que proposée dans le chapitre précédent. Nous avons considéré la gestion de l'espacement entre deux trains dans le système de contrôle-commande ferroviaire ERTMS niveau 3. Dans ce niveau, une ligne ferroviaire n'est plus divisée en cantons fixes mais en cantons mobiles dont la longueur est déterminée en temps réel par la position du train. Dans le cas étudié, les balises ferroviaires sont remplacées par un système GNSS. Un des rôles de la balise dans le niveau 3 d'ERTMS est de calibrer l'odométrie et les autres capteurs proprioceptifs. Pour ce cas d'étude, le système avec GNSS choisi devient un élément critique en terme de sécurité et induit, en cas de défaillance, des risques de collision. Trois situations parmi six liées à l'intégrité conduisant à ce risque ont été identifiées. Ces situations, caractérisées en terme d'intégrité, sont liées à la comparaison d'un niveau de protection PL qui borne l'erreur de position avec un niveau d'alerte AL. Pour déterminer l'intégrité de la localisation, il a été nécessaire de justifier les exigences sur cette intégrité pour la gestion de l'espacement entre deux train. Ainsi, un niveau d'alerte AL, un temps d'alerte TTA et un objectif de risque sur l'intégrité sont des exigences déterminées grâce aux spécifications ERTMS. Le système de localisation choisi pour ce cas d'étude est un système avec un récepteur GNSS associé à une centrale inertielle (INS) en hybridation serrée.

Grâce à des données GNSS réelles de l'équipe Geoloc de l'IFSTTAR et des routines Matlab® liées au fonctionnement de l'INS et de l'hybridation serrée [Groves, 2013], le fonctionnement du système GNSS/INS a pu être simulé. L'algorithme de contrôle de l'intégrité étendue, proposé au chapitre 3, a été appliqué à ce système. D'abord, les erreurs au sein d'un système GNSS/INS que nous avons identifiées ont pu être détectées sur des simulations du système GNSS/INS. Il s'agit de biais instantanés induits par le phénomène de multitrajet et d'erreurs à croissance lente liées à la dérive de l'INS qui n'est plus compensé par la calibration à chaque passage du train sur une balise. Une fois ces erreurs détectées ainsi que les détections manquées identifiées, le niveau de protection PL a été calculé à chaque instant par le contrôle de l'intégrité. La détection manquée des erreurs et la valeur de PL par rapport à AL permettent de déterminer les probabilités d'occurrence des 6 situations identifiées pour la gestion de l'espacement entre deux trains. La probabilité de risque sur l'intégrité est estimée à partir de ces probabilités. Les résultats sur un échantillon significatif composé de mesures GNSS issues de 8 jeux de données concaténées et de simulations sur le système INS montrent que l'objectif sur le risque d'intégrité n'est pas atteint ($1{,}29 \times 10^{-3}/h$ contre une exigence de $4{,}8 \times 10^{-6}/h$ issue de premières réflexions sur l'intégrité de la localisation ferroviaire [Filip et al., 2008b]). Ces résultats doivent prendre en compte les hypothèses décrites en fin de chapitre 4.

Au vu de ces résultats, des recommandations sont proposées à la fois sur le système GNSS/INS lui-même (redondance de capteurs), sur l'appui de systèmes d'augmentation satellitaire (EGNOS) et sur l'algorithme d'intégrité étendue proposé (phase de détection des erreurs et calcul du niveau de protection).

Perspectives

Plusieurs perspectives se dégagent de ces travaux de thèse. Elles concernent l'évaluation des performances de ces systèmes pour des applications ferroviaires de sécurité sur deux aspects : l'évaluation quantitative des attributs de sûreté de fonctionnement et l'évaluation de la sécurité grâce à l'intégrité. Du point de vue de la sûreté de fonctionnement, plusieurs perspectives sont à noter :

— L'évaluation de l'attribut de sécurité a été conduite en priorité afin d'apporter des éléments justificatifs pour qu'un système de localisation ferroviaire avec GNSS soit autorisé à être mis en service dans le système ferroviaire global. Cependant, l'évaluation des attributs de fiabilité, de disponibilité et de maintenabilité n'a pas été abordée. Tout d'abord, la maintenabilité des GNSS est hors de propos puisque ce sont des systèmes considérés comme non réparables dans le domaine ferroviaire. Les attributs de fiabilité et de disponibilité peuvent suivre le même raisonnement que pour la sécurité avec l'intégrité. En effet, au même titre que l'intégrité a été rapprochée de la sécurité, la fiabilité peut être rapprochée de la précision et la disponibilité de la disponibilité de service [Filip et al., 2008a]. Des pistes de démonstrations sont proposées dans [Beugin et al., 2010] mais la disponibilité de service dépend non seulement de la probabilité de risque sur l'intégrité mais aussi du risque sur la continuité de service d'un système GNSS. Les situations de risque sur la continuité doivent être identifiées dans un cas d'utilisation ferroviaire. La relation probabiliste entre la fiabilité et la précision d'un récepteur GNSS est démontrable en cherchant à exprimer la probabilité de succès $R(t)$ (paramètre caractérisant la fiabilité dans la norme [EN 50126, 2000]) en fonction de la probabilité d'occurrence de l'évènement $[PL(t_i) \leq AL]$, évènement complémentaire $[PL(t_i) > AL]$ considéré comme une situation critique en terme d'intégrité dans le chapitre 3 et 4. Au même titre que l'intégrité, la précision et la disponibilité de service sont des attributs de performances des systèmes qui s'appuient uniquement sur les satellites définis dans les normes aéronautiques. Par conséquent, la précision et la disponibilité de service doivent également être étendues aux systèmes fondés sur les GNSS et dans un contexte ferroviaire.

— Les paramètres proposés dans la norme [EN 50126, 2000] pour caractériser la sécurité sont donnés à titre d'exemple pour des applications ferroviaires et restent généraux. Les mesures de sensibilité ont servi à définir des critères pour le choix d'un système pour le chapitre 4 mais ces critères peuvent aussi être des paramètres spécifiques de la localisation ferroviaire caractérisant l'attribut de sécurité de la même manière qu'une probabilité de défaillance liée à la sécurité.

— Les deux paramètres identifiés lors de l'analyse causale (nombre de combinaisons critiques d'état de capteurs et leur persistance dans le temps) peuvent servir à déterminer quantitativement les paramètres caractérisant la sécurité de la norme [EN 50126, 2000]. Le nombre de combinaisons critiques peut alors être approché d'un taux de situations dangereuses ($H(t)$) et la persistance de ces combinaisons permettrait de calculer un temps de retour dans un état de sécurité ($TTRS$).

La contribution majeure de la thèse, à savoir l'évaluation de la sécurité des systèmes de localisation ferroviaires avec GNSS par la formalisation de l'intégrité étendue à ces systèmes, conduit également à des pistes d'amélioration et aux perspectives suivantes :

— L'algorithme de contrôle d'intégrité proposé dans le chapitre 3 s'appuie sur un algorithme de type *Fault Detection*. Les performances de la détection sont alors primordiales. Ces performances sont exprimées en termes de probabilité de détection manquée *pmd* et de probabilité de fausse alarme pfa. Dans ce mémoire, ces valeurs sont fixées par rapport aux normes aéronautiques ICAO [2006]. Des évaluations de performances de contrôle d'intégrité dans l'aéronautique et l'automobile ont déjà été proposées [Martineau et al., 2008] [Le Marchand, 2010] [Faurie, 2011]. Ces évaluations consistent en des études comparatives de différents algorithmes RAIM (fondés sur la méthode des moindres carrés, méthode du maximum de séparation, *etc.*.)

en termes de pfa, de pmd mais aussi sur la manière dont est calculé le niveau de protection PL. Nous proposons d'appliquer l'évaluation de la sécurité présentée dans le chapitre 3 sur des systèmes GNSS/INS associés à plusieurs contrôles de l'intégrité vus dans les travaux cités précédemment et de comparer les résultats en terme de risque sur l'intégrité et SIL déduit.

— Dans cette thèse, des étapes d'exclusion de fautes n'ont pas été considérées. L'étape de détection dans le contrôle d'intégrité a été suffisante pour conclure sur l'intégrité de la localisation fournie par le système GNSS/INS choisi dans le chapitre 4. L'exclusion apporte un gain sur les performances de localisation puisqu'elle rejette la source de localisation erronée. Cependant, cette étape engendre des situations dangereuses telles que l'exclusion manquée, l'échec de l'exclusion ou une mauvaise exclusion, des évènements liés au risque sur l'intégrité et au risque sur la continuité. Nous proposons de considérer une probabilité d'occurrence pour chacune de ces situations liées à l'exclusion pour recalculer un risque d'intégrité si un algorithme de type *Fault Detection and Exclusion* est utilisé comme dans [Faurie, 2011]. Des démonstrations probabilistes pour ces situations sont proposées dans [Filip et al., 2008b].

— La détection au sein de l'algorithme issue de ce travail de thèse repose sur des hypothèses statistiques relatives aux résidus discutées dans la sous-section 4.4.6 du chapitre 3. Afin que ces hypothèses soient valables, les résidus doivent être indépendants. De plus, leur distribution doit suivre des lois normales de moyenne et d'écart-type donnés afin de pouvoir appliquer le test du χ^2, utilisé pour la détection des biais instantanés. En pratique, ces hypothèses sont très fortes voire peu réalistes. C'est en cela que réside la faiblesse du test du χ^2. Il existe d'autres lois qui peuvent être testées telles que la loi de Rayleigh, la loi laplacienne, un mélange de lois gaussiennes. Ces lois peuvent être appliquées lors de tests tels que le test de Kolmogorov-Smirnov [Arnold and Emerson, 2011]. Cependant, le caractère non déterministe des pseudodistances suit difficilement une loi statistique donnée. La modélisation par un processus de Dirichlet des erreurs de pseudodistances proposée par [Viandier, 2011] pourrait certainement améliorer la détection des biais instantanés. La prise en compte de ces lois pour la modélisation des erreurs pourraient améliorer grandement les performances de détection de l'algorithme de contrôle d'intégrité proposé.

— Nous avons choisi de calculer le niveau de protection PL en fonction de la matrice d'observation H et de l'erreur minimal détectable du biais instantané (P_{biais}) et erreur à croissance lente (P_{rampe}). Il existe d'autres manières de calculer PL notamment par *overbounding* [Ahmad et al., 2014] dont nous prévoyons d'en utiliser les techniques. Il s'agit d'un processus qui a pour but de remplacer la distribution de l'erreur de position PE (seulement déduite de la position réelle) par un modèle conservatif simplifié. Ce modèle a pour objectif de prendre une marge suffisamment grande pour englober les risques inhérents aux erreurs non modélisées. La manière la plus simple est d'utiliser une loi normale centrée (moyenne nulle). Dans ce cas, PL sera de la forme $K \times \sigma$ où σ est l'écart-type des mesures de pseudodistance (+ mesure INS dans le cas d'un système GNSS/INS) et de K, un coefficient multiplicateur. Dans [RTCA, 2006] (*Radio Technical Commission for Aeronautics*), PL est exprimé sous la forme $HPL = K_H \times d_{mayor}$ avec K_H est un coefficient multiplicateur dépendant de la phase de vol (cf tableau 3.1 dans la section 3.4 du chapitre 3) et d_{mayor} est fonction de l'écart-type des mesures de pseudodistance et de la matrice S déjà vue dans le calcul de PL utilisé dans la thèse.

Production personnelle

Conférences internationales avec actes et comités de lecture

— **Sensitivity Assessment to Analyse Dependability of a Multisensor Localisation System based on GNSS.**
Legrand, C., Beugin, J., Conrard, B., Marais, J., Berbineau, M., El-Koursi, E.-M.
13th International Conference on ITS Telecommunication (ITST 2013), Tampere, Finlande, 5-7 Novembre 2013.

— **Causal Analysis Methodology of Multisensor Systems based on GNSS.**
Legrand, C., Beugin, J., Conrard, B., Marais, J., Berbineau, M., El-Koursi, E.-M.
The Second International Conference on Railway Technology (Railways 2014), Ajaccio, France, 8-11 Avril 2014.

— **Approach for evaluating the safety of a satellite-based train localisation system through the extended integrity concept.**
Legrand, C., Beugin, J., Conrard, B., Marais, J., Berbineau, M., and El-Koursi, E.-M.
The 25th European safety and reliability conference (ESREL 2015), Zurich, Suisse, 7-10 Septembre 2015.

Revue internationale

— **From extended integrity monitoring to the safety evaluation of satellite-based localisation system.**
Legrand, C., Beugin, J., Conrard, B., Marais, J., Berbineau, M., El-Koursi, E.-M.
Soumise en Octobre 2015, Acceptée en Avril 2016 au journal Reliability Engineering and System Safety.

Rapports d'avancement

— **État de l'art, analyse causale et analyse de sensibilité pour l'analyse de sûreté de fonctionnement de systèmes de localisation embarqués basés sur les GNSS**
Legrand, C.
Rapport d'avancement Railenium 2013.

— **Contributions sur l'intégrité de la localisation pour l'évaluation de la sécurité des systèmes de localisation basés sur les GNSS.**
Legrand, C.
Rapport d'avancement Railenium 2014.
— **Contribution reporting - Résumé, faits marquants, difficultés, résultats obtenus.**
Legrand, C.
Rapport d'avancement Railenium 2015.

Article en dehors du cadre de la thèse

— **Diagnosis of human operator behaviour in case of train driving : interest of facial recognition.**
Legrand, C., Richard, P., Benard V., Vanderhaegen F., Caulier, P.
The 30th European Annual Conference on Human Decision-Making and Manual Control (EAM12), Braunschweig, Allemagne, 11-12 Septembre 2012.

Annexe A

Annexe de la norme EN50126 concernant les paramètres de sécurité applicables dans le domaine ferroviaire

Au cours de la thèse, nous cherchons à caractériser des paramètres liés à l'attribut de sécurité dans le ferroviaire. Le tableau A.1 propose la liste de paramètres proposée dans la norme EN50126 EN 50126 [2000].

Tableau A.1 – Paramètres de sécurité

Paramètres	Symbole	Dimension
Temps moyen entre défaillances dangereuses consécutives	$MTBF(H)$	temps, distance, cycle
Temps moyen entre défaillances d'un "système de sécurité"	$MTBSF$	temps, distance, cycle
Taux de situations dangereuses	$H(t)$	défaillance/temps, distance, cycle
Probabilité de défaillance liées à la sécurité	$f_S(t)$	sans dimension
Probabilité de fonctionnement en "sécurité"	$S_S(t)$	sans dimension
Temps de retour à un état de sécurité	$TTRS$	temps

Le temps moyen entre défaillances dangereuses consécutives ou $MTBF(H)$ a été défini dans le chapitre 2.

Il s'agit d'exemples de paramètres de sécurité pour tout système ou sous-système ferroviaire. Par conséquent, d'autres paramètres peuvent être trouvés pour des systèmes plus spécifiques tels qu'un système de localisation. L'analyse de sensibilité et l'analyse causale mettent en évidence d'autres paramètres que l'on propose en perspective pour caractériser la sécurité : les mesures de sensibilités (instantanées et valeurs extrêmes) et un nombre de combinaisons critiques et leur persistance. Les combinaisons critiques sont des combinaisons d'état de capteur qui conduisent à un état inaccep-

table de la sortie d'un système multicapteur. Une position inacceptable est typiquement une situation dangereuse et le nombre de combinaisons amenant le système à fournir une position inacceptable se réfèrent donc à $H(t)$.

L'annexe C de la norme [EN 50126, 2000] propose également les paramètres liés à la fiabilité, maintenabilité, à la disponibilité et au soutien logistique. Il existe également un projet de modification de cette norme. Parmi les modifications, les paramètres de sécurité ont été retirés ou ajoutés. Parmi ces nouveaux paramètres, la probabilité d'incident contraire à la sécurité $p_{wsf}(t)$ est considérée de la même manière que la probabilité de défaillance liées à la sécurité $f_S(t)$. Seule la notation change et elle ne concerne que la version française de la norme [EN 50126, 2000]. La notation $f_S(t)$ est conservée puisque les modifications n'ont pas encore été validées (au moment de la rédaction du mémoire).

Tableau A.2 – Paramètres de performances de sécurité de l'annexe B du projet de norme pr50126-1 [PR NF EN 50126-1, 2015]

Paramètres	Symbole	Dimension
Taux de danger	$MTBF(H)$	1/temps, 1/distance, 1/cycle
Probabilité d'incident contraire à la sécurité	$p_{wsf}(t)$	sans dimension
Temps actif de retour à un état sûr	$TTRS$	temps

Annexe B

Filtrage de Kalman

À plusieurs reprises, nous faisons référence au filtrage de Kalman dans ce mémoire. On rappelle que les objectifs de la thèse n'étant pas la conception de système de ferroviaire localisation basés sur les GNSS mais que l'évaluation de la sécurité de ces systèmes. Cependant, le filtrage de Kalman mérite que l'on y consacre une annexe.

Le filtre de Kalman est un algorithme d'estimation en temps réel d'un nombre de paramètres (constants ou variants dans le temps) d'un système. Ces paramètres décrivant le système sont regroupés dans un vecteur appelé **vecteur d'état** $x(t)$ avec $x(t) = [p_1(t)\ p_2(t)\ p_3(t)\ ...\ p_n(t)]^T$ où $p_{1,...,n}(t)$ sont des paramètres modélisant un système quelconque. Un **modèle d'état** de ce système est nécessaire pour savoir comment ces paramètres ainsi que les erreurs sur les estimations sur ces derniers évoluent dans le temps. Le **vecteur d'observation** $z(t)$ est un ensemble de mesures des paramètres du système modélisé donc il est en fonction du vecteur d'état $x(t)$. De la même manière que le vecteur d'état, un **modèle d'observation** doit être fixé pour déterminer l'évolution du **vecteur de mesures $z(t)$**. Les équations B.1 et B.2 explicitent, respectivement, le modèle d'état et le modèle d'observation.

$$\dot{x}(t) = Fx(t) + G(t) \cdot w_s(t) \tag{B.1}$$

$$z(t) = Hx(t) + w_m(t) \tag{B.2}$$

Avec,
F et H, respectivement, la matrice d'état et la matrice d'observation dont le contenu dépend des propriétés du système,
$G(t)$, la matrice de distribution de bruit de système (elle permet de tenir compte d'un bruit (un "1" est placé dans la matrice à la ligne/colonne correspondante), défini dans le vecteur $w_s(t)$ ou non (un "0" dans la matrice)) sur un ou plusieurs paramètres de la modélisation du système,
$w_s(t)$ et $w_m(t)$ sont des bruits blancs Gaussiens.

Les observations étant discrètes, les équations B.1 et B.2 deviennent :

$$x_k = \Phi_{k-1}x_{k-1} + \Gamma_{k-1}w_{s,k-1} \tag{B.3}$$

$$z_k = H_k x_k + w_{m,k} \tag{B.4}$$

Φ_{k-1} étant la matrice de transition telle que $\Phi_{k-1} = \exp(F_{k-1}\ \tau_S)$ avec τ_S l'intervalle de temps entre t_k et t_{k-1}. Le calcul de l'exponentielle d'une matrice n'étant pas immédiat (l'exponentielle d'une

matrice n'est la matrice des exponentielles de chacun de ses éléments), il est possible d'approximer $\exp(F_{k-1})$ par son développement en série c'est à dire $\exp(F_{k-1}) \approx I - F_{k-1}\tau_S$. Γ_{k-1} est la forme discrétisée de la matrice de distribution du bruit du système, $G_(t)$.

La matrice Φ_{k-1} relie l'état précédent x_{k-1} avec l'état actuel x_k au travers du modèle d'état donné par l'équation B.3). Ce modèle d'état est une représentation possible d'un système réel qui s'appuie sur des paramètres connus. Le vecteur d'observation, z_k, contient les observations des propriétés du système et est fonction du vecteur d'état x_k. Le modèle d'observation (cf équation B.4) décrit comment le vecteur de mesure varie en fonction du vecteur d'état grâce à la matrice d'observation, H_k.

Le bruit d'état, w_s, et le bruit d'observation, w_m, sont des bruits blancs Gaussiens. Ils sont définis par des séquences de variables aléatoires qui respectent la propriété d'une distribution normale (cf équation B.5).

$$\mathbb{E}(w_i, w_j) = \begin{cases} \sigma_w^2, & \text{si } i = j \\ 0, & \text{si } i \neq j \end{cases} \tag{B.5}$$

avec, $\mathbb{E}$, l'espérance mathématique,
σ_w^2, est la variance de deux variables aléatoires w_i et w_j si $i = j$.

Les variables aléatoires décrivant un bruit blanc ne sont pas corrélées entre elles c'est à dire qu'un bruit n'est pas un signal de période donnée mais bien un signal totalement aléatoire. L'écart-type σ_w est obtenu par intégration d'un bruit blanc sur un intervalle de temps donné τ_w

$$\sigma_w = \sqrt{\frac{S_w^{f1}}{\tau_w}} \tag{B.6}$$

avec, S_w^{f1}, la densité spectrale de puissance du bruit blanc. En télécommunications, les bruits blancs ont une densité spectrale est constante pour une fréquence donnée, $f1$. La séquence constituant un bruit est déterminée de la manière suivante :

$$w_k = w_{k-1} + \sigma_w \cdot \mathcal{N}_k(0, 1) \tag{B.7}$$

avec,
w_k et w_{k-1}, le bruit blanc w à l'instant k et à l'instant précédent $k-1$,
σ_w, l'écart-type du bruit blanc w déterminé par l'équation B.6,
$N_k(0, 1)$ est une loi normale centrée réduite.

Les éléments du filtre de Kalman étant posés, voici le déroulement de l'algorithme d'un filtre de Kalman (illustrée par la figure B.1).

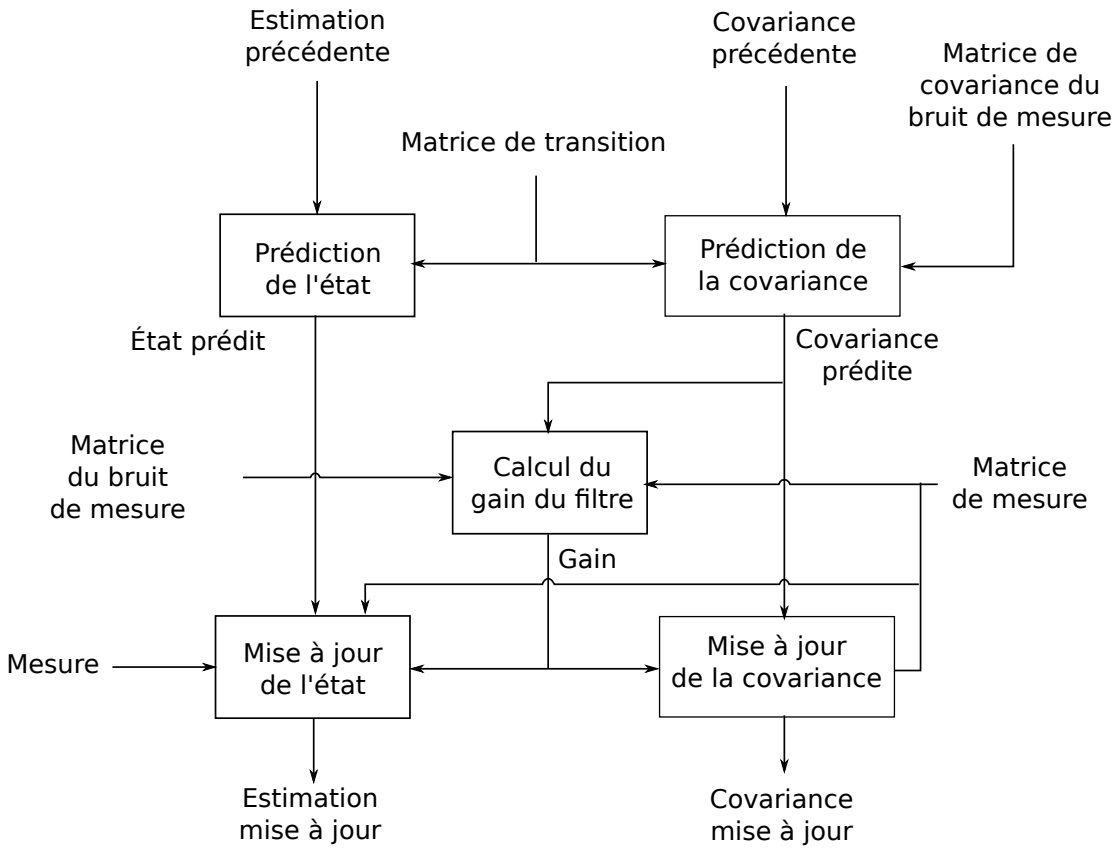


FIGURE B.1 – Fonctionnement du filtre de Kalman [Groves, 2013]

Le filtre de Kalman comprend deux grandes phases :

— La propagation ou prédiction d'un état estimé à un instant k (notée $\hat{x}_k$) avec l'estimation précédente (notée $\hat{x}_{k-1}$).
— La mise à jour de $\hat{x}_k$ grâce aux observations (mesures), z_k.

Nous proposons d'en décrire les principes en plusieurs étapes. D'abord, la phase de propagation se déroule de la manière suivante :

1. Calcul de la matrice de transition Φ_{k-1}.
2. Calcul de la matrice de covariance du bruit du système Q_{k-1} (variance du bruit d'état $\Gamma_{k-1} w_{s,k-1}$).
3. Propagation de l'estimation du vecteur d'état $\hat{x}_{k-1}^{+}$ vers $\hat{x}_k^{-}$.
4. Propagation de la matrice de covariance de l'erreur P_{k-1}^{+} vers P_k^{-}.

L'étape 1 est la détermination de la matrice Φ_{k-1}. Elle décrit comment le vecteur d'état change avec le temps. Cette matrice est liée au fonctionnement dynamique du système et relie l'estimation de l'état à l'instant k, $\hat{x}_k^{-}$, et celle à l'instant précédent $k-1$, $\hat{x}_{k-1}^{-}$. Le "-" indique les éléments calculés durant la phase de propagation (avant la mise à jour avec les observation z_k). L'erreur d'estimation de l'état doit elle aussi être propagée de l'instant $k-1$ vers k. Cette propagation de

l'erreur d'estimation nécessite la détermination de la matrice de covariance du bruit du système Q_{k-1} (étape 2). Cette matrice représente les incertitudes prises lors de l'estimation faite par le filtre de l'état du système. L'étape 3 est la propagation de l'estimation précédente (et mise à jour) du vecteur d'état $\hat{x}_{k-1}^{+}$ vers celle de l'instant actuel $\hat{x}_{k}^{-}$ (cf équation B.8). Le "+" indique les éléments mis à jour.

$$\hat{x}_{k}^{-} = \Phi_{k-1}\hat{x}_{k-1}^{+} \tag{B.8}$$

L'étape 4 est la propagation de la matrice de covariance de l'erreur de l'instant précédent et mise à jour P_{k-1}^{+} vers P_{k}^{-}. La matrice P représente l'erreur d'estimation commise par le filtre. Elle doit donc être propagé à chaque itération pour tenir compte de cette erreur. En plus de la matrice de transition Φ_{k-1}, cette propagation nécessite la matrice de covariance du bruit d'état Q_{k-1} (déterminée à l'étape 2) (cf équation B.9). Étant donné qu'il s'agit de propager une matrice, nous devons utiliser la transposée de Φ_{k-1} pour propager les lignes puis les colonnes de P.

$$P_{k}^{-} = \Phi_{k-1}P_{k-1}^{+}\Phi_{k-1}^{T} + Q_{k-1} \tag{B.9}$$

L'état du système x et l'erreur d'estimation du filtre P sont à présent propagés de l'instant $k-1$ à k. Si nous nous arrêtons là, l'erreur commise par le filtre augmentera à chaque itération et aboutira à de mauvaises estimations de l'état du système. Pour contrecarrer ce phénomène, les estimations et les erreurs d'estimation du filtre doivent être mises à jour grâces à de nouvelles observations provenant des mesures ou d'observations fournies par des capteurs. Cette phase de mise à jour (ou correction) se résume en six étapes :

5. Calcul de la matrice d'observation H_k.
6. Calcul de la matrice de covariance du bruit d'observation R_k.
7. Calcul du gain du filtre de Kalman, K_k.
8. Prise en compte des mesures z_k.
9. Mise à jour de l'estimation du vecteur d'état $\hat{x}_{k}^{-}$ vers $\hat{x}_{k}^{+}$.
10. Mise à jour de la matrice de covariance de l'erreur P_{k}^{-} vers P_{k}^{+}.

La matrice H_k a déjà été introduite précédemment et son calcul se fait à l'étape 5. Elle décrit comme le vecteur de mesure z_k évolue en fonction du vecteur d'état x_k. Comme H_k dépend de l'application, son calcul est décrit dans le mémoire.

L'étape 6 vise à déterminer la matrice de covariance du bruit de mesure R_k qui contient la modélisation de ces bruits (de la même manière que $\Gamma_{k-1}w_{s,k-1}$ contient la modélisation des bruits d'état). Elle est déterminée par l'équation B.10. Concrètement, elle prendra la forme d'une matrice diagonale dont chaque élément de la diagonale est la variance des observations moins leur estimation c'est à dire $z_k - H_k x_k^{-}$.

$$R_k = \mathbb{E}((z_k - H_k x_k^{-})(z_k - H_k x_k^{-})^{T}) \tag{B.10}$$

Le gain du filtre de Kalman (étape 7) est une matrice de pondération de la correction apportée par le filtre en fonction de la covariance de l'erreur P_{k}^{-} (cf équation B.9) et de celle du bruit de mesure R_k (cf équation B.11).

$$K_k = P_{k}^{-}H_{k}^{T}(H_k P_{k}^{-} H_{k}^{T} + R_k)^{-1} \tag{B.11}$$

L'étape 8 est la prise en compte des mesures disponibles et placées dans le vecteur d'observation z_k. Deux cas sont possibles : soit les mesures sont déterminées par le modèle de mesure (cf équation

B.2) soit les mesures, obtenues par un système réel, sont déjà disponibles.

L'étape 9 est la mise à jour de l'état $\hat{x}_k^-$ grâce au vecteur z_k (cf équation B.12) et le gain du filtre K_k (cf équation B.11).

$$\hat{x}_k^+ = \hat{x}_k^- + K_k(z_k - H_k\hat{x}_k^-) \tag{B.12}$$

La matrice de covariance de l'erreur P_k^- est ensuite mise à jour (étape 10) (cf équation B.13).

$$P_k^+ = P_k^-(I - K_kH_k) \tag{B.13}$$

Le déroulement d'un filtre de Kalman classique est ainsi posé. Dans cette forme classique, le modèle d'état B.1 et d'observation B.2 sont supposés linéaires. Or, ce n'est pas le cas des systèmes réels. Par conséquent, pour se rapprocher de la réalité, nous nous orientons vers une de ses extensions : le filtre de Kalman étendu. Il existe d'autres extensions du filtre de Kalman (*Unscented* ou sans parfum qui permet de traiter les fonctions non-linéaires sans passer par une phase de linéarisation, sujette à des approximations et principale faiblesse du filtre de Kalman étendu) et d'autres types de filtre : filtres particulaires (fondés sur des techniques probabilistes telles que les méthodes de Monte-Carlo). Dans ce mémoire, le filtre de Kalman étendu est suffisant pour mettre en œuvre un système de localisation ferroviaire GNSS/INS en hybridation serrée pour appliquer la méthodologie visant à évaluer la sécurité de ce système. Avec un filtre de Kalman étendu, les produits des matrices F et H avec le vecteur d'état $x(t)$ sont remplacés par des fonctions non linéaires f et h (cf équations B.14 et B.15) dépendantes de l'application. Les équations B.16 et B.17 montrent la forme discrétisée du modèle du système et de mesure.

$$\dot{x}(t) = f(x(t), t) + G(t) \cdot w_s(t) \tag{B.14}$$
$$z(t) = h(x(t), t) + w_m(t) \tag{B.15}$$
$$x_k = f(x_{k-1}, t_k - 1) + \Gamma_{k-1}w_{s,k-1} \tag{B.16}$$
$$z_k = h(x_k, t_k) + w_{m,k} \tag{B.17}$$

Afin de pouvoir être traitées par le filtre de Kalman, il est possible de linéariser les fonctions f et h en considérant les matrices jacobiennes F_{k-1} (cf équation B.18) dans la phase de propagation (étape 1 à 4) et H_k (cf équation B.19) dans la phase de mise à jour (étape 5 à 10).

$$F_{k-1} = \left.\frac{\partial f(x, t_k)}{\partial x}\right|_{x=\hat{x}_{k-1}} \tag{B.18}$$
$$H_k = \left.\frac{\partial h(x, t_k)}{\partial x}\right|_{x=\hat{x}_k} \tag{B.19}$$

Par la suite, il suffit de procéder au déroulement du filtre de Kalman décrit précédemment en tenant compte de ses nouvelles matrices F_{k-1} et H_k. On supposera que l'erreur causée par l'approximation faite en linéarisant ces matrices est négligeable. Pour s'affranchir de cette hypothèse, il faudra s'orienter vers un filtre de Kalman sans parfum ou un filtre particulaire.

Annexe C

Paramétrage des simulations du système GNSS/INS

Cette annexe est consacrée aux hypothèses de départ des simulations liées au fonctionnement du système GNSS/INS. Il s'agit des paramètres liés aux erreurs intrinsèques au système (cf tableau C.2) et aux mesures (cf tableau C.3). Étant donné que nous avons à disposition des données réelles GNSS, le reste du paramétrage se situe sur la partie INS et le filtre de Kalman étendu.

Tout d'abord, le vecteur $in\_profile$ représente le profil de déplacement réel. Il s'agit du vecteur issu du modèle réel de la figure 4.10. Le tableau C.1 décrit le contenu exact de ce vecteur. Nous renseignons dans ce vecteur, le trajet réel fourni avec les scénarios Geoloc.

Tableau C.1 – Contenu du vecteur $in\_profile$

Taille (lig x col)	Contenu
1 x 1	Temps en s
1 x 3	Latitude, longitude et hauteur réelle en rad
1 x 3	Vitesse dans le repère cartésien Nord-Est-Bas (NEB) en rad/s
1 x 3	Angle d'attitude (ou angles d'Euler) respectivement l'angle de roulis, tangage et lacet dans le repère NEB en rad

Le vecteur $initialization\_errors$ contient les erreurs de position, vitesse et des angles d'attitude. Il s'agit d'erreurs liées à l'imprécision du système de coordonnées WGS84 [1] et du modèle du champ de gravité locale [2].

1. WGS84 est représentation simplifiée de la Terre par une ellipsoïde.
2. Le champ gravitationnel terrestre n'est pas identique en tout point sur la Terre.

Tableau C.2: Contenu du vecteur *initialization_errors*

Taille (lig x col)	Contenu (valeurs initiales de :)	Valeur
1 x 3	Erreur en position[1] dans le repère NEB en m	$\begin{pmatrix} -0.4323 \\ -2.5711 \\ -10.8145 \end{pmatrix}$
1 x 3	Erreur en vitesse[1] dans le repère NEB en m/s	$\begin{pmatrix} -0.0011 \\ 0.0025 \\ -0.0043 \end{pmatrix}$
3 x 1	Erreur en attitude (ou angles d'Euler) respectivement l'angle de roulis, tangage et lacet dans le repère NEB en *rad*	$\begin{pmatrix} -0.05 \\ 0.04 \\ 1 \end{pmatrix} \times deg2rad$

$deg2rad = \frac{\pi}{180}$ (conversion degré en radian)

Le vecteur IMU_errors contient les valeurs par défaut des paramètres liés aux capteurs à l'image des paramètres de la modélisation des capteurs faite dans la sous-section 2.4.3 du chapitre 2.

Tableau C.3: Contenu du vecteur IMU_errors

Taille (lig x col)	Contenu	Valeur
1 x 3	Erreur de la position en *mètre* selon le repère NEB	$\begin{pmatrix} -0.4323 \\ -2.5711 \\ -10.8145 \end{pmatrix}$
1 x 3	Biais accéléromètrique selon le repère centré sur le mobile en m/s^2	$\begin{pmatrix} 900 \\ -1300 \\ 800 \end{pmatrix} \times \mu_g$
1 x 3	Biais gyroscopique selon le repère centré sur le mobile en rad/s	$\begin{pmatrix} -9 \\ 13 \\ -8 \end{pmatrix} \times deg2rad$
3 x 3	Facteur d'échelle accéléromètre selon le repère centré sur le mobile (*sans unité*)	$\begin{pmatrix} 500 & -300 & 200 \\ -150 & -600 & 250 \\ -250 & 100 & 450 \end{pmatrix} \times 1.10^{-6}$
3 x 3	Facteur d'échelle gyroscope selon le repère centré sur le mobile (*sans unité*)	$\begin{pmatrix} 400 & -300 & 250 \\ 0 & -300 & -150 \\ 0 & 0 & -350 \end{pmatrix} \times 1.10^{-6}$
3 x 3	Biais gyroscope lié à l'accélération de la pesanteur à la surface de la Terre selon le repère centré sur le mobile en $rad - sec/m$	$\begin{pmatrix} 0.9 & -1.1 & -0.6 \\ -0.5 & 1.9 & -1.6 \\ 0.3 & 1.1 & -1.3 \end{pmatrix} \times \frac{deg2rad}{3600g}$
1 x 1	Bruit de mesure accéléromètre en $ms^{-1.5}$	$100 \times \mu_g$
1 x 1	Bruit de mesure gyroscope en $ms^{-1.5}$	$0.01 \times \frac{deg2rad}{60}$
1 x 1	Niveau de quantification[1] accéléromètre en m/s^2	1.10^{-2}

1 x 1	Niveau de quantification gyroscope en rad/s	2.10^{-4}

[1]La quantification désigne l'approximation d'un signal continu en signal discret

$\mu_g = 9.80665.10^{-6}\ m/s^2$ (micro-g)

$g = 9.80665\ m/s^2$

Ces différents vecteurs permettent, suivant la figure 4.10, de générer les mesures INS. Il reste à configurer le filtre de Kalman. Cela concerne l'initialisation de la matrice de covariance (notée P) au début de la simulation, indispensable pour le bon fonctionnement du filtre. Le gain du filtre est fonction de cette matrice P. La matrice P est une matrice diagonale contenant les incertitudes sur l'estimation de chaque élément du vecteur d'état. On notera que l'incertitude sur les pseudodistances et leur dérivée est liée respectivement à l'erreur due au décalage d'horloge (*clock offset*) et à la dérive d'horloge (*clock drift*) récepteur/satellite. Cette matrice, mise à jour à chaque instant, doit être initialisée au démarrage de la simulation. Le vecteur TC_KF_config (pour *Tightly-Coupled Kalman Filter configuration*) contient les valeurs initiales de la matrice P (cf tableau C.4).

Tableau C.4 – Contenu du vecteur TC_KF_config

Taille (lig x col)	Contenu (Incertitude sur :)	Valeur
3 x 3	Attitude pour chaque axe en rad	$deg2rad$
3 x 3	Vitesse pour chaque axe en m/s	0.1
3 x 3	Position pour chaque axe en m	10
3 x 3	Biais accéléromètre pour chaque axe en m/s^2	$1000 \times \mu_g$
3 x 3	Biais gyroscope pour chaque axe en rad/s	$10 \times \frac{deg2rad}{3600}$
1 x 1	Erreur due au décalage d'horloge récepteur/satellite en m	10
1 x 1	Erreur due à la dérive d'horloge récepteur/satellite en m	0.1

Toutes ces valeurs permettent de faire fonctionner le système GNSS/INS.

Bibliographie

Ahmad, K. B., Sahmoudi, M., and Macabiau, C. (2014). Trusted overbounding position errors for gnss positioning in urban environments.

Albanese, A. and Marradi, L. (2005). The RUNE project : the integrity performances of GNSS-based railway user navigation equipment. In *Rail Conference, 2005. Proceedings of the 2005 ASME/IEEE Joint*, pages 211–218.

Álvaro Mozo García, Píriz, R., Samper, M. D. L., and Merino, M. M. R. (2011). Multisystem Real Time Precise-Point-Positioning, today with GPS+GLONASS in the near future also with QZSS, Galileo, Compass, IRNSS. In *International Symposium on GPS/GNSS, Taipei, Taiwan*.

Arlat and Laprie (1995). *Guide de la sûreté de fonctionnement*. Cépaduès-Editions.

Arnold, T. B. and Emerson, J. W. (2011). Nonparametric goodness-of-fit tests for discrete null distributions. *The R Journal*.

Arulampalam, M. S., Maskell, S., Gordon, N., and Clapp, T. (2002). A tutorial on particle filters for online nonlinear/non-gaussian bayesian tracking. *IEEE Transactions on signal processing*, 50(2) :174–188.

Ashby, N. (1997). Relativistic effects in the global positioning system. In *Gravitation and Relativity : At the Turn of the Millenium. 15th International Conference on General Relativity and Gravitation*, pages 231–258.

Barbu, G. (1999). APOLO - Advanced Position Locator system. Technical report, Laboratory of Intelligent Systems - Czech Republic.

Barbu, G. (2000). GNSS Rail User Forum Requirements of Rail Applications.

Bedrich, S. and Gu, X. (2004). GNSS-Based Sensor Fusion for Safety-Critical Applications in Rail Traffic. *Galileo and EGNOS Information Catalogue*, page 8.

Bérard, J. (2001). *Contributions à l'étude probabiliste des algorithmes d'évolution*. PhD thesis.

Bétaille, D. (2012). Intégrité du positionnement dans les transports terrestres.

Beugin, J., Filip, A., Marais, J., and Berbineau, M. (2010). Galileo for railway operations : question about the positioning performances analogy with the rams requirements allocated to safety applications. *European Transport Research Review*, 2(2) :93–102.

Beugin, J. and Marais, J. (2008). Application des principes de la sûreté de fonctionnement à l'évaluation du service de localisation par satellites dans le domaine ferroviaire. *Recherche, transports, sécurité*, (99) :89–103.

Bhatti, U. I. and Ochieng, W. Y. (2007). Failure modes and models for integrated GPS/INS systems. *Journal of Navigation*, 60(02) :327–348.

Bhatti, U. I. and Ochieng, W. Y. (2009). Detecting multiple failures in gps/ins integrated system : a novel architecture for integrity monitoring. *Journal of Global Positioning Systems*, 8(1) :26–42.

Bhatti, U. I., Ochieng, W. Y., and Feng, S. (2007). Integrity of an integrated GPS/INS system in the presence of slowly growing errors. Part I : A critical review. *GPS Solutions*, 11(3) :173–181.

Boulanger, J.-L. (2011). Maîtrise du SIL et gestion des certificats - Domaine ferroviaire. *Techniques de l'ingénieur - Transport ferroviaire*, base documentaire : TIB576DUO.(ref. article : d5560). fre.

Brenner, M. A. (1998). Navigation system with solution separation apparatus for detecting accuracy failures. US Patent 5,760,737.

Brown, R. G. (1992). A baseline GPS RAIM scheme and a note on the equivalence of three RAIM methods. *Navigation*, 39(3) :301–316.

Brown, R. G. and McBurney, P. (1988). Self-Contained GPS Integrity Check Using Maximum Solution Separation. *Navigation*, 35(1) :41–53.

Bustamante, J. and De Miguel, S. (2003). GADEROS - A technological approach to GNSS-aided railway traffic monitoring for conventional and low-density traffic lines - Interoperability of GNSS-based location with ERTMS / ETCS on-board. In *Intelligent Transport Systems and Services*, Madrid, Spain.

Campolongo, F., Cariboni, J., and Saltelli, A. (2003). Sensitivity analysis : the morris method versus the variance based measures. *Technometrics*.

CNES (2011). Guide EGNOS à l'usage des développeurs d'applications. Technical report, ESA.

CNRTL (2014a). Centre National de Ressources Textuelles et Lexicales - Définition de "Balise". URL : http ://www.cnrtl.fr/definition/balise. [En ligne ; consulté le 18 Mars 2014].

CNRTL (2014b). Centre National de Ressources Textuelles et Lexicales - Définitions de "Localisation". URL : http ://www.cnrtl.fr/definition/localisation. [En ligne ; consulté le 11 Mars 2014].

Conseil de l'Union Européenne (1999). Résolution du Conseil, du 19 juillet 1999, concernant la participation de l'Europe à une nouvelle génération de services de navigation par satellite - Galileo - Phase de définition. Journal officiel de l'Union européenne.

COP21 (2015). Contributions prévues déterminées au niveau national (INDC).

Diesel, J. and Luu, S. (1995). GPS/IRS AIME : Calculation of Thresholds and Protection Radius Using Chi-Square Methods. In *ION GPS-95*. Institute of Navigation.

Ding, L., Wang, H., Kang, K., and Wang, K. (2014). A novel method for SIL verification based on system degradation using reliability block diagram. *Reliability Engineering & System Safety*, 132(0) :36 – 45.

Doucet, A., Godsill, S., and Andrieu, C. (2000). On sequential monte carlo sampling methods for bayesian filtering. *Statistics and computing*, 10(3) :197–208.

Duquenne, F., Botton, S., Peyret, F., Bétaille, D., and Willis, P. (2005). *Les GPS : localisation et navigation par satellites*. Lavoisier.

Embrechts, P., Klüppelberg, C., and Mikosch, T. (2013). *Modelling extremal events : for insurance and finance*, volume 33. Springer Science & Business Media.

EN 50126 (2000). NF EN 50126 Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS).

EN 50128 (2001). NF EN 50128 Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Logiciels pour systèmes de commande et de protection ferroviaire.

EN 50129 (2003). NF EN 50129 Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Systèmes électroniques de sécurité pour la signalisation.

EN 60300-3-1 (2005). NF EN 60300-3-1 - Gestion de la sûreté de fonctionnement - Partie 3-1 : Guide d'application - Techniques d'analyse de la sûreté de fonctionnement - Guide méthodologique.

ERRAC (2002). Sur la voie d'une amélioration du transport ferroviaire en Europe : le programme stratégique de recherche sur le transport ferroviaire de l'Union Européen - Conseil consultatif européen pour la recherche sur le rail. Communiqué de presse.

European Commission (2011). Report from the commission to the European Parliament and the Council - Mid-term review of the European satellite radio navigation programmes.

European Railway Agency (2012). Memorandum of Understanding ERTMS. http ://www.era.europa.eu/Document-Register/Pages/Memorandum-of-Understanding-concerning-ERTMS.aspx.

Faurie, F. (2011). *Algorithmes de contrôle d'intégrité pour la navigation hybride GNSS et systèmes de navigation inertielle en présence de multiples mesures satellitaires défaillantes*. PhD thesis, Université de Bordeaux I.

Feng, S. and Ochieng, W. (2007). Integrity of navigation system for road transport. In *Proc. 14th World Congress of Intelligent Transportation Systems, Beijing*.

Feng, S., Ochieng, W. Y., Walsh, D., and Ioannides, R. (2005). A measurement domain receiver autonomous integrity monitoring algorithm. *GPS Solutions*, 10(2) :85–96.

Filip, A., Beugin, J., Marais, J., and Mocek, H. (2008a). Interpretation of the Galileo safety-of-life service by means of railway RAMS terminology. *Transactions on Transport Sciences*, 1(2).

Filip, A., Mocek, H., Bazant, L., Taufer, J., and Maixner, V. (2001). Architecture of GNSS Aided Signalling : Analysis and Experiments. In *World Congress on Railway Research. WCRR 2001*.

Filip, A., Mocek, H., and Suchanek, J. (2008b). Significance of the Galileo Signal-in-Space Integrity and Continuity for Railway Signalling and Train Control. In *Proceedings of 8 th World Congress on Railway Research (WCRR), Seoul, Korea*.

Goya, J., Zamora-Cadenas, L., Arrizabalaga, S., Brazález, A., Meléndez, J., and Mendizabal, J. (2015). Advanced Train Location Simulator (ATLAS) for developing, testing and validating onboard railway location systems. *European Transport Research Review*, 7(3) :1–18.

GRAIL (2007). GNSS introduction in the RAIL sector : GNSS subsystem requirement specification for enhanced ETCS applications. Technical report, Project funded by the European GNSS Supervisory Authority, 6th framework program.

Groupe banque mondiale (2015). Indicateurs du développement dans le monde - Lignes de chemin de fer (France).

Groves, P. (2013). *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems, Second Edition*. GNSS/GPS. Artech House.

Hewitson, S. (2003). Gnss receiver autonomous integrity monitoring : A separability analysis.

Hirwa, S. (2013). *Méthodes de commande avancées appliquées aux viseurs.* PhD thesis, Supélec.

Hougardy, A., Chiappini, A., and Guido, P. (2012). Introduction to ETCS braking curves. Technical report, European Railway Agency.

Hwang, P. Y. and Brown, R. G. (2006). Raim-fde revisited : A new breakthrough in availability performance with nioraim (novel integrity-optimized raim). *Navigation*, 53(1) :41–51.

ICAO (2006). Annex 10 (Aeronautical Telecommunications) To The Convention On International Civil Aviation, Volume I - Radio Navigation Aids, International Standards And Recommended Practices (SARPs).

IEC 60050 (2015a). IEC 60050 - Définition de la défaillance d'une entitée. URL : http ://www.electropedia.org/iev/iev.nsf/display ?openform&ievref=192-03-01.

IEC 60050 (2015b). IEC 60050 - Définition de l'intégrité. URL : http ://www.electropedia.org/iev/iev.nsf/display ?openform&ievref=191-19-07.

IEC 61508 (2010). IEC 61508 - functional safety of electrical/electronic/programmable electronic safety-related systems.

IEC 61508-4 (2010). IEC 61508-4 ed2.0 - functional safety of electrical/electronic/programmable electronic safety-related systems - part 4 : Definitions and abbreviations.

Kripke, S. A. (1963). Semantical analysis of modal logic i normal modal propositional calculi. *Mathematical Logic Quarterly*, 9(5-6) :67–96.

Kubrak, D. (2007). *Hybridisation of a GPS Receiver with Low-Cost Sensors for Personal Positioning in Urban Environment.* PhD thesis, Telecom Paris.

Kumamoto, H. and Henley, E. J. (1996). *Probabilistic risk assessment and management for engineers and scientists.* Wiley-IEEE Press.

Kuusniemi, H. (2005). User-level reliability and quality monitoring in satellite-based personal navigation.

Laneurit, J. (2006). *Perception multisensorielle pour la localisation d'un robot mobile en environnement extèrieur, application aux véhicules routiers.* PhD thesis, Universitè Blaise Pascal.

Lannoy, A. (2003). Retour d'expérience technique. *Techniques de l'ingénieur - Management de la sécurité*, base documentaire : TIB154DUO.(ref. article : se1041) :24.

Lau, L. and Cross, P. (2007). Development and testing of a new ray-tracing approach to gnss carrier-phase multipath modelling. *Journal of Geodesy*, 81(11) :713–732.

Le Marchand, O. (2010). *Autonomous approach for localization and integrity monitoring of a ground vehicle in complex environment*. PhD thesis, Université de Technologie de Compiègne.

Legrand, C., Beugin, J., Conrard, B., Marais, J., Berbineau, M., and El-Koursi, E.-M. (2013). Sensitivity Assessment to Analyse Dependability of a Multisensor Localisation System based on GNSS. In *13th International Conference on ITS Telecommunication (ITST 2013)*.

Legrand, C., Beugin, J., Conrard, B., Marais, J., Berbineau, M., and El-Koursi, E.-M. (2014). Causal Analysis Methodology of Multisensor Systems based on GNSS. In *Proceedings of the Second International Conference on Railway Technology*.

Legrand, C., Beugin, J., Conrard, B., Marais, J., Berbineau, M., and El-Koursi, E.-M. (2015). Approach for evaluating the safety of a satellite-based train localisation system through the extended integrity concept. In *Proceedings of the 25th European safety and reliability conference, ESREL 2015, Zurich, Switzerland, 7-10 Septembre 2015*.

Li, J. and Wu, M. (2009). The improvement of positioning accuracy with weighted least square based on snr. In *2009 5th International Conference on Wireless Communications, Networking and Mobile Computing*, pages 1–4.

Lindsay, P. A. (1998). A tutorial Introduction to Formal Methods. Technical report, Software Verification Research Centre School of Information Technology - University of Queensland.

Liu, H., Zheng, G., Wang, H., and Feng, C. (2010). Research on integrity monitoring for integrated GNSS/SINS system. In *2010 IEEE International Conference on Information and Automation (ICIA)*, pages 1990–1995. IEEE.

Liu, J., Tang, T., Gai, B., Wang, J., and Chen, D. (2011). Integrity assurance of GNSS-based train integrated positioning system. *Science China Technological Sciences*, 54(7) :1779–1792.

Lou, Y., Zhang, C., Zheng, Y., Xie, X., Wang, W., and Huang, Y. (2009). Map-matching for low-sampling-rate gps trajectories. In *Proceedings of the 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, pages 352–361. ACM.

Lu, D. (2014). *GNSS for Train Localisation Performance Evaluation and Verification*. PhD thesis, Nantong University (NTU).

Lu, D., Grasso Toro, F., and Schnieder, E. (2013). RAMS evaluation of GNSS for railway localisation. In *IEEE International Conference on Intelligent Rail Transportation (ICIRT)*, pages 209–214.

Lu, D. and Schnieder, E. (2015). Performance evaluation of GNSS for train localization. *IEEE Transactions on Intelligent Transportation Systems*, 16(2) :1054–1059.

Lu, Y., Peng, Z., Miller, A. A., Zhao, T., and Johnson, C. W. (2015). How reliable is satellite navigation for aviation ? Checking availability properties with probabilistic verification. *Reliability Engineering & System Safety*, 144 :95 – 116.

Manz, H., Schnieder, E., Becker, U., Seedorff, C., and Baudis, A. (2014). Approach to Certification of Satellite Based Localisation Unit in Railways. In *Proceedings of Transport Research Arena (TRA)*.

Maquin, D., Cocquempot, V., Cassar, J.-P., Staroswiecki, M., and Ragot, J. (1997). Generation of analytical redundancy relations for fdi purposes. In *IFAC Symposium on Diagnostics for Electrical Machines, Power Electronics and Drives, SDEMPED'97*, pages 86–93.

Marais, J., Meunier, B., and Berbineau, M. (2000). Evaluation of gps availability for train positioning along a railway line. In *Vehicular Technology Conference, 2000. IEEE-VTS Fall VTC 2000. 52nd*, volume 5, pages 2060–2067. IEEE.

Marradi, L., Foglia, L., Franzoni, G., Albanese, A., Di Raimondo, S., and Gabaglio, V. (2008). Girasole Receiver Development for Safety of Life Applications. In Re, E. and Ruggieri, M., editors, *Satellite Communications and Navigation Systems*, Signals and Communication Technology, pages 313–327. Springer US.

Marradi, L., Galimberti, A., Foglia, L., Zin, A., Pecchioni, C., Doronzo, M., González García-Consuegra, E. J., and Lekchiri, M. (2012). GNSS for enhanced odometry : the GRAIL-2 results. In *NAVITEC 2012, 6th ESA Workshop on Satellite Navigation Technologies*, Noordwijk, The Netherlands.

Martineau, A., Macabiau, C., Nikiforov, I., and Roturier, B. (2008). Performance of receiver autonomous integrity monitoring (RAIM) for vertically guided approaches. In *ENC-GNSS 2008, Conférence Européenne de la Navigation*.

Mercurio, D. and Thornsbury, E. A. (2015). New Uncertainty Importance Measure for Probabilistic Safety Assessment. In *Safety and Reliability of Complex Engineered Systems - Proceedings of the 25th European Safety and Reliability Conference, ESREL 2015, Zürich, Switzerland*.

Nahimana, D. F. (2009). *Multipath impact on the perfomances of satellite navigation systems : Contribution to the enhancement of lacation accuracy though bayesian modeling*. PhD thesis, Ecole Centrale de Lille.

Nguyen, T., Beugin, J., and Marais, J. (2014). RAMS analysis of GNSS based localisation system for the train control application. In *Computing, Management and Telecommunications (ComManTel), 2014 International Conference on*, pages 101–106. IEEE.

Nikiforov, I. (2005). Autonomous integrity monitoring of the GNSS. Technical report, Convention STNA - Astrée.

Nikiforov, I. (2015). Asymptotically Efficient Estimation of a Nonlinear Model of the Heteroscedasticity and the Calibration of Measurement Systems. *IEEE Transactions on Signal Processing*, 63(10) :2623–2638.

Nikiforov, I. V. and Choquette, F. (2003). Integrity equations for safe train positioning using gnss. In *Proceedings of the European Navigation Conference*.

Objectif Carbone (2009). 1er Bilan Carbone ferroviaire global - La ligne à Grande Vitesse Rhin-Rhône au service d'une Europe durable. Technical report, ADEME.

Ochieng, W. Y., Feng, S., Moore, T., Hill, C., and Hide, C. (2008). User level integrity monitoring and quality control for high accuracy positioning using GPS/INS measurements. *Journal of Global Positioning Systems*, 7(2) :104–114.

Ortiz, M. (2012). INTURB - étude sur intégrité du positionnement en environnement urbain. Technical report, IFSTTAR/COSYS/GEOLOC.

Panagiotakopoulos, D. (2009). *Robust statistical framework for monitoring the integrity of space-based navigation systems, and preparing the marketplace for integrity-based services.* PhD thesis, Imperial College London.

Parkinson, B. W. and Axelrad, P. (1988). Autonomous gps integrity monitoring using the pseudorange residual. *Navigation*, 35(2) :255–274.

Parlement Européen et du Conseil (2008). Directive 2008/57/CE du Parlement Européen et du conseil du 17 juin 2008 relative à l'interopérabilité du système ferroviaire au sein de la Communauté. Journal officiel de l'Union Européenne.

Peng, Z., Lu, Y., Miller, A., Zhao, T., and Johnson, C. (2014). Formal specification and quantitative analysis of a constellation of navigation satellites. *Quality and Reliability Engineering International.*

PR NF EN 50126-1 (2015). Projet destiné à remplacer la norme homologuée NF EN 50126-1, de janvier 2000. AFNOR.

Rail Transit Vehicle Interface Standards Committee (2004). IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements. *IEEE Std 1474.1-2004 (Revision of IEEE Std 1474.1-1999)*, pages 1–45.

Rausand, M. and Høyland, A. (2003). *System Reliability Theory : Models, Statistical Methods and Applications, Second Edition.* Wiley-Interscience.

Réglement 2015/1136 (2015). Réglement d'exécution (UE) numéro 2015/1136 de la Commission du 13 juillet 2015 modifiant le réglement d'exécution (UE) numéro 402/2013 concernant la méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques. Journal officiel de l'Union européenne.

Reliability Analysis Center (1995). Nonelectronic Parts Reliability Data. Technical report, RAC.

Rietdorf, A., Daub, C., and Loef, P. (2006). Precise positioning in real-time using navigation satellites and telecommunication. In *Proceedings of The 3rd Workshop on Positioning and Communication (WPNC06).*

Rispoli, F., Filip, A., Castorina, M., Di Mambro, G., Neri, A., and Senesi, F. (2013). Recent progress in application of GNSS and advanced communications for railway signaling. In *Radioelektronika, 2013 23rd International Conference*, pages 13–22.

Roturier, B., Chatre, E., and Ventura-Traveset, J. (2001). The SBAS integrity concept standardised by ICAO-application to EGNOS. *NAVIGATION-PARIS-*, 49 :65–77.

RTCA (2006). DO229D - Minimum operational performance standards for global positioning system/wide area augmentation system airborne equipment. Technical report, RTCA.

Saltelli, A., Tarantola, S., Campolongo, F., and Ratto, M. (2004). *Sensitivity Analysis in Practice : A Guide to Assessing Scientific Models*, chapter Global Sensitivity Analysis for Importance Assessment, pages 31–61. John Wiley & Sons, Ltd.

Schroth, G., Ene, A., Blanch, J., Walter, T., and Enge, P. (2008). Failure detection and exclusion via range consensus. In *European Navigation Conference 2008*.

SNCF Réseau (2008). Bilan LOTI du contrôle de vitesse par balises (KVB). SNCF Réseau - ex Réseau Ferré de France.

SUBSET-026-7 (2014). SUBSET-026-7 : System Requirements Specification Chapter 7 ERTMS/ETCS language. Technical report, UNISIG.

SUBSET-041 (2015). SUBSET-041 : Performance Requirements for Interoperability. Technical report, UNISIG.

Tartakovsky, A., Nikiforov, I., and Basseville, M. (2014). *Sequential Analysis : Hypothesis Testing and Changepoint Detection*. Chapman & Hall/CRC Monographs on Statistics & Applied Probability. Taylor & Francis.

Thevenot, V., Bruckmueller, T., Doederlein, C., Mattos, P., Sarfati, R., Lechner, W., and M., T. (2003). ECORAIL : A Step Towards Safe Railway Controlling Systems based on Satellite Positioning. In *ENC-GNSS 2003 - European Navigation Conference*, Graz, Austria.

Thomas, M., Lowe, D., Dumville, M., Roberts, W., Cross, P., Roberts, G., and Nunn, T. (2008). Dependability of GNSS on the UK Railways. In *Proceedings of the 8th World Congress on Railways Research*.

Thouvenot, H. and Pignal, O. (2007). Traction ferroviaire - Systéme de signalisation ERTMS. *Techniques de l'ingénieur - Transport ferroviaire*, base documentaire : TIB576DUO.(ref. article : d5545) :12. fre.

Toledo-Moreo, R., Zamora-Izquierdo, M., Úbeda-Miñarro, B., Gómez-Skarmeta, A. F., et al. (2007). High-integrity IMM-EKF-based road vehicle navigation with low-cost GPS/SBAS/INS. *Intelligent Transportation Systems, IEEE Transactions on*, 8(3) :491–511.

Tossaint, M., Samson, J., Toran, F., VENTURA-TRAVESET, J., HERNANDEZ-PAJARES, M., Juan, J., Sanz, J., and RAMOS-BOSCH, P. (2007). The Stanford–ESA Integrity Diagram : A New Tool for The User Domain SBAS Integrity Assessment. *Navigation*, 54(2) :153–162.

Vesely, W. and Rasmuson, D. (1984). Uncertainties in nuclear probabilistic risk analyses. *Risk Analysis*, 4(4) :313–322.

Viandier, N. (2011). *Modélisation et utilisation des erreurs de pseudodistances GNSS en environnement transport pour l'amélioration des performances de localisation*. PhD thesis, École Centrale de Lille.

Villemeur, A. (1988). *Sûreté de fonctionnement des systèmes industriels : fiabilité, facteurs humains, informatisation*. Collection de la Direction des études et recherches d'Électricité de France. Eyrolles.

Walter, T. and Enge, P. (1995). Weighted RAIM for precision approach. In *Proceedings of ION GPS*, volume 8, pages 1995–2004.

Wasle, E. and Ringert, J. (2003). Means of Navigation for Automatic Level Crossing Control and the Concept of the ECORAIL Project. *VGI – Österreichische Zeitschrift für Vermessung und Geoinformation*, 91(1) :61–67.

Wieser, A., Gaggl, M., and Hartinger, H. (2005). Improved positioning accuracy with high sensitivity GNSS receivers and SNR aided integrity monitoring of pseudo-range observations. In *Proceedings of ION GNSS*.

Wilson, J. L. (2001). Low-cost PND dead reckoning using automotive diagnostic links. In *Proceedings of the 20th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2007)*, pages 2066–2074.

Wynants, P. (2001). Rapport finale du projet LOCOPROL (Low Cost satellite-based train location system for signalling and train Protection for Low density traffic railway lines). Technical report, Alstom, Bombardier, Septentrio, Trasys, ESA.

Yu, J. (1998). Fault detection and exclusion used in a global positioning system GPS receiver. US Patent 5,841,399.

Zhu, G. (2014). *Trajectory-aided GNSS Land Navigation : Application to Train Positioning*. PhD thesis, 2014.

Zimmermann, A. and Hommel, G. (2005). Towards modeling and evaluation of ETCS real-time communication and operation. *Journal of Systems and Software*, 77(1) :47–54.

Liste des abréviations, des sigles et des symboles

PFD_{avg} Average Probability of Failure on Demand, 32

PFH Probability of a dangerous Failure per Hour, 32

ABAS Aircraft Based Augmentation System, 15

ADAS Advanced Driver Assistance Systems, 100

CBTC Communication Based Train Control, 106

CDDS Commercial Data Distribution Service, 17

DGPS Differential Global Positioning System, 17

DoD Department of Defense, 10

EGNOS European Geostationary Navigation Overlay Service, 11

ERA European Railway Agency, 20

FAST Function Analysis System Technique, 38

FDMS Fiabilité, Disponibilité, Maintenabilité, Sécurité, 30

FP filtre particulaire, 45

GAME Globalement Au Moins Équivalent, 31

GBAS Ground Based Augmentation System, 15

GLONASS Global'naya Navigatsionnaya Sputnikovaya Sistema, 10

GNSS Global Navigation Satellite Systems, 6

GPS Global Positioning System, 10

GRAIL GNSS introduction in the RAIL sector, 21

HAL Limite ou niveau d'alerte horizontale, 70

HPL Limite ou niveau de protection horizontale, 71

IR Integrity Risk, 71

IRNSS Indian Regional Navigational Satellite System, 12

KVB Contrôle de Vitesse par Balises, 19

MDT Mean Dowm Time, 36

MMSE Minimum Mean Square Error, 44

MSC Méthode de Sécurité Commune, 30

MTBF Mean Time Between Failure, 36

MTTF Mean Time To Failure, 36

MTTR Mean Time To Repair, 36

MUT Mean Up Time, 36

NSSE Normalised Sum of the Squared Errors, 78

OACI Organisation de l'Aviation Civile Internationale, 10

OS Open Service, 17

PE Position Error, 71

PPP Precise Point Positioning, 17

PPP Precise Point Positioning, 141

PPS Precise Positioning System, 11

QZSS Quasi-Zenith Satellite System, 12

RAIM Aircraft Autonomous Integrity Monitoring, 75

RAIM Receiver Autonomous Integrity Monitoring, 75

RTK Real Time Kinematic, 17

SA Selective Availability, 11

SADT Structured Analysis and Design Technique, 39

SARPs Standards and Recommended Practices, 69

SBAS Satellite Based Augmentation System, 15

SdF Sûreté de Fonctionnement, 30

SIL Safety Integrity Level, 31

Sol Safety of Life, 17

SPS Standard Positioning System, 11

SRS System Requirements Specification, 102

STI Spécification Technique d'Interopérabilité, 31

TTA Time To Alert, 70

UERE User Equivalent Range Error, 14

VAL Limite ou niveau d'alerte verticale, 70

VPL Limite ou niveau de protection verticale, 71

WAAS Wide Area Augmentation System, 11

WGS World Geodetic System, 11

Contribution à l'évaluation de la sécurité de systèmes de localisation ferroviaires basés sur les GNSS par la formalisation des concepts d'intégrité étendue

Résumé

Les GNSS (Global Navigation Satellite Systems), notamment le GPS sont aujourd'hui largement utilisés dans les systèmes de transport terrestre pour des applications sans impact sur la sécurité des biens et des personnes. Dans de telles situations, la qualité de l'information de localisation n'est pas un paramètre vital. Le service de localisation devient un élément critique dans un système ferroviaire. Les standards (EN 50126, EN 50128 et EN 50129) requièrent la détermination du degré de confiance que l'utilisateur peut placer dans le service délivré c'est à dire l'évaluation de la sûreté de fonctionnement avant la mise en service d'un nouveau système.

Un service de positionnement basé sur un GNSS souffre d'une variabilité de la précision inhérente aux différentes configurations environnementales qu'un train traverse tout au long d'une mission. Cependant, les GNSS intéressent les communautés de transport ferroviaire afin d'améliorer les systèmes de contrôle-commande des trains tout en substituant les balises au sol par une solution embarquée.

Après un état de l'art sur la localisation ferroviaire et sur les méthodes de sûreté de fonctionnement existantes, une analyse causale et de sensibilité sont faites afin de déterminer de nouveaux indicateurs pour évaluer la sécurité d'architectures de capteurs (avec un récepteur GNSS). Nous proposons ensuite une nouvelle approche pour l'évaluation de la sécurité des systèmes basés sur les GNSS grâce à l'intégrité, paramètre de performances des GNSS, étendu aux systèmes autres que GNSS et au milieu ferroviaire. Une évaluation de la sécurité sur un cas d'utilisation précis est réalisée grâce à l'approche proposée précédemment.

Mots-clefs : Systèmes de localisation basés sur les GNSS, Sécurité, Intégrité de localisation, Applications ferroviaires liées à la sécurité

Contribution to the safety evaluation of railway localisation systems based on GNSS by formalising extended integrity concepts

Abstract

Nowadays, GNSS (Global Navigation Satellite Systems) such as GPS are usually used in ground transportation systems for non-safety-relevant applications. In these situations, the quality of localisation information is not called into question. In the case of safety-related applications, the localisation service becomes critical in railway system. The standards (EN 50126, EN 50128 and EN 50129) require the determination of the degree of confidence that the user can be placed in the delivered service i.e. the RAMS analysis before putting into service of a new system.

A GNSS-based localisation service suffers from accuracy variability linked to the different environmental configurations that a train crosses all along a mission. However, with hybridisation solutions and combination of actual technologies, the GNSS integration increasingly interests the railway actors in order to ameliorate the train control system replacing balises by an embedded solution.

After a state-of-the-art on the railway localisation and existing RAMS methods, a causal and sensitivity methodologies are done in order to determine new paramters permitting to evaluate the safety of sensor architectures (with a GNSS receiver). We propose a new approach for safety evaluation of the GNSS-based systems through the integrity attribute, GNSS performances attributes, extended to the hybridised systems and in railway domain. A safety evaluation is performed on chosen architecture during sensibility and causal analyses thanks to the previous proposed approach.

Keywords: Satellite-based localisation system, Localisation integrity, Safety, Railway safety-related applications