utt
UNIVERSITÉ DE TECHNOLOGIE
TROYES

GROUPE RENAULT

THÈSE

PRÉSENTÉE À

L'UNIVERSITÉ DE TECHNOLOGIE DE TROYES

ÉCOLE DOCTORALE DES SCIENCES POUR L'INGÉNIEUR

par **Paula LAKOMICKI**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : OPTIMISATION ET SÛRETÉ DES SYSTÈMES

Démarche incrémentale pour qualifier la fiabilité du système de perception et de décision du véhicule autonome

---

Codirecteurs de thèse : Antoine Grall (UTT) et Bruno Castanier (Université d'Angers)
Date de soutenance : 20 décembre 2018

Devant la commission d'examen composée de :

Bruno Castanier ..	Professeur des universités, LARIS, Université d'Angers	Codirecteur de thèse
Mitra Fouladirad .	Professeur des universités, ICD-M2S, UTT	Examinateur
Antoine Grall	Professeur des universités, ICD-M2S, UTT	Codirecteur de thèse
Abdessamad Kobi ..	Professeur des universités, LARIS, Université d'Angers	Examinateur
Georges Oppenheim	Professeur émérite, LAMA, UPEM	Rapporteur
Mohamed Sallak ..	Maître de conférences-HDR, Heudiasyc, UTC	Rapporteur
Yves Tourbier	Expert optimisation et décision, Renault SA	Invité

– 2018 –

Titre Démarche incrémentale pour qualifier la fiabilité du système de perception et de décision du véhicule autonome

Résumé L'homologation en sécurité du véhicule autonome est primordiale pour sa mise en service opérationnelle. Ce véhicule présente la particularité d'être entièrement responsable de la sécurité de ses passagers et de son environnement. Les exigences en termes de fiabilité et de sécurité s'en trouvent accrues. Les processus classiques de qualification de la fiabilité ne permettent pas la prise en compte de conditions de fonctionnement fortement variable et possiblement pas ou mal identifiées préalablement. La recherche de la réduction du Time-To-Market rend inenvisageable une identification exhaustive des scenarios de roulage.
La thèse aborde la question de l'élaboration d'une méthode de certification/qualification de la fiabilité du système de perception et de décision du véhicule autonome. Elle pose les bases d'une démarche itérative pour la définition des scénarios de roulage de validation mêlant simulations numériques, essais sur piste et sur route ouverte. Cette démarche repose sur une extension du concept de fiabilité. Le modèle d'évaluation est étendu pour prendre en compte à la fois les incertitudes aléatoires, liées à la variabilité intrinsèque de l'environnement et les incertitudes épistémiques, liées à la connaissance incomplète du domaine de fonctionnement et du comportement du système. Une étude des performances de la méthode sur des cas d'études a été entreprise. La méthode proposée constitue une aide à l'organisation des essais et à la décision. Elle permet de dégager des recommandations de bonnes pratiques et ouvre des perspectives multiples.

Mots-clés Fiabilité, Véhicules autonomes, Prise de décision (statistique), Itération (mathématiques), Simulation par ordinateur

Title Incremental framework to qualify the reliability of the autonomous vehicle's perception and decision system

Abstract The autonomous vehicle safety certification is essential for its operational use. This vehicle has the particularity of being fully responsible for the safety of its passengers and its environment. This places particularly high demands on reliability and safety requirements. Conventional reliability qualification processes do not allow for highly variable operating conditions to be taken into account which may possibly not or poorly be identified in advance. Finally, the search for a reduction in Time-To-Market makes it impossible to envisage an exhaustive identification of driving scenarios.
The thesis work seeks to answer the question of developing a method for certifying/qualifying the reliability of the autonomous vehicle's perception and decision-making system. It lays the foundations for an iterative approach to defining validation scenarios combining numerical simulations, track tests and open road tests. This approach is based on an extension of the concept of reliability. The evaluation model is extended to consider both random uncertainties, related to the intrinsic variability of the environment, and epistemic uncertainties, related to incomplete knowledge of the system's operating domain and behavior. A first study of the method's performance on case studies is carried out. The proposed method is intended to assist in the organization of tests and help for decision-making. It makes it possible to identify recommendations for good practices and opens up multiple perspectives.

Keywords Reliability (Engineering), Autonomous vehicles, Statistical decision, Iterative methods (Mathematics), Computer simulation

Laboratoire d'accueil
Université de technologie de Troyes -
Institut Charles Delaunay
Laboratoire de Modélisation et Sûreté des Systèmes (LM2S)
12, rue Marie Curie
CS 42060 - 10004 Troyes Cedex

Entreprise d'accueil
Renault SA
Technocentre Renault
SCE DEA-SO [T] EE & Systems
1 avenue du Golf
78289 GUYANCOURT

Table des matières

Table des figures

Liste des tableaux

Introduction Générale

Les constructeurs automobiles développent depuis quelques années des véhicules disposant de fonctionnalités d'assistance au conducteur avec une prise en main partielle ou totale du véhicule (par exemple l'assistance au stationnement). Des véhicules autonomes roulent d'ores et déjà et sont en phase de tests dans le monde entier. Dans un avenir proche, ils seront disponibles au public afin d'apporter un confort de conduite, avec prise en charge totale du véhicule, lors de certaines phases de roulage comme par exemple la circulation dans un bouchon (vitesse lente) ou sur une autoroute (vitesse stabilisée). Le bénéfice visé est de renforcer la sécurité et de redonner du temps aux automobilistes.
L'homologation en sécurité du véhicule autonome est primordiale pour sa mise en service opérationnelle. Il n'existe actuellement aucune norme ou réglementation qui concerne ces véhicules. Les réglementations gouvernementales seront spécifiques à chaque pays et sont en cours de développement. Ce véhicule présente la particularité d'être entièrement responsable de la sécurité de ses passagers par l'intermédiaire de ses décisions de conduite ne faisant pas intervenir le conducteur. Les exigences ou objectifs de fiabilité, données en heure de roulage, seront par conséquent élevées pour garantir un haut niveau de sécurité. L'acceptation et la bonne perception du public est de plus primordiale pour mettre sur le marché une telle innovation. Elles renforcent la nécessité de garantir un tel niveau de fiabilité. Ce qui est difficile à valider. Le domaine de fonctionnement de ce véhicule, de grande dimension et fortement variable, est encore mal connu. Le système est encore nouveau et les retours d'expériences obtenus à partir des différents systèmes d'aide à la conduite ne permettent pas d'identifier tous ses modes de défaillance. Leurs fonctionnalités sont éloignées de celles des véhicules autonomes. En particulier les défaillances du système de perception et de décision du véhicule autonome sont les plus méconnues. En effet le système de perception qui prend en compte les informations des différents capteurs et les fusionnent pour donner une cartographie de l'environnement du véhicule autonome peut mal interpréter ce dernier et donner une information erronée au système de décision. Celui-ci choisit une action inappropriée qui met en danger l'ensemble des acteurs du système routier. Que ce soit objet de l'infrastructure, action du trafic routier ou perturbations liées à la météo, de nombreuses combinaisons peuvent perturber le système de perception et l'amener à une incompréhension inattendue. De même, les analyses de sécurité telles que les analyses préliminaires de risque ne permettent pas d'obtenir une liste exhaustive des événements possibles amenant à une défaillance.
L'évaluation et la validation de la fiabilité de perception et de décision ne sont que partiellement traitées dans le domaine automobile ou dans les autres domaines comportant des systèmes autonomes.
Les études de fiabilité des systèmes ADAS (systèmes d'aide à la conduite) réalisées ces dernières années concernent plus particulièrement la fiabilité de l'architecture du système en fonction des

défaillances d'un ou plusieurs composants [33] ou encore des évaluations de l'impact en termes de sûreté/sécurité de conduite, [54, 27].

Néanmoins la validation de la fiabilité de la perception de ces systèmes est peu abordée et le conducteur reste responsable de son véhicule. Les autres domaines (ex : ferroviaire, aéronautique) comportant des systèmes autonomes n'ont pas la même difficulté à estimer la fiabilité. L'environnement est en effet connu voire même bien maîtrisé. La certification réside dans l'évaluation du système à bien se comporter dans des scénarios spécifiques simulés. De plus les systèmes autopilotés dans l'aéronautique ou dans l'aérospatial restent secondés pour toute action sécuritaire.

L'objectif de cette thèse réalisée dans un contexte industriel se situe sur 2 volets. Le premier volet, plutôt d'ordre méthodologique et contributif au domaine de la sûreté de fonctionnement, est l'élaboration d'une stratégie générale pour l'élaboration d'un plan de validation du véhicule autonome en vue de la certification au niveau de la fiabilité dudit véhicule. Cette méthode doit être la plus générique possible, elle doit s'adapter à tout type de système et ne pas dépendre de la définition technique du véhicule, du niveau d'autonomie, des fonctionnalités du système ou encore du domaine de fonctionnement. Elle doit s'appuyer sur l'ensemble des ressources mises à disposition par l'entreprise.
Le second volet se situe plus sur l'accompagnement de l'entreprise d'accueil dans la formalisation ou la caractérisation d'un ensemble d'éléments relatifs à la fiabilisation du processus. En particulier une méthode d'évaluation quantitative de la fiabilité adaptée au contexte du véhicule autonome permettant d'évaluer d'une part l'ensemble des incertitudes liées au manque de connaissance (par exemple une liste non exhaustive de scénarios de conduite) peut permettre de mieux organiser les essais de roulage et de donner une indication sur les efforts à mener pour certifier le véhicule.
Le mémoire se centrera principalement sur le premier volet. Il est organisé en 2 parties.

La première partie regroupe trois chapitres. Elle fait ressortir le besoin de développer un plan de validation final en complément des méthodes de validation usuelles en sûreté de fonctionnement afin de garantir un niveau de fiabilité le plus élevé possible. Le chapitre 2 présente la problématique industrielle. Il caractérise les modes de défaillances du véhicule autonome et décrit les méthodes et outils de validation utilisées pour l'étude des systèmes ADAS. Les enjeux pour valider ce véhicule en termes de fiabilité sont ensuite dégagés en indiquant les limites des méthodes de validation actuelles dans l'entreprise.

Dans le chapitre 3, une étude bibliographique des méthodes d'évaluation de la fiabilité est proposée pour présenter l'applicabilité et les limites des approches disponibles au contexte du véhicule autonome.

Enfin le chapitre 4 propose une synthèse des verrous scientifiques et des moyens disponibles pour établir une nouvelle démarche de validation de la fiabilité. Nous détaillerons les principaux objectifs de cette étude et nous présenterons les hypothèses, procédures et modélisations choisies pour les atteindre.

La seconde partie propose une méthode générale pour la validation et l'estimation de la fiabilité. Elle complète les méthodes traditionnelles de sûreté et se positionne à la toute fin des

étapes de validation, avant les tests réalisés avec les clients. Cette seconde partie correspond aux trois derniers chapitres
Le chapitre 6 détaille une première organisation générale du déroulement itératif de la validation, comprenant des roulages sur route ouverte, des tests sur piste ou des tests numériques. Cette démarche doit être vue comme une feuille de route pour l'entreprise. Pour chaque type d'essai et chaque étape de la démarche, des manières de procéder sont suggérées. Pour s'assurer de la faisabilité de certaines étapes, des études ont été menées avec des niveaux d'approfondissement différents.

Le chapitre 7 donne un cadre de modélisation pour évaluer la fiabilité du véhicule autonome avec une marge d'erreur. Pour un niveau d'information donné le modèle proposé évalue les incertitudes aléatoires et les incertitudes épistémiques qui se réduisent avec les essais de validation.

le chapitre 8 propose d'évaluer les performances et l'efficacité d'une telle modélisation à partir de cas tests théoriques.

Première partie

Introduction et positionnement des travaux de thèse

Chapitre 1

Introduction

La "fiabilité" des véhicules est un des premiers critères de choix lors d'une acquisition d'une automobile et reste un des meilleurs arguments pour embellir l'image de marque d'un constructeur. Une succession de défaillances sur un modèle, rendant les véhicules inutilisables peut dégrader pendant plusieurs années le sentiment de sécurité des usagers qui se détourneront de cette marque. Pire que des pannes répétées immobilisant les véhicules, les pannes amenant à des événements dangereux ont des conséquences économiques et de réputation encore plus désastreuses. Le scandale des airbags Takata en 2015 en est une belle illustration. Ces airbags, par leur explosion fortuite en pleine conduite, ont causé la mort de 10 personnes, concerné plus de 19 millions de véhicules de plusieurs marques comme Honda, Toyota ou FCA aux Etats-Unis qui ont tous été rappelés.
En sûreté de fonctionnement, on distingue l'aptitude d'un composant ou d'un système à être en état de marche à un instant donné, que l'on nomme la disponibilité (le véhicule est prêt à l'emploi), de l'aptitude d'un produit à ne pas provoquer des accidents inacceptables, nommée : la sécurité (comme la défaillance de l'airbag Takata). Avant de désigner une discipline indispensable dans la réalisation d'un produit, la sûreté de fonctionnement est par définition l'aptitude d'un système à remplir une ou plusieurs fonctions requises dans des conditions données ; elle englobe principalement quatre composantes : la fiabilité (aptitude d'une entité à accomplir une fonction requise, dans des conditions données, durant un intervalle de temps donné), la maintenabilité (aptitude d'un produit à être maintenu ou remis en état de fonctionnement), la disponibilité et la sécurité selon la norme NF X60-500 [1].
Dans le domaine de l'automobile, la sécurité est prioritaire sur le reste des analyses de sûreté de fonctionnement au détriment de la disponibilité qui peut se retrouver réduite pour favoriser la sécurité. Il est par exemple préférable de mettre hors service le véhicule lors d'une révision si une pièce dite "sécuritaire" est détériorée plutôt que d'attendre la défaillance de cette pièce pendant l'utilisation du véhicule. Aucun ou peu de compromis sont faits entre les exigences de sécurité et le reste des activités de sûreté. Les exigences de sécurité sont définies dès le début de la phase de conception lors de la phase de définition du besoin et ne sont plus remises en question pendant le reste du développement. En phase de validation, phase dans laquelle se place le reste des activités de sûreté de fonctionnement, ces exigences et critères sont vérifiés avant la phase d'industrialisation et de production du produit.
La sécurité est si importante, qu'avec les prises de conscience à la fin du 20ème siècle du taux de mortalité lié aux accidents de la route, la sécurité des passagers du véhicule et des autres acteurs

du trafic routier est devenue la cible de la plupart des innovations réalisées. Les recherches de systèmes de sécurité se sont amplifiées. Les systèmes de sécurité dits « passifs », sont apparus pour limiter la gravité des accidents de la route comme les ceintures de sécurité, les parechocs et faces avant du véhicule conçus pour diminuer le choc avec un piéton, les airbags, appuie têtes, renforts de caisse, déformation de la structure... Plus récemment des technologies "actives" sont apparues pour, dans le meilleur des cas, éviter les accidents et aider le conducteur dans l'ensemble de ses actions de conduite ou bien d'en réduire leurs conséquences. On peut donner les exemples des ABS, ESP, régulateur et limiteur de vitesse. La plupart des véhicules vendus en Europe disposent d'un classement European New Car Assessment Program (Euro NCAP) [32] c'est-à-dire le « Programme européen d'évaluation des nouveaux véhicules », sous forme d'étoiles, gage de qualité et de sécurité. La course aux étoiles (ou d'autres types de classement hors Europe) a permis le développement de technologies de plus en plus sophistiquées d'aide à la conduite (Advanced driver-assistance systems ADAS). Nous pouvons citer les systèmes Automated Emergency Braking (AEB) qui freinent en urgence pour éviter une collision avec un piéton ou un véhicule, le maintien dans la voie, le radar de régulation à distance (adaptative cruise control ACC) qui s'additionne au régulateur de vitesse pour conserver les distances de sécurité avec le véhicule qui précède, etc. Devant l'émergence de toutes les technologies visant à informer et à gérer les situations à risque, l'arrivée du véhicule autonome représente le summum de la sécurité car l'homme (le conducteur) n'intervient plus dans la gestion de la conduite.

Dans certaines conditions de conduite, les véhicules autonomes remplacent le conducteur dans l'ensemble de ses actions de conduite. Le conducteur pourra s'il le souhaite sur des routes habilitées et dans des conditions de conduite autorisées, faire d'autres activités sans avoir à se concentrer sur la route. La partie intelligente du véhicule, que ce soit pour le système autonome AD (autonomous driving) ou ADAS, sera appelée dans ce mémoire : système de perception et de décision. Elle est en effet dotée :

- d'un système de perception, ensemble de capteurs dont les données sont fusionnées pour cartographier l'environnement autour du véhicule
- et d'un système de décision, qui choisit parmi des lois de commande prédéfinies les actions que doit adopter le véhicule autonome en fonction de la situation qu'il rencontre.

Ces deux systèmes lui permettent d'agir en toutes circonstances. Si le véhicule sort de son domaine de fonctionnement, il doit être capable d'inviter le conducteur à reprendre la main. Ou bien, si le conducteur ne le fait pas dans les délais, le système impose au véhicule de s'arrêter dans une zone sécuritaire. Initialement vu comme un simple assemblage de tous les systèmes actuellement présents ou en cours de développement, il remet en réalité en question l'organisation et les méthodes de conception et de validation appliquées aux ADAS déjà présents.

Les systèmes d'aide à la conduite sont homologués suivant deux procédures bien distinctes, les tests de performances, en Europe suivant l'Euro Ncap [22] et le respect des règles de sûreté de fonctionnement suivant la norme ISO26262 [37].
Pour la première, le système est testé principalement sur piste dans des conditions de fonctionnement bien définies. Ces systèmes agissent pour éviter ou réduire un accident et sont donc testés dans des conditions extrêmes. Pour éviter les pertes matérielles et humaines, on utilise des pantins et des véhicules fictifs, ce qui rend ces tests peu réalistes et parfois peu compatibles avec l'usage réel mais laisse malgré tout entrevoir le potentiel de ces systèmes. Leurs incompatibilités mènent parfois à des dérives. Des véhicules jugés performants lors des tests Euro Ncap peuvent

ne pas l'être dans des conditions réelles ou pire peuvent avoir des conséquences néfastes. Ces tests d'homologation évoluent et tendent à supprimer les dérives à partir des retours d'expériences. Cette manière de procéder est acceptable car ils sont une aide à la conduite et le conducteur reste responsable de son véhicule.
Les ADAS ne doivent cependant pas entraîner de nouveaux accidents pour lesquels ils seraient fautifs, comme les airbags Takata. C'est pourquoi la norme ISO26262, permettant de garantir la sécurité fonctionnelle des systèmes électriques et électroniques dans les véhicules automobiles, s'applique. Les critères d'homologation de ces systèmes se définissent à partir des niveaux de criticité ASIL ("automotive system integrity level") donnés dans cette norme. Ils sont qualitatifs et se déterminent suivant trois métriques : Sévérité, Exposition, Contrôle. La sévérité est la gravité des conséquences en cas d'accident. L'exposition est le pourcentage de temps pendant lequel le véhicule est confronté à une situation pouvant entraîner un accident en cas de défaillance. La contrôlabilité est la capacité du conducteur et des autres usagers à garder le contrôle en cas de défaillance. Dans de nombreux cas la contrôlabilité est grande ce qui limite le risque d'avoir un événement inacceptable et permet de définir des objectifs de fiabilité du système facilement atteignable avec un coût de validation raisonnable (par exemple si le régulateur de vitesse n'est plus capable de tenir la vitesse pour cause de forte pente, le conducteur est toujours capable de reprendre les pédales et d'appuyer sur la pédale de frein). Mais cette contrôlabilité tend à disparaître avec la multiplicité des fonctions que prennent les ADAS d'aujourd'hui et ne sera définitivement plus présente dans le contexte du véhicule autonome. On obtient alors des objectifs de sécurité et de fiabilité très élevés qui demandent une démarche de validation très coûteuse.

Le premier exemple d'une telle contrainte est le système AEB, le système de freinage d'urgence. La défaillance non souhaitée est un freinage intempestif pouvant entraîner une collision avec le véhicule qui le suit. Cette défaillance est instantanée et facile à détecter. Si le système demande à freiner alors que cela n'est pas nécessaire il est considéré comme défaillant. Il est ainsi possible de le tester sur une route publique dite "route ouverte" sans pour autant enclencher le système et mettre en danger les automobilistes. En effet, le système de détection et de décision est bien opérationnel mais il n'est pas relié à la pédale de frein, seule la demande de freinage est vérifiée. La défaillance opposée,"le système ne freine pas alors qu'il aurait dû" a moins d'importance du fait que le conducteur reste responsable. Partant de ces deux constats, il a été possible de mettre en place une stratégie permettant de réduire le coût de validation. La démarche choisie ne pourra malheureusement pas être appliquée au véhicule autonome pour lequel ces deux modes de défaillances sont aussi dangereux l'un que l'autre. La validation de ce système, de fonctionnalité moins complexe que le véhicule autonome, a requis un million de kilomètres de roulage aléatoires sur route ouverte.
Pendant ce roulage, des scénarios de conduite imprévus ont mis en défaut ce système. Ces scénarios sont des modes de fonctionnement qui n'avaient pas été identifiés pendant la phase de conception. Parmi ces nouveaux modes, nous en détaillons deux pour mieux comprendre cette omission.

— Dans un scénario, schématisé en 1.1, une succession de poteaux de petites tailles sont placés sur le trottoir à distance régulière pour empêcher le stationnement de véhicules. Ces poteaux sont vus à une fréquence proche de la fréquence d'échantillonnage des capteurs. Ils sont identifiés comme un unique objet inconnu mobile avec la même vitesse que celle du véhicule testé. En poursuivant sa course le véhicule détecte un piéton positionné juste à côté du poteau. Le système de détection considère que le poteau et le piéton sont le

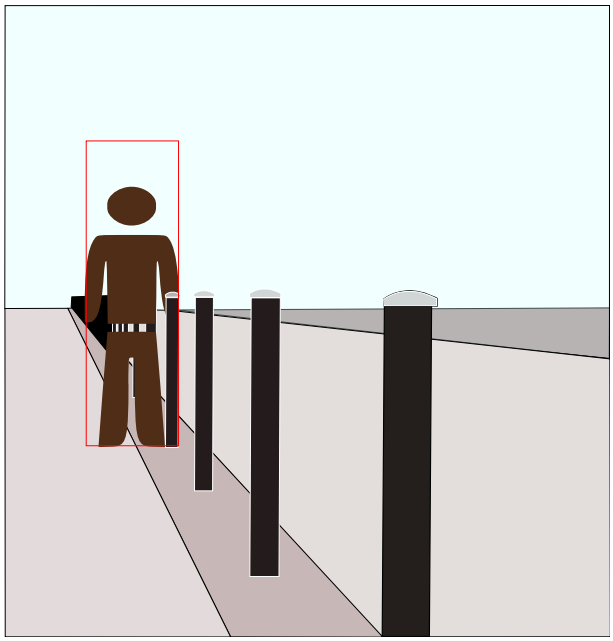


FIGURE 1.1 – Confusion entre piéton et poteaux

même objet. Il considère donc que le piéton avance à une vitesse égale à celle du véhicule. Le piéton, de trajectoire non parallèle à la route se rapproche un peu du véhicule sans intention apparente de traverser. Compte-tenu de la vitesse affectée au piéton, le système comprend que le piéton va arriver sur sa voie dans les instants qui suivent. Il demande alors le déclenchement du freinage d'urgence à tort.

— Dans un second scénario, le véhicule entre dans un parking souterrain. Pendant qu'il descend une forte pente pour entrer dans le parking, le système détecte une bouche d'égout située à la fin de la descente, il l'interprète comme un véhicule à l'arrêt car il n'a pas pris en compte la pente. Il demande alors le déclenchement du freinage d'urgence par erreur.

Ces deux modes de défaillance étaient difficiles à prévoir et n'étaient pas pris en compte lors de l'analyse préliminaire de risque. Ils sont loin d'être les seuls. Les analyses classiques de spécifications du besoin listant les modes de fonctionnement et de dysfonctionnement n'ont pas été suffisantes pour caractériser intégralement le domaine de fonctionnement de ce système.

Ce premier exemple montre les limites des méthodes et critères actuels pour certifier la sécurité et la fiabilité des véhicules autonomes. Le véhicule autonome, pour réaliser l'ensemble des fonctionnalités complexes qui lui sont imposées, intègre de nombreuses technologies différentes apportant des informations qui lorsqu'elles sont fusionnées peuvent être interprétées par le système de manière surprenante. Elles remettent en question notre manière intuitive d'analyser et de décomposer les scénarios de conduite auxquels nous sommes confrontés pour choisir les actions qui nous semblent les plus logiques et les plus sécuritaires. Au vu de la complexité, du nombre et de la connaissance de ces scénarios, l'analyse des modes de fonctionnement généralement attribués à la phase de spécifications du besoin se retrouve complétée et remise en question lors de la phase de validation. Les exigences de sécurité définies en début de conception du véhicule autonome ne seront complètes qu'après avoir identifié l'ensemble des modes de

fonctionnement. L'environnement du véhicule nous apparaît comme nouveau, en utilisant ces technologies fortement innovantes que l'on apprend tout juste à connaître. Les méthodes traditionnelles de validation principalement construites à partir de tests réels aléatoires sur route ouverte sont adaptées aux premiers ADAS. Ceux-ci, bien qu'étant des systèmes "sécuritaires" avec un niveau de sécurité très élevé, sont souvent l'assemblage de plusieurs sous-systèmes avec des objectifs de fiabilité relativement peu exigeants. Ces méthodes sont inabordables pour valider des critères de fiabilité extrêmement sévères qu'impose la forte responsabilité que portent les futurs ADAS et le véhicule autonome. Il faudrait attendre de nombreuses années avant de garantir la sécurité de ces systèmes [40]. De surcroît, la forte concurrence n'enlève rien au problème. Tous les constructeurs automobiles, les GAFA et même des start-ups se sont lancés dans la course du véhicule autonome. L'arrivée de ces véhicules est imminente, et un retard important de la sortie de ces systèmes risque de pénaliser l'une de ces entreprises. Les démarches de validation actuelles, incomplètes, trop longues et trop coûteuses doivent être adaptées pour permettre de garantir un niveau de fiabilité élevé tout en conservant un "time to market" acceptable pour un système fortement innovant toujours en cours de développement.

Cette première partie fait ressortir le besoin de construire une nouvelle démarche de validation appliquée au véhicule autonome.

Le chapitre 2 reprend la problématique industrielle brièvement exposée dans cette introduction. Dans un premier temps, il décrit l'ensemble des défaillances du système de perception et de décision du véhicule autonome et de leurs conséquences. Les enjeux pour valider ce véhicule en termes de fiabilité sont ensuite dégagés en indiquant les limites des méthodes de validation actuelles dans l'entreprise.

Dans le chapitre 3, une étude bibliographique des méthodes d'évaluation de la fiabilité est proposée pour présenter l'applicabilité et les limites des approches disponibles au contexte du véhicule autonome.

Enfin le dernier chapitre fait la synthèse des verrous scientifiques et des moyens disponibles pour établir une nouvelle démarche de validation de la fiabilité. Nous détaillerons les principaux objectifs de cette étude et nous organiserons les hypothèses, procédures et modélisations choisies pour les atteindre.

Chapitre 2

Problématique industrielle

2.1 Introduction

Devant les enjeux fixés pour 2022 de réduire de manière drastique le nombre de tués sur la route, les constructeurs automobile se sont lancés dans la conception de systèmes ADAS et AD de plus en plus innovants avec toujours plus de fonctionnalités pour faciliter la conduite de l'usager. Le niveau de sécurité accordé à ces systèmes est extrêmement élevé pour que ceux-ci soient utilisés en toute confiance. Le véhicule autonome sera l'un des premiers systèmes à agir seul sur la sécurité des usagers, sans surveillance humaine. Actuellement les systèmes auto-pilotés dans l'aéronautique ou dans l'aérospatial restent secondés pour toute action sécuritaire. Les systèmes autonomes ferroviaires, comme le système d'automatisation intégral des lignes 1 et 14 du métro parisien, quant-à-eux, fonctionnent dans un environnement bien maîtrisé. Leur infrastructure est contrôlée ce qui permet de partager le niveau de responsabilité entre l'infrastructure et le système autonome, contrairement à l'environnement de la voiture autonome qu'elle partage avec le reste de la population.
Pour mieux comprendre la complexité pour concevoir et valider de tels systèmes, nous reprenons leur classement par niveau d'autonomie réalisé par la SAE [15]. 6 niveaux d'autonomie ont été identifiés. Les systèmes de niveau d'autonomies 0, 1 et 2 sont présents sur les routes. Les niveaux 3,4 et 5 sont encore des sujets de recherche et vont apparaître très prochainement. Nous expliquons brièvement la progression des difficultés en fonction du niveau d'autonomie :

- **Niveau 0, aucune autonomie** : Le conducteur contrôle entièrement le véhicule et réalise toutes les tâches de conduite. Il peut être assisté par des systèmes produisant des alertes pour l'avertir d'un événement.
  On retrouve ici le véhicule des générations précédentes avec uniquement les systèmes de sécurité bien connus comme la ceinture de sécurité, l'ABS, l'ESC, les voyants d'alerte et tout autre système nous laissant complètement maîtres de notre véhicule.
- **Niveau 1, assistance du conducteur** : Le système peut gérer soit le contrôle du volant soit l'accélération et décélération du véhicule. Le conducteur doit à tout instant contrôler la conduite, il reste entièrement responsable.
  C'est à ce niveau qu'on trouve les premiers systèmes d'aide à la conduite comme le régulateur de vitesse, le limiteur de vitesse, ou plus récemment l'ACC (adaptative cruise control : conservant les distances de sécurité avec le véhicule qui précède).

— **Niveau 2, automatisation partielle** : Le système maîtrise dans des conditions d'usage spécifiées à la fois, les actions sur le volant, les accélérations et décélérations. Le conducteur est toujours présent pour vérifier l'ensemble de ses actions et reprendre la main dès que le système sort de ses limites de fonctionnement.
Par exemple, le système de maintien dans la voie sur autoroute est utilisé uniquement à très faible vitesse en condition de congestion de la circulation. Les actions de conduite sont assez basiques : il décélère, accélère et suit bien la trajectoire de la route.
Des systèmes de niveau 2 peuvent avoir de plus grandes fonctionnalités (actions de conduite réalisables par le véhicule) et dans un domaine de fonctionnement large (Ensemble de routes et de conditions d'usage possibles avec le système). La Tesla Autopilot est un autre exemple de niveau 2 avec de nombreuses fonctionnalités intégrées. Elle est capable de rouler dans beaucoup de situations.
Comme le conducteur supervise l'ensemble des manœuvres et doit intervenir à tout moment, le nombre, le champ de vue et les performances des capteurs requis pour atteindre l'objectif de fiabilité de ces systèmes restent limités. Il n'est pas nécessaire de placer un grand nombre de technologies différentes pour visualiser les mêmes zones. De plus les exigences de sécurité sur les règles de conduite, les algorithmes de fusion et de décision ont été élaborés selon un nombre limité de scénarios de conduite. Les scénarios impromptus ne seront sans doute pas gérés par ces véhicules. Pour éviter une perte de concentration du conducteur, ces systèmes sont souvent munis de capteurs à l'intérieur du véhicule pour vérifier son niveau de vigilance. Pour la Tesla, le conducteur doit garder ses mains sur le volant. Une caméra infrarouge de supervision détectant la position de la tête du conducteur est présente dans la Super Cruise de General Motor.
Plus les fonctionnalités offertes par le système sont complexes et plus la conception sera exigeante. Des capteurs très performants, avec une bonne capacité de détection, de précision, et des algorithmes capables d'identifier et d'interpréter des scénarios de plus en plus complexes devront être choisis. Une ville est bien plus compliquée à gérer (piétons avec des comportements et des trajectoires parfois erratiques) qu'un environnement relativement bien maîtrisé comme l'autoroute.
Pour garantir la sécurité des usagers, la surveillance du conducteur ne doit pas être plus importante que le niveau de vigilance en conduisant.

— **Niveau 3, automatisation conditionnelle** : Comme le système précédent, il contrôle le volant et l'accélération/décélération dans certaines conditions. Il détecte en plus sa sortie du domaine de fonctionnement et invite le conducteur à reprendre la main.
Les fonctionnalités ici peuvent être les mêmes que celles proposées au niveau 2, cependant le conducteur est autorisé à se déconcentrer partiellement de la route. Il n'est tenu responsable que s'il ne reprend pas la main lorsque le système le lui demande. Cela signifie que le système doit être capable d'identifier à temps un scénario qu'il ne sera pas capable de gérer. Pour la même fonctionnalité, le niveau de sécurité requis est donc beaucoup plus important. La définition technique comme le nombre, la redondance ou la performance des capteurs peut complètement évoluer. De nouveaux scénarios sont à prendre en compte comme ceux proches des limites de fonctionnement : une dégradation de la météo, l'approche d'une zone de travaux, la rencontre inattendue d'un piéton sur autoroute. Les conditions de reprise en main du conducteur ne doivent pas entraîner un accident. Celui-ci doit avoir le temps d'analyser la scène pour prendre des décisions.

— **Niveau 4, haute autonomie** : Le système réalise toutes les actions du niveau 3. L'hu-

main n'est plus tenu de reprendre la main si le véhicule lui demande d'intervenir et le véhicule doit être en mesure de gérer ce type de situation. Dès que le véhicule sort de son domaine de fonctionnement, il doit être capable de mettre en sécurité les usagers en réalisant des manœuvres d'urgence.
Les fonctions réalisées par ces systèmes peuvent être exactement les mêmes que précédemment. Ce niveau d'autonomie apporte une plus grande liberté au conducteur qui peut désormais réaliser d'autres activités sans se préoccuper de la route, comme dormir. Le véhicule est confronté à de nouvelles situations telles que celles comportant des manœuvres d'urgence à réaliser dans un domaine de fonctionnement proche des limites définies.

— **Niveau 5, entière autonomie** : Le véhicule doit être capable de gérer toutes les actions de conduite sur toutes les routes dans toutes les circonstances maîtrisables par l'homme.

De nouvelles technologies, toujours plus performantes, voient le jour afin d'offrir plus de liberté aux usagers grâce à de nouvelles fonctionnalités des systèmes AD. La diversité, le nombre et la performance des capteurs en assurent la sécurité. L'évolution est tellement rapide qu'elle laisse peu de temps pour bien appréhender ces technologies. Les phases de conception et de validation des AD sont impactées par l'amélioration continue de ces technologies. Il est difficile de spécifier ou de valider un système qui est sans cesse modifié. L'ajout d'une fonctionnalité dans un capteur peut de plus dégrader ses performances pour d'anciennes fonctionnalités. Par exemple l'ajout de détection des cyclistes peut impacter celle des piétons.

Cette étude s'intéresse à l'évaluation de la fiabilité pour la certification du système "intelligent" de perception et de décision du véhicule autonome. Actuellement les systèmes les plus avancés, des ADAS de niveau 2, sont conçus et validés suivant les approches de mécatronique. La mécatronique "est une démarche visant l'intégration en synergie de la mécanique, l'électronique, l'automatique et l'informatique dans la conception et la fabrication d'un produit en vue d'augmenter et/ou optimiser sa fonctionnalité", selon la norme NF E 01-010 (2008). Une application mécatronique bien conçue s'obtient en conservant une vision globale d'un système impliquant différentes disciplines jusqu'alors isolées. Elle prend en compte les couplages des informations au travers d'échanges et de travaux collaboratifs entre les acteurs des différentes branches. Une démarche de conception et de réalisation associée au système mécatronique permet d'aider le concepteur tout au long de son projet, depuis le cahier des charges jusqu'aux tests de réception du système. Le cycle de développement en V, d'abord utilisé en informatique, est la démarche prépondérante dans l'élaboration de tels systèmes [67]. Celui-ci est composé de 2 branches. La branche descendante correspond à une démarche de raffinements successifs qui se rapporte à la phase de conception, partant du général pour aboutir sur le particulier. La branche ascendante, quant à elle, retrace les phases d'intégration et de validation du système.

Dans la première partie de ce chapitre, nous donnons la définition de la fiabilité normalisée. Au travers du processus d'analyse classique de la sûreté de fonctionnement (SdF), nous décrirons les défaillances du système étudié et leurs conséquences. En expliquant le fonctionnement du système AD, nous discuterons de l'applicabilité et des limites de la méthode pour le véhicule autonome.

De nombreux outils et méthodes dédiés à la validation des ADAS et du véhicule autonome ont été mis en place. Ils aident à la définition des exigences et à leur vérification à différents

stades de développement et de validation du cycle en V. Nous les détaillons dans une seconde partie et dégagerons leurs applicabilités et leurs limites pour évaluer la fiabilité du véhicule autonome.

2.2 Caractérisation des défaillances et de leurs conséquences pour la définition des exigences SdF

Dans le domaine de sûreté de fonctionnement, on appelle fiabilité l'aptitude d'un système à fonctionner dans des conditions données, durant un intervalle de temps donné, selon la norme NF EN 13306 [61].

Le domaine de fonctionnement du véhicule autonome est défini par :
- un ensemble de routes répertoriées,
- des conditions climatiques et des horaires bien définis,
- des conditions d'usages bien choisies tels que la plage des vitesses autorisées, le positionnement du véhicule au démarrage du mode autonome tenant compte de la cinématique et des configurations du trafic routier autour.
- D'autres contraintes sur l'infrastructure comme les zones de travaux, des zones d'accidents et l'absence ou la non disponibilité des voies d'arrêt d'urgence restreignent également l'utilisation du véhicule autonome.

La durée choisie pour évaluer la fiabilité du véhicule autonome est de "une heure". Cette durée permet de comparer la fiabilité à l'objectif fixé par les analyses d'accidentologie et respecte également le format usuel des objectifs de fiabilité donnés par les normes automobiles, telle que la norme ISO26262 [37] que l'on présentera dans cette section. Pourtant ce format ne semble pas pertinent, les parcours d'une heure de roulage sont extrêmement variés. Il faut donc voir la fiabilité évaluée comme une grandeur moyenne sur l'ensemble des heures de conduite possibles dans le domaine de fonctionnement.

Les méthodes d'analyse fonctionnelle et dysfonctionnelle du besoin définissent le bon fonctionnement du système de perception et de décision.

2.2.1 Analyse dysfonctionnelle préliminaire et cotations pour limiter le risque

2.2.1.1 Objectif et description

L'analyse dysfonctionnelle d'un produit ou d'un système s'effectue à partir de l'analyse fonctionnelle faite au préalable par l'équipe de conception. Cette dernière consiste à raisonner en termes de besoins à satisfaire, exprimés sous forme de fonctions à remplir avec des critères de valeur, dans un environnement donné. L'analyse de sûreté de fonctionnement identifie les dysfonctionnements résultants, en déduit les exigences de sécurité associées et décline ces exigences aux sous-systèmes et composants à partir du cycle de développement en V. La fonction principale du système AD est de conduire le véhicule sur toute la portion de route demandée. Cette

Fonction	Mode de défaillance	Phase de vie	Scénario/situation aggravation	Effet Redouté Système	EIC	Gravité
Freiner	Fonction intempestive	Roulage	Le système freine régulièrement alors que ce n'était pas nécessaire	Freinage intempestif	Nausée / mécontentement	Significative
		Roulage	Le système freine fort alors que ce n'était pas nécessaire	Freinage fort intempestif	Frayeur	Significative
					Accident	Catastrophique
	Perte de fonction	Roulage	Le système ne freine pas alors que la situation le requiert	Pas de freinage	Frayeur	Significative
					Accident	Catastrophique
	Fonction dégradée	Roulage	Le système ne freine pas suffisamment alors que la situation le requiert	Freinage trop faible	Frayeur	Significative
					Accident	Catastrophique

Table 2.1 – Exemple d'APR pour la fonction freiner

fonction se découpe en un ensemble d'actions possibles et nécéssaires représentées sur la Figure 2.1. Il faut ajouter à cela les fonctions contraintes comme :

— Respecter le code de la route ou toute norme et réglementation qui lui sont applicables
— Fonctionner dans les conditions extérieures qui font parties de son domaine de fonctionnement(météo, infrastructure)
— Fonctionner dans l'environnement véhicule (trafic) pour lequel il est compatible.

Les modes de défaillances, formes de manifestation d'un dysfonctionnement, sont alors déduits de ces fonctions. Quelques modes sont détaillés sur la Figure 2.1. Les risques associés sont établis lors de l'analyse préliminaire des risques. Cette analyse identifie, évalue et hiérarchise ces risques dans le but de les réduire à un niveau acceptable. Les modes de défaillances du système sont associés à un événement indésirable pour le client (EIC). Un exemple est présenté par la Table 2.1 pour les modes de défaillances déduits de la fonction freiner.

Les exigences de sûreté de fonctionnement sont les critères de sûreté quantitatifs ou qualitatifs que doit respecter le produit. L'objectif de fiabilité, reliée à la probabilité d'occurrence de telles défaillances, est décidé à cette étape. L'APR et l'analyse fonctionnelle aident à la sélection du critère.
La norme ISO 26262 [37] prescrit un protocole pour mener à bien les études de sûreté de fonctionnement dans l'automobile. Elle est une déclinaison de la norme IEC 61508 applicable aux systèmes à base d'électronique et d'électronique programmable. Elle concerne les fautes et défaillances aléatoires des composants électroniques et les bugs logiciels des systèmes [11]. Elle définit des niveaux d'intégrité (connus sous le nom de « ASIL » : Automotive Safety Integrated Level) pour un système afin de sélectionner les activités de sécurité qui lui sont adaptées. Elle aide ainsi à la définition des exigences sur les systèmes automobiles embarqués. Les ASIL sont classés de A à D avec des exigences d'occurrence de ces événements associés. Par exemple un ASIL D qui est le niveau le plus grave demande une occurrence de la défaillance de 10^{-9} par heure. Elle est réalisée en tenant compte de :

— la contrôlabilité :
  La capacité du conducteur et des autres usagers à garder le contrôle en cas de défaillance
— l'exposition :
  Le pourcentage de temps pendant lequel le véhicule est confronté à une situation pouvant entraîner un accident en cas de défaillance
— et la sévérité :
  La gravité des conséquences en cas d'accident.

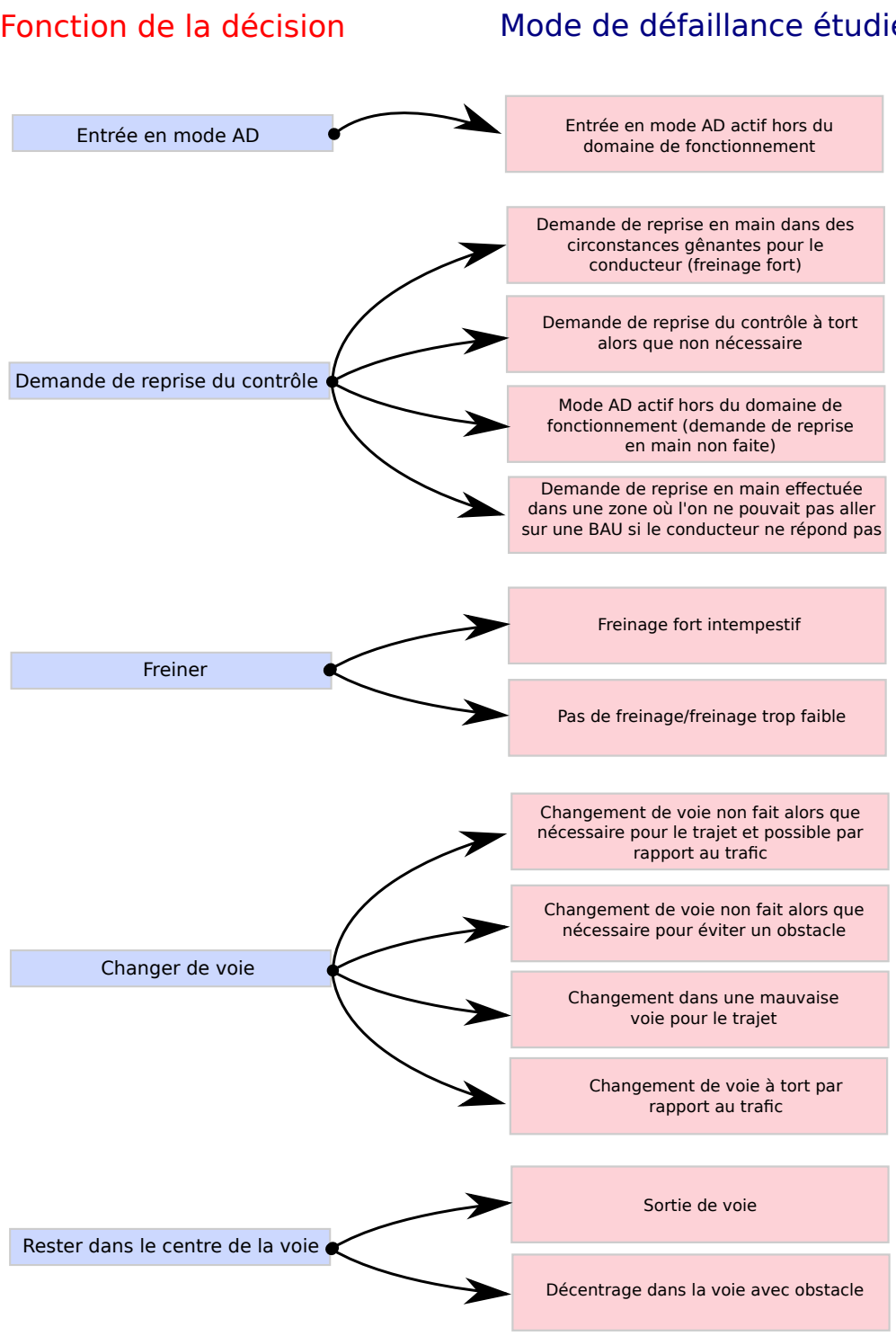


FIGURE 2.1 – Liste non exhaustive des défaillances possibles du véhicule autonome

2.2.1.2 Applicabilité et limites

La classification ASIL n'est adaptée qu'au système électronique ou électronique programmable des ADAS (système d'aide à la conduite) mais n'est pas adaptée à la partie "intelligente" du véhicule autonome. La norme ISO 26262 ne traite pas encore des erreurs d'algorithmes du système de perception et de décision. Une extension nommée SOTIF [3] (Safety Of The Intended Functionality) intégrera prochainement les défaillances du système de perception et de décision. Cependant si on l'appliquait au système AD, le niveau d'ASIL serait D. D'une part parce que le conducteur n'est pas tenu de contrôler le véhicule contrairement aux ADAS et d'autre part parce que la sévérité est la plus grande. Une défaillance pourrait entraîner une collision mortelle. Pour définir des exigences de sûreté de fonctionnement relatives aux défaillances du système AD, [26] dénombrent trois méthodes permettant de définir l'objectif d'occurrence des événements entraînant la défaillance du système.

— "Minimum Endogenous Mortality"(MEM)
  Le risque causé par un nouveau système ne doit pas augmenter de manière significative le taux de mortalité endogène des jeunes personnes, *i.e.* le taux de mortalité causé par des maladies ou des malformations congénitales.
— "As Low AS Reasonably Practicable"(ALARP)
  Des mesures pratiques et raisonnables doivent être réalisées pour limiter le risque afin d'avoir un risque négligeable.
— "Globalement Au Moins Aussi Bon"(GAMAB) et "Globalement Au Moins Equivalent"(GAME)
  Ici le système doit être aussi bon que le système qu'il remplace.

Pour la défaillance la plus grave du système, qui amène à un accident mortel, il a été finalement choisi d'exiger au système d'être dix fois plus fiable que le système qu'il remplace, soit le conducteur humain. Les études d'accidentologie fournies par le LAB (Laboratory of Accidentology and Biomechanics GIE PSA-RENAULT) et le CEESAR [65], ont permis de quantifier l'occurence des collisions mortelles et des collisions entraînant des blessés graves en France dans les conditions de conduite autorisées du système autonome. L'objectif trouvé est de 10^{-9} par heure.

Bien entendu, tout accident entraînant des dégâts corporels ou même bénins est à proscrire. De plus faible gravité, les exigences en terme de fiabilité seront moins élevées. Cependant il est difficile de prédire si un accident sera mortel ou non. Notamment il est impossible de prévoir un sur-accident lié à une première collision de faible ampleur dont le véhicule autonome serait responsable. Une première solution est de considérer que, quel que soit l'accident commis par le véhicule autonome, il sera mortel. Une seconde solution est de dissocier la probabilité d'occurrence de l'accident propre au système étudié et la probabilité que l'accident soit mortel. Cette dernière peut être obtenue par des statistiques sur le trafic routier actuel. La norme ISO26262 apporte d'ailleurs ce type d'information.

Pour s'assurer de la bonne acceptation de l'opinion publique sur ce système, ces défaillances ne sont pas les seules à prendre en compte. Des presque-accidents, comme une collision évitée de justesse, ou des comportements dangereux sont également à considérer comme des défaillances du système. Ils n'entraînent aucun dégât mais peuvent inspirer un sentiment d'insécurité auprès des utilisateurs. Nous les avons qualifiés de "Frayeur" dans l'exemple d'APR. Un événement est identifié comme dangereux quand des indicateurs de dangerosité que l'on explicite par la

suite franchissent un seuil fixé. Les indicateurs sont multiples et sont dédiés à plusieurs types d'accidents.

2.2.1.3 Indicateurs de dangerosité

La recherche d'indicateurs permettant de quantifier le caractère conflictuel d'une situation de roulage n'est pas un sujet nouveau. Principalement utilisé pour permettre de mieux concevoir les infrastructures routières et privilégier les architectures sans risque, les travaux ont été initiés dans les années 60 où les interactions dangereuses entre les véhicules sans collision appelées conflits ont été observées [35]. Cependant ces techniques sont issues d'interprétations subjectives sur ces interactions et ne permettent pas de comparer rigoureusement deux interactions [79]. Pour diagnostiquer le caractère sécuritaire des routes, il a été imaginé des indicateurs de sécurité permettant de quantifier l'approche d'une collision. Parmi les plus courants on peut citer le temps avant collision "time to collision" (TTC), le "Post Encroachment Time" (PET), le "Gap Time" (GT) et la proportion de distance d'arrêt (PSD) [28]. Aucun de ces indicateurs n'a été rigoureusement relié à la probabilité de collision mais il est admis qu'une telle relation existe. D'après St-Aubin et al. [79], le TTC semble être une variable suffisante sur autoroute. Ce TTC n'a pas de règle de calcul unique et dépend de la prédiction future des évènements. Longtemps réservé aux collision front arrière entre deux véhicules sur la même file [43], il est dans [79, 80] généralisé à plusieurs types de collisions. Néanmoins il n'est pas suffisant pour caractériser la dangerosité d'une situation. En effet il ne prend pas en compte l'ensemble des trajectoires possibles de chaque couple de véhicules. De plus certains conflits ne peuvent pas être bien réprésentés par le TTC. Les collisions avec des piétons [36] ou les sorties de voie intempestives ne sont pas prises en compte. Ismail et al. [36] mettent en évidence qu'un seul indicateur n'est pas suffisant pour prendre en compte l'ensemble des conflits possibles entre les véhicules et les piétons. Ils suggèrent une prise en compte des 4 indicateurs les plus utilisés,TTC, PET, DST,GT pondérés par la probabilité du type d'évènements. Koita [41] propose d'évaluer la dangerosité d'une trajectoire prise par le véhicule dans un virage. Les systèmes de "line departure warning" utilisent également des indicateurs de trajectoire pour prévenir l'automobiliste d'une sortie de voie. Enfin Mahmud et al. [53] font l'état de l'art de tous les indicateurs utilisés jusqu'à présent.
Actuellement aucun choix n'est fait, il est proposé de trouver de manière numérique l'indicateur ou les indicateurs les plus efficaces pour détecter une défaillance. Les multiples indicateurs, sélectionnés pour qualifier la défaillance, nous laissent supposer que les modes de défaillances sont multiples et répartis dans diverses scénarios de conduite. La difficulté pour trouver et expliquer tous ces cas de défaillances est accrue.

Tout comme les pyramides des risques industriels [7], il est envisageable qu'une relation statistique existe entre défaillances mortelles, défaillances corporelles ou presque accidents. La connaissance d'une telle relation simplifierait grandement les études de fiabilité. Elle permettrait d'une part de détecter plus rapidement une défaillance et d'autre part de valider un objectif de fiabilité moins élevé. Cette relation n'est malheureusement pas connue, et son existence n'est actuellement pas démontrée.

Pour décliner les exigences de SdF du système à ses composants, les AMDEC, analyse des modes de défaillances et leurs effets et leurs criticités, sont fréquemment utilisées.

2.2.2 Analyse des modes de défaillances et leurs effets (AMDE) et leurs criticités (AMDEC) attribués au système de perception et de décision

2.2.2.1 Objectif et description

L'analyse des modes de défaillance et de leurs effets est une méthode inductive qui permet de recenser les modes de défaillance des éléments composant le système et les causes immédiates de ces défaillances. On analyse leurs conséquences sur le système. Cette analyse peut se réaliser tout au long du cycle de développement du système. Une série d'AMDEC est souvent réalisée pour expliquer de plus en plus finement les défaillances du système.

Dans le contexte d'un système très innovant ces exigences sont souvent revues plusieurs fois car elles dépendent du choix technique qui peut évoluer et qui n'est pas connu en début de projet.

Pour appliquer l'AMDEC sur le système AD, nous détaillons le fonctionnement de ce système.

2.2.2.2 Applicabilité et limites

Pour être autonome, le véhicule est doté d'un système de perception qui cartographie son environnement et un système de décision qui interprète et prédit les intentions des automobilistes pour lui indiquer la trajectoire la plus sécuritaire (Figure 2.2). Le système de perception se découpe en deux grandes parties :

— Un ensemble de capteurs issus de technologies variées tels que radars, lidars, caméras, ultrasons, GPS, carte haute définition ou autres technologies de communication entre les véhicules et/ou avec l'infrastructure. Les capteurs sont positionnés tout autour du véhicule pour donner une vue à 360° de l'environnement. Ils sont pour la plupart, par petits groupes ou unitairement, fournis avec un algorithme "d'intelligence artificielle" qui détecte les éléments de l'infrastructure, de la signalisation latérale et horizontale et les objets du trafic routier fixes ou mobiles. Ces capteurs sont redondants : Les informations qu'ils transmettent se complètent et se répètent pour éviter d'éventuelles omissions d'objets ou de fausses détections d'objets. Chaque objet donné est suivi (tracking), il possède un unique identifiant par capteur pendant toute la période durant laquelle il est vu par le capteur. Le capteur attend de l'avoir vu plusieurs fois avant de transmettre l'information. Les capteurs sont très sensibles à de nombreux facteurs environnementaux, en particulier aux conditions climatiques et aux éléments de l'infrastructure. Perturbés, ils peuvent donner une information peu précise ou erronée.

— Un algorithme de fusion permet de réduire ces erreurs. Il synchronise les données transmises par les capteurs, et fusionne les informations redondantes en tenant compte des performances de chaque capteur pour obtenir une cartographie unique et plus précise de l'environnement. Cependant ces performances varient et un capteur jugé peu fiable en général peut s'avérer plus précis que les autres pour des conditions de la route particulières. Tout comme les algorithmes dans les capteurs, l'algorithme de fusion suit chaque objet. Les mesures qu'il réalise sur cet objet mélangent les prédictions issues des mesures précédentes avec les mesures à l'instant présent.

La décision prédit les intentions et trajectoires des autres automobilistes à partir des informations transmises par la perception. Elle s'adapte aux imprécisions éventuelles de la fusion pour

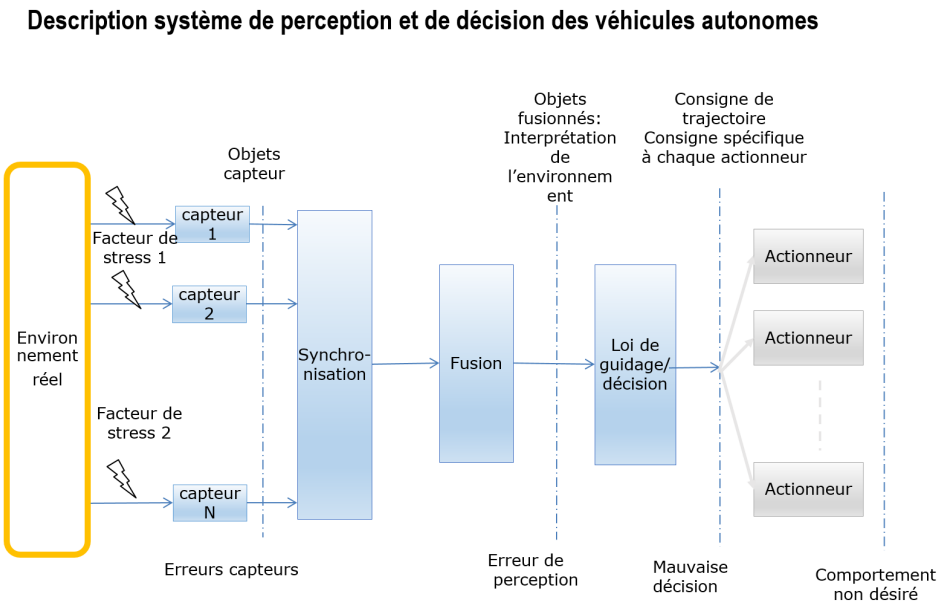


FIGURE 2.2 – Système de perception et de décision

trouver la trajectoire la plus sécuritaire. La trajectoire est transcrite sous forme de consignes au volant et aux pédales du véhicule.
Nous appelons actionneurs la partie mécanique de la voiture qui effectue les manœuvres demandée par le système de perception et de décision.

On répertorie un ensemble d'erreurs de différents types de ce système :

1. **Erreurs de perception**
   Comme énoncé précédemment, la perception est fortement impactée ou perturbée par des facteurs de l'environnement. Cela peut causer de multiples erreurs : de fausses détections, de non détections ou détections tardives, des erreurs de mesures de positionnement ou de trajectoires. Toutes ces erreurs combinées peuvent entraîner des défaillances inattendues. Par exemple lors d'une entrée de parking en forte pente le véhicule a confondu la bouche d'égout métallique avec un véhicule et a freiné brutalement.
2. **Mauvaise interprétation de la décision**
   La décision peut mal interpréter les intentions des acteurs du trafic routier. Cela peut être lié à une perception imprécise mais pas seulement. Les décisions choisies par les autres acteurs du trafic routier sont parfois difficiles à deviner, par exemple lors d'une négociation en voie d'insertion.
3. **Temps de latence des actionneurs**
   La vitesse de réaction des actionneurs fluctue avec son environnement. Le terrain peut par exemple être glissant. La vitesse de freinage est alors impactée et la décision peut mal anticiper le dénouement de la situation présente.
4. **Limites du domaine de fonctionnement**
   Lorsque les conditions d'utilisation des capteurs sont proches des limites de leur fonction-

nement, la perception risque d'être fortement bruitée. La décision en sera par conséquent impactée. Un auto-diagnostic des capteurs est réalisé mais il peut détecter un dysfonctionnement du capteur trop tardivement et entraîner une défaillance.

5. **Condition de reprises en main par le conducteur**
   Comme nous venons de le voir le système peut détecter sa sortie du domaine de fonctionnement. Il doit alors demander la reprise en main du conducteur. Si le conducteur n'est pas apte à récupérer les commandes, le système doit arrêter le véhicule de manière sécuritaire et le stationner dans un endroit sûr. Quand cette sortie est liée à la fin d'une route autorisée pour l'utilisation du mode autonome, la frontière peut parfois être mal choisie. La zone peut être dangereuse, par exemple l'infrastructure comporte, peu de temps après la fin du mode, un fort virage, une absence de voie d'arrêt d'urgence. La localisation du véhicule peut être imprécise et la fin de route peut être vue trop tardivement.
6. **Mauvaises exigences fonctionnelles**
   Au delà des erreurs de développement de l'algorithme de décision, qui peuvent entraîner des bugs ou des consignes de conduite incorrectes, les exigences fonctionnelles peuvent ne pas être appropriées dans certaines situations. Même un conducteur expérimenté dans des situations rares et dangereuses peut ne pas choisir l'action adéquate pour éviter un accident. De nombreux scénarios de conduite ont servi à ajuster les règles de conduite du véhicule autonome mais leur représentativité dans le domaine de fonctionnement est difficilement vérifiable.
7. **Perte d'un capteur entraînant un arrêt dangereux du mode autonome**
   Il faudrait ajouter à cela toutes les erreurs liées à la perte d'un élément. Le mode d'arrêt d'urgence du système doit alors être effectué sans ce capteur.

Enfin les défaillances des actionneurs possibles, mettant en difficulté la conduite autonome, ne sont pas abordées car elles sont maîtrisables par des méthodes plus classiques de sûreté de fonctionnement par ajout de redondance.

Les erreurs mentionnées peuvent survenir à tout moment de la conduite sans répercution sur la sécurité des passagers ou des acteurs du trafic routier. On appelle défaillance du système de perception et de décision du véhicule, une erreur de celui-ci amenant à un événement indésirable pour le client. Il est difficile de construire une AMDEC qui répartit les exigences aux différents composants. En effet un mode de défaillance est un mélange encore flou d'erreurs relatives aux algorithmes capteurs, à leur fusion et à la décision (Figure 2.3). Ils sont alors difficilement imputables à certains composants.
Pour les systèmes complexes, dont les comportements sont élaborés et les interactions avec l'environnement sont difficiles à prévoir, les méthodes par arbre de défaillances sont utilisées. Cependant cette modélisation n'est pas adaptée pour expliquer les interactions présentes dans l'algorithme de fusion.

Le domaine de fonctionnement reste encore mal caractérisé. De nombreux paramètres de l'environnement ou d'objets non identifiés peuvent perturber le bon fonctionnement du système de perception et entraîner une défaillance du système. De plus le comportement des automobilistes autour est parfois très étonnant. Les fonctions du système que nous avons présentées plus haut sont très générales. Les règles de conduite que doit adopter le véhicule autonome sont élaborées

à partir d'exemples de situations de conduite que rencontre le véhicule autonome. Comme nous l'avons vu, les règles de conduite peuvent être adaptées dans certaines circonstances mais peuvent entraîner un danger dans d'autres cas. En particulier les règles pour gérer des situations conflictuelles, qui requièrent de la négociation entre les participants, comme une voie d'insertion sur autoroute, sont très difficiles à instaurer. Des outils dédiés aux ADAS sont utilisés pour décliner ces exigences, mieux définir les règles de conduite et valider le système à chaque stade du cycle en V. La section suivante présente ces outils.

2.3 Stratégies d'analyse et outils de validation dans le panorama de la voiture autonome

Avec l'apparition rapide des nouveaux ADAS, l'industrie automobile s'est dotée d'outils et de techniques spécifiques pour mener à bien leur conception et validation : de nouveaux outils de réalité virtuelle à la pointe de la technologie, des pistes d'essais et des équipements dédiés, des moyens de collectes et de stockages de données pour les essais sur "route ouverte", des nouveaux protocoles à suivre... La première partie énumère les différents outils disponibles pour la validation à différent stade du cycle en V.
Bien que suffisant pour les ADAS actuellement présents, ils sont encore limités pour les futurs ADAS et le véhicule autonome. En particulier la validation finale de ces systèmes, garantissant un niveau de fiabilité élevé quelles que soient les conditions d'utilisation reste un sujet de recherche. Dans le contexte de grande concurrence entre les entreprises automobiles, les informations accessibles dans le domaine public sont minces. Les articles sur ce sujet mentionnent brièvement les méthodes mises en places que nous tâcherons d'exposer en seconde partie.

2.3.1 Déclinaison des exigences au travers du cycle en V et stratégie de validation associée

Le schéma 2.4 présente les méthodes et outils dédiés à la validation des ADAS et leur rôle dans le cycle en V. Cette partie développe les principales étapes.

2.3.1.1 Construction et verification des exigences SdF de conduite dans le système de décision

Description et objectif

Les règles de conduite, que doit respecter le véhicule autonome, sont élaborées pour satisfaire les exigences de sûreté haut niveau. Des logiciels comme les MIL "model in the loop" modélisent le comportement du véhicule autonome dans un scénario de trafic routier donné, par exemple une insertion d'un véhicule. Ces simulations permettent de vérifier que les actions choisies par le véhicule, suivant les règles de conduite implémentées, sont bien sécuritaires pour l'ensemble des acteurs du trafic. Cela permet de concevoir et de partiellement valider l'algorithme de décision. Seules les règles et les actions de conduite sont modélisées. Les informations transmises à l'algorithme sont parfaites et ne proviennent d'aucune information issue de modèles capteurs. Elles donnent à tout instant une image exacte de l'environnement du véhicule. Les champs de vue des

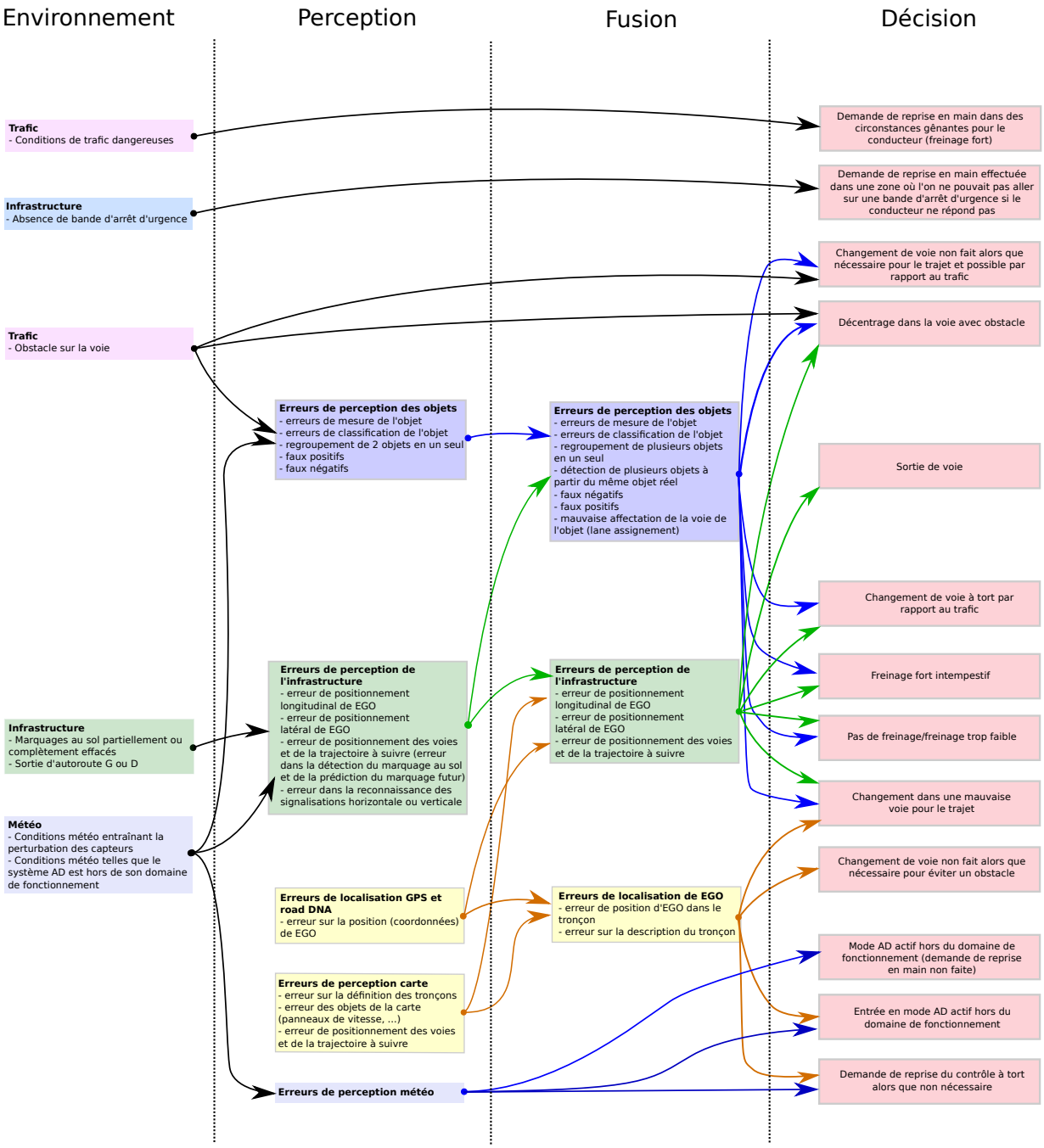


FIGURE 2.3 – Liste non exhaustive des erreurs qui peuvent entrainer des défaillances du véhicule autonome

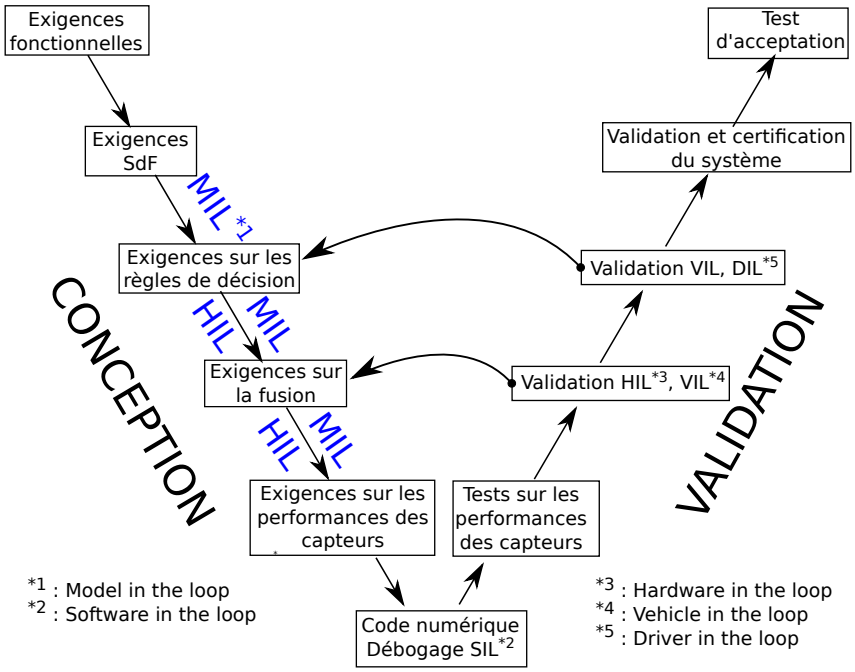


FIGURE 2.4 – Cycle en V du système de perception et de décision des ADAS et AD

capteurs parfaits peuvent néanmoins être ajoutés. Cela permet de valider le choix des capteurs et de leurs positions dans le véhicule. Cette sélection couvre complètement l'espace autour du véhicule autonome.

Applicabilité et limites

Ces outils sont encore très manuels et aident à la conception localement. Les scénarios sont réalisés un à un. Dans le contexte du véhicule autonome des milliers de scénarios différents sont possibles. Des outils permettant de concevoir ces scénarios de manière automatique sont en cours de développement. Nous présenterons plus tard les améliorations réalisées pour s'adapter au contexte du véhicule autonome.
Les exigences et les règles de conduite dépendent des scénarios choisis pour les définir. Si un scénario n'a pas été imaginé par les experts, les règles de conduite peuvent être inadaptées à la situation rencontrée.
Ces remarques sont valables pour les autres outils de simulation présentés dans cette section.
Parce que le niveau de détail est bas le temps de calcul des MIL est très petit, ce qui peut être un avantage pour réaliser un très grand nombre de simulations. Cependant les résultats obtenus peuvent manquer de réalisme.

2.3.1.2 Exigences sur le système de perception en sortie de fusion

Une modélisation plus fine des informations issues de la fusion peut être ajoutée dans le MIL. Dans le cas nominal, les objets sont détectés avec plus de réalisme. Le délai de détection est respecté et les obstructions par les différents objets qui gênent les capteurs sont prises en

compte. Elle peut intégrer des erreurs de perception après fusion. Par exemple les mesures des objets peuvent être bruitées et des fautes injectées telles des détections d'objets inexistants ou des non détections. Des critères de défaillance sur les erreurs en sortie de fusion pourraient être ainsi déduits :

— Une erreur de mesure maximale à ne pas dépasser,
— Un délai de détection au-dessus duquel la fusion est considérée comme défaillante,
— etc.

Pour inclure des temps de latence ou d'autres types d'erreurs dues à la partie électronique, les vrais composants électroniques sont intégrés. On parle alors de simulations HIL ("Hardware in the loop").

2.3.1.3 Exigences sur les informations transmises par les capteurs

Objectif et description

Les MIL et HIL sont ensuite complétés par des informations de modèles capteurs. On se place alors en sortie de capteurs. Les étapes de synchronisation et de fusion sont ainsi évaluées. Les vrais algorithmes capteurs avec ou non de vraies données collectées sont inclus dans le HIL.

Proposition d'application pour le véhicule autonome

Pour vérifier la robustesse du véhicule, les erreurs capteurs sont modélisées de la même manière qu'en sortie de fusion. On peut faire une première validation de la fusion et construire des exigences sur les performances des capteurs. Une fiabilité de perception capteur serait ainsi définie.

2.3.1.4 Validation des codes implémentés et débogages

Les simulations "software in the loop" (SIL) permettent de qualifier la fiabilité du logiciel implémenté dans le système embarqué. On vérifie qu'il n'existe pas de bugs ou on les corrige dans le cas contraire.

2.3.1.5 Validation des capteurs

Objectif et description

Nous pouvons décomposer la validation des exigences sur les capteurs en trois parties :

— La validation de la partie hardware :
C'est la fiabilité de la partie électronique du capteur. Les dysfonctionnements étudiés ici sont soit un arrêt intempestif soit une non transmission d'information. Les fournisseurs de capteurs réalisent ces tests.
— La validation de la fonction d'auto-diagnostic du capteur :
C'est à dire sa capacité à détecter une information erronée ou partielle quand il sort de son domaine de fonctionnement. Des bancs de tests sont proposés pour aider à cette validation.

— Enfin les erreurs de la perception capteur :
Ces erreurs sont des causes possibles de la défaillance du système de perception et de décision.

Les deux premières vérifications peuvent se faire de manière unitaire, capteur par capteur. La dernière validation peut commencer par des tests unitaires à partir des connaissances des caractéristiques physiques des capteurs (comme évaluer les capacités d'émissions et de réceptions des lidar ou des radars dans différents environnements ou vérifier la qualité d'image des caméras). Ce sont les fournisseurs qui sont en charge de cette prestation. Ils procurent ainsi une liste des caractéristiques au nominal de leurs produits. Cependant les performances des algorithmes des capteurs (comme la détection et la classification des objets) dépendent fortement de leur intégration dans le véhicule (position et fonctions choisies) et des conditions d'usage en particulier les conditions météorologiques ou les routes habilitées (type d'infrastructure). Des essais sur les capteurs intégrés dans le véhicule sont nécessaires pour estimer leurs erreurs et surtout leurs impacts sur le bon fonctionnement du système.

Limites actuelles

Il est très difficile de définir une exigence sur les résultats de mesure et de détection de l'algorithme de chaque capteur. Toutes les informations de tous les capteurs se retrouvent mélangées dans la partie fusion. Une erreur de la fusion est donc due à une combinaison d'erreurs des capteurs. Néanmoins une connaissance sur les performances des capteurs reste nécessaire. Les algorithmes de la fusion sont conçus à partir de ces informations. Ils donnent plus d'importance aux capteurs plus précis, par exemple les mesures des radars sont plus précises que celles de la caméra.
Ces capteurs sont fortement perturbés par des paramètres de l'environnement, nommés des facteurs de "stress", qui amplifient les erreurs des capteurs. La table 2.2 donne un exemple de facteurs de stress et de leurs effets.

Les simulations MIL et HIL actuelles modélisent très peu ces phénomènes de perturbation. Pourtant pour obtenir des résultats de simulations exploitables, il est nécessaire de les introduire. La contribution de chaque capteur et de la fusion sur les défaillances du système sera ainsi évaluée.

Proposition d'application

Cela peut se faire en injectant des erreurs corrélées aux conditions de route mais également à partir d'une estimation de la fiabilité de la perception de chaque capteur, comme proposé dans le paragraphe précédent.

Etats de l'art des stratégies de validation des capteurs

La construction des modèles d'erreurs ou l'évaluation de la fiabilité de perception capteur est réalisée à partir d'essais sur banc ou sur piste.
Ainsi, Rivero et al. [69] regardent l'effet sur le champ de vision (longueur et largeur) et la précision du lidar de la saleté présente sur la protection plastique du capteur. Ils donnent un modèle d'erreur qui sera intégré aux simulations. Pour cela ils positionnent plusieurs éléments plastiques

	Caméra	Radar	Lidar	Ultrason	GPS
Pluie Brouillard	- Diminue le champ de vision et la portée - Entraîne de faux négatifs	- Diminue le champ de vision et la portée - Entraîne de faux négatifs	- Entraîne des faux positifs, - Entraîne des faux négatifs, - Induit une erreur de position des objets	Entraîne des faux positifs	
Salissures sur la route	Mauvaise ou non détection des lignes		Diminue le champ de vision		
Inclinaison du soleil	- Diminue le champ de vision et la portée - Entraîne de faux négatifs, - Mauvaise détection des lignes				
Tunnel ou pont		Augmente le nombre de faux positifs		Augmente le nombre de faux positifs	Perte du signal
Glissière de sécurité métallique, objets métalliques		Augmente le nombre de faux positifs	Mauvaise position des objets		
Bâtiment, arbre	Entraîne des faux positifs et faux négatifs				Entraîne des erreurs de mesure

TABLE 2.2 – Exemple de facteurs de stress et leurs effets

à différents emplacements du véhicule pour récolter les salissures possibles sur la route. Ils étudient ensuite la capacité de réception et d'émission du capteur avec ces niveaux de salissures pour caractériser les perturbations résultantes. Duthon et al. [19] présentent un banc de test pour évaluer les performances de la caméra par temps de pluie ou de brouillard. Berk et al. [4] modélisent sur banc la probabilité de non détection et de fausse détection de chaque capteur. Gietelink et al. [29] proposent un banc dédié aux caractérisations capteur. Cependant ce banc reste quasi statique et ne prend pas en compte les différents facteurs de l'environnement.

Les tests cités sont statiques et ne tiennent compte que de certains paramètres. Pourtant la détection d'objet et les mesures sont dynamiques. La vitesse de chaque automobile environnante et du véhicule autonome jouent sur les performances des capteurs. Les essais dynamiques ne sont pas faciles à concevoir.
Sur route ouverte, il n'existe pas de "vérité terrain" : un système de mesure différent des capteurs du système AD donnant des mesures et permettant la détection de chaque objet. Seul un GPS différentiel est disponible mais sa portée est réduite à 200m ; bien trop court pour réaliser des scénarios à grande vitesse. Pour évaluer la détection des objets, les opérateurs peuvent annoter tous les objets de l'environnement pendant les roulages. Le nombre d'objets est trop grand pour que l'annotation humaine soit fiable. Les essais sur piste ne peuvent pas reproduire l'ensemble des situations. En particulier le nombre d'automobilistes, la taille de la piste et surtout les objets de l'infrastructure sont limités. Cependant on voit apparaître des pistes dédiées aux ADAS et aux AD, reproduisant finement les infrastructures. Par exemple, l'université du Michigan a reproduit une fausse ville pour tester des véhicules autonomes. De même pour l'entreprise TASS, ses pistes ont été cartographiées pour mesurer avec précision à chaque instant la position du véhicule.
Enfin des scénarios critiques incluant des piétons ou des scénarios risquant très probablement d'entraîner une collision peuvent être simulés à partir de pantins, de faux vélos, ou de voitures en toiles.

2.3.1.6 Validation des règles de décision

La validation des règles de décision ne se limite pas à des erreurs de robustesse liées à une perception imprécise, mais doit intégrer les réelles actions du véhicule et vérifier une demande de reprise en main sûre, pour laquelle le conducteur a le temps de comprendre la scène et de garder le contrôle pendant cette phase intermédiaire.
Les simulations "vehicle in the loop"(VIL) tiennent compte également des véritables réactions des actionneurs du véhicule. Le véhicule est testé sur piste mais le scénario reste numérique. Le véhicule testé sur piste répond à un scénario numérique. Sa réelle distance de freinage ou ses réelles trajectoires sont prises en compte. Enfin les simulations "driver in the loop" testent les interactions entre l'utilisateur et le véhicule autonome. Le conducteur est dans un simulateur de conduite très réaliste et pour chaque scénario ses réactions sont analysées. On peut ainsi valider l'ergonomie de l'interface homme machine, vérifier la sécurité des demandes de reprise en main du véhicule ou enfin s'assurer du confort du passager pendant la conduite en mode autonome. En effet, le sentiment de sécurité du passager est analysé dans ce dernier test.

2.3.1.7 Conclusion

Pour conclure, la déclinaison des exigences au niveau des composants lors du cycle de développement en V est difficilement applicable au système de perception et de décision du véhicule autonome. En effet, les algorithmes des capteurs et de la fusion qui composent le système ne sont pas à proprement parler défaillants. Ils peuvent réaliser des erreurs plus ou moins importantes qui une fois combinées avec celles de la décision peuvent mener à la défaillance du système ce qui entraîne un événement dangereux pour l'utilisateur. Ces erreurs sont multiples et sans conséquences prises indépendamment. Il n'est pas aisé de relier les erreurs des capteurs à des défaillances du système. Mais cela peut s'observer à l'aide de la simulation. Les outils de simulation permettent de définir et de vérifier les exigences à différents niveaux de conception. Ils sont utilisés pour des applications locales lors de la mise au point. Ils simulent le véhicule dans des conditions nominales et ne tiennent pas compte de la variabilité de l'environnement.
Tous ces outils et tests peuvent servir dans l'évaluation de la fiabilité. Pour certains, leurs niveaux de détails et de réalisme requièrent un temps de calcul énorme et une utilisation encore très manuelle difficilement automatisable. Inversement d'autres ne représentent pas fidèlement les conditions de roulage réelles.

Le système est très innovant. Les scénarios élaborés lors de la conception ne sont pas représentatifs de l'ensemble des conditions de route rencontrée par le véhicule autonome. Ils servent de base. Les algorithmes du système seront mis au point pendant les essais de roulage sur route ouverte.
Ces scénarios sont soit fabriqués à partir d'enregistrements lors de tests sur route ouverte que l'on détaillera par la suite, soit déduits à partir d'autres sources d'information :

- l'expérience de conduite de chaque acteur du projet,
- d'analyse préliminaire de risque,
- des données d'accidentologie collectées par des organismes publics, tels que la base de données GIDAS en Allemagne [60] ou des données du LAB.
- de conduite naturalistique [21, 14], analysant le comportement des automobilistes.
- ou enfin de vidéos issues de caméras de surveillances sur autoroute par exemple
- etc.

Cette base de connaissance n'est pas exhaustive et se construit avec la maturité du système.
Ces informations bien que partielles peuvent néanmoins être utiles dans l'élaboration d'un plan de validation de la fiabilité du véhicule autonome.

A ce stade le système est partiellement vérifié. La validation finale du système de perception et de décision a pour objectif de vérifier le bon comportement du système dans son environnement. La seconde partie présente les difficultés à organiser un plan de validation final. Il doit être réalisable, représentatif de l'usage du véhicule autonome et doit respecter le temps de mise sur le marché.

2.3.2 Stratégie de validation du système complet dans son environnement

Le dernier plan de validation doit permettre de certifier que le système complet est adapté à toutes les conditions de route. Les exigences bas niveaux sont alors toutes validées. Il se place en amont des essais d'acceptation avec des clients. Les règles de conduite implémentées dans

le véhicule autonome sont contrôlées, elles doivent être suffisantes et respectées à tout moment dans un environnement fortement variable et partiellement connu.
Nous présentons dans ce paragraphe les stratégies disponibles. Nous préférons mettre en garde le lecteur ; les stratégies des concepteurs automobiles ne sont pas rendues publiques. Ici, elles sont supposées à partir de communications disponibles et en les reliant aux dimensionnements choisis.

2.3.2.1 Test de validation réalisé par roulage aléatoire

La première méthode étudiée par les concepteurs automobiles pour dimensionner le plan de validation final est partie de l'hypothèse la plus pénalisante : le comportement du système est inconnu. Nous cherchons uniquement à vérifier, par des roulages aléatoires conformes à l'usage qui sera fait du véhicule, que la fiabilité du système respecte bien l'objectif souhaité. Kalra et Paddock [40] précise alors qu'il faudrait faire rouler le système sur plusieurs millions voire milliards de kilomètres dans les vraies conditions. Il serait aussi préférable que ces véhicules soient conduits par des clients lambda. Vraisemblablement, c'est la stratégie adoptée par Tesla. Les véhicules Tesla d'autonomie 2 (classification de la SAE) actuellement sur le marché sont pourvus de capteurs proches ou identiques à ceux qui serviront à l'autonomie 4. En roulant les clients testent leur système. Si un comportement inopportun du véhicule est observé, il est immédiatement enregistré et envoyé à Tesla pendant la nuit. Tesla a même précisé que le véhicule sera habilité à être utilisé en niveau 4 lorsque celui-ci aura été jugé fiable grâce aux roulages réalisés par les utilisateurs [82].
Cependant cette hypothèse part du principe que le système ne sera pas modifié pendant toute la période de validation. Sinon il n'est plus le même et l'hypothèse ne tient plus. Ce qui n'est pas le cas des algorithmes Tesla. Pendant que le client roule, deux algorithmes tournent en parallèle l'un est la version courante, l'autre la version en cours de développement. La non régression du nouvel algorithme est ainsi vérifiée. A défaut d'être meilleur, le nouvel algorithme doit être aussi fiable que le précédent. Dès qu'il est validé le nouvel algorithme remplace le précédent et ainsi de suite. Les roulages de validation sont ainsi conservés. Cette stratégie est dangereuse. Un changement de l'algorithme ou de la définition technique du véhicule sans garantie de non régression requiert une ré-interprétation des heures de conduite déjà effectuées. Le nouveau système pourrait être défaillant dans une situation ne posant aucun problème au système précédent.

2.3.2.2 Test de validation réalisé par mélange de roulage aléatoire, simulation ou re-simulation

Google et Toyota semblent adopter une stratégie proche de celle évoquée. La "Google car" roule depuis de nombreuses années aux Etats-Unis. Ces roulages sont de plus complétés par des roulages numériques qu'ils annoncent très réalistes [9]. Cependant les tests ne semblent pas complètement aléatoires. Il faudra vérifier que le roulage réalisé permet de bien évaluer la fiabilité du système, dans les mêmes conditions que l'usage client et s'assurer de la représentativité et du réalisme des simulations numériques. Toyota a annoncé que ses véhicules rouleront 8,8 milliards de kilomètres en alternant roulage numérique et roulage en conditions réelles. [62]

Contrairement à des systèmes classiques en phase de validation, la définition technique de l'AD

n'est pas figée. Les algorithmes peuvent être mis à jour pour s'adapter aux nouveaux scénarios de conduite rencontrés. En effet Tesla et Google semblent utiliser des technologies dites de "machine learning". Elles continuent d'apprendre avec les données collectées. Ils ont vraisemblablement une méthode de sélection et de classification des scénarios pour ne récupérer que les séquences de roulage qui semblent intéressantes pour l'apprentissage de l'algorithme.

L'utilisation d'autres types d'algorithme n'évitera pas d'éventuelles modifications au passage de scénarios nouveaux. Une méthode de validation classique, consistant à évaluer les performances d'un véhicule à définition technique figée pendant de nombreux kilomètres, n'est donc pas appropriée pour ce type de système. Il faudrait bien plus que des milliards de kilomètres.

Pour pallier à ce problème, pour la validation du système de perception de l'ADAS de freinage d'urgence, "Automotive Emergency Breaking" (AEB), l'entreprise Renault a choisi de procéder à de la re-simulation. Contrairement à la simulation qui teste numériquement le véhicule dans des scénarios imaginés et non rencontrés, la re-simulation consiste à tester le nouveau système avec les nouvelles mises à jour dans les conditions de conduite enregistrées pendant les roulages. Ce système permet de freiner fortement lorsqu'une collision lui semble inévitable et que le conducteur n'a pas réagi. La défaillance étudiée du système AEB est un freinage intempestif. Les enregistrements de roulage sont déroulés numériquement et appliqués à la nouvelle version du système. Si pendant ces tests, le système demande de freiner dans une situation qui ne demandait pas une action de ce système alors il est considéré comme défaillant. La re-simulation choisie est dite non bouclée. Les agissements du système ne remettent pas en cause les enregistrements futurs. Le dénouement est toujours le même. Ce n'est pas le cas pour les re-simulations nécessaires pour le véhicule autonome. En effet toute action du véhicule même non dangereuse va modifier le déroulement des scénarios futurs. Les acteurs de la route vont s'adapter aux actions du véhicule autonome. Prenons l'exemple d'un enregistrement, dans lequel un véhicule s'insère devant le véhicule autonome roulant à vitesse constante. Si la nouvelle version du système AD décide d'accélérer dans cette même séquence, le véhicule voulant s'insérer risque d'arrêter son action et rester sur sa voie. Les re-simulations doivent donc modifier les enregistrements pour reconstruire des scénarios de roulages réalistes. Le nouveau déroulement est prédit, mais cette prédiction est une interprétation possible du nouveau scénario. En réalité le scénario aurait pu être différent. Nous parlons alors de re-simulation bouclée qui est encore un sujet de recherche et de développement.

2.3.2.3 Stratégie d'une conception sûre pour aider à la validation : redondance ou système de surveillance pour éviter un danger

En mécanique ou en électronique, s'il est impossible d'évaluer la fiabilité d'une pièce hautement sécuritaire avec des objectifs de taux de défaillances de l'ordre de 10^{-8} ou 10^{-9} par heure, les ingénieurs redéfinissent la conception. Ils mettent en place des redondances, c'est à dire qu'ils conçoivent un fonctionnement parallèle de deux pièces moins fiables et indépendantes. Si une des pièces défaillit, la seconde est toujours présente et peut la remplacer.
S'il est impossible de mettre en place un tel parallélisme, un système de surveillance est souvent utilisé. Si une pièce ne fonctionne plus, un système annexe permet de détecter le dysfonctionnement et d'arrêter le fonctionnement ou de dégrader les fonctions du produit. C'est le cas par exemple des fusibles qui préviennent d'une électrocution après un court circuit.

On parle alors d'allocation de fiabilité. [51]
Cette stratégie fut adoptée pour l'AEB. Il est une aide : le conducteur reste toujours responsable s'il n'a pas freiné à temps et si le système n'a rien fait. Mais l'AEB ne doit pas augmenter le nombre d'accidents. S'il décide de freiner à tort et que cela entraîne une collision avec le véhicule de derrière, c'est le système qui est responsable. L'objectif du taux de la défaillance, intitulée "faux positifs"(le système a cru bon de freiner à tort), est par conséquent très faible. Pour éviter une phase de validation trop coûteuse, deux sous-systèmes de perception indépendants fonctionnent en parallèle. L'un est constitué de caméras et l'autre de caméras et de radars. Un ordre de freinage n'est réalisé que si les deux sous-systèmes ont prévenus du danger.
Cette stratégie ne peut pas être choisie pour le véhicule autonome. En effet le système AD est également responsable des "faux négatifs"(il n'a pas freiné alors qu'il aurait dû). Cette fonctionnalité est l'opposée de l'autre.
Ainsi dans le contexte du véhicule autonome, cette méthode risque de ne pas être aussi efficace car un compromis doit être fait entre les deux erreurs en fonction des performances des capteurs.

2.3.2.4 Validation par observations de toutes les conditions de conduite : Ontologie et plan d'expériences

Les dimensionnements du plan de validation proposés dans la section 2.3.2.1 ne prennent pas en compte la forte variabilité de l'environnement. Ils partent du principe que les milliards de kilomètres réalisés sont représentatifs de l'environnement. Les distances ou heures effectuées (selon le découpage choisi du parcours) sont supposées indépendantes, tirées aléatoirement dans tout l'espace des possibles. En effet le roulage de validation est découpé en heure ou en kilomètre. A chaque heure l'état défaillant ou non défaillant est supposé suivre une loi de Bernoulli. La non défaillance du système constatée au bout de n heures ou kilomètres, est donc une réalisation d'une loi binomiale de paramètres n et λ le taux de défaillances souhaité du véhicule.
Ce tirage aléatoire n'est en pratique pas facile à vérifier : dans le cas où les tests sont réalisés par des clients, les kilomètres parcourus risquent d'être assez répétitifs et de ne représenter qu'une partie des usages. Nous faisons souvent les mêmes trajets aux mêmes heures. Il faudrait distribuer le système à un très grand nombre d'usagers.
De plus, les tests seront en grande partie réalisés par des professionnels. Le choix et la fréquence des parcours aura sans doute un biais par rapport à l'usage. Il est donc judicieux de tenir compte de la variabilité des kilomètres possibles roulés avec le véhicule autonome. Micskei et al., Ulbrich et al. [56, 85] proposent d'utiliser des langages et des ontologies pour décrire les contextes d'utilisation des systèmes autonomes. La description des conditions de roulage, comprenant les objets de l'environnement et les règles de circulation, doit être la plus détaillée possible. Une base de cas tests pourra être extraite de cette représentation sémantique.
Ulbrich et al. [84] construisent une nomenclature pour décrire les scénarios rencontrés par le véhicule autonome. Les simulations numériques dites massives sont construites à partir de cette description en scénarios. Ce sont des simulations permettant de générer un très grand nombre de scénarios de la route. Elles proviennent d'une liste de configurations génériques appelées cas d'usage. Ceux-ci sont décrits par une scène initiale, un ensemble d'actions des automobilistes et une scène finale. Le chapitre 6 définit plus finement ces termes. Un scénario est une instanciation de ce cas d'usage, c'est-à-dire des valeurs initiales sont données aux paramètres décrivant le cas d'usage. Pour un même cas d'usage des milliers, voire des millions de scénarios peuvent être générés. Des méthodes de plan d'expériences sont alors proposées pour tester l'ensemble des

combinaisons possibles dans un cas d'usage.
Il existe des centaines de cas d'usage pour des systèmes AD avec un domaine de fonctionnement pourtant restreint. Ils peuvent être caractérisés par des centaines de paramètres. Un plan d'expériences complet ne peut pas être entièrement simulé, ce serait beaucoup trop coûteux. En effet, les scénarios durent entre 2min et 7min.
En roulage réel, la plupart des paramètres qui décrivent le cas d'usage ne sont pas maîtrisables. La météo, les comportements des automobilistes autour sont subis pendant les tests. De plus le niveau de granularité (la plus grande finesse) pour décrire un scénario n'est pas suffisant pour expliquer une défaillance du système. Deux scénarios décrits de manières identiques peuvent entraîner ou non une défaillance. Cela peut être lié aux décisions aléatoires des algorithmes des capteurs mais cela est surtout dû à la forte variabilité de l'environnement. Par exemple le faible changement d'orientation du soleil peut modifier toute la compréhension de la scène par la caméra.
Par conséquent, l'ensemble des combinaisons possibles ne peut pas être observé et même ne sera pas suffisant pour la validation.
Plusieurs scénarios peuvent avoir le même effet sur le comportement du système s'ils sont proches. D'autres encore n'ont pas besoin d'être observés car ils peuvent être peu ou pas critiques pour le véhicule. L'observation de cas extrêmes peut-elle suffire à valider le véhicule autonome ? Cette stratégie est présentée dans la suite.

2.3.2.5 Validation à partir d'un type parcours ou d'une base de cas tests

Supposons qu'il existe un parcours type, un parcours dit "enveloppe" moins long qu'un roulage aléatoire qui prendrait en compte toutes les variations extrêmes du domaine de fonctionnement. Une fois ce parcours traversé sans défaillance, le véhicule sera certifié fiable pour toute autre condition de conduite moins extrême. C'est la méthode adoptée pour la validation des automobiles depuis de nombreuses années. Après la validation des exigences bas niveaux du cycle en V, la voiture est testée sur piste. Elle est contrôlée dans toutes les conditions qui peuvent accélérer ou entraîner une défaillance d'un sous-système du véhicule : à toutes les vitesses, sur une route stressante (ex pavée, avec des dos d'âne, des nids de poule, des flaques d'eau salée, de jets d'eau puissants, etc.). Le test est dit accéléré. La fréquence des conditions stressantes pour le véhicule, ses composants mécaniques et électroniques, est plus grande que leur fréquence d'apparition dans le pays de vente souhaité. Il est de plus aggravant. Les conditions sont plus contraignantes que dans la vie réelle. Ainsi la fiabilité du véhicule dans ces conditions est plus basse. Il est nécessaire de rouler moins longtemps pour atteindre des exigences de fiabilité moins grandes. Parce que les modes de défaillance sont connus, il existe une relation entre la fiabilité dans cet univers stressant et la fiabilité dans des conditions d'usage. De plus pour certains composants, il n'est pas nécessaire d'attendre leur rupture. Des analyses sur le niveau d'endommagement ou la vétusté des pièces induisent directement leur fiabilité.
Pour la vérification des ADAS les tests ne sont pas aggravants. L'amplitude des phénomènes stressants ne peut pas être augmentée et leurs fréquences sont difficilement maîtrisables surtout pour les facteurs climatiques et les configurations de conduite. Cependant une liste de cas à examiner pendant des roulages sur route ouverte est élaborée pour attester du bon fonctionnement de ces systèmes. On appelle ces cas tests des "field operational tests" (FOT) [23, 46, 66]. Ils sont un panel de scénarios de conduite pouvant être rencontrés par le véhicule. Pour certifier la performance des ADAS, des tests EURONCAP sont proposés [22]. Ce sont des tests sur piste

ou sur route ouverte bien quadrillés et bien définis. Si le véhicule réussit l'ensemble des tests alors il obtient les cinq étoiles. Dans le cadre de l'AEB, ces tests sont réalisés sur piste avec l'utilisation de pantins, pantins sur vélos et de faux véhicules pour reproduire des évènements de collision sans perte humaine ni matérielle. Le niveau de réalisme n'est cependant pas suffisant pour garantir un bon fonctionnement du système dans toutes les situations réelles.
Pour réduire le nombre de tests Zhao et al. [90] choisissent de réaliser une méthode de Monte Carlo accélérée par tirage d'importance sur les paramètres d'un cas d'usage. Ils prennent pour exemple le cas d'une insertion d'un véhicule. Ils estiment que seuls trois paramètres suffisent à expliquer la défaillance du véhicule dans ce cas d'usage. Ils déterminent leur distribution par des roulages naturalistiques [14] ayant pour but d'observer le comportement des usagers. Puis ils modifient ces distributions pour sélectionner en priorité des tests critiques. Ils estiment ainsi la fiabilité du véhicule plus rapidement dans ce cas d'usage.
Suivant la même idée pour ne pas tester toutes les configurations, Rocklage [70] décompose un parcours type de conduite en succession de scènes de conduite (configuration statique). Il propose une méthode alternant tests numériques et tests réels. Les tests numériques servent à valider le véhicule tandis que les tests réels permettent de collecter de nouvelles scènes à implémenter dans les tests numériques. La sélection des scènes réelles se fait à partir d'une mesure de distance entre les scènes. Si une scène est très éloignée de la base de connaissance, alors elle est enregistrée et implémentée.

2.3.2.6 Modèles et preuves formels

Mobileye, fournisseur de caméra embarquée, a récemment publié un article [78] présentant une preuve formelle de la sécurité des systèmes autonomes. Selon lui, si le système respecte bien l'ensemble des règles de sécurité établies sous forme de formules mathématiques, alors il n'est pas nécessaire de procéder à des essais de validation sur route ouverte ou numérique. Toujours selon lui, cette course à la donnée n'est pas atteignable et ne démontre rien. Seules des règles bien définies et bien implémentées suffisent. Ce type de validation est utilisé en informatique pour construire et valider des exigences sur les codes implémentés à chaque niveau de raffinement dans le cycle en V. Qu'en est-il des erreurs de perception ? Un véhicule autonome bien discipliné inconscient de son aveuglement peut-il respecter les règles qui lui sont imposées. Les règles mathématiques supposent une connaissance exhaustive de toutes les conditions de conduite. L'environnement peut-il être entièrement décrit par un modèle mathématique ?

2.3.2.7 Conclusion

Après avoir passé en revue les différentes stratégies adoptées pour les ADAS et pour les systèmes AD de la concurrence, cinq grandes stratégies se dégagent :

— La validation par roulage aléatoire sur route ouverte, qui demande un temps de validation beaucoup trop long par rapport à la date de mise sur le marché.
— Des roulages sur route ouverte guidés suivant un protocole qui sélectionne les scénarios à observer. Néanmoins la connaissance sur les événements amenant à une défaillance n'est pas exhaustive. Il est difficile de définir à l'avance un plan de validation, de durée raisonnable, qui comprend tous les usages possibles avec le véhicule autonome.

— Les essais sur piste qui sont complétés par des équipements spécifiques allant du simple pantin à la ville reconstituée. Les usages simulés du véhicule autonome restent limités par les équipements disponibles, la taille des pistes.
— Les simulations numériques avec des niveaux de réalisme plus ou moins élaborés. Ces simulations ne représentent pas des parcours types avec le véhicule autonome, mais testent le véhicule dans des scénarios de conduite bien définis.
— Les informations extérieures qui peuvent compléter la connaissance du fonctionnement du système AD. Ces informations aident dans l'identification de nouveaux scénarios mais le comportement du système dans ces scénarios n'est pas vérifié.

Ces outils et stratégies ont toutes des avantages et des inconvénients. Cependant aucune méthode complète donnant un fil conducteur des essais à réaliser pour certifier la sécurité du véhicule autonome n'est publiée.

2.4 Conclusion

2.4.1 Bilan des difficultés pour valider le véhicule autonome

Les méthodes de développement des systèmes mécatroniques à l'aide d'un cycle en V permettent de vérifier à chaque niveau d'intégration le bon comportement du système étudié. Pendant la phase de conception, l'ensemble des modes de fonctionnement et de défaillance est identifiés. En phase de validation, tous les événements amenant à des défaillances sont connus. L'unique incertitude étudiée, pour l'évaluation de la fiabilité, est liée au caractère aléatoire intrinsèque de l'environnement du système. Ce type d'incertitude, appelée incertitude aléatoire est propagée pour étudier son impact sur le comportement du système. Bien que l'environnement soit aléatoire il est bien caractérisé. De plus la connaissance de cet environnement permet de réduire les plans de validation à réaliser. Les essais ne comportent que des événements critiques, ceux qui ont le plus d'influence sur la fiabilité du système. Ils sont donc optimisés afin de garantir un temps de mise sur le marché acceptable tout en certifiant un niveau de sécurité élevé des véhicules.
Ainsi évaluer la fiabilité d'un système présuppose une connaissance exhaustive des usages de celui-ci. Pour le véhicule autonome cela signifie que la totalité des parcours possibles d'une heure en mode autonome est connue. La grande difficulté pour valider un système innovant tel que le véhicule autonome réside en grande partie au manque de connaissance de ses modes de défaillance dans son domaine de fonctionnement, lui même partiellement connu et fortement variable.

Les outils mis en place pour les ADAS actuels ne suffisent pas. Ils sont principalement une aide à la conception pour des applications locales. Ils sont depuis peu améliorés pour être utilisés massivement dans le contexte de la validation du véhicule autonome.
Les ADAS, jusqu'alors simples aides à la conduite sont secondés par le conducteur qui reste vigilant. Leurs défaillances n'ont pas ou peu de conséquences catastrophiques pour les usagers. Les exigences de fiabilité sont par conséquent moins strictes. Les méthodes de validation dédiées à ces systèmes sont malheureusement inadaptées aux véhicules autonomes dont les exigences en termes de fiabilité sont beaucoup plus élevées.

La certification du système AD requiert d'abord d'enrichir la base de connaissance pour mettre en évidence tous les modes de défaillances du système et des événements amenant à ces défaillances.

Le système ne sera attesté fiable que lorsque la base de connaissance aura été jugée "complète" ou suffisamment représentative du domaine de fonctionnement et que le bon fonctionnement du système aura été validé dans cette base.

Les stratégies adoptées par les concurrents pour la validation finale consistent à collecter de l'information par des roulages sur route ouverte (ce qui est extrêmement coûteux mais nécessaire) et à reproduire des scénarios de conduite par simulation numérique ou sur piste suivant un protocole qui n'est pas rendu public. Aucune méthode générale de validation et d'évaluation de la fiabilité n'est diffusée.

2.4.2 Contexte et positionnement des travaux de thèse par rapport au besoin industriel

Les travaux de cette thèse ont été réalisés à partir d'un véhicule développé par le groupe de projet TRAJAM puis poursuivi par le projet ILIAD au sein de l'entreprise RENAULT. Le système étudié est prévu pour fonctionner en niveau d'autonomie 4 selon les définitions données par la SAE.
Pour la validation de ce système, tout comme Google ou Tesla, Renault envisage de combiner des roulages aléatoires sur route ouverte, des roulages numériques, des essais sur piste ou des roulages ciblés pour chercher les zones concentrant le plus d'éléments perturbateurs pour le système.

A fréquence régulière, les données collectées pendant les essais réels sont analysées. Une base de connaissance est alors enrichie de nouvelles séquences temporelles. Elles présentent un intérêt pour mieux décrire la variabilité du domaine de fonctionnement et le comportement du véhicule dans ce domaine. L'objectif de ces roulages est de vérifier le bon comportement du système dans l'ensemble des scénarios rencontrés, mais également de détecter des scénarios qui sont différents de ceux enregistrés jusqu'alors et pour lesquels le comportement du véhicule n'est pas prévisible. Les roulages numériques complètent les études. Ils permettent d'une part de re-simuler le véhicule dans l'ensemble des scénarios enregistrés, lorsqu'une modification de l'algorithme a été nécessaire. Et d'autre part ils ajoutent dans la base de connaissance, la prévision du comportement du véhicule dans d'autres scénarios proches de ceux observés en roulage réel mais avec des valeurs différentes des paramètres de l'environnement. Le bon comportement du système est ainsi attesté sur un plus grand ensemble de scénarios avec de nombreuses combinaisons.
Si les roulages numériques ne peuvent pas reproduire une séquence temporelle, un nouveau cas d'usage est créé dans le but d'accroître la connaissance autour de ce scénario. Si de plus, dans certaines situations, ces roulages ne sont pas réalistes et, si une combinaison n'est pas présente en roulage sur route ouverte, les roulages sur piste peuvent aider à reconstruire ces combinaisons jugées manquantes.

Une méthodologie générale de validation du système complet doit être élaborée. Elle doit aider dans la sélection des essais à réaliser et doit faire correspondre les résultats obtenus pour évaluer la fiabilité du véhicule autonome en un temps raisonnable de validation afin de respecter le time to market.
L'objectif de la thèse est d'initier cette méthodologie générale qui est vue comme une road map pour Renault.

Chapitre 3

Etude bibliographique : Evaluer la fiabilité d'un système innovant

3.1 Introduction

Les scénarios de conduite, que suit et doit comprendre le véhicule autonome, peuvent être assimilés à de multiples modes de fonctionnement. L'une des particularités de l'analyse du système est la très grande variabilité et la diversité de ces scénarios liées à des contextes différents d'usage, des environnements de roulage très éclectiques, sans parler des conditions climatiques, de luminosité, etc. Les exigences et spécifications actuelles ainsi que le développement des algorithmes aujourd'hui embarqués reposent sur l'identification d'un ensemble de scénarios issus des bases de données des différents constructeurs et de retours d'experts. Cependant, il est nécessaire dans un cadre de validation globale du système autonome de se poser la question de la représentativité de cette base de connaissance. Cette représentativité peut porter sur deux points, à savoir le niveau d'exhaustivité de la base des scénarios connus ainsi que l'identification et la caractérisation des paramètres d'importance pour la description des situations et la prise de décision qui s'en suit. Plusieurs types d'essais (numériques, sur piste fermée ou en condition réelle) sont mis en place. Les efforts à mettre en oeuvre, le choix des types d'essais ainsi que l'intégration de ces résultats d'essais sont encore aujourd'hui mal orientés. De plus, l'augmentation des exigences de fiabilité des voitures autonomes avec un taux de défaillance de l'ordre de 10^{-9} par heure d'utilisation, indépendamment des parcours, associé à la réduction des coûts et du temps de mise sur le marché, imposent clairement la construction d'une méthodologie générale pour l'évaluation de la fiabilité du système en conditions de roulage réel et pour l'orientation des efforts afin d'améliorer la représentativité de la base des connaissances.
Estimer la fiabilité du véhicule autonome revient à mesurer l'impact de l'ensemble des incertitudes sur le comportement du système. Les méthodes appliquées dans le domaine de l'automobile tiennent uniquement compte de deux types d'incertitude : la variabilité intrinsèque de l'environnement et l'incertitude ajoutée lors de la qualification de la première incertitude, c'est à dire l'estimation des paramètres qui caractérisent cette incertitude. En effet les incertitudes aléatoires sont identifiées et évaluées à partir de données extraites du système. Leur analyse passe d'abord par la collecte d'un échantillon représentatif du problème posé puis par une modélisation statistique de ce problème après examen de cet échantillon. Plus l'échantillon est grand et moins

il y a d'incertitude sur les paramètres estimés. Ce qui se traduit par une variabilité réduite de l'estimateur ou de la variable aléatoire qualifiant l'incertitude.

La connaissance partielle du comportement du système dans son environnement doit être prise en compte dans l'estimation de la fiabilité. En effet la non connaissance de certains scénarios entraîne la modélisation erronée de la fiabilité du système. Elle est vue comme une nouvelle source d'incertitude. Sallak et al. [75] proposent de distinguer les types d'incertitudes pour mener à bien les études de fiabilité. La distinction la plus courante sépare les incertitudes aléatoires, liées à la variabilité intrinsèque du domaine de fonctionnement du véhicule, et les incertitudes épistémiques, liées au manque de connaissance. Pour chaque type d'incertitude, des modélisations différentes sont choisies afin de les propager au niveau du fonctionnement du système et ainsi évaluer la fiabilité de celui-ci. Les incertitudes épistémiques ne sont pas réellement des phénomènes aléatoires. Dès que le niveau de connaissance augmente, ces incertitudes se réduisent. La connaissance acquise est jugée "complète" lorsque ces incertitudes n'ont plus d'influence dans l'estimation de la fiabilité. Les incertitudes aléatoires, quant à elles, sont irréductibles. L'article confronte deux points de vue pour prendre en compte le second type d'incertitudes. La modélisation doit être déterministe car les modèles aléatoires n'ont pas de sens et ne peuvent pas bien les représenter. Contrairement à la deuxième approche qui la choisit probabiliste et caractérise alors l'incertitude de l'expert du phénomène étudié.

L'estimation de la fiabilité nécessite la construction d'un modèle. Celui-ci caractérise les incertitudes sur le comportement du véhicule liées à la forte variabilité intrinsèque de l'environnement. Il caractérise également les incertitudes liées à la collecte des données et à la taille de l'échantillon. Enfin il intègre les incertitudes dues à l'incomplétude de la base de connaissance, i.e. les scénarios manquants dans la modélisation, entraînant une modélisation erronée du comportement du système.

Le fonctionnement du système est dynamique. Par pas de temps régulier, le système autonome analyse la scène présente et décide des actions qu'il doit effectuer. Chaque scène requiert une action bien distincte de l'ensemble de ses composants et des algorithmes. Dans une première partie, nous analyserons les modèles usuels pour traiter des défaillances des systèmes complexes dynamiques afin d'en sélectionner un adapté au contexte du véhicule autonome.

Les modélisations probabilistes sont dotées de paramètres. La qualification des différents paramètres s'opère par analyse et collecte de données. Ces estimations doivent pouvoir se faire avec l'ensemble des moyens mis à disposition par l'entreprise Renault.
Par ailleurs, l'environnement du véhicule autonome est très variable et le problème est de grande dimension. En effet de nombreuses variables de l'environnement peuvent perturber le système : elles caractérisent les actions et la cinématique du trafic, les conditions météorologiques, les éléments de l'infrastructure, etc. La représentativité de la base de données collectées sera de ce fait sujette à des incertitudes et les estimations réalisées seront entachées d'erreur. En seconde partie nous discuterons des techniques d'inférence statistiques permettant à la fois d'estimer les paramètres et de caractériser les incertitudes associées.

Parce que la fiabilité requise est très élevée, les événements amenant à une défaillance risquent d'être rares et difficiles à observer. Les stratégies adoptées dans ce contexte se concentrent princi-

palement sur des méthodes d'échantillonnages efficaces qui permettent de sélectionner les événements les plus "utiles" pour l'évaluation de la fiabilité. La troisième partie présentera une revue de ces stratégies.

Enfin la dernière partie se concentrera plus particulièrement sur les scénarios inconnus, modes de fonctionnement non identifiés pendant la phase de spécification du besoin. Par ce manque de connaissance, le modèle de fiabilité établi est erroné et doit être réajusté pour prédire l'impact de tels scénarios sur le comportement du système.

3.2 Modélisation de la fiabilité des systèmes complexes

L'estimation de la fiabilité d'un système passe par la modélisation du fonctionnement et du dysfonctionnement de celui-ci dans son environnement. Nous devons construire un modèle de fiabilité adapté au véhicule autonome.

Le phénomène de défaillance est un phénomène dynamique. Le système évolue dans le temps jusqu'à rencontrer un événement perturbateur qui entraîne la défaillance du système. Au regard du fonctionnement, de la manière dont se produit l'événement et du comportement du système face à cet événement de nombreuses stratégies de modélisations existent.

Certaines modélisations ne font pas intervenir le temps dans le processus de défaillance. On parle alors de modélisation statique. Ce sont des modèles qui décomposent le système ou son fonctionnement en blocs reliés. Le système est alors vu comme un assemblage de composants. La fiabilité résultante tient compte des rôles des composants et de leur fiabilité dans la défaillance du système. Elle est la conséquence de la défaillance simultanée des divers composants ou sous-fonctions. Ceci permet entre autres de bien séparer les modes de défaillance et d'allouer les objectifs de fiabilité au niveau des composants. Nous pouvons citer les modèles de blocs diagrammes de fiabilité, les arbres de défaillances [67]. Aucune relation temporelle entre les différents blocs n'est intégrée. Comme nous l'avons vu dans le chapitre précédent ce type de modélisation n'est pas adaptée au système de perception et de décision. En effet les interactions entre les différents composants sont complexes et ne sont pas facilement modélisables par des blocs.

Pour la grande majorité des systèmes dynamiques, le temps est primordial pour modéliser les dysfonctionnements. Nous nous intéressons plus particulièrement aux modélisations généralement attribuées aux systèmes complexes.
La fiabilité prévisionnelle des systèmes à comportement et événements dynamiques se modélise à partir de processus stochastiques [12]. Ce sont des enchaînements de variables aléatoires. Une réalisation d'un processus est appelée une séquence temporelle d'états. On parle de processus discrets si la variable de temps est dénombrable et de processus continus, dans le cas contraire. Les processus à états discrets reproduisent les changements d'états saccadés du système alors que les processus continus se rapportent à une dégradation graduelle et progressive du système. L'autre élément distinctif entre les processus est l'absence ou la présence plus ou moins longue de mémoire dans le fonctionnement du système. Par exemple pour un fonctionnement d'un système par état discret, l'événement suivant peut apparaître comme une fonction d'une succession de plusieurs états.

Les processus sans mémoire sont appelés des processus de Markov car ils vérifient la propriété de Markov : *La distribution conditionnelle de probabilité des états futurs, étant donnés les états passés et l'état présent, ne dépend que de l'état présent et non pas des états passés (absence de « mémoire »).* Les plus courants sont :

1. Le processus de Bernoulli : chaîne de Markov à temps discret et de variables aléatoires à valeurs binaires.
2. Les chaînes de Markov à espace d'états discret : pour lesquels le temps est dénombrable, l'ensemble des valeurs prises par les variables aléatoires, appelé espace d'états, est fini.
3. Les chaînes de Markov à espace d'états continu : les variables aléatoires du processus ont des valeurs continues.
4. Le processus de Poisson homogène : processus à accroissements indépendants stationnaires sur $\mathbb{N}$; Un processus de Markov à temps continu sur un ensemble fini ou dénombrable est issu de ce processus,
5. Le mouvement brownien : processus à accroissements indépendants stationnaires sur $\mathbb{R}$; Les processus de Markov continus sur $\mathbb{R}$ ou $\mathbb{R}^n$ se basent sur ce processus.

On peut également citer des processus non markoviens souvent choisis pour des calculs de fiabilité tels que :

— Les processus semi-markoviens [47] :
Un processus semi-Markovien garde une évolution de type markovienne (absence de mémoire) mais le temps de séjour dans un état peut suivre une loi quelconque.
— Les processus de Poisson non homogènes, ils sont une extension des processus de Poisson homogènes pour des accroissements non stationnaires. Ils sont souvent utilisés pour des modèles de croissance de fiabilité.

Dans le cadre des systèmes complexes, le formalisme des automates est usuellement employé. Il s'applique aux systèmes dynamiques hybrides. Ce sont des modélisations intermédiaires entre des défaillances liées à un phénomène discret et des défaillances liées à un phénomène continu. Les systèmes évoluent dans des états discrets, chacun d'eux étant caractérisé par une évolution propre au cours du temps des variables physiques. Les événements discrets sont aléatoires alors que l'évolution temporelle des variables physiques reste déterministe. Ils sont modélisés par des graphes d'états comme les chaînes de Markov et les réseaux de Pétri stochastiques [5].

— **Chaîne de Markov** : Un support graphique représente ces processus, Figure 3.1. Il est appelé graphe des états et permet de visualiser les différents états d'un système qui sont représentés par des cercles et reliés entre eux par des arcs orientés qui représentent la transition d'états de départ vers des états d'arrivée.
— **Réseaux de Pétri** : Les réseaux de Pétri sont utilisés pour décrire les processus de commande séquentielle dynamique. Ils comportent deux parties, une partie statique et une partie dynamique, Figure 3.2.
  — La partie statique ou réseau de Pétri est constituée de places, de jetons, de transitions et d'arcs. Un état du système est une position des jetons dans les places.
  — La partie dynamique est obtenue par les mouvements des jetons au travers des transitions. Les jetons sont alors différemment répartis dans les places ce qui devient le nouvel état du système. Un jeton franchit une transition, il ne peut pas y stagner.

  Un réseau de Pétri est dit de plus stochastique (RdPS) lorsque le franchissement des transitions est aléatoire. Les RdPS à loi exponentielle sont également des chaînes de

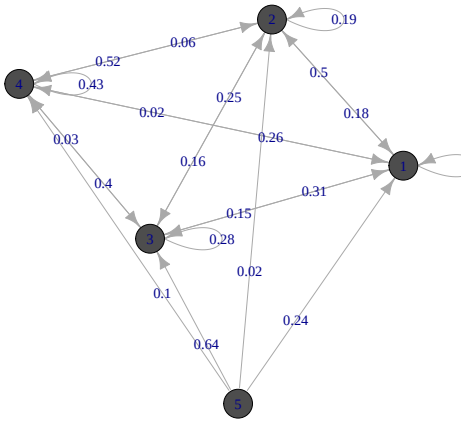


FIGURE 3.1 – Exemple de chaînes de Markov

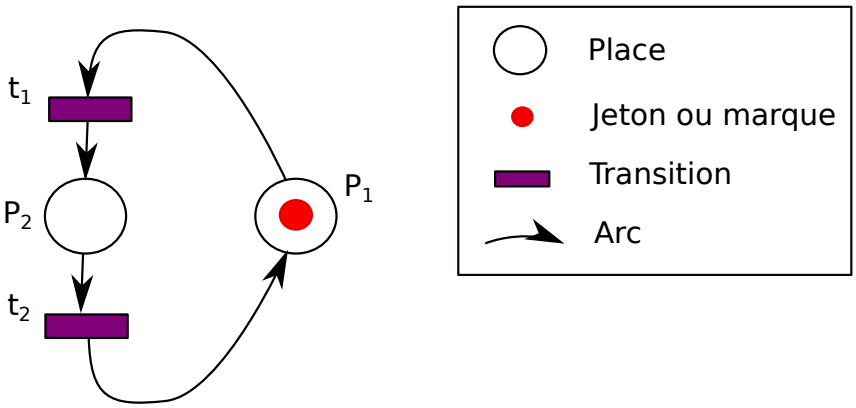


FIGURE 3.2 – Exemple de réseaux de Pétri

Markov. Les RdPS avec processus de marquage (mouvement des jetons) est un processus semi-markovien. Cette modélisation permet de représenter plus largement les systèmes qui n'ont pas de propriétés aussi restrictives que les chaînes de Markov.

Enfin, pour prendre en compte des rapports de causalités entre les événements les réseaux bayésiens sont souvent utilisés. Ils sont issus également d'un mélange entre théories des graphes et théories des probabilités. Ce sont des graphes orientés acycliques où les variables sont les sommets des graphes. Ils partent du théorème de Bayes, et décrivent les relations causales entre les variables, de manière probabiliste avec des probabilités conditionnelles. Les réseaux bayésiens dynamiques sont une extension des réseaux bayésiens et peuvent représenter l'évolution temporelle de variables par des pas de temps discrets. Cette dernière modélisation peut prendre en compte les probabilités conditionnelles entre les variables de l'environnement pour amener à un scénario défaillant.

La modélisation hybride semble intéressante pour bien représenter le fonctionnement du système AD. En effet le comportement aléatoire du véhicule autonome réside en grande partie dans les scénarios qu'il rencontre. Les états seraient ici les scénarios rencontrés par le véhicule. En suivant ces modélisations, un même scénario rencontré plusieurs fois entraîne toujours le même dénouement. Ceci pourrait être vrai si les scénarios étaient entièrement paramétrables, mais certains niveaux de détails ne peuvent pas être pris en compte comme la couleur des voitures, la forme précise des tunnels, etc. Il faut ajouter à cela les réactions des acteurs du trafic devant la conduite du mode AD, qui peuvent être très différentes d'une personne à une autre. Le comportement du véhicule autonome dans un même scénario doit donc être modélisé de manière aléatoire.
Peu d'information existe encore sur le véritable comportement du véhicule autonome. Actuellement les modélisations choisies dans la littérature sont très générales et peuvent s'appliquer à n'importe quel système qui requiert un niveau de fiabilité aussi élevé.
Devant l'ensemble des modélisations énoncées notre choix se porte sur la modélisation la plus facile à mettre en place et qui semble dans un premier temps convenir pour représenter le système AD. Cette description permettra de mieux comprendre et de mieux percevoir le déroulement des essais de validation avec le véhicule. Elle est la base pour la construction d'une méthodologie permettant d'évaluer la fiabilité du système. La modélisation pourra être complexifiée pour mieux représenter le système mais nous souhaitons de prime abord construire une démarche simple que l'on adaptera au problème au fur et à mesure.

Tout d'abord un processus représentant les successions de scénarios rencontrés semble adapté au véhicule et à son fonctionnement. Un processus discret pour lequel chaque état est un scénario représente bien ce phénomène. Nous n'avons pas d'information concernant la mémoire que doit contenir ce processus. Le séquencement des scénarios caractérisant le trafic, comme une insertion d'un véhicule, le suivi d'un autre, paraît sans mémoire. Seule la configuration de route à la fin d'un scénario influence l'apparition d'un nouveau. Par exemple, un scénario dans lequel le véhicule autonome, appelé ego, reste derrière un autre véhicule et est doublé par un deuxième plus rapide à sa gauche sera probablement poursuivi par un scénario dans lequel ce même véhicule de gauche se rabat devant ego (Figure 3.3). D'autres paramètres physiques et continus tels la pluie, requièrent peut-être d'ajouter plus de mémoire dans le modèle mais cela ne peut se déterminer que par retour d'expériences. Pour le moment nous supposons pour simplifier qu'une probabilité conditionnelle entre deux scénarios suffit pour bien représenter ce phénomène. Un

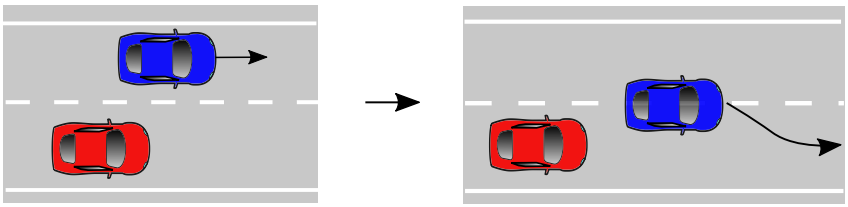


FIGURE 3.3 – Enchaînement de deux scénarios, ego se fait doubler puis le véhicule se rabat

scénario pluvieux est supposé entraîner plus probablement un scénario pluvieux qu'un scénario ensoleillé et les probabilité ne changent pas en fonction du temps passé dans un scénario pluvieux. On obtient ainsi une chaîne de Markov. Il existe une infinité de scénarios de la route. L'insertion d'un véhicule peut se faire en tout temps, tout type de route, à toutes les vitesses, etc. Chaque combinaison est un scénario. Le processus se rapprochant le plus de ce phénomène semble être une chaîne de Markov à espace d'états infini. La modélisation à état infini requiert une bonne connaissance des états possibles et de leur probabilité. Or certaines combinaisons sont inconnues et vont entraîner la conception d'un modèle erroné de la fiabilité du système. Pour ajuster ce modèle et prendre en compte l'impact de ces combinaisons inconnues dans le calcul de la fiabilité il faut arriver à les identifier. Cette manière de modéliser risque de poser problème pour distinguer les nouveaux scénarios. De part leur infinité chaque scénario rencontré par le véhicule est unique. Cependant certains sont très proches de ceux déjà observés tandis que d'autres sont très différents et jamais imaginés par les experts. Nous supposons qu'ils peuvent être regroupés en un nombre fini de classes, que l'on nomme cas d'usage. L'utilisation du véhicule autonome peut être ainsi modélisée par une chaîne de Markov à états finis. Les scénarios rencontrés non présents de la base de connaissance pourront de ce fait être identifiables car ils ne seront pas caractérisés par les groupes présents et entraîneront la construction de nouvelles classes.

La modélisation choisie donnera une bonne estimation de la fiabilité du système seulement si sa construction et les estimations de ses paramètres sont calculées à partir d'une base de connaissance suffisamment représentative du domaine de fonctionnement. Dans la seconde section de ce chapitre nous présentons les différentes techniques d'inférence statistique afin de bien estimer les paramètres du modèle.

3.3 Qualification des incertitudes aléatoires

Les méthodes d'inférence statistique consistent à expliquer un phénomène aléatoire au travers d'un modèle probabiliste. Nous appelons observations de la variable aléatoire x, les n éléments $(x_i)_{i\in\{1,\cdots,n\}}$ de l'échantillon. Pour décrire le déroulement aléatoire de la variable x, une distribution est affectée à chaque instant aux observations x_i. Soit $f_1(x_1|\theta_1)$ la densité de x_1 de paramètre θ_1 sur un espace mesurable et les densités conditionnelles $f_i(x_i|\theta_i, x_1, \cdots, x_{i-1})$ des observations x_i sachant les observations précédentes $x_1, \cdots, x_{i-1}$. Les distributions sont connues alors que leurs paramètres sont inconnus et sont l'objet des techniques d'inférences pour obtenir une information sur leur valeur. La description générale de la variable aléatoire x est donnée par (3.1).

$$f(\mathbf{x}|\boldsymbol{\theta}) = f_1(x_1|\theta_1)\prod_{i=2}^{n} f_i(x_i|\theta_i, x_1, \cdots, x_{i-1}) \tag{3.1}$$

avec le vecteur $\mathbf{x} = x_1, \cdots, x_i$.
C'est une forme très générale, elle représente tout type d'observations sur un horizon temporel fini avec dépendance ou non. Dans le cas d'observations indépendantes et identiquement distribuées (iid) cette modélisation peut s'écrire comme (3.2). $\boldsymbol{\theta}$ est alors le paramètre θ.

$$f(\mathbf{x}|\boldsymbol{\theta}) = \prod_{i=1}^{n} f(x_i|\theta) \tag{3.2}$$

Les inférences, sur les distributions ou les paramètres, sont regroupées en deux paradigmes : fréquentiste et bayésien.

3.3.1 Inférences fréquentistes ou statistiques inférentielles

La connaissance des variables étudiées ne se construit qu'au travers de dénombrement des valeurs des variables d'intérêt à partir des données collectées. Les variables sont supposées suivre des lois qui peuvent être paramétriques ou non. Soit on souhaite évaluer les valeurs des paramètres de la loi, alors on parle d'estimation statistique, soit on souhaite valider ou rejeter une hypothèse sur la distribution ou les paramètres de la variable. Dans ce contexte on parle de tests statistiques.

1. **Estimations statistiques**
   La liste des estimateurs est grande. Leur choix dépend fortement de la grandeur à estimer. On les sélectionne à partir de critères comme le biais de l'estimateur, son erreur quadratique, sa vitesse de convergence, son efficacité et sa robustesse. Les premiers estimateurs que l'on peut citer sont l'estimateur de la moyenne empirique (3.3) et la variance sans biais empirique (3.4) de la variable d'intérêt y, n étant la taille de l'échantillon et $(y_i)_{i\in\{1,\cdot,n\}}$ les observations de y.

$$\overline{y} = \frac{1}{n}\sum_{i=1}^{n} y_i \tag{3.3}$$

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{n}(y_i - \overline{y})^2 \tag{3.4}$$

   En utilisant le théorème central limite, on sait que l'erreur est de l'ordre de $\sqrt{N}$. De plus, plus la variance est grande plus l'erreur est importante initialement. Ce théorème ne s'applique que lorsque le tirage est suffisamment homogène et représentatif de l'espace paramétrique. La méthode des moindres carrés permet d'estimer les paramètres d'une fonction. Ils sont calculés pour minimiser la somme quadratique des déviations des données aux prédictions du modèle.
   Les M-estimateurs, dont le maximum de vraisemblance, obtenus par la minimisation d'une fonction dépendant des données et des paramètres du modèle, permettent d'obtenir des estimateurs plus robustes que ceux précédemment décrits.
   Les critères d'information d'Akaike, "Akaike information criterion"(AIC), et bayésien,

"Bayesian information criterion"(BIC) permettent de tenir compte du nombre de paramètres et de la taille de l'échantillon pour calibrer le modèle. Le choix du modèle peut se faire par minimisation d'un des deux critères.

Les paramètres du modèle de fiabilité choisi dans la section 3.2 sont des probabilités qui peuvent être très petites ou très proches de un. Les précisions requises de ces paramètres sont très grandes puisque le niveau de fiabilité attendu est très élevé. Ce type d'estimation risque de demander une très grande taille d'échantillon. La durée des essais pour obtenir une bonne estimation risque d'être trop importante pour respecter la date de mise sur le marché. De plus le problème est de grande dimension, il est très difficile de collecter des données représentatives de l'ensemble des usages possibles avec un nombre restreint de scénarios observés respectant l'usage client. Par conséquent les estimations seront fortement biaisées avant de rencontrer les scénarios plus rares apportant plus d'information sur le comportement du système.

2. **Tests statistiques**
   Un test statistique met en confrontation au minimum deux hypothèses. Il s'agit par exemple d'une démarche consistant à rejeter ou à ne pas rejeter une hypothèse statistique, appelée hypothèse nulle, en fonction d'un jeu de données. Il peut être paramétrique : une hypothèse initiale est alors faite sur la distribution des données et la décision valide ou invalide une affirmation sur les valeurs des paramètres. Il peut, au contraire, ne pas être paramétrique et dans ce cas aucune hypothèse au préalable de la distribution n'est nécessaire.

   Plutôt que d'estimer des paramètres qui demandent un nombre conséquent de données pour obtenir une estimation précise, les valeurs des paramètres sont ici supposées et sont soit réfutées soit acceptées avec un certain niveau de confiance. Cela peut réduire le nombre d'essais à réaliser mais ces hypothèses sont très sensibles aux modèles qui sont mis en opposition. Si la modélisation choisie est erronée les conclusions le seront également.

3.3.2 Inférences bayésiennes

L'objectif des inférences bayésiennes est d'exploiter toutes les informations disponibles au préalable sur la variable d'intérêt pour évaluer le paramètre du modèle θ avant d'entamer une procédure d'inférence sur θ. Elles sont principalement utilisées lorsque le nombre d'observations est insuffisant pour donner une bonne estimation avec des inférences fréquentistes. Le paramètre θ, étant inconnu, est vu comme une variable aléatoire nommé Θ. Sa densité $f_\Theta(\theta)$ est donnée *a priori* à partir des informations obtenues sur x. Cette densité sera actualisée au vu des n observations $(x_i)_{i\in\{1,\cdots,n\}}$. On nomme cette dernière la densité *a posteriori* $f_{\Theta|x}(\theta|x_1,\cdots,x_n)$. Elle est une inversion de la vraisemblance, *i.e* la densité $f_{x|\Theta}(\mathbf{x}|\theta)$ développée en (3.2). Le théorème de Bayes est spécifiquement utile pour exprimer cette inversion.

Théorème 3.1. *Théorème de Bayes*
Soit Ai une partition de l'ensemble des possibles, et B un événement alors :

$$P(A_i|B) = \frac{P(B|A_i)P(A_i)}{\sum_j P(B|A_j)P(A_j)} \tag{3.5}$$

pour tout Ai de la partition.

La densité *a posteriori* est ainsi obtenue par (3.6).

$$f_{\Theta|x}(\theta|\mathbf{x}) = \frac{\prod_{i=1}^{n} f_{x|\Theta}(x_i|\theta) f_{\Theta}(\theta)}{\int_{\Omega} f_{x|\Theta}(\mathbf{x}|\omega) f_{\Theta}(\omega) \mathrm{d}\omega} \tag{3.6}$$

Avec Ω l'ensemble des valeurs possibles de Θ. Le dénominateur de cette expression est la densité marginale de x, pour les observations $\mathbf{x}$, notées $f_x(\mathbf{x})$. Elle est constante pour une observation donnée. On note alors que la densité *a posteriori* est proportionnelle au produit $f_{x|\Theta}(\mathbf{x}|\theta) f_{\Theta}(\theta)$ soit

$$f_{\Theta|x}(\theta|\mathbf{x}) \propto f_{x|\Theta}(\mathbf{x}|\theta) f_{\Theta}(\theta) \tag{3.7}$$

Les inférences bayésiennes présentent un fort intérêt dans le cadre de notre étude. La fiabilité recherchée est très grande. Par conséquent les paramètres du modèle de fiabilité choisi ne pourront être estimés correctement qu'après un très grand nombre d'observations. Or de nombreuses informations de différentes formes peuvent enrichir et aider à la sélection de distributions *a priori* des paramètres du modèle. Une mise à jour bayésienne pourra donner une estimation plus rapidement fiable de ces paramètres que la méthode fréquentiste. D'autant plus qu'une estimation même erronée en début d'estimation sera corrigée avec les observations mais elle peut quand même biaiser les résultats.

La qualité des estimations est dépendante des données collectées pendant la phase de validation. La précision requise de l'estimation de la fiabilité impose de développer une stratégie d'échantillonnage efficace pour respecter les contraintes de coût et de délais pour la validation des véhicules autonomes. Cette stratégie doit tenir compte du manque de connaissance qui peut biaiser les analyses.

3.4 Optimisation des plans d'essai : Différentes méthodes d'échantillonnage

Les estimations des paramètres du modèle de fiabilité seront réalisées à partir des données extraites des tests de différentes natures : numériques, sur pistes ou réels sur route ouverte. Quelque soit la nature des tests, la dimension du problème étudié, la connaissance partielle du domaine et la forte variabilité empêchent une sélection exhaustive des scénarios de roulage. Des stratégies d'échantillonnage adaptées à chaque type de tests peuvent aider à la construction du plan de validation final. Elles aident la mise en place d'une stratégie d'ordonnancement des plans d'essais permettant de limiter la durée de validation tout en collectant l'ensemble des données nécessaires à la bonne estimation de la fiabilité du système. Nous présentons ici un aperçu des méthodes disponibles d'échantillonnage.

3.4.1 Echantillonnage par tirage aléatoire

La méthode la plus classique pour extraire un échantillon est de tirer aléatoirement les données. Quand les essais sont numériques, on parle de tirage de Monte-Carlo [55]. Elle est principa-

lement employée pour des estimations numériques de grandeurs moyennes ou des intégrales. Elle est souvent associée à l'estimateur de la moyenne empirique vu précédemment. Cet estimateur converge vers la valeur d'intérêt en $\frac{\sqrt{n}}{\sigma}$, avec σ l'écart type de l'estimateur dont le carré est sa variance. Souvent cette variance est également estimée et on donne une vitesse de convergence de l'ordre de $\frac{1}{\sqrt{n}}$. Cependant cette variance a un rôle dans la précision des estimations. Plus cette variance est grande et plus la taille de l'échantillon sera grande pour obtenir une estimation précise de la variable d'intérêt. Pour réduire la taille de l'échantillon, quand l'appel de la fonction numérique ou les essais sont trop coûteux, des techniques de réduction de variance sont utilisées comme les tirages d'importance ou l'échantillonnage stratifié.
Les tirages d'importances [72], utilisent une distribution biaisée de celle étudiée, afin de réduire sa variance. Les tirages ciblent plus rapidement les valeurs d'intérêt souvent situées en queue de distribution.
L'échantillonnage stratifié, dont l'échantillonneur par hypercube latin, réduit la variance. L'espace des variables d'entrée est découpé en sous espaces disjoints pour sélectionner des points dans chaque sous-espace.
Les échantillonneurs de Monte-Carlo par chaîne de Markov [31], quant à eux, réduisent le nombre de tirage à réaliser à partir d'une chaîne de Markov de même distribution que celle souhaitée. La réalisation de plusieurs séquences de cette chaîne, suffisamment grandes et réparties dans l'espace de recherche, peut être analysée comme des réalisations de la distribution étudiée. Ces derniers tirages sont souvent reliés à des inférences bayésiennes.

En grande dimension et pour une grande précision de la fiabilité souhaitée les méthodes purement aléatoires sont très coûteuses en durée d'essais et ne pourront pas permettre de valider à temps le véhicule autonome. Une autre stratégie d'échantillonnage est nécessaire pour la remplacer ou la compléter afin de réduire le temps de validation.

3.4.2 Méthodes de Quasi-Monte Carlo

L'objectif de ces méthodes est de trouver de meilleurs estimateurs et avoir une plus grande vitesse de convergence [59]. Pour ce faire des suites déterministes sont construites pour être uniformément réparties dans l'espace. L'uniformité de ces suites est vérifiée par un critère, nommé discrépance. La discrépance mesure l'écart à l'uniformité d'une suite de points. Plusieurs mesures de discrépance existent. Les suites dites quasi-aléatoires sont élaborées en minimisant la discrépance. On peut citer les séquences de Sobol, Halton, van der Corput, Faure, etc..
Ce type de méthode, réservé aux essais numériques, ne permettra pas de réduire drastiquement les essais de validation. Elles sont aussi coûteuses que les méthodes de Monte-Carlo. Elles donnent cependant une estimation moins dépendante de l'échantillon extrait.

3.4.3 Echantillonnage par plans d'expériences

Un plan d'expériences est un ensemble déterministe de points [63]. Tous les paramètres d'entrée sont étudiés comme des variables discrètes. Ils prennent un nombre fini de valeurs appelées niveaux. Ce plan rassemble des combinaisons des niveaux des paramètres d'entrée. Ces combinaisons sont choisies pour valider et expliquer un modèle préalablement établi selon des hypothèses sur les effets de chaque paramètre et de leurs interactions sur la sortie étudiée. Le plan d'ex-

périences permet ainsi d'acquérir de nouvelles connaissances en maîtrisant certains paramètres d'entrée et apporte un résultat représentatif du problème étudié en un minimum d'essais.
Les plans d'expériences sont utiles quand le phénomène physique est bien appréhendé et que les interactions entre les paramètres sont suffisamment connues pour réduire le nombre d'essais. Dans notre contexte ce n'est pas le cas. La forme des zones de défaillance dans l'espace des paramètres, les interactions entre les paramètres, leurs influences supposées ne sont pas connues. Avec la dimension du problème, le plan d'expériences nécessaire pour limiter les erreurs d'interprétation sera très coûteux. Certains plans ne tiennent pas compte de la probabilité d'occurrence de la zone dans lequel le point est tiré et cela pourrait être une combinaison improbable et donc impossible à observer. Cependant un plan peut permettre d'observer des combinaisons plus rares et donner une vue plus globale des conditions de route pouvant être rencontrées par le véhicule autonome.

3.4.4 Echantillonnage itératif (iterative sampling)

Ce dernier type d'échantillonnage est un ensemble de plans de tests programmés de manière séquentielle. Les points sont sélectionnés pour minimiser ou maximiser un critère ou une fonction. La fonction à optimiser est un modèle de substitution de la sortie étudiée. Son appel est beaucoup moins coûteux que la réalisation d'essais ou de calculs de la véritable sortie. L'objectif est de préciser la sortie étudiée uniquement dans les zones d'intérêt. Le modèle simple (ou méta-modèle) propose de tester les points qui sont le plus probablement situés dans la zone d'intérêt. On donne ici quelques exemples :

- Les méthodes de surfaces de réponses [30]
- Les méthodes "Efficient Global Optimization" (EGO) associées à des modèles de krigeage [39]. Elles utilisent les incertitudes données par le modèle de krigeage à partir des variances des estimations et raffinent la précision des évaluations de l'optimisation en fonction des besoins du problème.
- Les méthodes FORM/SORM [13] (développement en série de Taylor limitée au premier ordre et second ordre : first and second order reliability methods) employées en mécanique des structures dans le contexte des problèmes contraintes/résistances.
- Les méthodes d'échantillonnage à partir de classifications non supervisées peuvent également être choisies pour ne sélectionner que les points à la frontière des classes, et pour lesquels une faible variation des paramètres d'entrée entraîne une forte variation de la réponse du problème.

Une approche itérative pour tester le véhicule autonome semble être adaptée pour la construction du plan de validation du système. Au lieu d'effectuer des tests aléatoires sur les routes habilitées, il est peut être possible de définir un critère à optimiser avec une méthode associée pour qualifier efficacement les incertitudes aléatoires et ainsi obtenir une estimation précise de la fiabilité du véhicule autonome.
Ces méthodes semblent plus naturelles pour qualifier un problème statique ou de courte durée. La plupart ne tire pas profit de signaux temporels générés pendant le test. En effet pendant le roulage, les vitesses, positions, accélérations, de chaque véhicule mesurées par le système AD sont enregistrées à chaque instant que ce soit pour des essais physiques ou des essais numériques. Les analyses citées pour décider des futurs essais à réaliser modélisent la variation d'une sortie sous forme d'un scalaire en fonction des paramètres d'entrée.

Si la dimension est trop importante, la quasi-totalité des méthodes présentées ci-dessus sont inefficaces. En effet la plupart des publications actuelles relatives à ces méthodes ont pour objectif d'étendre celles-ci à des problèmes de plus grande dimension mais le sujet reste ouvert. Cependant il est en réalité très rare que l'ensemble des paramètres d'entrée choisis pour la modélisation aient la même influence sur la réponse étudiée. Au préalable, des méthodes d'analyse de sensibilité sont appliquées pour réduire la dimension. La valeur de la réponse peut être, de plus, la résultante d'une combinaison des paramètres d'entrée. La dimension peut être amoindrie en utilisant des méthodes de réduction de dimension comme les analyses en composantes principales ou les décompositions en valeurs singulières. Ces deux dernières méthodes peuvent être appliquées sur l'ensemble des données temporelles.

3.4.5 Enrichissement virtuel des données : techniques de Bootstrap

C'est une méthode de re-échantillonnage à partir des points existants. Elle tire dans un échantillon initial plusieurs sous-échantillons de plus petites ou de même tailles avec remise des points. Cette méthode permet d'avoir une meilleure estimation d'une grandeur comme l'espérance d'une distribution.

L'efficacité de toutes ces méthodes d'échantillonnage dépend beaucoup de la phase de conception ou de validation courante. La sélection d'une de ces méthodes se fait en considérant :

— la dimension du problème,
— les interactions et les corrélations entre les paramètres d'entrée,
— le nombre, l'occurrence et la forme de zones de défaillance.

Dans le cadre du véhicule autonome, les méthodes citées sont adaptées à des analyses numériques et beaucoup moins à des essais réels. En effet, sur route ouverte les paramètres sont très peu contrôlables. Néanmoins, une indication sur les valeurs à observer peut aider à la sélection des routes, heures et saisons pour les observer plus probablement. Un mélange de toutes ces stratégies est envisagé. Il faut à la fois conserver des tirages purement aléatoires ou se concentrant sur des zones peu visitées pour enrichir la connaissance sur le problème et construire un modèle fidèle au phénomène étudié. Mais les essais ne peuvent pas être uniquement aléatoires car les zones de défaillance seront trop tardivement trouvées. Des plans d'expériences initiaux peuvent permettre de mieux cartographier le comportement du véhicule dans l'univers des possibles. De plus les zones de défaillance sont à rechercher efficacement. Pour ce faire une stratégie d'échantillonnage itératif semble la plus adaptée à notre problème. L'acquisition de connaissance va faire apparaître de nouvelles zones susceptibles d'entraîner des défaillances qui seront mieux caractérisées par des essais successifs autour de ces zones. Les procédures itératives nécessitent un critère d'arrêt afin de définir la fin de la procédure de validation. Ce critère d'arrêt doit tenir compte de l'existence de scénarios inconnus et non identifiés. Pendant la phase de validation de nombreux scénarios seront identifiés mais il reste à quantifier l'impact de scénarios rémanents. Avec la durée des tests, ces scénarios vont se raréfier et n'auront plus d'impact sur l'estimation de la fiabilité du véhicule autonome. Leur recherche ne sera plus utile pour valider les exigences définies. Caractériser la robustesse de la base de donnée acquise pendant les essais peut aider à certifier le système. Pour ce faire, l'évaluation de la fiabilité doit inclure une nouvelle source d'incertitude liée à ce manque de connaissance. L'incertitude liée à la non connaissance d'un cas d'usage ne peut pas être propagée de manière

classique. Un coefficient correcteur ou l'ajout d'une erreur au modèle de fiabilité semble un bon moyen d'en tenir compte. Cette influence doit cependant se réduire au fur et à mesure qu'un nouveau cas d'usage apparaît. Ainsi l'enrichissement de la base de connaissance pourrait être représenté.

3.5 Evaluation des incertitudes épistémiques au niveau système

La classification des incertitudes n'est pas un sujet nouveau. Dès le IVème siècle avant J-C, les grecs distinguaient les incertitudes dites épistémiques liées au manque de connaissance et les incertitudes aléatoires liées à la variabilité intrinsèque du système étudié. La classification des incertitudes dans l'une de ces deux catégories varient selon les domaines. Il est parfois difficile de distinguer l'une ou l'autre. Cette distinction a pour intérêt de mieux cibler les incertitudes qui peuvent être réduites afin de répondre plus rapidement au problème posé. La notion d'incertitude réductible et irréductible est parfois employée, pour aller dans ce sens.
Contrairement aux incertitudes aléatoires, les incertitudes épistémiques sont réductibles par un accroissement des connaissances. N'étant pas dues à des phénomènes physiques aléatoires des théories non probabilistes modélisent ce type d'incertitude et ajoutent une sécurité supplémentaire dans l'estimation de la fiabilité d'un système.

3.5.1 Théories non probabilistes

Les méthodes non probabilistes se focalisent sur la quantification des incertitudes épistémiques. En théorie des intervalles [57], les paramètres incertains sont encadrés à l'intérieur d'intervalles. La théorie des probabilités imprécises développée par Walley [86] regroupe la théorie de fonctions de croyance (ou théorie de Dempster-Shafer) [77], la théorie des possibilités [17], et la théorie des ensembles flous [88]. Elle définit un cadre général de représentations des incertitudes. Les paramètres sont encadrés par deux distributions, basse et haute. Cela est intéressant quand les paramètres sont mals connus et le modèle bien identifié. La théorie des ensembles flous s'établit sur des opinions d'experts. Des ensembles, dits flous, contiennent des éléments qui sont affectés à des degrés d'appartenance. Ceux-ci sont définis par des fonctions d'appartenance à valeur dans l'intervalle $[0, 1]$. La théorie des possibilités étend la logique floue. Elle ajoute une règle de normalisation à la définition des ensembles. Enfin dans la théorie des évidences, la probabilité de l'ensemble des éléments incertains est englobée par deux distributions : croyance et plausibilité. La croyance représente la part totale de croyance soutenant l'ensemble, la plausibilité représente la part maximale qui pourrait soutenir cet ensemble.
Le principe de ces théories est de ne pas modéliser les paramètres incertains de manière aléatoire. Ils sont supposés déterministes. Ils l'auraient été s'ils avaient été connus et doivent être représentés comme tels. Une modélisation aléatoire de ces paramètres ajoute un biais, une information sans rapport avec le vrai phénomène. Cette analyse est sujette à débat. Une modélisation est toujours perfectible. Des phénomènes jugés aléatoires peuvent, après une étude approfondie, être modélisés par une fonction déterministe d'autres variables aléatoires. En reprenant leur hypothèse, les incertitudes dues à la méconnaissance des paramètres de cette nouvelle fonction sont épistémiques et doivent être représentés de manière déterministe. Le séparation entre épistémique et aléatoire n'est pas si évidente.

Dans notre étude, incertitudes épistémiques et aléatoires peuvent être entremêlées. Par exemple, la contribution sur la fiabilité d'un scénario inconnu peut être mal catégorisée. Ce scénario peut être classifié dans un nouveau cas d'usage jusqu'alors inconnu (incertitude épistémique) ou alors il est une réalisation d'un cas d'usage, à la frontière de cette classe connue. Dans ce dernier cas c'est la propagation des incertitudes aléatoires des paramètres de l'environnement qui influe sur la fiabilité. La distinction entre les cas d'usages et la détection d'un nouveau cas sont encore subjectives.
Les méthodes présentées ajoutent une borne de sécurité supplémentaire avec les connaissances des experts. Cependant dans notre cas, aucune connaissance ne peut être apportée pour ce type d'incertitude.
En théorie probabiliste, des probabilités caractérisent les incertitudes épistémiques. Ces probabilités sont des descriptions subjectives des phénomènes mal connus. Cette théorie a l'avantage de rester robuste à de mauvaises distinctions entre incertitudes épistémiques et aléatoires. Elle prend en compte toutes ces incertitudes de manière globale et n'est pas pénalisée par des erreurs de jugement.
Dans cette thèse, nous avons opté pour les théories probabilistes. Les modélisations de croissance de fiabilité, surtout celles utilisées en fiabilité logiciel, pourrait aider à modéliser l'apparition de tels scénarios. Une analogie entre découverte d'un bug et découverte de scénario nouveau est en effet intuitive. Nous exposons les principes de ces modèles dans la section suivante.

3.5.2 Evaluation de la fiabilité prévisionnelle de logiciels par des modèles de croissance de fiabilité

La fiabilité d'un logiciel, probabilité de ne pas rencontrer de bugs pendant une durée d'utilisation donnée, pour un usage identifié, contribue à garantir la qualité de celui-ci. Un bug, est une erreur humaine dans l'écriture du code entraînant un dysfonctionnement du logiciel. La difficulté du programme, l'expérience des développeurs, l'imbrication des différents algorithmes sont autant de paramètres favorisant la génération de bugs dans le logiciel. Ils ne sont pas contrôlables, et leurs effets sur la fiabilité sont difficilement quantifiables. Des méthodes dites "white box" pour intégrer les connaissances sur l'architecture du système sont utilisées. Elles décrivent le fonctionnement du logiciel au travers de son architecture par une décomposition modulaire du logiciel. Elles n'évitent pas l'usage de méthodes dites "black box" au niveau des sous-blocs de l'algorithme parmi lesquels se trouvent les modèles de croissance de fiabilité que nous exposons dans cette partie.
Les modèles de croissance de fiabilité sont pertinents pour juger de la qualité d'un logiciel à un instant donné. Pendant la phase de débogage, ils prédisent l'apparition d'un nouveau bug à partir des temps d'apparition des précédents. Cette prédiction relève également de la vitesse de détection de bugs et de l'efficacité du débogage. L'état d'avancement est ainsi jaugé, les développeurs peuvent en déduire une date de mise sur le marché du logiciel.
En plus de 40 ans, les modèles de croissances se sont multipliés [64, 52]. Initiés par Duane [16], Jelinski et Moranda [38], ils ont connus de nombreuses variantes pour s'adapter à l'objectif de prédiction (comme évaluer l'avancement du débogage ou certifier de la qualité du logiciel avant sa mise sur le marché), au contexte de développement, aux méthodes de débogages et à la complexité des algorithmes.
Toutes ces analyses supposent que la séquence des temps de défaillance du logiciel $(T_i)_{i\geq 0}$ est un processus stochastique où T_i, le i-ème temps de défaillance du logiciel, est une variable aléa-

toire et $T_0 = 0$. Ils étudient les réalisations de ce processus, ou celles du processus résultant : $X_i = T_i - T_{i-1}$ pour $i \geq 1$, la durée entre deux défaillances successives.
Ces modèles définissent la croissance de fiabilité comme un processus de comptage des erreurs résiduelles dans le code caractérisé par sa fonction de valeur moyenne. Les paramètres de ces modèles sont usuellement estimés par la méthode du maximum de vraisemblance ou par la méthode des moindres carrés, d'autres travaux proposent de les évaluer par inférence bayésienne [42].
Soit $N(.)$ la fonction de comptage associée à ce processus qui est définit par 3.8, $N(t)$ est le nombre de défaillances observées pendant le temps t.

$$N(t) = \sum_{i \geq 0} \mathbf{1}(T_i \geq t) \quad (N(0) = 0) \tag{3.8}$$

Nous présentons ici les expressions des variables évaluées.

- La fonction de la valeur moyenne (MVF) : $M(t) = \mathbb{E}[N(t)]$
- Le taux instantané d'occurrence des défaillances au temps t :

$$\frac{dM}{dt}(t)$$

- La fiabilité du logiciel

$$R_t(s) = \mathbb{P}\left(N(t+s) - N(t) = 0 | N(t), T_1, \cdots, T_{N(t)}\right) \quad s \geq 0$$

- Le temps moyen avant une défaillance $MTTF(t) = \int_0^{+\infty} R_t(s)ds$

Le premier modèle construit par Jelinski et Moranda [38] spécifiquement pour la fiabilité des logiciels date de 1972. Ils font les hypothèses suivantes :

- Au départ de chaque test, le logiciel contient un nombre fini mais inconnu N de fautes.
- Chaque faute détectée est supprimée en un temps supposé négligeable, aucune faute n'est introduite au cours des différentes corrections.
- A chaque instant, l'intensité de défaillance conditionnelle est supposée être proportionnelle au nombre de fautes résiduelles :

$$\frac{dM}{dt}(t) = \Phi(N - N(t))$$

  avec $\Phi \in \mathbb{R}_+$ la constante de proportionnalité qui représente la qualité de corrections. Elle est constante au cours du temps et indépendante des fautes supprimées.
- Les paramètres N et Φ sont estimés par maximum de vraisemblance.

La simplicité des hypothèses de ce modèle fait qu'en pratique, elles ne sont jamais vérifiées [48]. A ces hypothèses trop simplistes s'ajoutent certains problèmes d'estimation des paramètres. En effet, sous certaines conditions techniques, l'estimateur de maximum de vraisemblance de N est infini ou complètement aberrant. Littlewood et Sofer [48] proposent alors une estimation des paramètres par inférence bayésienne.
Actuellement les processus choisis en majorité sont :

- soit des processus markoviens, principalement des processus de poissons homogènes, aucun débogage n'est alors effectué,

— soit des processus de poisson non homogènes (NHPP) lorsque le logiciel est modifié au cours du temps.

Nous pouvons faire un parallèle entre notre étude et les analyses de fiabilité des logiciels. En effet l'apparition d'un nouveau scénario et son insertion dans la base de connaissance peuvent être assimilées à l'apparition d'un bug puis à sa correction. Une fois enregistré le nouveau scénario ne sera plus jamais considéré comme nouveau. Il aura ainsi disparu de la liste inconnue des scénarios non rencontrés. L'adaptation d'un modèle de croissance peut potentiellement évaluer la probabilité d'apparition d'un tel scénario. Nous présentons d'abord les NHPP.

Les processus de poisson non homogènes reposent sur l'hypothèse que l'occurrence de la défaillance entre deux défaillances est proportionnelle au nombre d'erreurs résiduelles dans le programme. L'estimation des paramètres se fait par la résolution de l'équation différentielle (3.9).

$$\frac{dM(t)}{d(t)} = b(t)[a(t) - M(t)] \tag{3.9}$$

dont les fonctions $a(t)$ et $b(t)$ différent entre les modèles. Une augmentation de $a(t)$ entraîne une augmentation du nombre d'erreurs dans le logiciel. De même une augmentation de $b(t)$ augmente le taux de détection d'erreurs. Cette solution est donnée par l'équation (3.10)

$$M(t) = e^{-B(t)} \left[m_0 + \int_{t_0}^{t} a(\tau) b(\tau) e^{B(\tau)} d\tau \right] \tag{3.10}$$

avec $B(t) = \int_{t_0}^{t} b(\tau) d\tau$ et $M(t_0) = m_0$ est la condition marginale de l'équation (3.9) avec t_0 le temps initial du processus de débogage. La fonction de fiabilité est alors donnée par (3.11).

$$R(x|t) = e^{[-M(t+x)-M(t)]} \tag{3.11}$$

[64] donne une table non exhaustive des modèles NHPP, Table 3.1. On peut les classer en plusieurs catégories. Tout d'abord il y a des modèles de forme concave. Ils traduisent un taux de détection proportionnel au nombre de bugs restant dans le logiciel. La vitesse de détection des bugs est considérée comme constante. Il y a ensuite les modèle dits "S-Shaped". L'intensité de défaillance est une fonction en S du temps : d'abord la détection est lente puis les essais ciblent plus rapidement les défaillances et enfin les fautes se font plus rares et la détection ralentit. Enfin il y a des modèles plus complexes pour introduire des phases de déboggages imparfaites avec l'ajout de nouveaux bugs. D'autres encore tiennent compte de correction différée, de la dépendance entre les fautes, des paramètres environnementaux (modèles de Cox) , etc. Nous ne présenterons pas tous les modèles existants, ils sont très nombreux. Chaque modèle a été construit pour s'adapter au mieux au projet associé au logiciel voulu. Il n'y pas de règle préétablie pour la sélection du modèle. Le choix se fait empiriquement. A partir d'un échantillon déjà présent les prédictions des différents modèles sont comparées avec les résultats obtenus. On réalise une première élimination des modèles sur l'ensemble des données. Puis on vérifie sur un nombre plus faible de modèles, en enrichissant petit à petit l'echantillon, la vitesse de convergence des modèles et leur cohérence, pour en distinguer le "meilleur".

3.5.3 Modèles Concaves

3.5.3.1 Modèle de Duane

Le modèle de Duane [16] n'a pas été développé pour la fiabilité logicielle mais reste le plus utilisé dans ce domaine. Il est défini comme *le NHPP dont l'intensité est une puissance du temps* (3.12) [25].

$$M(t) = \alpha t^{\beta} \tag{3.12}$$

Il a la spécificité de ne pas seulement modéliser une croissance. La valeur de β modifie la monotonie de ce processus :

— si $\beta > 1$ alors $\frac{dM(t)}{d(t)}$ est croissante et la fiabilité est décroissante ;

— si $\beta < 1$ alors $\frac{dM(t)}{d(t)}$ est décroissante et la fiabilité est croissante ;

— si $\beta = 1$ alors $\frac{dM(t)}{d(t)}$ est constante et la fiabilité ne change pas.

3.5.3.2 Modèle de Goel Okumoto(G-O) ou Modèle exponentiel

Le choix du modèle repose sur les hypothèses suivantes. Tout d'abord il existe à l'instant initial un nombre aléatoire N de fautes résiduelles ayant pour espérance a. La correction de la défaillance est parfaite, elle n'introduit pas de nouvelles fautes. L'intensité de la défaillance est supposée proportionnelle au nombre de fautes encore incluses dans l'algorithme avec un facteur de proportionnalité b

$$M(t) = a(1 - e^{-bt}) \tag{3.13}$$
$$a(t) = a \tag{3.14}$$
$$b(t) = b \tag{3.15}$$

3.5.3.3 Modèle de Yamada avec débuggage linéaire

Ce modèle est construit en supposant un débuggage imparfait. L'introduction de nouvelles fautes est une fonction linéaire du temps de validation avec un taux fixe α. Le taux de détection d'erreur est constant.

3.5.4 Modèles S-shaped

3.5.4.1 Modèle Delayed S-shaped

Il est une modification du modèle G–O pour construire une courbe en S. Le logiciel contient à l'instant initial un nombre aléatoire N de fautes, dont l'espérance est a. Quand une défaillance survient, la faute incriminée est parfaitement corrigée et aucune nouvelle faute n'est introduite.

3.5.4.2 Pham–Nordmann–Zhang

Le débuggage est supposé imparfait. L'introduction de nouvelles fautes est une fonction linéaire du temps de validation et le taux de détection des erreurs est une fonction en S du temps.

3.5.5 Estimation des paramètres des modèles par inférence bayésienne

La bonne estimation de ces modèles demande un échantillon conséquent et donc d'avoir détecté au préalable un nombre important de bugs. Des méthodes par inférence bayésienne à la place du maximum de vraisemblance sont alors mises en place.
C'est en essayant de résoudre les problèmes d'estimation du modèle de Jelinski et Moranda que certains chercheurs ont utilisé les méthodes d'inférence bayésienne. Littlewood et Sofer [48] résolvent ces problèmes inférentiels en modifiant le modèle. Ils introduisent un nouveau paramètre $\lambda = \Phi N$, la fonction intensité de défaillance a alors la forme suivante :

$$\frac{dM(t)}{d(t)} = \lambda - \Phi N(t)$$

Ils choisissent des lois *a priori* Gamma pour les paramètres positifs λ et Φ, et donnent sous ces hypothèses les expressions de la fiabilité *a posteriori*, la loi *a posteriori* du taux de défaillance courant, ainsi que la loi *a posteriori* du nombre résiduel d'erreurs. Plus récemment Yin et Trivedi [87], Kuo et Yang [42] présentent des méthodes d'estimation plus efficaces par inférence bayésienne pour des modèles NHPP tel le modèle de Goel Okumoto ou des modèles "S-Shaped".

Une mise à jour des paramètres des modèles n'est rendue possible qu'après l'apparition d'un nouveau bug. Elle ne tient pas compte de la dernière durée pendant laquelle aucune défaillance n'a été observée. Pourtant lorque le nombre de défaillances est très rare elle peut donner une information importante sur la probabilité d'apparition d'une prochaine défaillance. Les modèles bayésiens tirent partie de cette donnée. Nous détaillons le plus connu, le modèle de Littlewood-Verral.

3.5.6 Modèles bayésiens

Les modèles bayésiens prennent une position subjective pour prédire la fiabilité des logiciels. La fiabilité d'un logiciel doit croître si aucune défaillance n'est observée. Les modèles sont alors alimentés de deux types d'information, le nombre de fautes détectées et le temps cumulé de bon fonctionnement. De plus des informations *a priori* sur des projets ou algorithmes précédant l'étude et proche du logiciel étudié enrichissent la prédiction bayésienne.
Littlewood-Verral [49] reprennent bien ces hypothèses. Ils supposent également que les corrections réalisées ont une efficacité aléatoire, elles peuvent soit améliorer soit altérer le logiciel. Pour rendre compte de ce phénomène, la distribution du temps de défaillance est exponentielle avec un taux aléatoire. La distribution de ce taux est donnée *a priori* par une loi gamma. On obtient alors la forme du modèle à partir de 3 paramètres α, β_0, β_1 (3.16) [24]

$$\frac{dM(t)}{d(t)} = \frac{(\alpha - 1)}{\sqrt{\beta_0^2 + 2\beta_1 t(\alpha - 1)}} \tag{3.16}$$

Nom du modèle	**Forme de la courbe**	**MVF (m(t))**	**commentaires**
Duane	Concave	$M(t) = \alpha t^{\beta}$	
Goel–Okumoto (G–O) ou modèle exponentiel	Concave	$M(t) = a(1 - e^{-bt})$ $a(t) = a$ $b(t) = b$	taux de détection constant déboggage parfait nombre de défaillances fini
Delayed S-shaped	S-shaped	$M(t) = a[1 - (1 + bt)e^{-bt}]$	
Inflection S-shaped	S-shaped	$M(t) = \frac{a(1-e^{-bt})}{1+\beta e^{-bt}}$ $a(t) = a$ $b(t) = \frac{b}{1+\beta e^{-bt}}$	G-O si $\beta = 0$
Yamada exponential	S-shaped	$M(t) = a\left(1 - e^{-r\alpha[1-exp(-\beta t)]}\right)$ $a(t) = a$ $b(t) = r\alpha\beta e^{-\beta t}$	
Yamada Ohba Osaki	S-shaped	$\frac{dM(t)}{d(t)} = ab^2te^{-bt}$ $a \in \mathbb{R}^+$ $b \in \mathbb{R}^{+*}$	taux de panne gamma
Musa Okumoto	Concave	$M(t) = a\ln(1 + bt)$	taux de panne géométrique nombre de défaillances infini
Yamada Rayleigh	S-shaped	$M(t) = a1 - e^{-r\alpha[1-exp(-\beta\frac{t^2}{2})]}$ $a(t) = a$ $b(t) = r\alpha\beta e^{-\beta\frac{t^2}{2}}$	
Yamada débuggage exponentiel	Concave	$M(t) = \frac{ab}{\alpha+b}(e^{\alpha t} - e^{-bt})$ $a(t) = ae^{\alpha t}$ $b(t) = b$	taux de détection constant introduction de bugs exponentielle
Yamada débuggage linéaire	Concave	$M(t) = a(1 - e{-}bt)(1 - \frac{\alpha}{b}) + \alpha at$ $a(t) = a(1 + \alpha t)$ $b(t) = b$	taux de détection constant introduction de bugs linéaire
Pham–Nordmann –Zhang	S-shaped et concave	$M(t) = \frac{a(1-e^{-bt})(1-\frac{\alpha}{b})+\alpha at}{1+\beta e^{-bt}}$ $a(t) = a(1 + \alpha t)$ $b(t) = \frac{b}{1+\beta e^{-bt}}$	
Pham–Zhang	S-shaped et concave	$M(t) = \frac{1}{1+\beta e^{-bt}}\left[(c + a)(1 - e^{-bt}) - \frac{a}{b-\alpha}(e^{-\alpha t} - e^{-bt})\right]$ $a(t) = c + a(1 - e^{-\alpha t})$ $b(t) = \frac{b}{1+\beta e^{-bt}}$	introduction de bugs exponentielle

TABLE 3.1 – Liste des modèles de NHPP usuels

3.5.7 Sélection du modèle dans notre contexte

Les analyses de croissance sont multiples et diverses. Elles s'adaptent au problème souhaité. La sélection peut se faire à partir d'hypothèse sur le déroulement du projet mais en pratique le modèle est choisi empiriquement après analyses des temps d'apparition des premiers bugs.
Dans le cadre de notre étude, il faudrait attendre d'obtenir de premiers résultats pour appliquer un modèle approprié. Cependant plusieurs hypothèses conviennent mieux pour expliquer l'apparition de scénarios nouveaux. Premièrement, il sera difficile d'accélérer la recherche compte tenu de la non connaissance actuelle du système. Un modèle exponentiel à taux de détection constant semble préférable. D'autre part le notion de débogage imparfait n'a pas vraiment de sens dans la détection de scénario. Une fois détecté il est connu et n'est alors pas remplacé par un nouveau scénario. Notre choix s'oriente naturellement vers un modèle exponentiel de type Goel-Okumoto.

3.6 Conclusion

L'évolution temporelle d'un système dynamique est représentée dans la littérature par un processus stochastique. La fiabilité peut ainsi en être déduite par propagation des incertitudes. Le modèle probabiliste décrivant le processus est constitué de toutes les connaissances acquises du problème étudié. Pour construire ce processus, un découpage séquentiel d'un parcours type avec le véhicule autonome est élaboré de façon à obtenir un modèle simple en adéquation avec le problème posé. Il en résulte une chaîne de Markov. Parce qu'aucune information n'est disponible sur le sujet, ce modèle peut être remis en cause et devra être réadapté, après retour d'expériences. Les connaissances sont trop minces pour garantir un modèle représentatif. D'une part, du fait de la grande variabilité de l'environnement du véhicule autonome, les estimations des paramètres obtenus par analyses des données collectées peuvent être imprécises. Pour tenir compte de ces incertitudes et mieux qualifier la fiabilité du véhicule autonome les paramètres sont représentés par des variables aléatoires et sont évalués par inférences statistiques qui peuvent être soit fréquentistes soit bayésiennes. Compte tenu des valeurs à estimer (des probabilités très petites ou au contraire très proches de un), les méthodes fréquentistes requièrent une quantité de données très importantes pour donner des estimations pertinentes de ces paramètres. Les méthodes bayésiennes, qui ajoutent dans l'évaluation les connaissances des experts, peuvent donner plus rapidement une bonne estimation de ces paramètres et ont été sélectionnées dans notre étude. Ainsi les distributions des variables aléatoires caractérisant les paramètres sont données *a priori* avec les connaissances disponibles et seront actualisées par une procédure bayésienne avec la collecte de nouvelles données tout au long des essais de validation.
D'autre part, la non connaissance de certains scénarios doit pénaliser la fiabilité du système. Cette fiabilité va augmenter avec l'enrichissement de la base de connaissance dès qu'une nouvelle classe de scénario est identifiée. Des incertitudes dites épistémiques sont alors introduites. Elles peuvent être associées à des éléments déterministes sous formes d'intervalles ou d'ensembles incertains. Mais elles peuvent également être aléatoires. L'accroissement de la fiabilité peut se rapprocher des modèles de croissance de fiabilité des logiciels. Ceux-ci contribuent à l'élaboration d'éléments correcteurs adaptant le modèle et apportant ainsi un meilleur reflet de la confiance que l'on peut donner au système à chaque étape de validation.
Cette représentation du problème pose un cadre pour la composition d'un plan de validation. Les roulages peuvent être organisés dans le but de réduire efficacement les incertitudes épistémiques.

La durée des essais pourrait en être écourtée. Après analyse de différentes stratégies d'échantillonnage, les procédures itératives semblent les plus adaptées pour organiser les essais que ce soit des essais numériques ou réels. En effet avec un apport de connaissance les essais peuvent être dirigés pour sélectionner les scénarios qui précisent le mieux la fiabilité du système. Les essais aléatoires restent néanmoins très importants pour modifier la modélisation du problème qui risque d'être erronée en début de validation.

Chapitre 4

Objectifs de la thèse

L'homologation en sécurité du véhicule autonome est primordiale pour sa mise en service opérationnelle. Ce véhicule présente la particularité d'être entièrement responsable de la sécurité de ses passagers par l'intermédiaire de ses décisions de conduite ne faisant pas intervenir le conducteur. Valider ces objectifs, en conséquence très sévères, est difficile à réaliser.
Le véhicule autonome, pour réaliser l'ensemble des fonctionnalités complexes qui lui sont imposées, intègre de nombreuses technologies différentes. La diversité, le nombre et la performance de celles-ci en assurent la sécurité. Une fois fusionnées, les informations qu'elles fournissent peuvent être mal interprétées par le système. Il en résulte des événements indésirables pour le client.

Le domaine de fonctionnement de ce système de grande dimension et fortement variable est encore mal connu. De plus l'évolution très rapide de ces nouvelles technologies empêche de bien les appréhender. En conséquence, le système est encore nouveau et les retours d'expériences obtenus à partir des différents systèmes d'aide à la conduite ne permettent pas d'identifier tous ses modes de fonctionnement ni de défaillance lors de la spécification du besoin.
Dans le domaine de l'automobile, la définition des exigences de sûreté et leurs vérifications suivent une procédure descendante puis ascendante pour valider étape par étape le système à chaque niveau d'intégration des composants et sous-systèmes jusqu'à arriver à la validation du système complet. La certification finale du système est effectuée à partir d'un dernier plan de validation permettant d'aider à garantir une fiabilité globale au moins égale au niveau souhaité. Il consiste à faire rouler le véhicule dans un univers stressant comportant tous les événements pouvant déclencher des défaillances du système.

La méconnaissance de ces événements rend la conception d'un tel plan impossible au début de la phase de validation. La certification du système AD requiert d'abord d'enrichir la base de connaissance pour mettre en évidence tous les modes de défaillances du système et des événements amenant à celles-ci. Le système ne sera attesté fiable que lorsque la base de connaissance aura été jugée "complète" ou suffisamment représentative de son environnement et que le bon fonctionnement du système aura été validé dans cette base.
Pour garantir une durée d'essais respectant la date de mise sur le marché, Renault envisage de concevoir un plan de validation final qui combine des roulages sur route ouverte, des roulages numériques et des essais sur piste. L'organisation de ce plan doit être associée à une méthode d'évaluation de la fiabilité. Les méthodologies proposées dans la littérature sont soit trop coû-

teuses soit insuffisantes pour évaluer la fiabilité d'un tel système.

La fiabilité du système de perception et de décision évalue la confiance que l'on peut accorder au système à la fin de chaque étape de validation. Elle apporte une mesure de l'état de connaissance du bon fonctionnement du système dans tous les scénarios de conduite contenus dans le domaine de fonctionnement.
La modélisation de la fiabilité doit reproduire l'évolution dynamique du système pendant son utilisation. Celle-ci est couramment représentée par un processus stochastique. Les paramètres de ce modèle sont incertains, et devront être précisés avec l'accroissement de connaissance. Ce modèle est de plus incomplet. Certains scénarios ne sont pas connus et seront détectés pendant les roulages de validation. Le modèle de fiabilité est pénalisé pour se prémunir d'une conséquence intempestive de la rencontre d'un scénario inconnu. Il provient d'hypothèses caractérisant bien la procédure de validation. Cette pénalisation décroît avec l'enrichissement des connaissances.

L'objectif de cette thèse est de proposer une modélisation de la fiabilité du système et de contribuer à l'élaboration d'un plan de validation final permettant d'estimer la fiabilité et d'enrichir efficacement la base de connaissance du problème. Parce qu'aucune démarche de validation n'est rendue publique, cette thèse doit proposer une méthodologie générale de validation qui doit être vue comme une feuille de route par Renault. La mise en oeuvre des étapes et essais de validation présentés restera à réaliser par Renault. De plus le modèle de fiabilité choisi reste un premier prototype qui devra être poursuivi et réadapté au contexte.

L'étude bibliographique permet d'initier une première organisation possible du plan de validation et apporter de premières solutions de modélisation : Pour modéliser la fiabilité du véhicule autonome, un parcours d'une durée donnée est découpé en successions de scénarios rencontrés par le système. Ce sont de courtes séquences temporelles dans lesquelles les actions des usagers sont bien définies. Ces scénarios sont rangés dans des classes nommées cas d'usage. L'enchaînement des classes est modélisé par une chaîne de Markov à états finis, choisie pour sa simplicité et son adéquation avec le problème étudié. La fiabilité peut ainsi être évaluée.

L'évaluation des paramètres de ce modèle est entâchée d'incertitudes compte tenu de la forte variabilité et la grande dimension du domaine de fonctionnement. Ces incertitudes peuvent être évaluées par inférences statistiques bayésiennes ou fréquentistes. Les paramètres mal connus, jusqu'alors déterministes, sont remplacés par des variables aléatoires. Les distributions de ces variables décrivent la vision subjective des acteurs du projet du problème étudié. Elles seront actualisées par une procédure bayésienne avec la collecte de nouvelles données.

Les incertitudes épistémiques liées à la non connaissance de certains scénarios de conduite doivent être prises en compte pour ajuster le modèle de fiabilité susceptible d'être erroné. Des méthodes probabilistes ou non probabilistes propagent ce type d'incertitude pour retranscrire l'impact du manque de connaissance sur la confiance à donner au système. Les méthodes probabilistes ont été privilégiées. Un modèle de croissance de fiabilité des logiciels représente bien l'accroissement de connaissance avec l'apparition de nouveaux scénarios et sera intégré au modèle. Son choix se fait empiriquement, à partir de la vitesse d'apparition des cas d'usages déjà détectés. Néanmoins, dans notre étude nous préférons partir du modèle de Goel-Okumoto. En effet les hypothèses nécessaires à ce dernier modèle semblent être en adéquation avec le problème.

Enfin une méthode itérative d'échantillonnage est envisagée pour sélectionner les points d'intérêt dans le domaine de recherche, c'est-à-dire ceux pour lesquels la réduction des incertitudes a le plus d'effet sur l'évaluation de la fiabilité.

Deuxième partie

Contribution de la thèse

Chapitre 5

Introduction

La certification de la fiabilité du véhicule autonome devrait passer par la construction d'un plan de roulage de validation représentatif de l'ensemble des conditions d'usage de celui-ci. Cette validation fait face principalement à deux challenges qui sont de l'ordre de l'évaluation des technologies et, étant donnée la recherche du niveau complet d'autonomie, de l'évaluation de la connaissance de l'ensemble de l'environnement dans lequel évoluera le véhicule autonome. Aujourd'hui, au vu des efforts de l'ensemble des acteurs du véhicule autonome, les choix de technologies associés aux algorithmes de traitement de l'information arrivent à un certain niveau de stabilité. Il n'en reste pas moins qu'il est nécessaire d'en évaluer leurs performances fiabilistes par rapport aux différentes situations préalablement identifiées. Sur le second point de la connaissance de l'environnement, la question reste ouverte et la fiabilité du véhicule autonome ne sera totalement démontrée qu'au fur et à mesure des usages, en phase d'exploitation même du véhicule, avec l'identification de nouvelles configurations de conduite jusqu'alors non imaginées. L'un des objectifs du plan de validation sera donc l'estimation du niveau d'exhaustivité de la base de connaissances liées aux situations de roulage que rencontrera le véhicule autonome.

Il est tout à fait raisonnable de penser que le plan de validation sera constitué de séquences de roulage et que les systèmes et algorithmes de décision seront éventuellement actualisés en fonction aussi des situations rencontrées. Par ailleurs, les premiers résultats permettront eux-mêmes de définir les séquences à venir du plan de validation. Nous nous positionnons dans une approche séquentielle d'un plan de roulage.

Dans un tel contexte, plusieurs questions peuvent être soulevées. La première question peut être liée à la validité de la notion de fiabilité qui est traditionnellement définie en fonction de conditions de fonctionnement bien établies. D'autres questions pourraient être liées plus à la méthodologie même de la construction du plan de validation avec notamment le choix des roulages à venir ainsi que le critère d'arrêt qui devra permettre d'évaluer le niveau de certitude ou de confiance sur le niveau de complétude de la base de connaissance alors acquise.

Le nombre de fonctionnalités et le degré d'autonomie et de délégation de ces véhicules augmenteront graduellement au cours des prochaines années avec la sortie de nouveaux véhicules toujours plus innovants. La diversité des véhicules à valider et le time-to-market réduit pour répondre à la concurrence, qui restreint le temps de validation, amène à utiliser des moyens de validation moins

chronophages et plus contrôlables que des roulages sur route ouverte. Les simulations numériques jusqu'alors utilisées localement pour aider à la conception dans des configurations de conduite précises, sont en cours d'amélioration pour être utiliser de manière "industrielle" et servir non seulement à la mise au point mais également à la validation du système. Les essais sur piste, largement utilisés pour la validation des systèmes mécaniques des véhicules, sont également à adapter pour servir à la validation des ADAS et des AD. Ces essais sont complémentaires. Ils apportent de l'information sur le fonctionnement du système dans son environnement qui n'est plus complètement une boîte noire. Cette connaissance partielle n'est actuellement pas utilisée pour dimensionner et organiser le plan de validation afin d'estimer la fiabilité du véhicule autonome. Les informations apportées par chaque type d'essai ne sont pas reliées dans une base de connaissance commune.

L'objectif de cette thèse est de proposer une méthode générale qui organise les essais de validation dans le but d'estimer avec précision la fiabilité du véhicule autonome. Elle complète les méthodes traditionnelles de sûreté et se positionne à la toute fin des étapes de validation, avant les tests réalisés avec les clients. Une première organisation générale du déroulement itératif de la validation, comprenant des roulages sur route ouverte, des tests sur piste ou des tests numériques est détaillée dans le chapitre 6. Cette démarche s'appuie sur le niveau de connaissance acquis à une étape de validation. Elle recherche les zones dans l'espace des scénarios du domaine de fonctionnement encore mal spécifiées et pour lesquelles le comportement du véhicule est incertain. Cette démarche est une feuille de route pour l'entreprise. Pour chaque type d'essai et chaque étape de la démarche, des manières de procéder sont suggérées. Pour s'assurer de la faisabilité de certaines étapes, des études ont été menées avec des niveaux d'approfondissement différents. En particulier une méthode de sélection des scénarios numériques est proposée pour tester efficacement le véhicule autonome, et des modèles d'erreur capteurs sont proposés pour améliorer le niveau de réalisme des simulations numériques. Ces derniers résultent d'analyse d'essais sur piste. La méthode décrite dans ce document est un premier concept à adapter aux systèmes étudiés. Par conséquent aucun dimensionnement d'un plan de validation, *i.e.* une quantification de la durée des essais réels ou numériques, n'est apporté.

La modélisation et formalisation du déroulement d'un parcours de validation avec le véhicule autonome rassemblent les résultats obtenus dans chaque type d'essai en une base de connaissance. Pour un niveau d'information donné il est possible d'évaluer la fiabilité du système AD avec une marge d'erreur. L'objectif de ce chapitre 7 est de proposer un cadre de modélisation pour réduire la marge d'erreur en "temps réel".
Les modèles de fiabilité traditionnels caractérisent le bon fonctionnement du système pendant une durée dans un domaine bien défini dont les variabilités sont connues mais aléatoires. Ces modèles doivent être adaptés pour évaluer les incertitudes liées à la base de connaissance.

Le modèle de fiabilité est une aide à la décision. Il peut contribuer à la planification des futurs essais ou à programmer la fin des essais quand le système est jugé suffisamment fiable. Il est choisi modulaire pour être ré-adapté au véhicule à valider.

La démarche de validation et le comportement du modèle établi sont illustrés à l'aide d'exemples théoriques dans le chapitre 8. De nombreux cas tests ont été réalisés dans le but d'évaluer l'effi-

cacité de la méthode et de développer des idées d'analyses pour aider à la décision. Par exemple il peut aider à la planification des futurs essais de validation. Il peut détecter les paramètres influents pour lequel une étude plus approfondie est nécessaire. Il permet d'évaluer le risque d'un arrêt trop précipité des essais de validation.

Chapitre 6

Méthodologie générale de validation de la fiabilité

6.1 Introduction

Les méthodes actuelles de sûreté de fonctionnement, dans les différents domaines et en particulier en mécatronique et informatique, sont adaptées à des systèmes bien définis dont les modes de fonctionnement et de défaillances sont bien connus et anticipés. Les métriques et critères classiques de sûreté garantissent une bonne qualité et la sécurité du système. Les essais en phase de validation, permettant d'évaluer l'ensemble des métriques, sont réalisés après la phase de conception sur un système proche du système final de définition technique figée. Le caractère novateur du véhicule autonome entraîne une problématique bien différente. Ce système reste encore mal connu et de nouveaux modes de fonctionnement sont découverts pendant les essais de roulage. La conception des exigences de fonctionnement et de sécurité, la définition technique (ensemble des capteurs et leurs positionnements dans le véhicule), et même les algorithmes des capteurs de fusion et de décision évoluent avec la découverte de nouveaux scénarios. Ces scénarios sont vus comme de nouvelles combinaisons de paramètres et d'interactions entre les automobilistes. Pendant la période de validation, la découverte de nouveaux scénarios ne sera pas terminée. Validation et mise au point se trouvent entremêlées. Comme nous l'avons énoncé à plusieurs reprises dans ce document, il n'est pas réalisable ni même nécessaire d'essayer le véhicule sur l'ensemble des scénarios du domaine de fonctionnement. L'objectif est d'effectuer un ensemble d'essais réduit qui englobent toutes les utilisations possibles avec le véhicule autonome. Alors la fiabilité, prédite à partir de l'analyse du système dans les usages testés, peut être considérée égale à celle du système dans le domaine complet. Il n'est cependant pas possible en début de validation d'établir et de décrire tous les protocoles d'essais à réaliser pendant la phase de validation. Ils dépendent du niveau de connaissance à l'instant présent et seront réadaptés après acquisition de nouvelles données sur le système.

Une procédure de validation itérative est présentée dans ce chapitre. Elle a pour objectif de réduire les essais de validation en les comparant à des essais purement aléatoires. Elle qualifie étape après étape, la fiabilité du véhicule autonome et donne ainsi une indication sur l'état d'avancement de la procédure de validation. Elle utilise les moyens disponibles au sein de l'en-

treprise : outils de simulations numériques et tests "physiques". Chaque type de roulage a ses avantages et inconvénients, pour la validation du véhicule autonome, détaillés dans la première section de ce chapitre. Les types de roulage se complètent.

Afin d'effectuer des essais de validation moins longs qu'un roulage purement aléatoire, la démarche s'appuie sur 7 axes :

1. Une base de connaissance rassemble et organise l'ensemble des scénarios connus en cas d'usage pour représenter l'usage du véhicule.
2. Les cas d'usage contribuent à la fiabilité du système et leurs contributions sont évaluées séparément. On estime d'une part les probabilités des usages possibles avec le véhicule autonome, et d'autre part la probabilité de défaillance du système dans chaque cas d'usage.
3. Une grande partie des roulages sur route ouverte est remplacée par des roulages numériques.
4. Les scénarios simulés sont choisis itérativement pour expliquer plus rapidement les zones de défaillance.
5. Pour assurer la représentativité des résultats obtenus en simulation, ces roulages sont calibrés ou enrichis à l'aide d'une étude du comportement du véhicule autonome sur piste.
6. Les roulages sur route ouverte, ne seront pas tous aléatoires. Le véhicule sera également testé dans des conditions spécifiques déterminées à l'aide des résultats obtenus avec les simulations. Ces roulages doivent être choisis pour préciser plus rapidement la fiabilité estimée.
7. Enfin une démarche itérative permet de redéfinir étape après étape les essais à réaliser afin de préciser l'estimation de la fiabilité. Cette estimation servira de critère d'arrêt quand elle sera supérieure à l'objectif de fiabilité souhaité et que son évolution se stabilisera.

Il n'est pas possible de tout traiter en trois ans de thèse. L'ensemble des axes, sur le plan des méthodes, sont analysés avec des niveaux d'approfondissement différents. Ils sont avancés sur certains points ou plus à titre de recommandations prospectives. Nous décrivons dans la seconde section la méthode générale proposée et détaillerons en troisième section chaque axe en donnant des perspectives sur les études à mener pour les développer.

6.2 Moyens d'essais disponibles pour la validation du véhicule autonome

Le chapitre 2 a donné un aperçu des moyens disponibles utilisés actuellement pour valider les systèmes d'aide à la conduite. Nous classons en 4 catégories les types de roulages possibles pour tester le véhicule :

1. Les roulages "aléatoires" sur route ouverte réalisés par un client lambda ou un professionnel
2. Les roulages numériques
3. Les roulages "ciblés" sur route ouverte effectués par un professionnel
4. Et les roulages sur piste.

6.2.1 Roulage aléatoire sur route ouverte

1. **Objectif et description**
   Un roulage sur route ouverte pour tester le véhicule autonome, est un parcours choisi parmi les routes habilitées et les conditions d'utilisation autorisée avec le véhicule mode AD activé. Ce test doit être exécuté par des professionnels formés, vigilants et prêts à reprendre en main le véhicule. Mais il peut être également effectué en prêtant le véhicule à des potentiels clients également formés pour gérer le système. Il permet à lui seul d'estimer la fiabilité du système et de valider le véhicule autonome.
   Toutes les données communiquées entre les différents organes électroniques du véhicule sont enregistrées à chaque instant de la conduite. Ces enregistrements sont des "dump"(données brutes enregistrées), qui sont ensuite intégrées dans une base SQL sous formes d'objets observés. On parle de données temporelles. Les enregistrements seront analysés en post-traitement pour vérifier le bon comportement du système et pour identifier les différents scénarios de conduite observés par le véhicule.

2. **Applicabilité et limites**
   Ces roulages permettent de collecter un maximum d'informations sur le comportement réel du véhicule autonome. Toutes les conditions réelles, et les facteurs pouvant perturber le système sont réunis. Il permet de vérifier le comportement du système dans chaque configuration de conduite qu'il rencontre. Les résultats de ces analyses sont totalement fiables.
   Si le système est de plus conduit par des clients, les conditions et fréquences d'usages sont respectées car elles permettent d'observer de nouveaux scénarios de conduite, d'analyser des modes de défaillance non identifiés lors de la phase de spécification du besoin.

   Ces roulages sont très coûteux. Les véhicules instrumentés sont conçus sous forme de prototypes. Les enregistrements de ces roulages sont revisionnés et analysés ce qui peut prendre plus de temps que le roulage lui-même. Enfin les données collectées sont ensuite stockées dans des grandes bases de données de plus d'une dizaine de péta octets qui doivent être entretenues et conservées un long moment(10 ans).
   L'inconvénient de l'aléa est, par définition, l'impossibilité de contrôler les scénarios et configurations à rencontrer. Les scénarios, qui sont observés pour des systèmes très fiables comme le véhicule autonome, apportent souvent peu d'information sur les limites de fonctionnement. Les scénarios les plus fréquents, sont très bien interprétés par le véhicule et très proches les uns des autres. Il faut attendre très longtemps avant de pouvoir observer des défaillances du véhicule.
   De plus il n'y a pas la possibilité d'avoir une vérité terrain, c'est-à-dire un système plus performant permettant de donner les "réelles" informations sur les scénarios rencontrés. La seule manière de détecter une défaillance du système est d'attendre que le professionnel ou le client reprenne la main jugeant le comportement de celui-ci trop dangereux. Ce sentiment reste très suggestif en fonction des individus.

   Des caméras de contexte en plus de tous les capteurs nécessaires pour le bon fonctionnement du système sont présentes. Elles permettront de mieux comprendre les enregistrements pendant les analyses de conduite pour détecter des scénarios entraînant un com-

portement anormal du véhicule. Cependant, la durée des essais est gigantesque. Il est impossible de tout re-visualiser en post traitement par la suite. Les séquences de roulage doivent être indexées pour la mise en place de requête. Pendant les roulages réalisés par les professionnels, il est possible d'annoter les données temporelles en ajoutant des informations de contexte. Un co-pilote est en effet également présent. Il est muni d'une tablette sur laquelle il appuie à chaque instant pour donner les conditions de route qu'il observe au moment présent. Les informations qu'il annote doivent être en nombre limité pour éviter les erreurs humaines. D'autres informations extérieures de contexte sont collectées ultérieurement à partir des données horaires et GPS, comme le type d'infrastructure, les conditions météo récupérées aux stations météo à proximité.

6.2.2 Roulages guidés sur route ouverte

1. **Objectif et description**
   L'objectif de ces roulages est de sélectionner un ensemble de parcours dits "enveloppes" contenant toutes les conditions perturbant le système AD non encore observées. La durée des essais est supposée plus petite que les roulages aléatoires.
2. **Applicabilité et limites**
   Le niveau de connaissance actuelle des systèmes AD dans leur environnement et la variabilité de l'environnement ne permettent pas de sélectionner ce type de parcours. Nous ne connaissons pas tous les fonctionnements du système ni les conditions qui amènent à des défaillances du système.

   Les roulages sur route ouverte sont encore très peu contrôlables. Les parcours dépendent de :
   — l'infrastructure que l'on peut bien cartographier mais pas modifier,
   — la météo qui est prévisible mais pas contrôlable,
   — des conditions de trafic très peu contrôlables et un peu prévisibles.
   Ces roulages sont réels. Une prise de risque pour observer une condition extrême de conduite n'est bien entendue pas envisageable.

6.2.3 Roulages numériques

1. **Objectif et description**
   Les roulages numériques semblent une bonne alternative aux roulages réels. De multiples modèles numériques existent pour simuler le comportement du véhicule autonome dans son environnement. Certains ont des hauts niveaux de réalisme mais se construisent encore manuellement pour analyser un comportement très précis, d'autres sont nettement moins réalistes mais sont plus rapides à calculer que le temps réel de roulage.
   Les logiciels de simulation utilisés au sein de l'entreprise jusqu'alors dédiés à une utilisation manuelle et peu automatisable sont améliorés pour générer automatiquement des scénarios. Ils sont générés par la construction de "scénarios type" appelés "cas d'usage". Pour un même cas d'usage une infinité de scénarios peut être générée en faisant varier des paramètres qui le décrivent.

2. **Applicabilité et limites**
   Le niveau de réalisme doit être suffisant pour que le comportement du véhicule en simulation permette de prédire avec un minimum d'erreurs le comportement réel du véhicule dans des configurations semblables. Comme nous l'avons présenté les simulations actuelles ne tiennent pas compte des éléments de l'environnement qui perturbent le fonctionnement des capteurs.
   Pour se servir de ces types de roulage dans l'évaluation de la fiabilité, il faut pouvoir générer automatiquement un très grand nombre de parcours types représentatifs des usages possibles avec le véhicule et vérifier si le système a été défaillant ou non pendant ces roulages. Or actuellement les simulations sont des scénarios indépendants les uns des autres. Ainsi, rien ne relie ces scénarios entre eux pour correspondre à un usage du véhicule.

6.2.4 Essais sur piste

1. **Objectif et description**
   Les roulages sur piste ont l'avantage d'être plus contrôlables que les essais sur route ouverte et peuvent les remplacer. En effet les scénarios de conduite sont simulés. S'ils sont trop dangereux, des objets factices, comme des pantins et des véhicules en toile, peuvent remplacer les véhicules et les êtres humains. De plus une vérité terrain est possible. La piste peut être entièrement cartographiée par une carte haute définition où la position de chaque élément est connu. Des systèmes de mesures tels que le GPS différentiel peuvent être utilisés pour localiser précisément le véhicule autonome. Cependant les objets mesurés doivent être distants au maximum de 200 m de la station de référence.
2. **Applicabilité et limites**
   Peu d'éléments de l'infrastructure sont disponibles, les scénarios de conduite ne sont pas tous reproductibles sur piste (ponts, bâtments, ...). Les conditions météorologiques sont autant contrôlables que sur route ouverte. De plus, tout comme les roulages numériques, les scénarios sont simulés indépendamment les uns des autres. Un parcours possible avec le véhicule ne peut pas être caractérisé par ce type d'essai.

La table 6.1 résume les différents avantages et inconvénients de chaque roulage.
Les différents roulages se complètent et peuvent tous contribuer à la certification du véhicule autonome. Cependant pour sélectionner les essais à réaliser avec chaque type de roulage il faut avoir une bonne connaissance de l'usage du véhicule autonome. Cette connaissance s'acquière grâce aux résultats des essais. Les essais peuvent être réorientés pour compléter cette connaissance avec un budget restreint.
Dans la section suivante nous présentons une méthodologie générale pour valider le véhicule autonome. L'objectif de cette méthodologie est de choisir les types de roulage au fur et à mesure du processus de validation à budget restreint.

6.3 Démarche de validation itérative pour mieux guider les roulages vers les zones incertaines avec un critère d'arrêt

Le dimensionnement d'un plan de validation unique, construit en début de phase de validation ne semble pas pertinent. L'apport de nouvelles connaissances modifie la modélisation imparfaite

	Roulage Numérique	**Roulage sur route ouverte effectué par un client lambda**	**Roulage sur route ouverte effectué par un professionnel**	**Roulage sur piste**
Réalisme	faible	très bon	très bon	moyen
Contrôlabilité	totale	aucune	très faible	moyenne
Coût et temps de roulage	le moins coûteux	très coûteux	le plus coûteux	assez coûteux
Représente l'usage client	non : ce sont des scénarios étudiés séparément	oui : il est identique à l'usage client	presque : seulement s'ils sont aléatoires	non : ce sont des scénarios étudiés séparément
Vérité terrain	oui : tout est connu	non : seuls les enregistrement de la voiture peuvent être récupérés	Très faible avec l'aide des opérateurs	oui avec la connaissance de la piste et d'outils de mesure plus précis
Accélération possible	oui : il est possible de cibler les zones encore incertaines	non	oui : si les roulages sont guidés et non aléatoires, cependant de nombreux paramètres ne sont pas contrôlables	oui : plus que des roulages sur route ouverte, mais certains paramètres ne sont pas contrôlable

TABLE 6.1 – Table de comparaison entre les différents roulages

du problème étudié et permet d'identifier les zones de l'environnement qui comportent le plus d'incertitudes. Une démarche itérative est préconisée pour la validation d'un tel système. Cette démarche ne peut pas uniquement comporter des roulages ciblés. Elle doit conserver des roulages aléatoires dans le cas où certains cas d'usage ou paramètres importants de l'environnement ne soient pas contenus dans la base de connaissance. Nous décrivons dans cette partie un déroulement possible des étapes de validation. Cette démarche doit être vue comme un processus pour l'évaluation et la validation d'un véhicule autonome sachant qu'aujourd'hui le produit n'est pas mûr. Elle est un point de départ avant l'apparition d'un procédure réglementaire imposée par les "autorités". Les contributions de chaque type d'essai sont détaillées séparément.

6.3.1 Rôle des roulages réels sur route ouverte avec le véhicule autonome

A fréquence régulière (hebdomadaire, mensuelle, etc..) les données collectées pendant les essais réels sur route ouverte avec le véhicule autonome sont analysées. Pendant le post-traitement, les scénarios observés sont rangés et indexés par les cas d'usage qui les caractérisent. C'est à cette étape que de nouveaux cas d'usage sont détectés. La base de connaissance est alors enrichie. Les enchaînements entre les cas d'usages sont comptés pour remettre à jour leur probabilité d'occurrence. Le bon comportement du véhicule dans chaque cas d'usage rencontré est vérifié pour remettre à jour les probabilités de défaillance. Enfin l'apparition de nouveaux cas d'usage peut aider dans la prédiction de futurs cas d'usage comme cela sera présenté dans le chapitre 7. Le schéma 6.1 présente ces étapes.

6.3.2 Rôle des roulages numériques

Les roulages numériques complètent les études, Figure 6.2. Ils permettent d'une part de resimuler les scénarios déjà enregistrés lorsqu'une modification de l'algorithme a été nécessaire. D'autre part, ils prédisent le comportement du véhicule dans d'autres scénarios non observés qui sont ajoutés à la base de connaissance. Lorsqu'un nouveau cas d'usage est détecté, il est alors numérisé en un cas d'usage numérique, ce qui accroît la connaissance. L'analyse des roulages numériques peut permettre de guider les roulages réels vers des zones encore jugées incertaines pour enrichir la base de connaissance plus efficacement.

6.3.3 Rôle des essais sur piste

Si les roulages numériques, dans certaines situations, ne sont pas réalistes et si une combinaison n'est pas présente en roulage sur route ouverte, les roulages sur piste permettent de reconstruire ces combinaisons jugées manquantes et ainsi contribuent à l'évaluation de la probabilité de défaillance. Comme nous l'avons vu dans la section 6.4.5, ces roulages peuvent également aider à la calibration des roulages numériques et à l'amélioration de ces roulages pour les rendre plus représentatifs de la réalité, Figure 6.3.

6.3.4 Rôle des informations externes

D'autres données sont disponibles pour estimer la fréquence d'appariton des cas d'usages. Tout véhicule suffisamment instrumenté peut contribuer à cette évaluation. Plusieurs projets

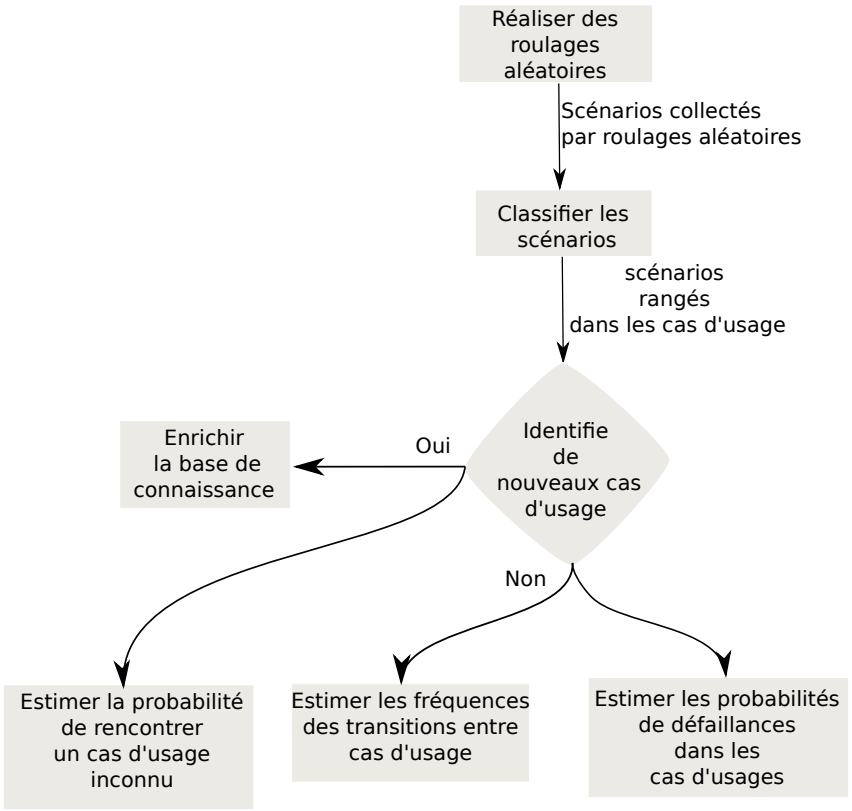


FIGURE 6.1 – Rôle des roulages réels aléatoires

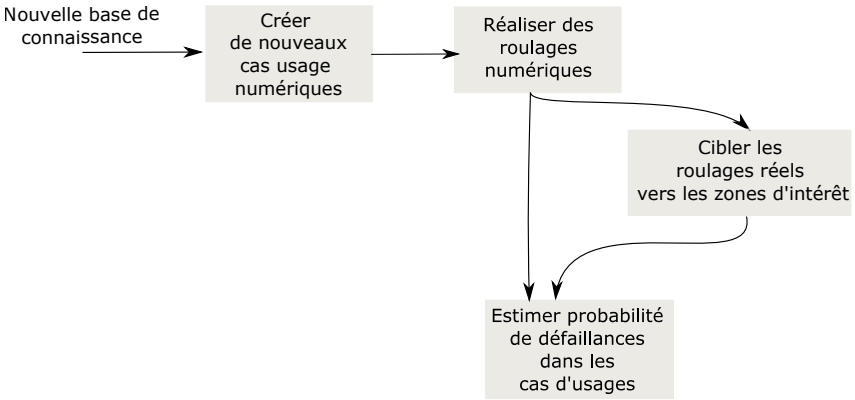


FIGURE 6.2 – Rôle des roulages numériques

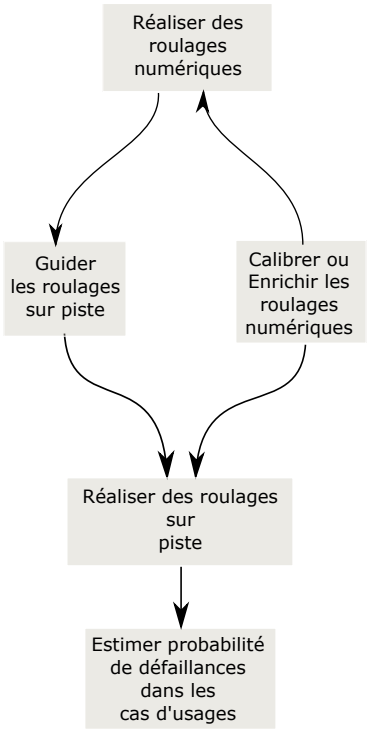


FIGURE 6.3 – Rôle des essais sur piste

européens, comme le projet MOOVE, ont été lancés dans le but de collecter des données pour les acteurs du véhicule autonome. Celles-ci ont l'avantage d'être proches des données communiquées par le système de perception et de décision. Ainsi le calcul des fréquences d'apparition pourra être réalisé sur ce type de données sans un grand effort d'adaptation. Les roulages naturalistiques sont riches d'information. D'autres sources telles que les statistiques météorologiques, ou les cartes des routes habilitées enrichissent ces estimations. Enfin d'autres données extérieures comme les caméras de surveillance des autoroutes ou toutes sources de données apportent des renseignements sur les cas d'usage et leurs fréquences. Certains cas d'usage très rares et inconnus seront potentiellement identifiés si l'ensemble de ces données sont analysées. Leur rôle est schématisé dans la Figure 6.4. Ces données peuvent aider à estimer les fréquences d'apparition des cas d'usage. Les analyses proposées sont à sélectionner en fonction de leur pertinence et du temps nécessaire pour collecter et traiter les différentes données. Elles sont données à titre d'exemple.

6.3.5 Evaluation de la fiabilité à chaque étape de la validation et critère d'arrêt

Enfin à chaque étape de la validation, la fiabilité est estimée à partir de (Figure 6.5) :
— la fréquence d'apparition des cas d'usages,
— la probabilité de défaillance dans ces cas d'usages
— et la probabilité d'apparition d'un cas d'usage inconnu.

La méthode d'estimation est présentée dans le chapitre 7. Cette fiabilité se précisera au fur et à mesure des estimations.

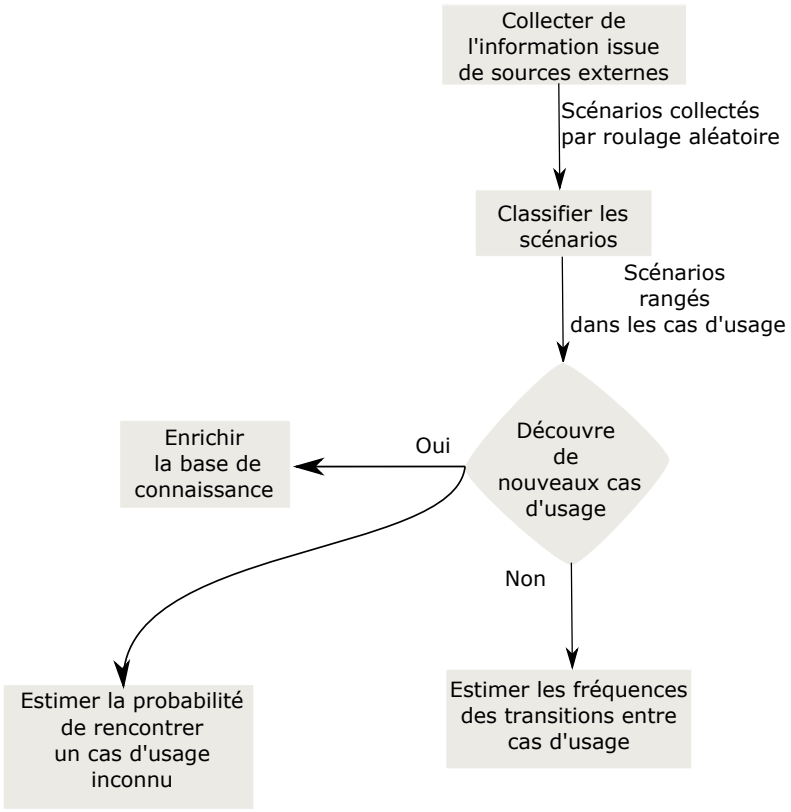


FIGURE 6.4 – Rôle des informations externes

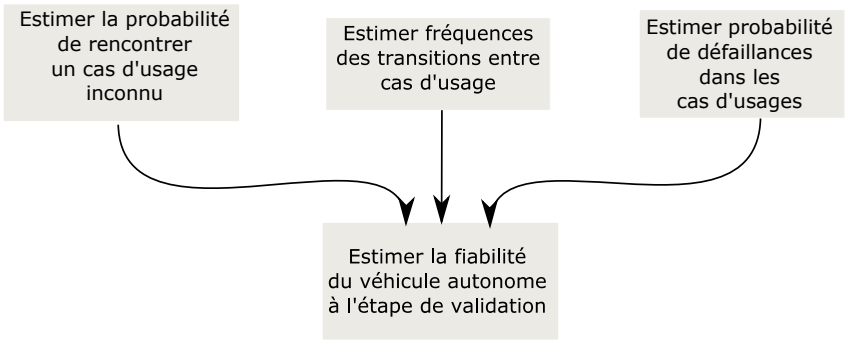


FIGURE 6.5 – Estimation de la fiabilité à chaque étape

Ce modèle de fiabilité va aider à la conception d'un critère d'arrêt des essais de validation. Tant que la fiabilité estimée reste imprécise et diffère beaucoup d'une itération à l'autre alors une nouvelle étape de validation est lancée. Si la variation de la fiabilité diminue et si cette fiabilité converge vers une valeur supérieure à l'objectif alors le système est supposé atteindre l'objectif de fiabilité souhaité. Nous verrons dans le chapitre 8 l'évolution du modèle en fonction des étapes de validation et de l'acquisition d'une nouvelle donnée dans un cas test théorique. Nous présenterons les performances et les limites d'utilisation du modèle, pour connaître les précautions à prendre avant d'autoriser l'arrêt de la procédure. L'analyse de la fiabilité estimée peut contribuer à guider les roulages de validation et cibler les zones encore incertaines dans le domaine de fonctionnement. Nous ne développerons pas de méthodologie à ce sujet mais nous présenterons dans un exemple le potentiel d'une telle procédure pour réduire les essais de validation.

Le Figure 6.6 résume l'ensemble des étapes à réaliser à chaque étape de la procédure de validation itérative. Les couleurs des blocs représentent la degré d'approfondissement des analyses des axes de la démarche, effectuées pendant cette thèse. En rouge, les méthodes sont peu ou pas étudiées. En vert, les méthodes ont été le plus travaillées. La section suivante détaille ces analyses.

6.4 Analyses axe par axe

6.4.1 Construction d'une base de connaissance exploitable : description des scénarios de conduite et classification

Lors de la phase de conception, au moment de la spécification du besoin, les exigences fonctionnelles et les exigences de sécurité sur le système ont été définies. Elles s'appuient sur une analyse des actions de conduite que doit réaliser le véhicule confronté aux comportements des autres automobilistes. Des cas d'usage, courtes séquences temporelles qui décrivent un enchaînement d'actions du trafic routier, servent de base pour construire des règles de conduite à respecter par le véhicule autonome. Ces cas d'usage sont une description sémantique d'un événement possible. Ils ne mentionnent pas les conditions de route :

— La scène dans laquelle se produisent les actions n'est pas décrite (les conditions météo, les types de route/infrastructure,etc.)
— Les objets n'intervenant pas dans la description ne sont pas pris en compte(autres véhicules)

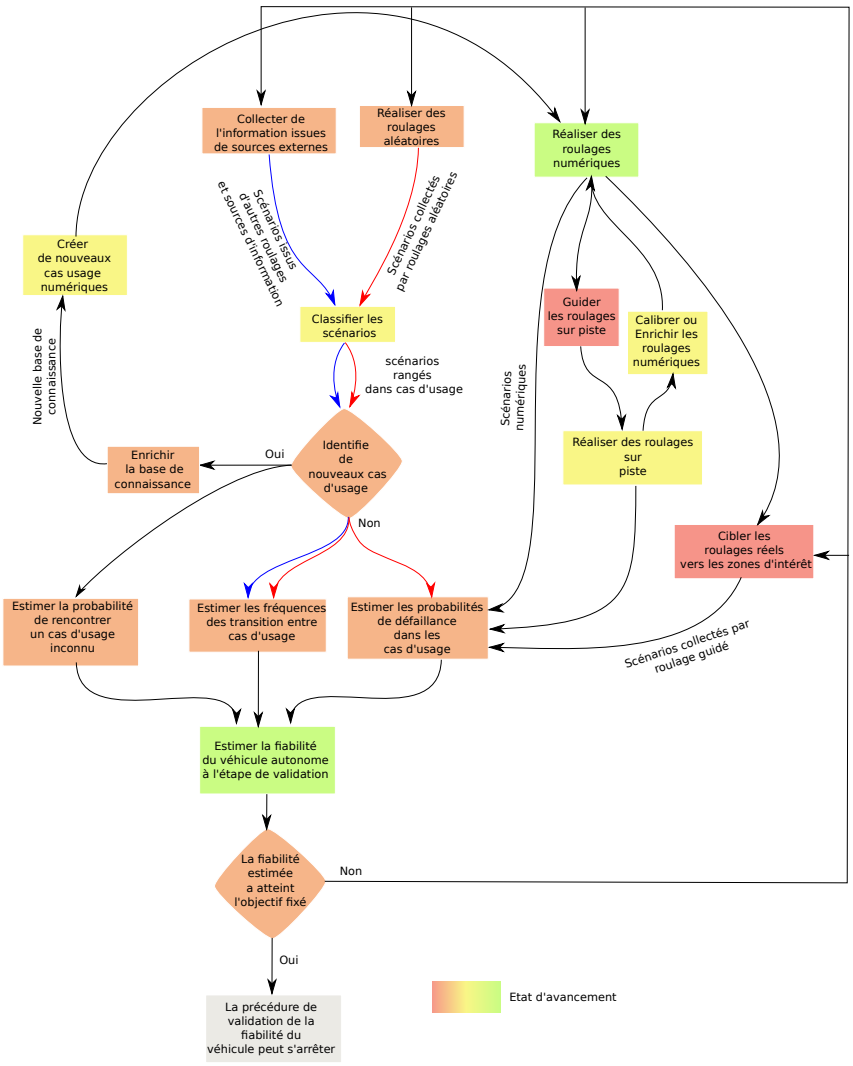


FIGURE 6.6 – Procédure de validation

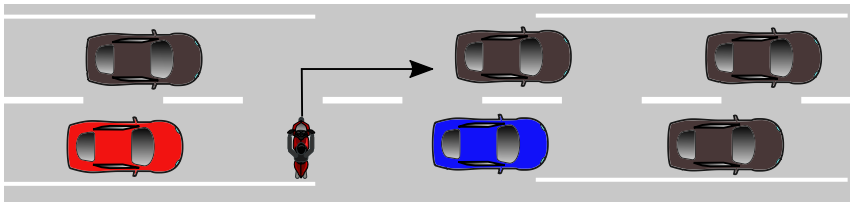


FIGURE 6.7 – Circulation perpendiculaire d'une moto

— De même aucune indication sur les profils de vitesse, d'accélération et de position de chaque automobiliste n'est donnée.

Un cas d'usage peut alors représenter de nombreux scénarios différents en fonction des paramètres. Un grand nombre d'objets et de paramètres de l'environnement peuvent potentiellement influer sur le comportement du véhicule. Ils peuvent perturber la bonne compréhension du scénario. La liste des cas d'usage actuelle est de plus incomplète. Certains comportements des automobilistes ou paramètres de l'environnement ne sont pas décrits par un cas d'usage. Ces nouveaux événements peuvent remettre en question l'ensemble des choix et des essais réalisés pendant les étapes du cycle en V. Ils ne sont connus qu'après retour d'expériences des essais réalisés avec le véhicule autonome, ou toute autre source d'information mettant en lumière ce nouveau cas d'usage. Par exemple un nouveau cas d'usage nommé "circulation perpendiculaire d'une moto" a été identifié après la défaillance du véhicule (Figure 6.7). Ce cas d'usage fait intervenir une moto qui change de voie perpendiculairement à la route, alors que les véhicules sont presque à l'arrêt. Parce que ce scénario est quasi statique les radars et lidars perçoivent mal les mouvements de la moto. De plus la caméra n'analyse pas bien la scène du fait que sa base d'apprentissage contient moins de motos dans cette position particulière. Son algorithme n'est pas robuste à ce type de scénario. Bien que le scénario observé est dorénavant bien appréhendé de multiples variantes peuvent entraîner des défaillances. C'est pourquoi ce nouveau cas d'usage est créé.

Dès lors, les connaissances des experts doivent être traitées sous un format exploitable afin de les comparer au domaine réel. Quantifier la part de non connaissance permet d'estimer plus précisément la fiabilité du véhicule. La base de connaissance proposée dans ce document se construit en partant de l'hypothèse qu'un trajet parcouru par le véhicule autonome peut se découper en une séquence de scénarios reliés les uns aux autres. En effet les actions choisies par les automobilistes dépendent des actions précédentes, leur décision se modifie en fonction de leur interprétation de la scène présente. Il existe bien une relation entre les scénarios de la séquence. La connaissance est organisée en un catalogue de scénarios distincts. Pendant des roulages de validation sur route ouverte de nouveaux scénarios sont observés. Il faut déterminer leur apport dans l'enrichissement de la base de connaissance. Sont-ils des scénarios très proches des précédents et donc apportent peu d'information ou au contraire sont-ils très différents et doivent être ajoutés au catalogue des scénarios ? Actuellement cette distinction se fait manuellement, le catalogue choisi reprend les mêmes cas d'usages que précédemment. Cependant ceux-ci intègrent désormais tous les paramètres possibles. Ces paramètres sont des variables qualitatives, quantitatives continues ou quantitatives discrètes. Des ensembles de valeurs sont attribués à chaque paramètre. Pour le paramètre météo, l'ensemble fini des valeurs est $\{pluie, soleil, brouillard, nuage\}$. Le paramètre vitesse initiale est caractérisé par un intervalle $[30km/h; 90km/h]$. Le paramètre nombre de voies comporte un ensemble fini de valeurs discrètes $\{1, 2, 3\}$. En simulation numérique, un scénario

se modélise automatiquement à partir de cette dernière description. Cependant le nombre de paramètres est plus restreint car le modèle numérique ne peut pas tout prendre en compte.
De nouveaux cas d'usage sont ajoutés au catalogue car ils ont surpris les acteurs du projet. Souvent ils sont détectés lorsqu'un scénario a mis en défaut le véhicule. Le cas d'usage généralise, après analyse, le scénario rencontré. Pourtant des scénarios proches, sans conséquence notable, avaient déjà été observés antérieurement. Une autre manière de détection des nouveaux scénarios doit être trouvée pour automatiser la découverte de ceux-ci et les détecter plus rapidement sans attendre d'observer une défaillance du système. Il est d'autant plus important que cette identification soit automatique, car la durée des roulages risquent d'être très grande. Ce qui va générer une nombre colossal de données à analyser en post-traitement.
Il est proposé de mettre en place une méthode de classification statistique ou numérique. Un scénario est dit "nouveau" s'il est différent des autres scénarios, c'est à dire qu'il est distant de ceux déjà imaginés ou observés. Cependant la notion de "distance" est très vague et même très difficile à définir. Plusieurs interprétations et méthodes de classification sont possibles et nous donnons ici quelques propositions :

- Deux scénarios sont distants l'un de l'autre parce qu'ils entraînent un comportement différent du véhicule. Dans cette classification les actions sont comparées. Deux actions peuvent pourtant être régies par deux règles de conduites distinctes. Par exemple une règle impose de décélérer en présence de piéton. Une autre impose de décélérer lorsque le véhicule autonome est trop proche du véhicule le précédant. Dans les deux cas le véhicule décélère. La moindre amélioration du système, que ce soit en termes d'algorithmes ou de définitions techniques entraîne la redéfinition de cette distance.
- Un scénario est distant des précédents parce qu'il ne peut être rangé dans aucune classe définie. Cette dernière classification ne demande pas obligatoirement la définition d'une distance entre les scénarios au préalable. Une méthode d'apprentissage supervisé peut ranger les scénarios selon des classes déjà définies.
- La fiabilité pourrait servir de mesure de distance entre les scénarios.
- Enfin une méthode numérique de classification peut être envisagée. Partant des cas d'usages numériques, un scénario réel peut être caractérisé par un cas d'usage s'il existe un scénario numérique issu de ce cas d'usage reproduisant le scénario réel. Si ce n'est pas le cas alors un nouveau cas d'usage est créé.

Les résultats de cette thèse dépendent de l'existence d'une telle classification. Néanmoins le choix de la classification n'influe pas sur la méthode mise en place par la suite.
La méthode envisagée par Renault est une méthode d'apprentissage supervisé et fait l'objet d'un projet en collaboration avec l'INRIA [68]. Les classes prédéfinies sont les cas d'usages identifiés lors de l'analyse fonctionnelle du besoin.
Dans la suite de ce document les classes construites seront également appelées des cas d'usages quelque soit la classification choisie.

Une utilisation du véhicule autonome est modélisée par une séquence de scénarios, chacun caractérisé par un cas d'usage. La classification des scénarios apportent de plus une méthode rapide pour annoter les données des roulages sur route ouverte. Pendant la phase de post-traitement, les séquences temporelles sont découpées et indexées par les cas d'usage qui les caractérisent. Il est ainsi plus facile d'aller rechercher une séquence temporelle particulière avec certaines caractéristiques précises.
Certains cas d'usages ont plus d'effet sur l'évaluation de la fiabilité du véhicule autonome. S'ils

sont plus rares, certains des scénarios classés non encore observés dans ce cas d'usage pourraient entraîner une défaillance du système. Au contraire d'autres cas d'usages sont rencontrés très fréquemment et sont bien gérés par le véhicule. Pour accélérer les roulages de validation, il serait important de s'affranchir des roulages aléatoires en réalisant des roulages ciblés qui permettraient de faire apparaître les cas d'usage les plus impactants dans l'évaluation de la fiabilité. Cependant la fiabilité du système intègre deux composantes, l'usage du véhicule et sa probabilité de défaillance. Réaliser un roulage ciblé perd cette première composante au risque de produire des séquence de cas d'usage non réalistes. Nous présentons dans la section suivante une manière d'évaluer la contribution de chaque cas d'usage pris séparément.

6.4.2 Contribution de chaque cas d'usage dans l'évaluation de la fiabilité

La fiabilité se modélise à partir de la classification des scénarios en cas d'usage. Cette description en séquence de cas d'usage n'est pas suffisante pour évaluer la fiabilité du système en sélectionnant des parcours. Les roulages privilégient les zones du domaine de fonctionnement qui perturbent le plus le système de perception et de décision du véhicule autonome ou impactent le plus la fiabilité du système. En effet les séquences de scénarios observés pendant ces roulages ne respecteront pas l'utilisation en clientèle du véhicule et risquent de biaiser l'évaluation. La fiabilité d'un système, par définition, intègre deux composantes : la fréquence d'occurrence des modes de fonctionnement qui représentent l'usage de l'entité étudiée et la défaillance possible de cette entité dans ces différents modes de fonctionnement. Pour élaborer une démarche de validation, tirant parti de l'ensemble des moyens d'essais et des informations disponibles, le modèle de fiabilité sélectionné est scindé en deux composantes : séquences possibles d'apparition des différents cas d'usage d'une part et défaillance du système dans chaque cas d'usage d'autre part. Nous supposons alors que la défaillance du système n'est liée ni à une succession de scénarios, ni à la transition entre deux scénarios mais elle est le résultat d'une mauvaise interprétation du scénario présent par le système de perception et de décision. La séquence de roulage est supposée s'arrêter dès l'apparition d'une défaillance.
Nous émettons l'hypothèse d'une séparation possible entre l'ensemble des paramètres caractérisant la fréquence d'apparition des différents cas d'usages et l'ensemble des paramètres caractérisant la défaillance. Ce découpage sera présenté dans le chapitre 7 qui propose une modélisation de la fiabilité.
Un roulage purement aléatoire n'est plus le seul type d'essais possible pour préciser la fiabilité du système. Certains essais pourront évaluer les occurrences d'apparition des différents cas d'usages d'autres s'intéresseront plus spécifiquement aux probabilités de défaillance.

Les roulages numériques et les roulages ciblés sur route ouverte, ne correspondent pas à l'usage du client du véhicule et seront principalement utiles dans l'étude de la probabilité de défaillance du véhicule autonome dans chaque cas d'usage.

D'autres sources d'information externes (les caméras de surveillance sur autoroute, les données des roulages de validation des ADAS, les informations météorologiques, etc) apportent une précision sur les fréquences d'apparition des cas d'usage. Si la classification des cas d'usage est indépendante du comportement du système autonome, alors l'usage du véhicule autonome est identique à celui de n'importe quel véhicule. Les données de ces sources contribuent directement à l'évaluation des fréquences d'apparition des cas d'usage. Sinon, ces informations restent utiles

pour l'estimation de ces fréquences, elles seront une valeur *a priori* et devront être complétées par l'analyse des données issues de roulages avec le véhicule autonome.

6.4.3 Remplacer les roulages réels par des simulations numériques pour évaluer la probabilité de défaillance

Les occurrences des usages possibles du véhicule autonome et les probabilités de défaillance dans chaque cas d'usage sont estimées séparément pour évaluer la fiabilité du système autonome. Les roulages numériques sont un atout majeur pour estimer les probabilités de défaillance dans chaque cas d'usage. Bien que le nombre de paramètres simulés dans les cas d'usages soit assez limité et que par conséquent le niveau de réalisme des modèles est plutôt bas, ces roulages ont le fort avantage d'être complètement maîtrisables. Des combinaisons rares mais probables de paramètres peuvent être simulées. La simulation peut prédire le comportement du véhicule dans des scénarios non rencontrés. Elles comportent de plus une vérité terrain. Les résultats de simulation apportent une explication aux défaillances observées et peuvent aider à la mise au point des algorithmes du système. Parce que les roulages numériques sont complètement tributaires de notre niveau de connaissance du problème posé, l'estimation de la probabilité de défaillance dans chaque cas d'usage est erronée et doit être complétée par des analyses de roulages réels réalisés avec le véhicule. La mise à jour de cette estimation *a priori* est présentée dans le chapitre 7.
Le modèle numérique sélectionné est dans cette thèse une donnée d'entrée, nous ne préconisons pas de modèle particulier. Les seules exigences pour obtenir une probabilité de défaillance exploitable sont les suivantes :

- La génération des scénarios doit se faire automatiquement à partir de valeurs d'entrée pour chaque paramètre données dans un plan d'expériences.
- Plusieurs centaines de scénarios à plusieurs milliers seront générés. Cela dépend du nombre de paramètres définissant le cas d'usage. Il faut donc un outil de simulation qui puisse prédire le comportement du véhicule autonome en un temps raisonnable.
- Plus le niveau de réalisme est grand et plus on peut avoir confiance en les résultats obtenus. Cette confiance va permettre de réduire la durée des essais réels. Il y a de grandes chances qu'une simulation très réaliste intègre un très grand nombre de paramètres. La durée et le nombre de simulation risquent d'être importants. Un compromis doit être trouvé entre temps de simulation et qualité de prédiction des simulations.
- Il est possible d'étudier le comportement du véhicule autonome sur plusieurs simulations successives. D'abord à l'aide d'un modèle peu coûteux, puis après avoir identifié les zones probables de défaillance il faut faire appel à des outils de simulation plus élaborés dans un domaine restreint.

Nous suggérons une manière d'utiliser ces roulages numériques pour estimer la probabilité de défaillance du système dans ces cas d'usage.
Actuellement un cas d'usage numérique est caractérisé par un ensemble de paramètres principalement liés à des objets du trafic routier et à quelques objets de l'infrastructure.
L'évaluation de la probabilité de défaillance dans un cas d'usage ne peut pas se faire sans les distributions jointes des paramètres du cas d'usage. Ces distributions peuvent être évaluées à partir des résultats obtenus lors d'analyse de conduite naturalistique comme le fournit le projet UDRIVE [21]. Les simulations numériques peuvent être déterministes ou aléatoires.
Elles sont déterministes quand les trajectoires des automobilistes sont dictées par des règles

fixées de conduite et quand aucune perturbation des trajectoires n'est introduite. Une perturbation peut par exemple être une petite oscillation du véhicule pour aller d'un point A vers un point B. Dans ce type de simulation les erreurs de l'algorithme de fusion ou de chaque algorithme des capteurs, modélisées par des variables aléatoires, ne sont pas intégrées. La section 6.4.4 présente une méthode d'optimisation des essais de simulation adaptée actuellement à ce type de simulation.
Les simulations sont aléatoires quand elles tiennent compte des incertitudes sur les trajectoires des automobilistes et/ou des erreurs des modèles de la fusion ou des capteurs. Des études pour reproduire différents modèles de comportement des conducteurs sont en cours.

L'évaluation de la probabilité de défaillance peut se faire par propagation de l'ensemble des incertitudes comprises dans la simulation. Dans la littérature, le choix se porte le plus souvent sur des méthodes de Monte Carlo accélérés. Zhao et al. [90] proposent de réaliser des tirages d'importance pour évaluer plus rapidement la probabilité de défaillance. Ils choisissent d'étudier le cas d'usage "insertion de véhicule" et ne sélectionnent que trois paramètres qu'ils considèrent les seuls nécessaires à caractériser la collision du véhicule. Les distributions conjointes de ces trois paramètres sont obtenues par des conduites naturalistiques. Les roulages numériques beaucoup plus rapides que les roulages réels restent néanmoins coûteux en temps de calcul. L'évaluation de la fiabilité par méthode de Monte Carlo ne semble pas pertinente. En effet pour certains cas d'usages plus d'une centaine de paramètres sont à prendre en compte. L'échantillon tiré aléatoirement devra être gigantesque pour garantir un recouvrement homogène de l'espace des paramètres. Nissan a choisi la méthode CTD (combinatorial test designs, [89]) en transformant tous les paramètres continus en paramètres discrets. Cette méthode considère l'espace des paramètres comme un ensemble fini de points. Tout point dans le domaine de fonctionnement et n'appartenant pas à cet ensemble ne sera pas prédit. Si le nombre de niveaux est trop faible, des points défaillants risquent de ne pas être détectés. Une méthode d'optimisation, permettant de rechercher plus rapidement les zones de défaillances avant de procéder à la propagation des incertitudes, nous semble une bonne alternative pour évaluer la probabilité de défaillance. Huang et al. [34] proposent de réaliser un échantillonnage séquentiel à l'aide d'une méthode de surface de réponse avec un modèle de krigeage et une procédure de descente de gradient heuristique. L'inconvénient du modèle de krigeage c'est qu'il n'est pas applicable sur des paramètres qualitatifs ni à des problèmes de grandes dimensions. Néanmoins certaines extensions existent dans la littérature [10, 20]).
Une méthode d'optimisation est proposée pour découvrir rapidement l'ensemble des zones de défaillance inconnues dans le cas d'usage étudié. Le nombre de cas d'usage à étudier est conséquent, actuellement 200 cas ont été répertoriés. Pour chaque cas d'usage, le problème étudié risque d'être assez différent. Une méthode unique d'optimisation, jugée la plus efficace après avoir fait l'objet d'une étude approfondie sur un ou plusieurs cas d'usage, risque de ne pas avoir la même efficacité dans un autre cas. L'amélioration des algorithmes de fusion et de décision, au fur et à mesure des étapes de validation, vont complexifier le problème d'optimisation. Les zones de défaillance se feront de plus en plus rares.
Elles seront sans doute parsemées dans tout l'espace des paramètres et de formes différentes. En effet, dans le chapitre 2, nous avons discuté de la difficulté de relier la défaillance du véhicule autonome à un indicateur de dangerosité. Pourtant la collision du système n'est pas le seul événement inadmissible pour valider le véhicule autonome. Les quasi-accidents, les sorties de voie sont aussi pénalisants. Plusieurs indicateurs de dangerosité et critères associés ont été sélection-

nés pour définir la défaillance. Certains partageront les mêmes zones de défaillance, d'autres au contraire présenteront des défaillances dans de nouvelles zones disjointes.
Le niveau de fiabilité requis pour le véhicule autonome implique que la probabilité de défaillance du système étudiée sera très petite. Cela ne veut pas forcément dire que le volume des zones de défaillances est petit dans l'espace des paramètres, mais qu'il est relié à un événement rare en tenant compte des distributions des paramètres.
Pour réduire le nombre d'essais de validation à réaliser et détecter l'ensemble des zones de défaillance nous avons mis en place un mélange d'algorithmes d'optimisation intitulé ADValue.

6.4.4 Optimiser les roulages numériques pour cibler les zones de défaillance : l'algorithme ADValue

ADValue a pour objectif de réduire le nombre de scénarios de façon intelligente pour valider un use case. Il programme les plans de tests de façon séquentielle dans le but de détecter les zones de défaillance pour un coût de calcul minimal. Il ne se focalise pas sur une seule méthode, mais intègre et adapte les méthodes stochastiques et surfaces de réponses au contexte de la validation du véhicule autonome.
ADvalue est un ensemble d'algorithmes qui coopèrent entre eux pour trouver les scénarios défaillants et qui sont en compétition pour le partage du budget de calculs, c'est-à-dire le nombre de scénarios à simuler. Un algorithme est appelé «expert». Il exploite les résultats des scénarios déjà calculés pour en proposer de nouveaux. Son budget, au fil des itérations d'ADValue, dépend de sa performance, c'est-à-dire sa capacité à découvrir de nouveaux scénarios défaillants ou à préciser la frontière entre défaillance et non défaillance.
ADValue est une méthode itérative avec un plan d'expériences initial et des séries de calculs proposées par les différents experts ou algorithmes.
A chaque itération, l'espace de recherche est découpé en zones de défaillance et de non défaillance. La version actuelle d'ADValue fait un découpage à partir d'un arbre de décision [71] nommé le modèle CART ("Classification And Regression Trees ", [8]). C'est un arbre binaire qui découpe l'espace des paramètres en feuilles selon le critère de segmentation appelé l'indice de diversité de Gini (6.1).

$$I_G(f) = \sum_{i=1}^{m} f_i(1 - f_i) = \sum_{i=1}^{m} f_i - \sum_{i=1}^{m} {f_i}^2 = 1 - \sum_{i=1}^{m} {f_i}^2 \tag{6.1}$$

où m est le nombre de valeurs prises par la variable à prédire et f_i la partition avec l'étiquette i de l'espace des paramètres. Il donne une explication de la variable d'intérêt, voir Figure 6.8. La feuille affecte la variable d'une valeur. L'embranchement de l'arbre représente les règles sur les paramètres d'entrée, c'est-à-dire les combinaisons de ces paramètres d'entrée pour que la variable d'intérêt prenne la valeur de la feuille. Cet arbre est construit pas à pas en partageant les points de part et d'autres d'une frontière choisie sur une variable d'entrée. La division et la variable d'entrée sont choisies pour maximiser le critère de segmentation.
Nous avons choisi cette méthode pour expliquer la défaillance car elle donne une description facile d'interprétation des zones de défaillances et de non défaillances. La variable d'intérêt est l'état non défaillant et défaillant du système. Les zones de défaillances sont ici des hypercubes dans l'espace des paramètres d'entrée. Si les distributions des paramètres sont des lois uniformes, la probabilité de défaillance est alors la somme des volumes des feuilles caractérisant la défaillance. Pour d'autres types de lois, les probabilités des zones de défaillance pourront se calculer à partir

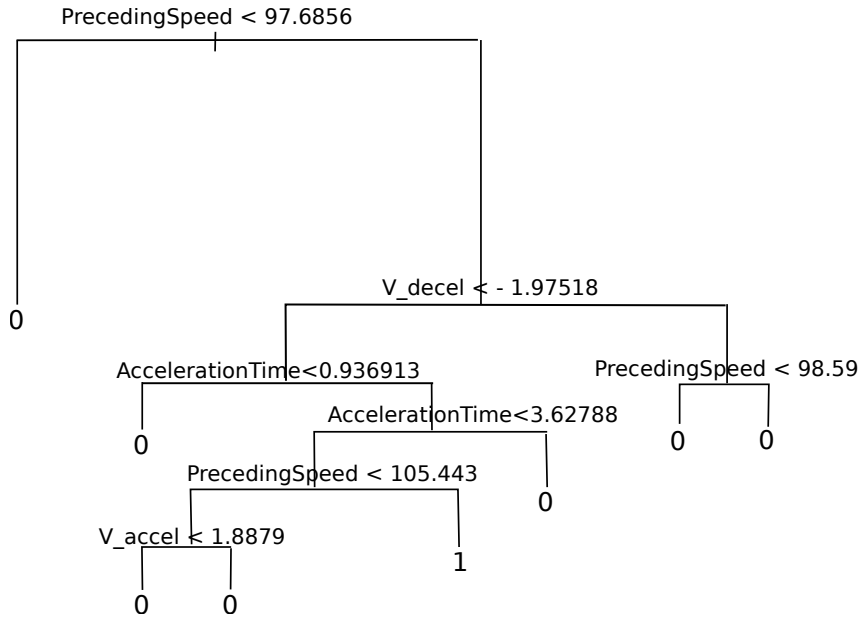


FIGURE 6.8 – Exemple de diagramme CART obtenu lors de l'analyse du cas d'usage suivi de véhicule pour l'indicateur "durée avant de retourner à une distance sécuritaire", 1 indique les feuilles comportant des défaillances, 0 les zones sans défaillance

des fonctions de répartitions conjointes des paramètres d'entrée.

Pour sélectionner les scénarios les plus pertinents, afin de préciser le modèle CART à l'étape suivante, deux experts sont actuellement implémentés, nommés "Findborders" et "Densify".

Findborders

Findborders ajoute des scénarios situés sur le segment entre deux scénarios. L'un entraine une défaillance du système, l'autre n'en entraîne pas. Cet algorithme a pour but de détecter les scénarios proches de la frontière des zones de défaillance et de non défaillance comme observé sur la Figure 6.9.

Densify

Densify reçoit un budget de scénarios à réaliser et départage le nombre de scénarios à ajouter par feuille. Son choix est fait en fonction du volume V_{f_i}, du nombre de points N_{f_i}, du taux d'erreurs ϵ_{f_i} et de la probabilité de défaillance F_{f_i} estimés dans chaque feuille. Une petite feuille, dense (comportant un très grand nombre de points répartis de manière homogène dans toute la feuille), avec des scénarios entraînant soit des défaillances soit des non défaillances est suffisamment bien prédite, elle n'a pas besoin de nouveaux points pour être précisée. Tandis qu'une feuille large avec peu de scénarios, mal répartis dans sa fraction, avec une grande proportion de défaillances et de non défaillances, nécessite plus de points pour être mieux précisée.
A l'étape suivante, les nouveaux scénarios à tester sont sélectionnés et répartis dans les feuilles

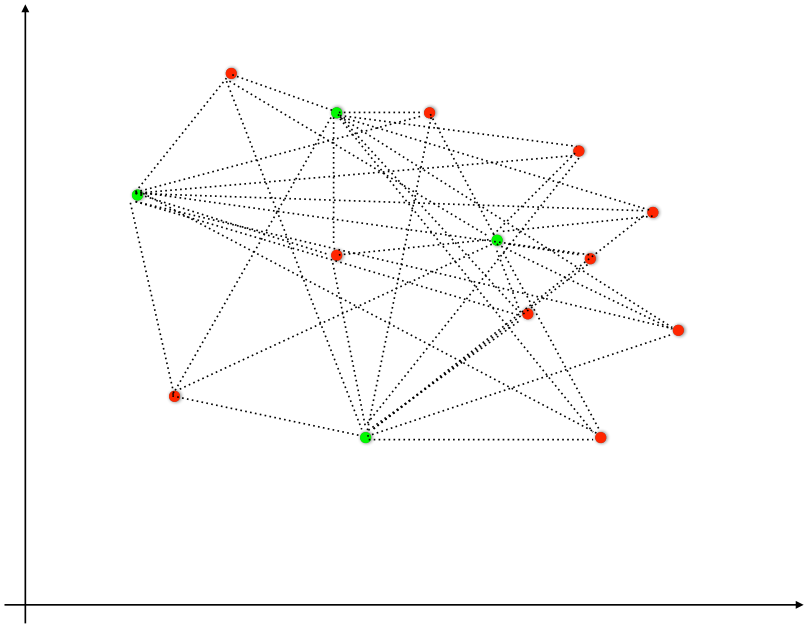


FIGURE 6.9 – Illustration de l'algorithme Findborders [83]

de manière homogène par une méthode de maximisation de l'entropie nommée *dmaxDesign* dans le package *DiceDesign* du logiciel R [18].

Actuellement, les deux experts ont le même budget calcul. Ils proposent tous les deux de nouveaux points. La fonction "select" reprend les points proposés et éliminent les points redondants ou très proches selon le même critère que la fonction *dmaxdesign*.

Cette première version d'ADValue a été testée sur un premier cas d'usage numérique. Le cas d'usage étudié est le "suivi de véhicule", Figure 6.10. Pour ce cas d'usage, seuls deux véhicules sont simulés : le véhicule autonome et un véhicule devant lui. Le véhicule autonome suit le véhicule de devant avec initialement la même vitesse que lui. Puis le véhicule de devant va faire des cycles d'accélérations et de décélérations successives identiques. Les paramètres de ce cas d'usages sont résumés dans la table 6.2.

Quatre critères associés à des indicateurs de dangerosité ont été choisis pour l'analyse :
- La décélération maximale admissible du véhicule autonome de $-3m.s^2$.
- La distance minimale de sécurité. Dans la réglementation française elle est calculée en respectant un écart de deux secondes entre les véhicules, avec l'hypothèse que les vitesses de ceux-ci sont constantes.
- La durée maximale autorisée au véhicule autonome pour retrouver une distance de sécurité si celle-ci a été enfreinte alors que le véhicule autonome n'était responsable.
- L'écart latéral maximal ; la distance maximale entre le centre de la voie et le centre d'inertie du véhicule.

Un premier plan d'expériences suivi de deux itérations de scénarios avec ADValue ont été

FIGURE 6.10 – Capture d'écran du cas d'usage simulé avec le logiciel Scaner

variables	noms	type	intervalle ou niveau	unité
vitesse initiale du véhicule précédent	$PrecedingSpeed$	quantitative continue	$[10; 110]$	km/h
distance inter-véhicule initiale	$DistanceInterVehicule$	quantitative continue	$[3,5; 200]$	m
durée des accélérations	$AccelerationTime$	quantitative continue	$[0; 5]$	s
accélération 1	V_accel	quantitative continue	$[1; 3]$	ms^{-2}
accélération 2	V_decel	quantitative continue	$[-3, 0]$	ms^{-2}
terrains	$Ground\_Network$	qualitative	8 terrains différents possibles faisant varier la largeur de la voie et la pente de la route	
type du véhicule précédent	$Vehicle\_Type\_1$	qualitative	une moto ou une voiture ou un camion	

TABLE 6.2 – Paramètres du cas d'usage "suivi de véhicule"

simulés. Le premier plan d'expériences sélectionne les points probables (tirés aléatoirement selon les distributions des paramètres) les plus proches des points du plan factoriel complet. Ce plan factoriel comprend 2 niveaux pour les variables quantitatives et l'ensemble des niveaux des variables qualitatives. Parmi les 768 scénarios du plan factoriel, 481 points ont été sélectionnés. Les deux itérations produisent 77 nouveaux points. Nous analysons un total de 558 points.

Les analyses réalisées avec le logiciel ADValue sont illustrées par l'étude d'une des quatre sorties : la variable d'écart latéral maximal nommée "lateral lane decentering". La Figure 6.11 présente le modèle CART obtenu après les deux itérations.

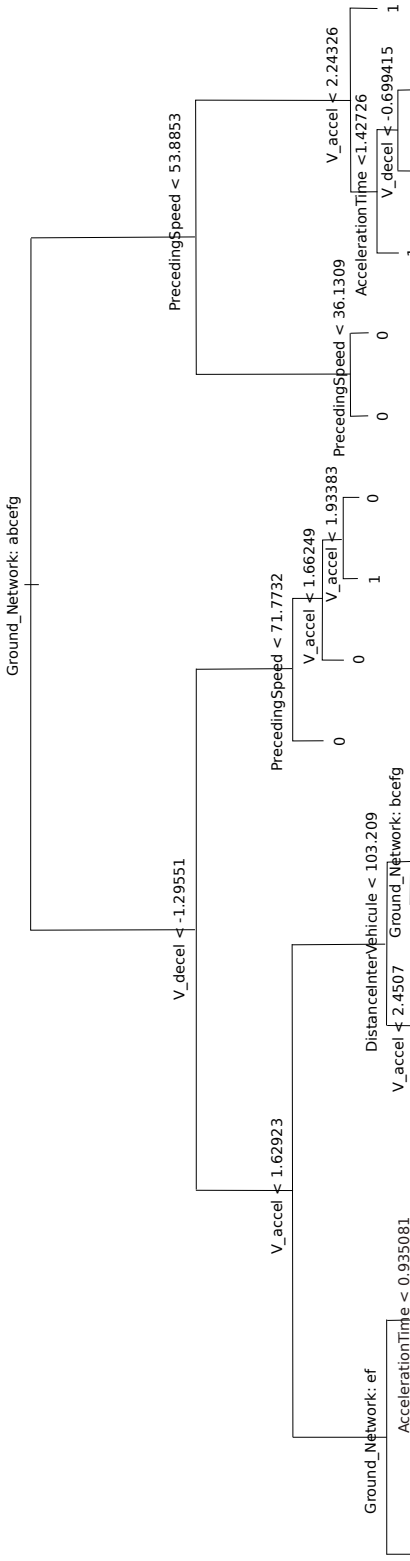
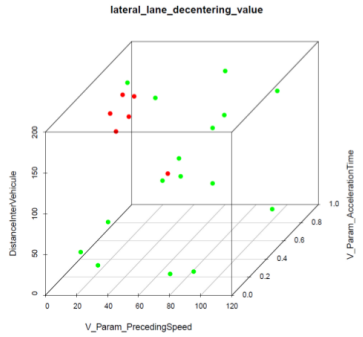


FIGURE 6.11 – Diagramme CART de la sortie "lateral lane decentering"

Leaf number	Nb of points in leaf	Output value	% of points with output value = 0	% of points with output value = 1
16	24	0	79%	21%
68	15	0	93%	7%
69	7	1	29%	71%
140	21	1	43%	57%
141	8	1	0%	100%
71	17	1	0%	100%
36	40	0	65%	35%
37	40	0	95%	5%
38	56	0	100%	0%
39	13	0	85%	15%
10	114	0	100%	0%
22	35	0	100%	0%
46	7	1	43%	57%
47	38	0	89%	11%
12	35	0	97%	3%
13	10	0	60%	40%
28	15	1	0%	100%
58	21	1	48%	52%
59	7	1	0%	100%
15	35	1	0%	100%

FIGURE 6.12 – Table des feuilles du modèle CART

Après deux itérations, le pourcentage d'erreurs du modèle est de $10,22\%$. A première vue un modèle linéaire n'est pas suffisant pour expliquer l'ensemble des zones défaillantes. Un second diagramme CART est réalisé en ajoutant les croisements des variables et le carré des variables. L'erreur décroît $(8,07\%)$ mais reste élevée.
La Figure 6.12 est une table avec l'ensemble des feuilles du premier diagramme, le nombre de points par feuille, leur valeur attribuée, et les pourcentages de mauvais classement des points.
Les couples de feuilles $(68,69),(140,141),(58,59),(36,37)$ ne sont pas bien expliqués (il reste des erreurs). Leur séparation n'est pas satisfaisante. Les points des couples pris un à un sont rassemblés pour réaliser une analyse discriminante [76] et ainsi voir si une combinaison linéaire des paramètres d'entrée permet d'expliquer les deux zones.
Le couple $(68,69)$ est totalement prédit par cette analyse discriminante. La Figure 6.13 présente un nuage de points selon trois variables pour montrer où se trouve la zone unique de défaillances. Cependant toutes les variables ont été nécessaires pour expliquer cette zone et pas seulement ces trois paramètres. Elle donne également le taux de bon classement. CART n'aurait jamais pu donner une explication de ce couple. En effet les coupures que CART réalise sont parallèles aux axes et ne suivent pas de combinaisons linéaires des paramètres. Si de nouveaux points avaient été ajoutés dans la feuille, les nouvelles feuilles résultantes auraient été erronées et dessineraient un escalier le long de la frontière oblique entre zone de défaillance et de non défaillance comme schématisé en Figure 6.14. Il est envisagé de remplacer le modèle CART par un modèle de CART oblique [58] découpant, selon les combinaisons linéaires des variables, pour améliorer ADValue.
Pour les autres couples, des analyses discriminantes linéaires et quadratiques sont effectuées. Ainsi les couples sont en général mieux et quelque fois complètement expliqués. La Figure 6.15 rassemble les erreurs des analyses discriminantes dans les feuilles pour les quatre sorties analysées. Pour la sortie "lateral lane decentering" 39% de feuilles restent mal prédites contre 60% sans l'analyse discriminante quadratique par feuille. Cette dernière sera un nouvel expert qui sera ajouté à l'algorithme ADValue.



Linear discriminant analysis :

prediction / response value	0	1
0	16	0
1	0	6

Misclassification rate = 0%

FIGURE 6.13 – Explication du couple de feuilles 68 et 69

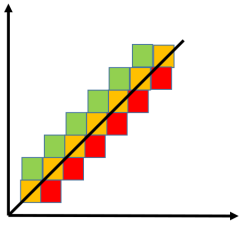


FIGURE 6.14 – Comportement du modèle Cart lorsqu'il doit expliquer une frontière oblique. En rouge sont présentées les feuilles expliquant la défaillance, en vert les feuilles sans défaillance et en orange un mélange de défaillance et de non défaillance.

Toutes les méthodes présentées ne tiennent compte que des paramètres d'entrée et de sortie des scénarios. Pourtant les données temporelles (ensemble des valeurs des variables à chaque instant) enregistrées lors de chaque simulation de scénario peuvent mieux expliquer la défaillance. Deux zones de défaillance éloignées dans l'espace des paramètres peuvent décrire en réalité la même cause de défaillance. Certains scénarios peuvent en effet être symétriques. Par exemple, une collision, causée par l'insertion d'un véhicule qui décélère alors que le véhicule autonome conserve une vitesse constante, est le même mode de défaillance qu'une collision, causée par l'insertion d'un véhicule à vitesse constante alors que le véhicule autonome était en train d'accélérer. Pourtant ces deux collisions sont éloignées dans l'espace des paramètres. Pour illustrer nos propos une décomposition en valeur singulière [76] a été réalisée sur plusieurs enregistrements de scénarios simulés. Sur les 22 variables temporelles (paramètres d'entrée et de sortie) seuls 4 à 6 vecteurs propres expliquent plus de 90% des données (Figure 6.16). Des méthodes de réduction de dimension semblent des experts prometteurs pour ADValue.

Avec 558 points pour 7 variables, l'algorithme ADValue apporte déjà des éléments de réponse sur la forme et le nombre de zone de défaillances d'un premier cas d'usage comme le suivi de véhicule. Pour vérifier que les analyses sont pertinentes, elles seront comparées à des analyses réalisées avec un très grand nombre de points de ce cas d'usage.

Le nombre de défaillances observé est assez grand. En effet, le système étudié est encore jeune et en phase de conception. Les experts implémentés sont adaptés à ce type de problème. Cependant quand les défaillances se feront plus rares, ils ne pourront plus convenir. D'autres experts, analysant les valeurs des variables de sortie au lieu d'une valeur binaire (défaillance/ non défaillance).

Total number of leaves : 28 Ratio of unexplained leaves = 39%

lateral_lane_decentering_value

# Leaves	prediction	nb pts	error
12	39	1	
	1	4	45 4%
16	38	8	
	6	40	92 15%
36	62	8	
	2	8	80 13%
39	67	0	
	0	2	69 0%
46	36	2	
	1	6	45 7%
58	8	0	
	2	18	28 7%
68	16	0	
	0	6	22 0%
140	9	0	
	0	20	29 0%
Nb Leaves	8	Nb of unexplained leaves	5

longitudinal_deceleration_value

# Leaves	prediction	nb pts	error
13	4	0	
	0	95	99 0%
58	5	1	
	1	8	15 13%
121	5	0	
	0	8	13 0%
122	20	0	
	0	4	24 0%
126	12	5	
	3	52	72 11%
248	16	0	
	0	9	25 0%
250	8	0	
	2	27	37 5%
254	4	0	
	2	51	57 4%
511	2	0	
	1	49	52 2%
nb Leaves	9	Nb of unexplained leaves	5

safety_distance_value

# Leaves	prediction	nb pts	error
9	291	0	
	0	1	292 0%
13	36	3	
	4	35	78 9%
20	4	0	
	0	6	10 0%
58	17	0	
	0	3	20 0%
61	14	0	
	0	15	29 0%
63	31	0	
	0	6	37 0%
101	15	0	
	0	2	17 0%
121	13	0	
	0	6	19 0%
nb Leaves	8	Nb of unexplained leaves	1

duration_to_safety_value

# Leaves	prediction	nb pts	error
100	16	0	
	0	1	17 0%
410	5	0	
	0	8	13 0%
818	6	0	
	0	5	11 0%
nb leaves	3	Nb of unexplained leaves	0

FIGURE 6.15 – Ensemble des feuilles expliquées pour chaque variable

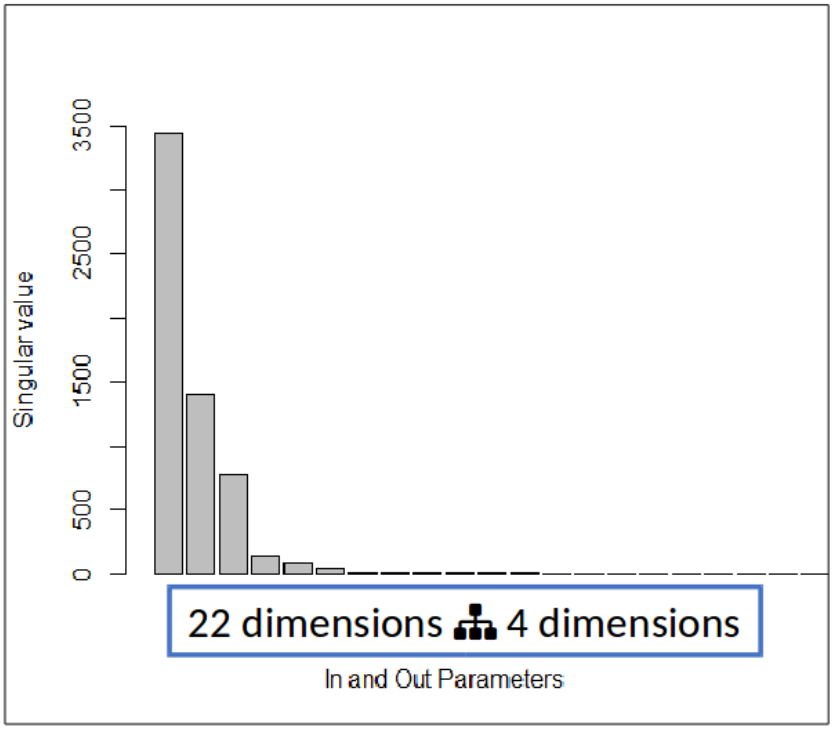


FIGURE 6.16 – Histogramme des valeurs singulières d'un des scénarios simulés

Par exemple l'arbre CART oblique pourrait découper selon les valeurs de "lateral lane decentering" et non uniquement le dépassement ou non du seuil maximal autorisé. Des algorithmes comme la descente du gradient, le krigeage dans les feuilles, des régressions dans les feuilles sont d'autres experts envisagés. Enfin des méthodes de réseaux de neurones, pour réduire la dimension du problème étudié, fait l'objet d'un sujet de thèse.
Actuellement aucune règle d'allocation du budget entre les experts n'est proposée et sera le sujet d'un futur chantier afin d'expliquer en un temps raisonnable les zones de défaillance sans biaiser les résultats. Les experts efficaces doivent avoir plus de poids que les autres experts et les experts inefficaces doivent être éliminés. Cette allocation de budget doit également tenir compte du temps de calcul nécessaire à chaque expert. Un compromis doit être fait entre le temps de réflexion avec ADValue et les temps de simulations des scénarios pour charger au mieux la machine.

6.4.5 Réaliser des scénarios sur piste : calibration ou enrichissement du modèle numérique

Les roulages numériques actuels ne tiennent compte que des paramètres trafics, et peuvent contenir des modèles d'erreur de capteurs dans des conditions idéales de fonctionnement. L'influence des paramètres de l'environnement sur le fonctionnement des capteurs n'est actuellement pas modélisée. Pourtant les positions et les vitesses relatives des objets du trafic, les paramètres météorologiques, les objets de l'infrastructure perturbent les capteurs. Les données transmises par les capteurs peuvent être erronées. Tout d'abord le champ de vue peut se réduire entraînant alors des faux négatifs (un objet n'est pas détecté) ou des détections tardives. Certains objets de l'infrastructure sont connus pour augmenter le nombre d'artefacts (objets détectés alors qu'ils n'existent pas et qui disparaîssent très rapidement) qui peuvent finir par être considérés comme des objets, que nous appellons des "ghosts". Les mesures réalisées sur les objets (tailles, positions, vitesses, accélérations) peuvent être bruitées dans des conditions climatiques particulières comme avec de la pluie ce qui peut produire des mesures erronées. Des objets peuvent être mal classés, un piéton peut être considéré comme un objet inconnu. Les décisions prises ne sont pas nécessairement les mêmes en fonction du type d'objet. Plusieurs objets sont parfois regroupés en un même objet ou inversement un même objet peut être vu deux fois à des positions différentes. Tous ces types d'erreur doivent être intégrés dans les modèles de simulation pour augmenter le réalisme des simulations numériques ou à défaut doivent servir pour corriger le calcul de fiabilité en ajoutant un coefficient de sécurité qu'il faudra bien dimensionner.
Pendant cette étude, nous avons initié une procédure pour construire des modèles d'erreur en fonction des paramètres de l'environnement. Dans un premier temps, nous avons listé l'ensemble des objets ou paramètres de l'environnement perturbant les capteurs, puis nous avons commencé une description de leurs effets. Quels capteurs étaient perturbés, quelles fonctionnalités et sous quelles formes ?
L'environnement peut entraîner :

- Des erreurs systématiques sur les capteurs. Nous donnons un exemple d'erreur systématique avec le radar sur la Figure 6.17. Ces phénomènes sont liés à la géométrie de la scène. Cela peut être intégré dans les modèles numériques. L'identification de ces erreurs systématiques n'est pas encore terminée, les fournisseurs apportent et complètent une liste décrivant l'ensemble de ces erreurs.
- une réduction du champ de vision. Les performances des capteurs sont donc modifiées en fonction des paramètres de l'environnement choisis pour la simulation.

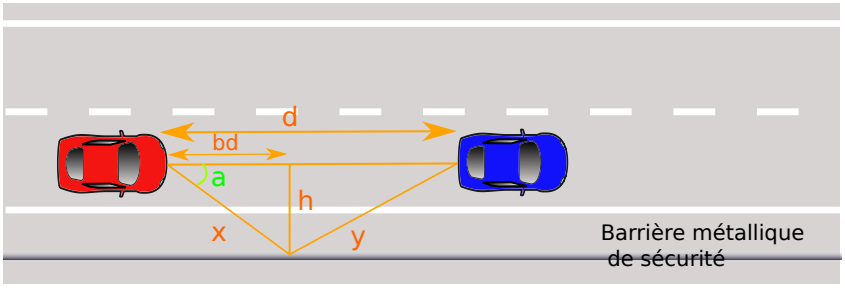


FIGURE 6.17 – Exemple d'une erreur systématique : pour un certain angle a propre au radar à côté d'une glissière de sécurité le véhicule qui précéde sera vu à une distance bd inférieure à la distance réelle d

— L'augmentation du nombre d'artefacts de manière homogène dans le champ de vision. C'est le cas des tunnels qui font rebondir les échos radars dans toutes les directions.
— l'obstruction partielle de la vision des capteurs. C'est surtout le cas des caméras et les logiciels de simulation qui modélisent bien ce phénomène.
— Le bruit sur la mesure et la détection des objets, comme le brouillard sur la caméra.

Nous nous sommes intéréssés plus particulièrement à ce dernier phénomène. Des essais sur piste ont été réalisés avec l'aide de l'entreprise IAV dans un aérodrome. Nous donnons en annexe des exemples de tests réalisés. Nous avons effectué des scénarios issus de cas d'usage simple comme le suivi de véhicule. Nous avons testé plusieurs combinaisons de paramètres, vitesse, position, météo pour évaluer leur influence sur les performances des capteurs. A chaque essai, nous avons étudié le temps de détection des objets présents dans le scénario, leur position relative au moment où ils ont été détectés pour caractériser le champ de vue et nous avons comparé les mesures de chaque capteur sur chaque objet avec un GPS différentiel qui a servi de vérité terrain. Il a été proposé de construire un bruit gaussien des mesures qui varient selon les paramètres de l'environnement. En effet les logiciels de simulation peuvent intégrer ce type de bruit. Moyenne et écart type des erreurs de mesures ont été estimés en fonction de la vitesse et de la position de chaque objet par l'entreprise IAV pour chaque essai différent faisant varier scénarios et environnement. Ces bruits gaussiens pourront être intégrés au simulation.

Ces modèles conviennent bien pour des variations lentes de positions et de vitesses mais sont inadaptés à des sauts rapides de ces paramètres. Par exemple l'essai où le véhicule précédent oscille de sa voie par à-coups très rapides gène beaucoup les capteurs, en particulier les radars qui sont perturbés par la vitesse angulaire des véhicules. Beaucoup de travaux sont à mener pour construire des modèles d'erreurs adaptés à chaque cas d'usage. Le projet SVA de l'IRT systemX comprend un work package dédié à ce sujet [2].
Les essais sur piste sont limités en termes de paramètres et d'objets de l'environnement. Cependant, comme exposé dans le chapitre 2 des pistes dédiées au véhicule autonome avec des objets de l'infrastructure et des faux bâtiments se construisent. Elles sont de plus cartographiées précisément avec des lidars pour mettre en place une réalité terrain.

Travailler sur des modèles d'erreurs spécifiques à chaque phénomène et à chaque capteur risque d'être très laborieux et alourdir les calculs réalisés en simulation. D'autant que chaque essai sera spécifique à la physique des capteurs étudiés. Une évaluation de la fiabilité des capteurs comme

proposé dans le chapitre 2 tenant compte de la fréquence de chaque condition environnementale serait peut être préférable pour le calcul de la fiabilité du système. Ce serait un pré-requis à imposer au fournisseur de capteur. Nous n'avons pas investigué sur des méthodes de calibration mais cela pourrait être une autre piste pour améliorer le réalisme des simulations numériques.

6.4.6 Cibler les roulages sur route ouverte pour réduire la durée de validation

La méthode d'évaluation de la fiabilité sélectionnée rend possible la mise en place de roulages guidés qui permettraient de réduire la durée des essais de validation par rapport à des roulages purement aléatoires. Les roulages de validation sont guidés pour cibler les zones du domaine de fonctionnement encore mal connues et qui sont supposées contribuer le plus dans l'évaluation de la fiabilité.

Nous n'avons pas pu travailler sur ce point. Cependant il nous semble qu'une méthode d'optimisation dans le but de minimiser la variance de l'estimation de la fiabilité est une piste à creuser. Elle devra aider à répartir la durée des essais entre essais aléatoires et essais ciblés à la prochaine itération.
Un exemple dans le chapitre 8 nous permettra de tester cette possibilité.

6.5 Conclusion

Le caractère novateur du véhicule autonome rend incomplètes les analyses et méthodes classiques de sûreté de fonctionnement. La conception et les essais de validation dépendent du niveau de connaissance du problème posé. Cette connaissance évolue en fonction des retours d'expériences avec le véhicule. Une nouvelle démarche de validation est nécessaire pour compléter les méthodes classiques afin de certifier de la sécurité d'un tel véhicule. Elle ne remplace pas les méthodes courantes qui restent le point de départ de la validation.

La stratégie de validation proposée dans ce document part de l'hypothèse que la durée des tests de roulage est partitionnée en séquences de scénarios. Ceux-ci sont de courtes séquences temporelles de quelques minutes, ils décrivent :

- Le comportement du trafic routier,
- Les conditions climatiques,
- Les règles de conduite,
- Les objets de l'infrastructure.

Ils sont regroupés en cas d'usage selon une classification choisie. Chaque cas d'usage influence la fiabilité du véhicule autonome. Leur contribution respective s'évalue selon deux composantes : les fréquences de chaque enchaînement de cas d'usage et les probabilités de défaillance du système dans ces cas d'usage. De cette manière, la démarche de validation peut combiner l'ensemble des moyens disponibles dans l'entreprise.
Les essais numériques et les essais ciblés sur piste ou sur route ouverte servent à évaluer les probabilités de défaillance dans les cas d'usage. Les essais aléatoires sur route ouverte et les sources externes d'informations sont utiles dans l'estimation de la probabilité d'occurrence des séquences de cas d'usage.

Pour chaque étape de la méthode proposée, des études de faisabilité ont été menées. Certaines étapes comme l'optimisation des roulages numériques ouvrent de nombreuses perspectives d'amélioration en proposant de nouveaux algorithmes plus adaptés à la problématique étudiée. D'autres, comme les roulages ciblés et les roulages sur piste requièrent un travail plus approfondi. En particulier, rien ne démontre actuellement que des roulages ciblés peuvent réduire la durée des essais nécessaires pour estimer précisément la fiabilité du véhicule autonome. De plus, guider des roulages sur route ouverte n'est pas si simple. Cela suppose que le domaine de fonctionnement soit suffisamment contrôlable pour observer les scénarios souhaités. Les enregistrements déjà effectués devront être analysés pour identifier les routes et les conditions de route qui augmentent la fréquence d'apparition de tels scénarios.

La démarche de validation est itérative et s'associe à une méthode d'estimation de la fiabilité pour construire un critère d'arrêt au processus de validation. L'estimation de la fiabilité part de l'ensemble des hypothèses évoquées dans ce chapitre et est le sujet du chapitre 7.

Chapitre 7

Construction d'un modèle incrémental de fiabilité

7.1 Introduction

Dans le chapitre précédent, nous avons décrit un processus général de validation de la fiabilité de la voiture autonome qui permet d'une part d'orienter les efforts d'enrichissement de la base de connaissances et d'autre part de renforcer l'identification des paramètres influents et d'en assurer une meilleure caractérisation. Ce processus repose sur la construction du modèle d'évaluation de la fiabilité et son ajustement en fonction des informations acquises au fur et à mesure du processus de validation. Dans ce nouveau chapitre, nous nous proposons de détailler un premier modèle d'évaluation de la fiabilité et de présenter le formalisme d'actualisation associée après une séquence de roulage de la voiture. Nous rappelons brièvement dans cette introduction des éléments de contexte à la caractérisation de la fonction de fiabilité sur un roulage donné ainsi que les verrous actuels sur ce champ.

Un roulage défini par un temps de parcours, ici une heure, est décomposé en séquence de scénarios contigus. Ceux-ci, de courtes séquences temporelles d'une ou deux minutes, décrivent :

- Le comportement du trafic routier
- Les conditions climatiques
- Les règles de conduite
- Les objets de l'infrastructure

Ces scénarios de conduite sont eux-mêmes décrits par un ensemble de paramètres qui les caractérisent. La variabilité des situations rend alors leur dénombrement quasiment impossible. Aussi, nous proposons un regroupement de scénarios par similarité en fonction de l'ensemble des paramètres qui les caractérisent et de leurs valeurs associées. Un groupe de scénarios similaires sera appelé cas d'usage. Des définitions détaillées du scénario et du cas d'usage seront proposées dans la section 7.2. D'un point de vue fiabiliste, il peut être entendu que pour des scénarios d'un même cas d'usage, si tant est qu'ils soient bien classés, le véhicule autonome devrait réagir d'une manière similaire. Toutefois, une certaine variabilité pourrait être introduite surtout pour des scénarios positionnés en limite de classe pour lesquels généralement les algorithmes de décision ou même les systèmes de détection peuvent être moins bien spécifiés. Par ailleurs, notons que

cette classification est définie de manière arbitraire en fonction de la base de connaissances à l'instant donné et que tout nouveau scénario non préalablement identifié pourrait soit remettre en cause la définition même des cas d'usage ou dans une moindre mesure l'identification d'un nouveau cas d'usage. Quoiqu'il en soit, une reclassification de certains scénarios serait à envisager.

Au vu de cette discussion, le modèle de fiabilité que nous nous proposons de construire doit permettre de capturer l'ensemble des incertitudes aléatoires – pouvant être associées à la variabilité dans un cas d'usage donné – et épistémiques – associées à la non-connaissance de certains scénarios et la difficulté résiduelle de classification. La modélisation qui en découle découple la contribution liée à l'exposition du véhicule autonome dans chaque cas d'usage (c'est-à-dire la fréquence d'apparition de chaque cas d'usage) et le comportement du véhicule autonome dans ces cas d'usage :

— D'une part elle évalue les probabilités de défaillance du système dans chaque cas d'usage,
— D'autre part elle estime les probabilités de transitions entre les cas d'usage.

On considère alors que l'apparition d'un scénario inconnu pourra éventuellement remettre en cause :

— l'évaluation des paramètres du modèle, par exemple lorsqu'ils appartiennent à un cas d'usage mal caractérisé,
— la forme du modèle, par exemple lorsque des cas d'usage doivent être ajoutés la description du problème.

Comme spécifier préalablement, le processus d'évaluation de la fiabilité est itératif en fonction des roulages programmés. A l'issue d'un roulage et en fonction de son analyse de comportement, on pourra déterminer la séquence des scénarios visités, éventuellement identifier des scénarios inconnus et, ramenée à la base de connaissances, actualiser les probabilités de défaillance dans les cas d'usage correspondants aux différents scénarios ainsi que les probabilités de transitions entre scénarios. Il est ainsi nécessaire d'évaluer ces quantités pour la base de connaissances initiale. D'un point de vue pratique, on pourra estimer ces probabilités de défaillance dites *a priori* à partir des cas d'usage contenus dans la base actuelle par le biais des résultats de simulations numériques et sur piste. Les estimations de probabilité de transition quant à elles pourront par ailleurs être complétées par des données externes comme des enregistrements effectués lors de validations de systèmes ADAS antérieurs ou des données météo. On abordera ces paramètres du modèle comme des variables aléatoires et on supposera la convergence de l'estimateur de la fiabilité vers une probabilité que l'on nommera *fiabilité vraie*. Le reste du chapitre s'organise comme suit. La section 7.3 décrit le modèle de fiabilité choisi et ses paramètres. Dans la section 7.4, la mise à jour bayésienne des paramétres du modèle pour les cas d'usages connus est discutée. Enfin la section 7.5 présente comment l'impact d'un cas d'usage inconnu est intégré au modèle. Les modélisations choisies sont volontairement classiques pour une meilleure compréhension du phénomène étudié et une meilleure prise en main par les industriels. La contribution de cette thèse réside dans l'application et l'adaptation de telle méthode dans le contexte du véhicule autonome.

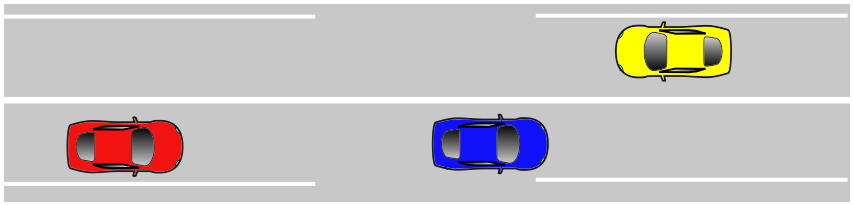


FIGURE 7.1 – schéma d'un suivi d'un véhicule sur une voie

7.2 Description d'une utilisation du système et du processus de validation

Supposons qu'on utilise le système du véhicule autonome pendant un parcours d'une durée donnée. Pendant ce parcours le système rencontre une succession de scénarios de conduite qui demandent un comportement spécifique du système pour s'adapter à ces scénarios. Pour chaque scénario rencontré, le système peut l'analyser de manière suffisante pour fonctionner correctement ou il peut mal l'interpréter et défaillir (comme défini dans le chapitre 2). Les scénarios de conduite sont décrits par un ensemble de paramètres qui les caractérisent. Le domaine de fonctionnement est alors représenté par l'espace des paramètres dont les valeurs varient dans des intervalles définis. Un scénario est un point de cet espace. Parce que la finesse de la description du scénario n'est pas suffisante pour déterminer quels scénarios entraînent une défaillance du système, on suppose que pour chaque scénario rencontré le système peut défaillir avec une certaine probabilité. Nous donnons ici un exemple fictif de domaine de fonctionnement pour étayer nos propos. Nous proposons un premier mode autonome qui ne fait que suivre un véhicule sans possibilité ni d'être dépassé ni de dépasser un véhicule, par exemple sur une route avec deux voies à double sens, schématisée en 7.1. L'unique type de scénario est une accélération ou une décélération du véhicule précédent que le véhicule autonome doit bien anticiper. Ces scénarios sont expliqués par seulement trois variables : la vitesse du véhicule précédent, la distance initiale avec le véhicule précédent, l'accélération (positive ou négative) du véhicule précédent. Ce sont les paramètres initiaux des scénarios. La figure 7.2 montre le domaine de fonctionnement paramétré où chaque point représente un scénario avec une certaine probabilité.
La probabilité de défaillance dans un scénario dépend des paramètres qui décrivent celui-ci. Elle n'est pas dépendante du temps, la durée du scénario n'a pas d'influence sur la mauvaise compréhension du système.
Cependant, si la durée des scénarios d'un même cas d'usage varie ou si elle diffère entre les cas d'usage alors elle doit être prise en compte dans le calcul de fiabilité. En effet, pour un temps d'utilisation fixé, le nombre de scénarios rencontrés fluctue d'un parcours à l'autre et a un impact sur la fiabilité résultante.

Il n'est pas faisable d'évaluer la probabilité de défaillance du système dans chaque scénario rencontré car ils sont beaucoup trop nombreux. Il est proposé par la suite de regrouper les scénarios ressemblants dans des cas d'usage, comme schématisé en figure 7.3. Ces cas d'usage sont des sous-espaces du domaine de fonctionnement et sont décrits par un sous-ensemble de paramètres du domaine de fonctionnement dont les valeurs varient dans des intervalles potentiellement restreints. Le parcours ne sera alors plus décrit précisément par l'ensemble des scénarios observés par le véhicule mais sera défini par la séquence de cas d'usage dans lesquels sont rangés les scé-

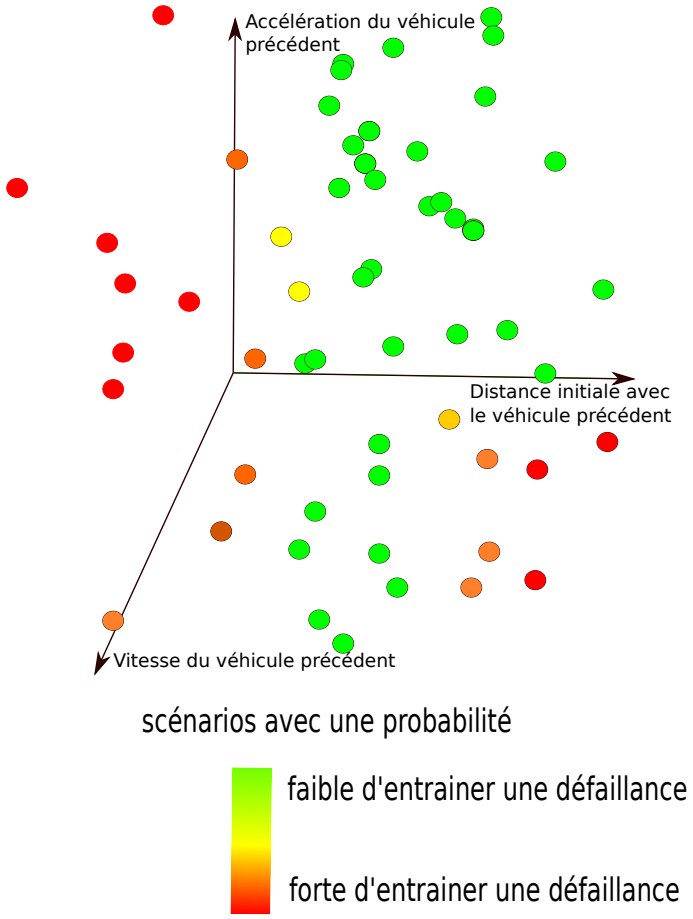


FIGURE 7.2 – exemple de scénarios dans un domaine de fonctionnement restreint

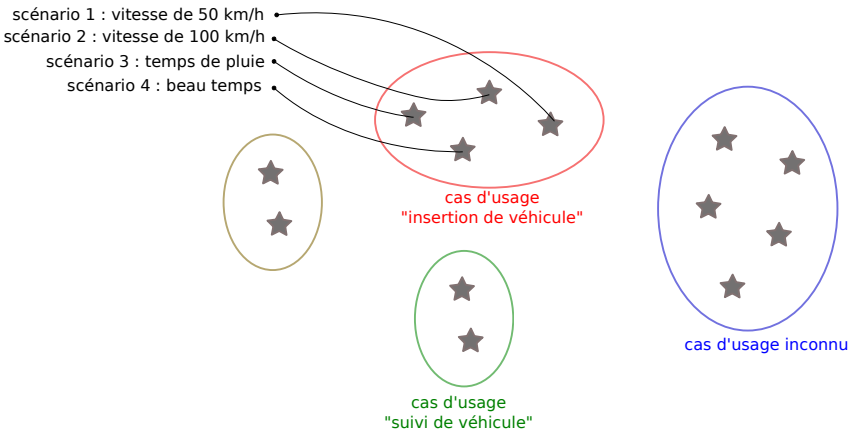


FIGURE 7.3 – regroupement des scénarios en cas d'usage

narios rencontrés.

La technique de classification des scénarios et leur critère de ressemblance choisis n'ont pas d'importance pour la construction et l'évaluation du modèle incrémental proposé dans ce chapitre. Cependant la classification a un impact sur la vitesse de convergence de ce modèle, et donc l'efficacité ou la pertinence de la méthode proposée dans le chapitre 6.

Supposons que cette classification est faite de manière statistique.
A un instant donné de validation les données collectées permettent de regrouper les scénarios en cas d'usage. Les scénarios observés ultérieurement sont rangés dans les différentes classes et font un peu évoluer les contours/délimations de la classe sans impacter de manière drastique l'évaluation de la fiabilité. Si un scénario est éloigné des classes existantes et change significativement les critères à optimiser, une nouvelle classification sera réalisée. On considérera que ce scénario est un nouveau scénario. Il apporte une information significative dans la base de données. Une nouvelle classe est soit ajoutée, par exemple si les distances entre les classes sont très grandes. Soit les classes sont reconfigurées. L'évaluation de la fiabilité risque de changer significativement. La classification peut être également mise à jour lorsque la paramétrisation choisie a été constatée insuffisante pour décrire un scénario observé. De nouveaux paramètres sont ajoutés à la description des scénarios de roulage. De la même manière ce scénario est considéré comme nouveau. Cette dernière mise à jour risque d'avoir un plus grand impact sur le calcul de fiabilité.
Ces exemples montrent qu'il est possible de détecter des scénarios remettant en cause la classification choisie. Leurs dates d'apparition peuvent être enregistrées et servir pour calibrer un modèle de croissance de fiabilité. Ce modèle apportera une indication sur la probabilité de rencontrer un scénario nouveau qui impacte significativement la classification établie et le contour des classes.

La méthode de classification n'est pas l'objet de cette thèse mais reste importante. Elle est supposée ranger le scénario dans un unique cas d'usage qui le définit. La définition de ces cas d'usage est supposée indépendante de la définition technique du système de perception, des règles de fusion ou des règles de conduite du véhicule autonome. Ces cas d'usage décrivent de manière objective un enchaînement d'actions des automobilistes et du véhicule autonome.

Pour mieux comprendre la démarche et clarifier ces terminologies, la description suivante des cas d'usage est proposée à titre d'exemple. Un cas d'usage donné se définit par une scène initiale dans laquelle se trouve le véhicule autonome, un enchaînement d'actions des véhicules environnant, une scène finale ainsi qu'un ensemble de paramètres initiaux issus de l'environnement et du véhicule autonome qui varient selon des intervalles donnés. Par exemple on définit le cas d'usage "insertion d'un véhicule" par :

- une scène initiale : au moins un autre véhicule est à côté du véhicule autonome
- des actions :
  - le véhicule se positionne devant le véhicule autonome
  - puis s'insère sur la voie du véhicule autonome devant lui
- une scène finale : le véhicule est positionné devant le véhicule autonome
- un ensemble de paramètres initiaux : des paramètres qualitatifs (le type des véhicules autour du véhicule autonome, la voie de chaque véhicule, la voie du véhicule autonome, la présence de ponts/ panneaux, les paramètres météo), des paramètres quantitatifs discrets (nombre de voies, nombre de véhicules, etc.), des paramètres quantitatifs continus(vitesses, positions, accélérations,etc.) qui varient dans des intervalles définis (vitesses comprises entre 50km/h et 80 km/h, etc.)

Les cas d'usage sont donc toutes les partitions de l'ensemble des scénarios rencontrables par le véhicule autonome, y compris les scénarios inconnus. Pour une classification choisie, le nombre de cas d'usage est supposé fini et inconnu. En effet la classification choisie délimite les frontières entre les cas d'usage, selon les scénarios enregistrés dans la base de données incomplète. Pendant une étape de roulage sur route ouverte, lors de la procédure de validation, de nouveaux scénarios très différents des précédents vont apparaître et ne pourront pas être rangés dans les cas d'usage connus. Soit la classification choisie est conservée et intègre ces nouvelles classes au fur et à mesure sans modifier les précédentes, soit la classification est jugée obsolète et de nouvelles classes sont formées. Ce nombre de cas d'usage est donc susceptible d'évoluer.

Un modèle de fiabilité est établi à partir de la description du domaine de fonctionnement dans la section suivante.

7.3 Description générale du modèle de fiabilité

Bien que moins bien maitrisé que sur piste, le séquencement des scénarios sur route ouverte présente, hors apparition soudaine d'un événement non contrôlé, un comportement peu erratique. Ainsi, la connaissance des scénarios précédents permet d'estimer, dans une certaine mesure, une probabilité d'occurrence de scénarios relativement bien identifiés dont certains paramètres resteront du même ordre, en ôtant les scénarios inconnus, les événements soudains et impromptus etc. Il est, comme cité précédemment, difficile d'évaluer l'ensemble des probabilités de transition d'un scénario à un autre aussi c'est à l'échelle du cas d'usage que nous mènerons cette étude. A titre d'illustration de ce que nous venons d'écrire, par exemple, un scénario issu du cas d'usage "suivi de véhicules par temps de pluie" entraînera plus probablement un cas d'usage "insertion d'un véhicule par temps de pluie" plutôt qu'une "insertion d'un véhicule avec un soleil éblouissant". Pour simplifier le problème il est supposé que les scénarios sont faiblement dépendants et que seul le scénario présent influe sur l'apparition du scénario futur. Cette hypothèse permet de

réduire le nombre de paramètres du modèle qui reste malgré tout très grand. En augmentant la mémoire, la méthodologie restera la même mais le grand nombre de paramètres risque de ralentir la procédure. La séquence des scénarios est alors modélisable par une chaîne de Markov qui est définie par la définition 7.1.

Définition 7.1. Soit $(\Omega, \mathcal{F}, \mathbb{P})$ un espace probabilisé et $\boldsymbol{X} := (X_n)_{n\in\mathbb{N}}$ un processus stochastique à valeurs dans un espace d'état dénombrable E. Le processus $\boldsymbol{X}$ est une chaîne de Markov si pour tout $n \in \mathbb{N}^*$ et $i_0^n \in E$, il satisfait l'équation (7.1).

$$\mathbb{P}(X_{n+1} = j|X_0 = i_0, X_1 = i_1, \cdots, X_{n-1} = i_{n-1}, X_n = i) = \mathbb{P}(X_{n+1} = j|X_n = i). \tag{7.1}$$

Toujours pour simplifier l'exposé, on suppose que l'ensemble des scénarios de chaque cas d'usage a la même durée Δ_t. Nous supposons que la découpe en scénarios peut permettre une description de scénarios de même durée. On peut artificiellement découper un scénario plus long en deux scénarios qui se suivent obligatoirement en jouant sur les probabilités de transition entre les cas d'usage.
La probabilité que le scénario, apparaissant au temps $t_{k+1} = (k+1)\Delta t$, $k \geq 0$, appartienne à un cas d'usage donné dépend du cas d'usage caractérisant le précédent scénario au temps $t_k = k\Delta t$. La matrice de transition de cette chaîne de Markov est notée $P = (P_{i,j})_{i,j\in\{1,\cdots,N\}^2}$.
$P_{i,j}$ est la probabilité que le scénario issu du cas d'usage u_j apparaisse au temps t_{k+1} sachant que le scénario au temps t_k appartient au cas d'usage u_i :

$$P_{i,j} = \mathbb{P}\left(X_{k+1} \in u_j | X_k \in u_i\right) \tag{7.2}$$

Où X_{k+1} est la variable aléatoire qui représente le scénario observé au pas de temps k, i.e. entre t_k et t_{k+1} :

$$t_0 \cdots t_k \xrightarrow[X_{k+1}]{\Delta t} t_{k+1}$$

On note S_i la probabilité de survie du véhicule autonome dans le cas d'usage u_i c'est à dire la probabilité que le système fonctionne bien quand il rencontre un scénario issu du cas d'usage u_i pendant toute la durée du scénario Δt. Cette probabilité dépend uniquement du cas d'usage dans lequel se trouve le système.

Dans la suite de cette section une démarche générale pour évaluer la fiabilité du véhicule autonome est proposée. On notera dans la suite $R(h)$ la fiabilité du véhicule autonome après une durée d'utilisation $h\Delta t$ avec $h \geq 0$, on évalue cette fiabilité de la manière suivante.

7.3.1 Initialisation

Pour simplifier le calcul, le système est supposé ne pas défaillir dans le scénario initial au temps 0. Par exemple les conditions d'activation du mode AD sont plus restrictives que celles nécessaires pendant son utilisation pour garantir un fonctionnement optimal du véhicule. On note Π_0 le vecteur des probabilités des cas d'usage π_{0i} et T la date de la première panne. Au pas de temps 1 le système a rencontré un scénario X_1. La fiabilité du système après $t_1 = \Delta t$, $R(1)$, est la probabilité de ne pas défaillir pendant t_1 quel que soit le scénario observé pendant ce laps

de temps.
La probabilité $\mathbb{P}([T > t_1] \cap [X_1 \in u_i])$ que le système rencontre le cas d'usage u_i au pas de temps 1 et qu'il soit fonctionnel après le temps t_1 est donnée par :

$$\mathbb{P}([T > t_1] \cap [X_1 \in u_i]) = \sum_{j=1}^{N} \mathbb{P}(X_0 \in u_j)\mathbb{P}(X_1 \in u_i | X_0 \in u_j)\mathbb{P}(T > t_1 | X_1 \in u_i) \tag{7.3}$$

On note S_i la probabilité $\mathbb{P}(T > t_1 | X_1 \in u_i)$ de survie du véhicule autonome dans le cas d'usage u_i, d'où :

$$\mathbb{P}([T > t_1] \cap [X_1 \in u_i]) = \sum_{j=1}^{N} \pi_{0i} P_{ij} S_i \tag{7.4}$$

Toutel les probabilités de survie dans chaque cas d'usage sont rassemblées dans la matrice diagonale notée S. On note $P = (P_{i,j})_{i,j \in \{1,\cdots,N_p\}^2}$ la matrice de transition. Soit $Q^{(1)}$ le vecteur colonne dont la ième composante est $\mathbb{P}([T > t_1] \cap [X_1 \in u_i])$, il s'exprime à l'aide de P et S :

$$Q^{(1)^T} = \Pi_0^T \times (P \times S) \tag{7.5}$$

Soit $\mathbb{1}_{N_p}$ le vecteur de taille N_p composé de 1. La fiabilité se calcule en sommant les probabilités $\mathbb{P}([T > t_1] \cap [X_1 \in u_i])$ pour chaque cas d'usage u_i avec $i \in \{1, \cdots, N_p\}$.

$$R(1) = \Pi_0^T \times (P \times S) \times \mathbb{1}_{N_p} \tag{7.6}$$

7.3.2 Fiabilité à l'état k

La fiabilité à n'importe quel temps sera alors obtenue par récurrence.
Ainsi, au pas de temps $k-1$, nous supposons que le vecteur $Q^{(k-1)}$, représentant pour chaque cas d'usage u_i avec $i \in \{1, \cdots, N\}$ la probabilité $\mathbb{P}([T \geq (k-1)\Delta t] \cap [X_{k-1} \in u_i])$, s'exprime à l'aide des matrices P et S par l'expression :

$$Q^{(k-1)^T} = \Pi_0^T \times (P \times S)^{k-1} \tag{7.7}$$

Au pas de temps k,

$$\begin{aligned}
R(k) &= \mathbb{P}(T \geq t_k) \\
&= \sum_{i_k=1}^{N_p} \sum_{i_{k-1}=1}^{N_p} \mathbb{P}(T \geq (k-1)\Delta t \cap X_{k-1} \in u_{i_{k-1}})\mathbb{P}(X_k \in u_{i_k} | X_{k-1} \in u_{i_{k+1}})\mathbb{P}(T > t_k | X_k \in u_{i_k}) \\
&= \sum_{i_k=1}^{N_p} \sum_{i_{k-1}=1}^{N_p} Q_{i_{k-1}}^{(k-1)} P_{i_{k-1} i_k} S_{i_k} \\
&= Q^{(k-1)^T} \times (P \times S) \times \mathbb{1}_{N_p}
\end{aligned} \tag{7.8}$$

On observe alors que $Q^{(k)}$ s'exprime par :

$$\begin{aligned}
Q^{(k)^T} &= Q^{(k-1)^T} \times (P \times S) \\
&= \Pi_0^T \times (P \times S)^k
\end{aligned} \tag{7.9}$$

On obtient ainsi la même expression au pas de temps k

Finalement, la fiabilité du véhicule autonome calculée au temps $h\Delta t$ vaut :

$$R(h) = \Pi_0^T \times (P \times S)^h \times \mathbb{1}_{N_p} \tag{7.10}$$

Cette modélisation, n'est pertinente que si l'ensemble des cas d'usage sont connus et leurs paramètres sont bien estimés. Ce n'est malheureusement pas le cas. Un ensemble restreint de scénarios est initialement connu et cet ensemble s'enrichit avec les étapes de validation. Le modèle ainsi défini doit donc être adapté pour prendre en compte le manque de connaissance sur les scénarios de conduite dans l'évaluation de la fiabilité.
Nous présentons dans un premier temps l'estimation des paramètres du modèle caractérisant les cas d'usage connus.

7.4 Évaluation des paramètres du modèle de fiabilité dans les cas d'usage connus

Considérons un processus de validation itératif :
À chaque étape de validation, le véhicule autonome est testé sur route ouverte pendant une durée $d_v = v\Delta t$ avec $v \in \mathbb{N}$ le nombre de scénarios observés pendant cette étape. Supposons qu'avant de commencer la procédure de validation, N_0 cas d'usage ont été identifiés, avec $N_0 \leq N$ (nombre total de cas d'usage identifiés et non identifiés). A l'étape de validation p on note N_p le nombre de cas d'usage connus, initiaux et identifiés pendant l'étape p et les précédentes.
Dans cette partie nous détaillons la mise à jour des paramètres du modèle de fiabilité caractérisant les cas d'usage connus.

La contribution de l'ensemble des cas d'usage connus dans le modèle de fiabilité se traduit dans l'estimation des variables suivantes :

- Les probabilités de survie dans les cas d'usage $(S_i)_{i\in\{1,\cdots,N_p\}}$
- Les probabilités de transition entre les scénarios des différents cas d'usage $(P_{i,j})_{i,j\in\{1,\cdots,N_p\}^2}$

7.4.1 Probabilité de défaillance du système dans les différents cas d'usage connus

La probabilité de survie du système dans le cas d'usage u_i est la probabilité que le système fonctionne correctement en rencontrant un scénario issu du cas d'usage u_i. Évaluer cette probabilité à partir de roulage sur route ouverte par une méthode d'estimation empirique est physiquement infaisable. Les probabilités sont extrêmement faibles pour obtenir une estimation précise. De plus certains cas d'usage sont plus rares et donc très peu de tests seront réalisés pour évaluer la survie du système. Il faudrait rouler bien trop longtemps pour rencontrer suffisamment de scénarios issus de ce cas d'usage.
Le chapitre 6 présente une manière d'évaluer la probabilité de défaillance du système dans chaque cas d'usage à l'aide des simulations numériques. Les simulations numériques sont en effet beaucoup moins coûteuses que les roulages réels et sont de plus contrôlables. On suppose qu'il est

possible de donner une première estimation de la probabilité de survie du système à partir de ces simulations $\widehat{S}_i$. Ces modèles numériques représentent de manière imparfaite le comportement du système, ils peuvent manquer de réalisme. De nombreuses erreurs de modélisation peuvent biaiser l'évaluation de la probabilité de survie. Les probabilités estimées par les simulations numériques ne peuvent pas être intégrées au modèle en l'état. Elles sont des valeurs initiales servant à construire les distributions *a priori* des estimations de probabilités de défaillance (événement contraire à la survie) vues comme des variables aléatoires pour rendre compte de leurs caractères incertains car mal connues. Ces distributions sont mises à jour par inférence bayésienne à partir des données issues des roulages sur route ouverte. Elles serviront aux calculs de la fiabilité par le modèle présenté dans la section 7.3.
L'inférence bayésienne est une méthode permettant de déduire la probabilité d'un événement à partir de probabilités d'autres événements déjà évaluées. Elle s'appuie principalement sur le théorème de Bayes. Elle développe une relation entre les observations du système étudié, le modèle choisi pour le représenter et les paramètres à réévaluer. La densité *a posteriori* des variables aléatoires d'intérêt sont déduites, après analyse des données, de la vraisemblance et de la densité *a priori*.

L'approche présentée s'est inspirée des travaux de Lv et al. [50]. Ils proposent une inférence bayésienne afin d'accélérer l'estimation de la fiabilité d'un logiciel d'avionique en utilisant des séquences incrémentales d'essais. Cet algorithme automatise l'atterrissage et le décollage de l'avion. Il est utilisé dans différents modes d'opération dans lesquels le système présente une probabilité de défaillance. Chaque probabilité de défaillance est considérée en tant que variable aléatoire avec une distribution étendue. Les paramètres de cette distribution sont actualisés à l'issue de chaque test, par l'intermédiaire d'une approche par inférence bayésienne, dans l'optique de converger vers la « vraie » probabilité de défaillance. Les essais sont définis dans le but d'améliorer les distributions de probabilité de défaillance qui affectent le plus la fiabilité du système.
La problématique du véhicule autonome est très proche de celle exposée. En effet les modes d'opération sont dans ce contexte les cas d'usage. Tout comme l'article, nous souhaitons évaluer les probabilités de défaillance. Et donc nous présentons comment cette méthode a été adaptée à notre problématique.

Nous détaillons cette mise à jour bayésienne après l'étape de validation p. Supposons que pendant cette étape la séquence $\mathbf{x} = (x_v)_{v\in\mathbb{N}}$ des scénarios a été observée. Soit $N_i^{(p)}$ le nombre de fois où le cas d'usage u_i a été observé pendant la séquence. Il vient

$$N_i^{(p)} = \sum_{k=1}^{v-1} \mathbf{1}_{\{x_k \in u_i\}} \tag{7.11}$$

Soit $f_i^{(p)}$ le nombre de défaillances constatées du système dans le cas d'usage u_i pendant l'étape de validation p. Dans le cas d'usage u_i, pendant la séquence $\mathbf{x}$, l'état survie/défaillant du système est supposé suivre une loi binomiale de paramètre $1 - S_i$, la probabilité de défaillance, et $N_i^{(p)}$. En effet après chaque scénario issu de u_i, on constate la défaillance ou survie du système qui est une épreuve de Bernoulli. Les variables aléatoires associées au processus de Bernoulli suivent une loi binomiale.

1. **Vraisemblance**
   Pour chaque cas d'usage u_i la vraisemblance associée à la séquence $\mathbf{x}$ est donnée par

l'équation (7.12).

$$\mathbb{P}(f_i^{(p)}|S_i) = \binom{N_i^{(p)}}{f_i^{(p)}}(1-S_i)^{f_i^{(p)}} S_i^{N_i^{(p)}-f_i^{(p)}} \tag{7.12}$$

2. **Distributions *a priori* des probabilités de survie**

La probabilité de survie S_i n'étant pas connue, son estimateur, $\widehat{S_i^{(p-1)}}$, est supposé suivre une loi bêta de paramètres $\alpha_i^{(p-1)}$ et $\beta_i^{(p-1)}$. Ces paramètres sont obtenus en étudiant les résultats de l'étape précédente $p-1$ (7.13).

$$1 - \widehat{S_i^{(p-1)}} \sim \text{beta}(\alpha_i^{(p-1)}, \beta_i^{(p-1)}) \tag{7.13}$$

Le choix de la densité *a priori* est subjectif. Le type de distribution est choisi pour ses propriétés :
— le conjugué de la loi bêta avec une binomiale en inférence bayésienne est également une loi bêta comme nous le verrons en calculant la densité *a posteriori*.
— la loi bêta est définie sur $[0, 1]$, ce qui est nécessaire pour caractériser des probabilités.
Les paramètres de cette distribution doivent permettre de quantifier notre connaissance initiale de la probabilité de défaillance et sont choisis selon la méthode présentée dans la suite de cette section.

3. **Distribution *a posteriori***

La loi *a posteriori* est donnée à partir du théorème de Bayes. En reprenant la forme générale des mises à jour bayésienne (3.7) présentée dans le chapitre 3, on peut exprimer cette loi par l'équation (7.14)

$$\mathbb{P}(\widehat{[S_i^{(p)}} = si]|f_i^{(p)}) \propto \binom{N_i^{(p)}}{f_i^{(p)}} \frac{1}{\text{B}(\alpha_i^{(p-1)}, \beta_i^{(p-1)})} (1-s_i)^{f_i^{(p)}+\alpha_i^{(p-1)}-1} s_i^{N_i^{(p)}-f_i^{(p)}+\beta_i^{(p-1)}-1} \tag{7.14}$$

avec B la fonction bêta.
Elle est proportionnelle à une loi binomiale. A la fin de l'étape de validation p la distribution du paramètre $\widehat{S_i^p}$ est donnée par (7.15)

$$\widehat{S_i^{(p)}}|f_i^{(p)} \sim \text{beta}(\alpha_i^{(p-1)} + f_i^{(p)}, \beta_i^{(p-1)} + N_i^{(p)} - f_i^{(p)}) \tag{7.15}$$

soit

$$\widehat{S_i^{(p)}}|f_i^{(p)} \sim \text{beta}(\alpha_i^{(p)}, \beta_i^{(p)}) \tag{7.16}$$

La mise à jour de la distribution des probabilités de défaillance dans chaque cas d'usage se fait donc simplement après chaque étape de validation. Il reste à choisir au mieux les paramètres $\alpha_i^{(0)}$ et $\beta_i^{(0)}$ de la distribution *a priori* initiale en début de validation.

Les simulations numériques du véhicule autonome apportent une première estimation de la probabilité de défaillance dans chaque cas d'usage. Les paramètres des distributions *a priori* peuvent

être déterminés à partir de ces valeurs. Reprenons $\widehat{S}_i$, la probabilité estimée par simulation numérique dans le cas d'usage u_i. Nous posons :

$$\alpha_i^{(0)} = \omega_i(1-\widehat{S}_i) \qquad \text{et} \qquad \beta_i^{(0)} = \omega_i\widehat{S}_i \tag{7.17}$$

avec ω_i un coefficient de $\mathbb{R}^{+*}$. La distribution *a priori* aura alors pour espérance l'équation (7.18)

$$E[1-\widehat{S_i^{(0)}}] = \frac{\alpha_i^{(0)}}{\alpha_i^{(0)}+\beta_i^{(0)}} = 1-\widehat{S}_i \tag{7.18}$$

qui est la probabilité de défaillance estimée par la simulation numérique et pour variance donnée par l'équation (7.19).

$$\text{var}[1-\widehat{S_i^{(0)}}] = \frac{\alpha_i^{(0)}\beta_i^{(0)}}{(\alpha_i^{(0)}+\beta_i^{(0)})^2(\alpha_i^{(0)}+\beta_i^{(0)}+1)} = \frac{(1-\widehat{S}_i)\widehat{S}_i}{(\omega_i+1)} \tag{7.19}$$

Le poids ω_i n'a donc aucun impact sur l'espérance de la distribution mais influe sur la variance de celle-ci. Plus ce coefficient est grand et plus l'étendue de la distribution sera resserrée sur l'espérance de la fonction. Il caractérise donc la confiance *a priori* que l'on a de la probabilité de défaillance estimée par les simulations numériques.
L'espérance *a posteriori* de la probabilité de survie à l'état 1 après $N_i^{(1)}$ visites dans le cas d'usage u_i et après avoir observé $x_i^{(1)}$ défaillances du système, est alors donnée par l'expression suivante.

$$E\left[1-\widehat{S_i^{(1)}}|X_i = x_i^{(1)}\right] = \frac{(N_i^{(1)}+\alpha_i^{(0)})}{(N_i^{(1)}+\alpha_i^{(0)}+\beta_i^{(0)})} \tag{7.20}$$

D'où

$$E\left[1-\widehat{S_i^{(1)}}|X_i = x_i^{(1)}\right] = \frac{N_i^{(1)}}{(N_i^{(1)}+\alpha_i^{(0)}+\beta_i^{(0)})} \times \frac{x_i^{(1)}}{N_i^{(1)}} + \frac{\alpha_i^{(0)}+\beta_i^{(0)}}{(N_i^{(1)}+\alpha_i^{(0)}+\beta_i^{(0)})} \times (1-\widehat{S}_i) \tag{7.21}$$

et

$$E\left[1-\widehat{S_i^{(1)}}|X_i = x_i^{(1)}\right] = \frac{N_i^{(1)}}{(N_i^{(1)}+\omega_i)} \times \frac{x_i^{(1)}}{N_i^{(1)}} + \frac{\omega_i}{(N_i^{(1)}+\omega_i)} \times (1-\widehat{S}_i) \tag{7.22}$$

$\frac{\omega_i}{N_i^{(1)}}$ n'est autre que l'estimateur de la moyenne empirique de la probabilité de défaillance du système dans le cas d'usage u_i. Nous observons donc que l'espérance *a posteriori* est une somme pondérée de l'estimateur fréquentiste et de la valeur *a priori* de la probabilité de défaillance. Plus le poids ω_i est grand et plus la valeur donnée *a priori* aura de l'influence sur le résultat final. l'estimateur empirique converge vers la vraie probabilité de survie avec une vitesse en $\sqrt{N_i}$, $N_i \in \mathbb{N}$ étant le nombre de fois où u_i a été observé. Cette expression montre que l'espérance *a posteriori* converge vers la probabilité à estimer avec une vitesse qui varie selon la valeur de l'espérance *a priori* donnée et le poids choisi.

Les connaissances qu'apportent les simulations numériques peuvent de cette manière facilement être intégrées dans le modèle de fiabilité. Les distributions *a priori* peuvent se construire en choisissant judicieusement les coefficients ω_i en fonction de la confiance que l'on peut donner aux résultats des simulations numériques. Cette confiance peut s'identifier en tenant compte du niveau de réalisme des essais numériques et des premiers retours d'expériences sur le comportement du système dans les cas d'usage connus. Nous allons maintenant décrire une méthode similaire pour les probabilités de transition entre les cas d'usage.

7.4.2 Estimation de la matrice de transition

Supposons premièrement que nous connaissions tous les cas d'usage caractérisant le domaine de fonctionnement. On note $\mathbf{X} = (X_n)_{n\in\mathbb{N}}$ la chaîne de markov représentant les usages du véhicule autonome, nous notons $\mathcal{U}$ son espace d'état composé de l'ensemble des cas d'usages. Cette chaine de Markov est supposée être ergodique (définition 7.2), tout scénario issu d'un cas d'usage donné sera observé par le véhicule autonome au bout d'un certain temps quel que soit le cas d'usage du scénario initial.

Définition 7.2. La chaîne de Markov $(X_n)_{n\in\mathbb{N}}$ est dite irréductible si pour tout $i, j \in \mathcal{U}$

$$\mathbb{P}_i(T_j < \infty) > 0 \tag{7.23}$$

avec $T_j = \inf\{k > 0 : X_k \in \{u_j\}\}$ le temps de retour dans l'état j. Si, de plus il existe un état $a \in E$ tel que

$$\mathbb{P}_a(T_a < \infty) = 1, \tag{7.24}$$

alors la chaîne $(X_n)_{n\in\mathbb{N}}$ est dite irréductible et récurrente. La récurrence est positive si l'espérance de cette variable aléatoire, $\mathbb{E}_a(T_a)$, est finie. Une chaîne de Markov irréductible et récurrente positive est appelée ergodique.

Cette hypothèse est très forte mais réaliste sur un horizon temporel infini il faudra vérifier que la classification choisie permette cette hypothèse.
Soit $\mathbf{x} = x_1, x_2 \cdots, x_n$ l'ensemble des scénarios observés pendant cette étape, $\mathbf{x}$ est une réalisation de $\mathbf{X}$.

La probabilité de cette réalisation $\mathbb{P}(\mathbf{X} = \mathbf{x})$ est donné par l'équation 7.25.

$$\mathbb{P}(\mathbf{X} = \mathbf{x}) = \mathbb{P}(X_1 = x_1) \prod_{k=2}^{k=n} \mathbb{P}\left(X_k = x_k | X_{k-1} = x_{k-1}\right) \tag{7.25}$$

Nous proposons dans un premier temps d'estimer les probabilités de transition par maximum de vraisemblance à l'étape de validation p avec $\mathcal{U}_p = \mathcal{U}$.

1. **Estimation par maximum de vraisemblance**

   Soit N_i^{pv} le nombre de fois où le cas d'usage u_i a été observé pendant l'ensemble des séquences de validation et $N_{i,j}^{pv}$ le nombre de fois que le cas d'usage u_j est observé après la rencontre de u_i.

   $$N_i^{pv} = \sum_{k=1}^{pv-1} \mathbf{1}_{\{X_k=i\}}$$

   et

   $$N_{i,j}^{pv} = \sum_{k=1}^{pv-1} \mathbf{1}_{\{X_k=i, X_{k+1}=j\}}$$

La vraisemblance de la matrice de transition est alors donnée par :

$$L(p) = \prod_{i=1}^{N_p} \prod_{j=1}^{N_p} P_{i,j}^{N_{i,j}^{pv}} \tag{7.26}$$

et les estimateurs du maximum de vraisemblance associés sont [6].

$$\widehat{P}_{i,j}^{pv} = \begin{cases} \frac{N_{i,j}^{pv}}{N_i^{pv}}, & \text{si } N_i^{pv} \neq 0 \\ 0, & \text{si } N_i^{pv} = 0 \end{cases} \tag{7.27}$$

Selon le théorème 7.1, $\frac{1}{n}N_i^n$ et $\frac{1}{n}N_{i,j}^n$ convergent. Soit $\mu = (\mu_i)_{i \in N_p}$ le vecteur stationnaire donné par le théorème 7.2, $\widehat{\mu}_i = \frac{1}{n}N_i^n$ est l'estimateur empirique de μ_i.
$\widehat{P}_{i,j}^{pv}$ est le ratio de deux variables qui convergent vers deux nombres réels finis et strictement supérieurs à zéro, on en conclut qu'il converge presque sûrement vers $P_{i,j}$. Selon Billingsley [6], cet estimateur converge avec une vitesse de $\sqrt{pv}$.

Théorème 7.1. *Loi forte des grands nombres :*
Pour tout $x \in \mathcal{U}_p$ et tout $(i,j) \in \mathcal{U}_p^2$

$$\frac{1}{n}N_i^n \xrightarrow[n\to\infty]{\mathbb{P}_x - p.s.} \mu_i \tag{7.28}$$

$$\frac{1}{n}N_{i,j}^n \xrightarrow[n\to\infty]{\mathbb{P}_x - p.s.} \mu_i P_{i,j} \tag{7.29}$$

Théorème 7.2. *La chaîne de Markov $(X_n)_{n\in\mathbb{N}}$ est ergodique si et seulement si elle admet une mesure stationnaire $\mu(\cdot)$, complètement déterminée par le vecteur $\boldsymbol{\mu}$ appelé vecteur stationnaire, qui vérifie l'égalité suivante :*

$$\boldsymbol{\mu} = \boldsymbol{\mu} P \tag{7.30}$$

Si ces cas d'usages ne sont pas connus, les probabilités de transition estimées seront biaisées car le modèle de Markov sera mal choisi. Elles ne convergeront réellement vers les vraies probabilités de transition que lorsque l'ensemble des cas d'usages auront été observés. Ces estimateurs restent néanmoins nécessaires pour l'évaluation de la fiabilité. Ils seront réajustés pour tenir compte des cas d'usages manquants dans la section 7.5.
Nous présentons par la suite une autre méthode d'estimation également biaisée, une méthode par inférence bayésienne, permettant d'estimer plus rapidement ces probabilités de transition en apportant de la connaissance provenant de sources diverses d'information.

2. **Avec une information *a priori* par inférence Bayésienne**

Il est peu probable qu'aucune information ne soit disponible sur l'occurrence d'un cas d'usage connu. On suppose que pour certains cas d'usage une probabilité *a priori* est donnée. Strelioff et al. [81] estiment les paramètres d'une chaîne de Markov d'un ordre k avec $k \geq 0$ par inférence Bayésienne. L'ordre k correspond à la mémoire du modèle. Ils précisent qu'en plus de mettre à jour les paramètres du modèle de manière efficace,

cette méthode d'estimation donne un critère de comparaison entre plusieurs modèles de Markov choisis. Les modèles comparés sont des modèles de Markov dont l'ordre diffère. Dans notre contexte, nous nous restreignions à une chaîne de Markov (d'ordre 1). Si ce choix est insuffisant pour modéliser le problème, il est alors tout à fait possible d'étendre le modèle à un ordre plus important. Cela entrainera un nombre conséquent de paramètres à évaluer mais cela ne changera pas fondamentalement la stratégie mise en place dans cette étude.

Le scénario rencontré à un instant donné est supposé suivre une loi Multinomiale $M_i(P_{i1}, \cdots, P_{iN_p})$. Nous notons $\boldsymbol{P}_i$ le vecteur des probabilités de transition depuis u_i vers le cas d'usage de l'instant suivant. Nous souhaitons évaluer les paramètres $(\boldsymbol{P}_i)_{i\in\{1,\cdots,N_p\}}$ de l'ensemble des N_p lois multinomiales décrivant la chaîne de Markov.

(a) **Vraisemblance** :
Soit la séquence $\mathbf{x} = \{x_0, x_1, \cdots, x_v\}$ des scénarios observés pendant l'étape p de validation. La vraisemblance $L(p)$ s'exprime suivant une équation similaire à (7.26).

(b) **Loi *a priori*** :
On suppose que les vecteurs des estimateurs $\widehat{\boldsymbol{P}_i^{(p-1)}}$, à l'étape $p-1$, suivent des lois *a priori* de Dirichlet $D(\alpha_{i1}^{(p-1)}, \cdots, \alpha_{iN_p}^{(p-1)})$, de densités exprimées en (7.31). La loi de Dirichlet est vue comme la généralisation multinomiale de la loi bêta.

$$f(\widehat{P_{i1}^{(p-1)}} = p_{i1}, \ldots, \widehat{P_{iN_p}^{(p-1)}} = p_{iN_p}|\alpha_{i1}^{(p-1)}, \ldots, \alpha_{iN_p}^{(p-1)}) = \frac{1}{\mathrm{B}(\alpha_{i1}^{(p-1)}, \ldots, \alpha_{iN_p}^{(p-1)})} \prod_{j=1}^{N_p} p_{ij}^{\alpha_{ij}^{(p-1)}-1} \tag{7.31}$$

avec $\mathrm{B}(\alpha_{i1}^{(p-1)}, \ldots, \alpha_{iN_p}^{(p-1)})$ la constante de normalisation qui est la fonction bêta multinomiale

$$\mathrm{B}(\alpha_{i1}^{(p-1)}, \ldots, \alpha_{iN_p}^{(p-1)}) = \frac{\prod_{j=1}^{N_p} \Gamma(\alpha_{ij}^{(p-1)})}{\Gamma\left(\sum_{j=1}^{N_p} \alpha_{ij}^{(p-1)}\right)} \tag{7.32}$$

La loi *a priori* de l'ensemble des $\widehat{\boldsymbol{P}_i^{(p-1)}}$ peut alors s'écrire :

$$f(\widehat{\boldsymbol{P_i}^{(p-1)}} = \boldsymbol{p_i}, \ldots, \widehat{\boldsymbol{P_{N_p}}^{(p-1)}} = \boldsymbol{p}_{N_p}; \alpha_{11}^{(p-1)}, \ldots, \alpha_{1N_p}^{(p-1)}, \ldots, \alpha_{ij}^{(p-1)}, \ldots, \alpha_{N_pN_p}^{(p-1)}) = \prod_{i=1}^{N_p} f(\widehat{P_{i1}^{(p-1)}} = p_{i1}, \ldots, \widehat{P_{iN_p}^{(p-1)}} = p_{iN_p}|\alpha_{i1}^{(p-1)}, \ldots, \alpha_{iN_p}^{(p-1)}) \tag{7.33}$$

(c) **Loi *a posteriori*** :
La loi *a posteriori* est donnée à partir du théorème de Bayes, en reprenant l'expression (3.7), on peut exprimer la loi *a posteriori* par (7.34).

$$f(\widehat{\boldsymbol{P_i}^{(p)}} = \boldsymbol{p_i}, \ldots, \widehat{\boldsymbol{P_{N_p}}^{(p)}} = \boldsymbol{p}_{N_p}|\mathbf{x}) \propto \frac{1}{\prod_{i=1}^{N_p} \Gamma\left(\sum_{j=1}^{N_p} \alpha_{ij}^{(p-1)}\right)} \prod_{i=1}^{N_p} \prod_{j=1}^{N_p} \Gamma(\alpha_{ij}^{(p-1)}) p_{ij}^{\alpha_{ij}^{(p-1)}+N_{i,j}^{(p)}-1} \tag{7.34}$$

La densité de la loi *a posteriori* est proportionnelle au produit des densités de lois de Dirichlet de paramètres α_{ij}^{p} d'expression (7.35).

$$\alpha_{ij}^{(p)} = \alpha_{ij}^{(p-1)} + N_{i,j}^{(p)} \tag{7.35}$$

L'inférence bayésienne Dirichlet-Multinomiale est donc la généralisation de l'inférence bayésienne Bêta-Binomiale à une variable aléatoire multivariée.
Nous devons maintenant sélectionner les paramètres des distributions *a priori* initiales en début de validation. La méthode employée est exactement la même que celle présentée dans la section 7.4.1. Supposons que nous pouvons dégager des premières estimations des probabilités de transition,$(\widehat{P_{ij}})_{j\in\{1,\cdots,N_p\}}$, depuis un cas d'usage u_i vers les $(u_j)_{j\in\{1,\cdots,N_0\}}$ à partir de données issues de sources variées d'information. Nous posons le poids ν_i dans $\mathbb{R}^{+*}$, et nous exprimons les paramètres,$(\alpha_{ij}^{(0)})_{j\in\{1,\cdots,N_p\}}$ de la loi de Dirichlet *a priori* quelque soit j de la manière présentée dans l'équation (7.36).

$$\alpha_{ij}^{(0)} = \widehat{P_{ij}} \times \nu_i \tag{7.36}$$

Le poids ν_i a exactement la même fonction que le poids ω_i, (7.22), pour l'inférence Bayésienne Bêta-Binomiale : il caractérise la confiance que l'on peut donner aux estimations *a priori* des probabilités de transition.

En effet l'espérance de la variable aléatoire *a priori* $\widehat{P_{ij}^{(0)}}$ est donnée par :

$$E\left[\widehat{P_{ij}^{(0)}}\right] = \frac{\alpha_{ij}^{(0)}}{\sum_{j=1}^{N_p}\alpha_{ij}^{(0)}} = \widehat{P_{ij}} \tag{7.37}$$

Sa variance est :

$$Var\left[\widehat{P_{ij}^{(0)}}\right] = \frac{\widehat{P_{ij}}(\widehat{P_{ij}}-1)}{(\nu_i+1)} \tag{7.38}$$

Enfin l'espérance *a posteriori* $\widehat{P_{ij}^{(1)}}$ est exprimée par :

$$\begin{aligned} E\left[\widehat{P_{ij}^{(1)}}|N_{i,j}=N_{i,j}^{(1)}\right] &= \frac{\alpha_{ij}^{(0)}+N_{i,j}^{(1)}}{(\nu_i+N_i^{(1)})} \\ &= \frac{\widehat{P_{ij}}\times\nu_i+N_{i,j}^{(1)}}{(\nu_i+N_i^{(1)})} \\ &= \widehat{P_{ij}}\times\frac{\nu_i}{(\nu_i+N_i^{(1)})}+\frac{N_{i,j}^{(1)}}{N_i^{(1)}}\times\frac{N_i^{(1)}}{(\nu_i+N_i^{(1)})} \end{aligned} \tag{7.39}$$

Nous retrouvons bien des expressions semblables aux distributions *a priori* et *a posteriori* des probabilités de défaillances.

Nous avons vu comment évaluer les différents paramètres de la chaîne de Markov dans le cas où tous les cas d'usage sont connus. Malheureusement il est très probable que certains cas d'usage ne soient pas connus et que le nombre d'états de la chaîne de Markov soit plus important. Dans la partie 7.5 nous allons montrer comment intégrer de nouveaux paramètres dans le modèle de fiabilité pour tenir compte de l'influence d'un cas d'usage inconnu dans le calcul de fiabilité.

7.5 Évaluation des paramètres du modèle de fiabilité pour tenir compte des cas d'usage inconnus

Des cas d'usage inconnus dans le domaine de fonctionnement rendent le modèle de fiabilité incomplet. Ni leurs probabilités d'occurrence ni les probabilités de survie du système dans ces cas d'usage ne sont intégrées dans le modèle. La fiabilité évaluée est donc biaisée par le faible niveau de connaissance. Pour pallier à ce problème, un nouveau cas d'usage, nommé le cas d'usage inconnu, est ajouté artificiellement au modèle pour rendre compte de l'impact de ce défaut de connaissance. Ce cas d'usage est caractérisé comme les autres cas d'usage par deux types de paramètres, les probabilités de transition depuis et vers ce cas d'usage et la probabilité de survie du système supposée dans le cas d'usage. La première partie de cette section propose une méthode d'estimation de la probabilité d'apparition d'un nouveau cas d'usage. La seconde partie montre comment supposer la probabilité de survie du véhicule dans un cas d'usage inconnu. Enfin la dernière partie intègre ces nouveaux paramètres dans le modèle de fiabilité du système.

7.5.1 Évaluation de la probabilité d'apparition d'un cas d'usage inconnu

Au cours des étapes de validation, de nouveaux cas d'usage apparaissent et enrichissent petit à petit le modèle. Le nombre de cas d'usage nouvellement identifiés dépend du niveau de maturité du système, de l'étendue du domaine de fonctionnement et des roulages de validation réalisés. Tout comme en fiabilité des logiciels, la vitesse de détection des bugs et leur correction dépendent de plusieurs paramètres qui sont principalement liés au niveau de maturité et aux méthodes de conception et de validation en plus de l'algorithme à développer lui- même. Dans le chapitre 3, nous faisons l'analogie entre l'apparition de scénarios issus de nouveaux cas d'usage et l'apparition de bugs dans un logiciel. Un modèle de croissance de fiabilité des logiciels évalue la probabilité d'apparition d'un futur bug en analysant les temps d'apparition des bugs déjà observés. Le modèle choisi est le modèle de Goel Okumoto. Les hypothèses sous-jacentes nous semblent appropriées dans notre contexte comme expliqué dans le chapitre 3. Cependant en fiabilité des logiciels, le choix du modèle se fait après analyse des premières apparitions des bugs. Il peut ne pas bien prédire la probabilité d'apparition d'un futur cas d'usage. Il est tout à fait possible de le remplacer par un modèle plus précis. Cela ne remet pas en cause la construction générale du modèle. Nous rappelons les hypothèses du modèle de Goel Okumoto :

- Il existe un nombre aléatoire N de cas d'usages résiduels ayant pour espérance a.
- Une fois un nouveau cas d'usage rencontré, celui-ci est connu et ne fait plus partie de la liste des inconnus (corrections parfaites).
- La vitesse d'apparition des cas d'usage est supposée proportionnelle au nombre de cas d'usage encore inconnus avec un facteur de proportionnalité b.

Nous précisons ici la méthode d'estimation employée pour obtenir la probabilité d'apparition d'un nouveau cas d'usage. L'expression de la valeur moyenne d'apparition de nouveaux cas d'usage après l'instant t pour le modèle de Goel Okumoto est donnée par :

$$M(t) = a(1 - e^{-bt}) \tag{7.40}$$

Pour évaluer les paramètres du modèle, la méthode du maximum de vraisemblance est souvent employée. Cette méthode est efficace pour un nombre important de cas d'usage déjà observés.

Dans l'hypothèse où de rares cas d'usage sont détectés, les méthodes d'optimisation pour maximiser la vraisemblance ne convergent pas et ne donnent alors aucun résultat. Pour obtenir une approximation même après l'apparition d'un unique cas d'usage, nous préférons utiliser une méthode d'inférence bayésienne dite "non informative" par l'usage de la probabilité *a priori* de Jeffrey et nous suivons la procédure choisie par Yin et Trivedi [87]. On pose $p(a,b) \propto \frac{1}{a}$.
Soit $\mathbf{t} = (t_1, \cdots, t_{n_p})$ le vecteur des temps d'apparition des n_p nouveaux cas d'usage rencontrés depuis le début des validations jusqu'à la dernière séquence de validation p. La vraisemblance de ce vecteur en considérant le modèle de Goel Okumoto de paramètres a et b est exprimée par :

$$p(\mathbf{t}|a,b) = e^{-a(1-e^{-bt_{n_p}})} \times a^{n_p} b^{n_p} e^{-b\sum_{i=1}^{n_p} t_i} \tag{7.41}$$

On en déduit la probabilité *a posteriori* des paramètres a et b de ce modèle donnée par les équations suivantes :

$$p(a,b|\mathbf{t}) \propto p(a,b)p(\mathbf{t}|a,b) \tag{7.42}$$

$$p(a,b|\mathbf{t}) \propto \frac{1}{a} \times e^{-a(1-e^{-bt_{n_p}})} \times a^{n_p} b^{n_p} e^{-b\sum_{i=1}^{n_p} t_i} \tag{7.43}$$

La probabilité de ne pas observer de nouveaux cas d'usage à l'instant suivant est donnée par l'expression (7.44) :

$$\overline{P_u^{(p)}} = 1 - P_u^{(p)} = e^{-(a(1-e^{-b(t_{n_p}+1)})-a(1-e^{-b(t_{n_p})}))} = g(a,b) \tag{7.44}$$

Cette probabilité est également une variable aléatoire de fonction de répartition :

$$F_{\overline{P_u^{(p)}}}(\overline{P_u^{(p)}} = l) = \int_{D_l} p(a,b|\mathbf{t}) da db \tag{7.45}$$

avec $D_l = \{(a,b)|g(a,b) \leq l\}$. La fonction de répartition est construite empiriquement par la méthode de Monte Carlo sur les paramètres a et b. La variable aléatoire caractérisant la probabilité des cas d'usage inconnus peut ainsi être ajoutée au modèle comme nous le montrerons dans la section 7.5.3.

7.5.2 Évaluation de la survie du véhicule autonome dans un cas d'usage inconnu

Il est naturellement impossible de prédire la probabilité de survie du système dans un cas d'usage inconnu. Pour autant le modèle de fiabilité doit comptabiliser un potentiel danger à ne pas connaître ce type de cas d'usage. Plusieurs hypothèses sont possibles pénalisant plus ou moins fortement la fiabilité estimée. On pourrait premièrement décider qu'un cas d'usage inconnu ne peut pas être bien analysé par le véhicule autonome et quoiqu'il advienne cela débouchera sur une défaillance. On peut également supposer que le cas d'usage inconnu ne doit pas être si éloigné de ceux déjà observés. Les règles du code de la route restent les mêmes et le système pourra malgré tout s'adapter avec les lois de commande implémentées. En partant de cette dernière hypothèse, nous proposons de prendre S_u la probabilité de survie du véhicule autonome dans un cas d'usage inconnu comme la plus faible des probabilités de survie des cas d'usage connus, cf. (7.46) . Les

probabilités estimées de survie des cas d'usage connus sont des variables aléatoires, S_u est donc également une variable aléatoire.

$$S_u = \min_{u_i \in \mathcal{U}_p} \widehat{S}_i \tag{7.46}$$

Si cette hypothèse influence fortement les évaluations de la fiabilité, des études dédiées devront être engagées pour obtenir un modèle qui pénalise l'évaluation de la fiabilité afin d'éviter tout arrêt prématuré des essais de validation sans ralentir inutilement la phase de validation dans le cas d'une pénalisation trop forte.
Si beaucoup de cas d'usage inconnus ont été détectés pendant les roulages de validation, il serait toutefois possible et préférable de proposer une nouvelle estimation de S_u. S_u serait évaluée en analysant la réaction du véhicule autonome lorsqu'il a rencontré un cas d'usage inconnu.

7.5.3 Intégration de nouveaux paramètres dans le modèle de fiabilité

On se propose d'intégrer les paramètres estimés précédemment dans le modèle de fiabilité. Pour cela on nomme $\widetilde{\boldsymbol{P}}$ la nouvelle matrice de transition intégrant le cas d'usage inconnu et $\widetilde{\boldsymbol{S}}$ la matrice diagonale des probabilités de survie du véhicule autonome en ajoutant la probabilité S_u.

— **Transition d'un cas d'usage connu ou inconnu vers un cas d'usage inconnu**

La probabilité du système de rencontrer un cas d'usage inconnu après la durée Δt quel que soit le cas d'usage à l'instant précédent est estimée par la méthode de Goel Okumoto à l'étape p et est notée $P_u^{(p)}$.
Soit $\mathcal{U}^{(p)\star} = \mathcal{U}^{(p)} \cup \{u_u\}$ l'ensemble contenant les cas d'usage connus et le cas d'usage inconnu, pour tout cas d'usage $u_i \in \mathcal{U}^{(p)\star}$ rencontré à l'instant $k\Delta t$, la probabilité de rencontrer un cas d'usage inconnu à l'instant $(k-1)\Delta t$ est alors exprimée par (7.47).

$$\widetilde{P_{iu}}^{(p)} = P_u^{(p)} \tag{7.47}$$

— **Transition d'un cas d'usage connu vers un cas d'usage connu**
La probabilité de rencontrer un cas d'usage connu après avoir rencontré le cas d'usage u_i vaut :

$$\sum_{j \in \{1,\dots,Np\}} \widetilde{P_{ij}}^{(p)} = 1 - P_u^{(p)} \tag{7.48}$$

Or les probabilités de transition sont estimées, $\widehat{P_{ij}}^{(p)}$, en supposant que l'ensemble des cas d'usage connus décrivent complètement le domaine de fonctionnement. Nous avons l'égalité $\sum_{j \in \{1,\dots,Np\}} P_{ij} = 1$. Nous réévaluons les probabilités de transition entre les cas d'usage connus en ajoutant la probabilité du cas d'usage inconnu. Les probabilités sont ajustées en conservant le même poids. On se propose alors de calculer ces transitions selon :

$$\widetilde{Pij}^{(p)} = \widehat{P_{ij}}^{(p)} \times \left(1 - P_u^{(p)}\right) \tag{7.49}$$

— **Transition d'un cas d'usage inconnu vers un cas d'usage connu**
Ne connaissant pas les cas d'usage inconnus il ne semble pas évident de trouver des

transitions vers les cas d'usage connus. On se propose de donner la même probabilité pour chaque transition. On a alors pour tout $i \in \{1, \cdots, N_p\}$ (7.50)

$$\widetilde{P_{ui}} = \frac{1}{N_p}(1 - P_u^{(p)}) \tag{7.50}$$

7.6 Modèle de fiabilité ajusté

Cette dernière section a pour but de faire la synthèse du modèle présenté tout au long de ce chapitre. En repartant de la forme générale de la fiabilité exprimée dans l'équation (7.10), nous exprimons son ajustement à l'étape de validation p pour prendre en compte les incertitudes épistémiques. Nous posons $\Pi_0^{(p)}$ le vecteur des probabilités d'apparition du cas d'usage initial, qui est vu en début de parcours. Il peut soit être connu et l'apparition d'un nouveau scénario s'interprète par l'ajout d'une dimension au vecteur. Il peut soit être estimé à chaque étape de validation de la même manière que les probabilités de transition. La fiabilité pour un nombre h de scénarios fixés est donnée dans l'équation (7.51)

$$R(h)^{(p)} = {\Pi_0^{(p)}}^T \times \left(\widetilde{P^{(p)}} \times \widetilde{S^{(p)}}\right)^h \times \mathbb{1}_{N_p+1} \tag{7.51}$$

avec $\widetilde{P^{(p)}}$ la matrice des probabilités de transition ajustées à l'étape p, construite à partir de la matrice des transitions estimée dans le domaine restreint $\mathcal{U}_p$ à l'étape p, $\widehat{P^{(p)}}$, et la probabilité d'apparition d'un cas d'usage inconnu,$P_u^{(p)}$, estimée à l'étape de validation p,

$$\widetilde{P^{(p)}} = \begin{bmatrix} \widehat{P^{(p)}} \times (1 - P_u^{(p)}) & P_u^{(p)} \\ {\mathbb{1}_{N_p}}^T \times \frac{(1-P_u^{(p)})}{N_p} & P_u^{(p)} \end{bmatrix} \tag{7.52}$$

et $\widetilde{S^{(p)}}$ la matrice diagonale des probabilités de survie ajustée à l'état p qui combine la matrice diagonale des probabilités $\widehat{S^{(p)}}$ de survie estimée dans le domaine restreint et $S_u^{(p)}$ la probabilité de survie prédite à l'étape p. L'estimation de la fiabilité est résumée sur la Figure 7.4.

$$\widetilde{S^{(p)}} = \begin{bmatrix} \widehat{S^{(p)}} & 0 \\ 0 & S_u^{(p)} \end{bmatrix} \tag{7.53}$$

Nous obtenons ainsi un modèle modulaire adapté au problème posé.

7.7 Conclusion

Nous avons présenté un cadre général et l'avons exposé au travers d'une configuration particulière comme preuve de faisabilité. La modélisation résultante décompose la fiabilité pour estimer séparément la contribution de chaque cas d'usage composant le domaine de fonctionnement. Elle découple également les probabilités de survie du système de chaque cas d'usage et les transitions entre ces derniers. Les paramètres ne sont pas bien connus et leurs estimations devront être

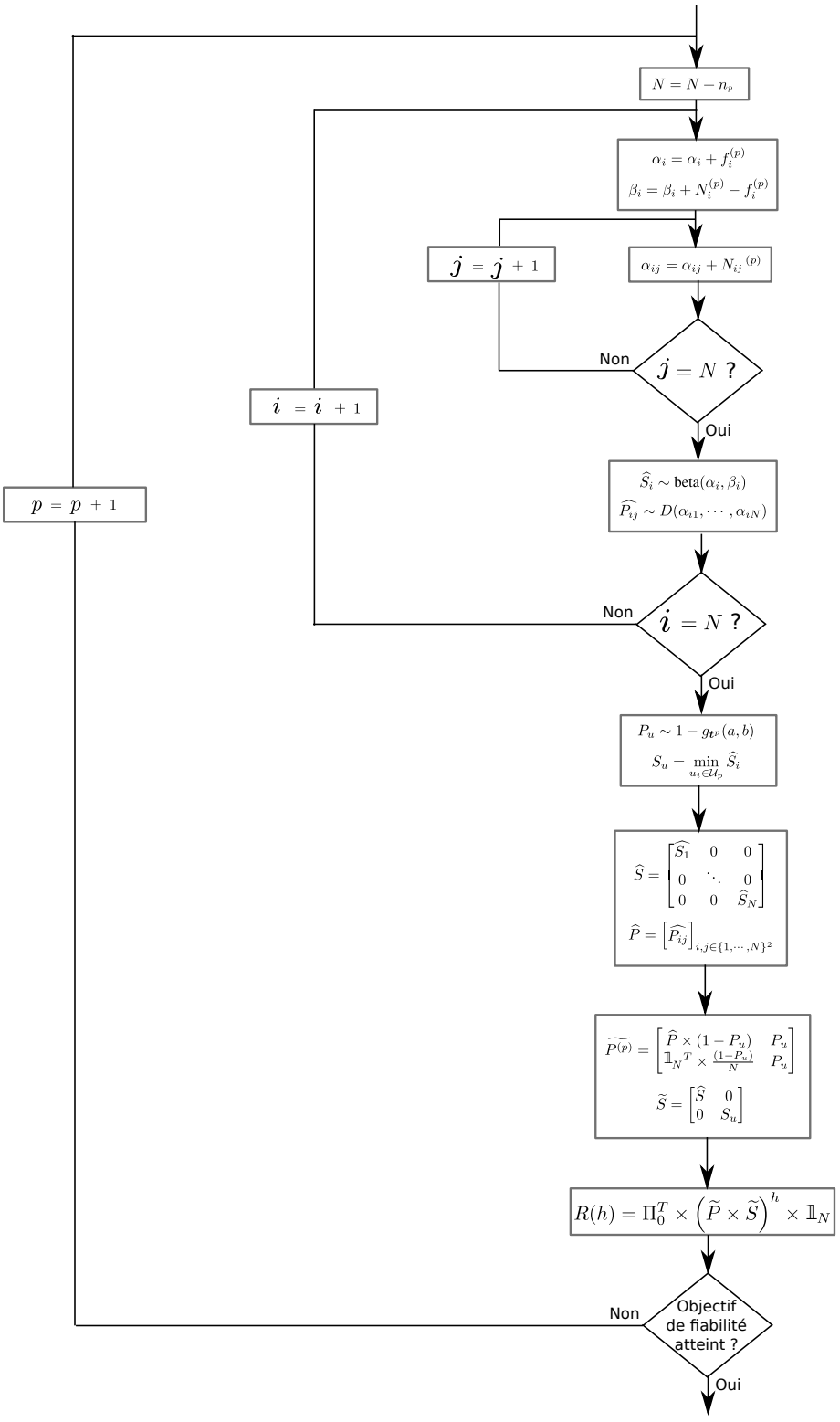


FIGURE 7.4 – Logigramme de l'estimation itérative de la fiabilité du système

renforcées pendant les essais de validation. Pour se faire, ils sont donnés *a priori* et mis à jour par inférence bayésienne.
Le modèle global est composé de plusieurs sous-parties :

- la chaîne de Markov qui représente l'enchaînement des cas d'usages,
- les distributions *a priori* des paramètres, bêta-binomiale pour les probabilités de survie et Dirichlet-multinomiale pour les probabilités de transition,
- le modèle de croissance de fiabilité de Goel-Okumoto pour évaluer la probabilité des cas d'usages inconnus avec une inférence bayésienne pour estimer ses paramètres.
- la plus faible des probabilités de survie dans les cas d'usages connus pour prédire la probabilité de survie du système dans le cas d'usage inconnu

Le caractère modulaire de ce modèle nous donne l'opportunité de modifier les sous-parties sans remettre en question toute la structure présentée. De premières analyses sur des cas tests académiques ou sur des premiers systèmes peuvent mettre en évidence les sous-parties qui demandent un travail plus approfondi.

Le découplage de ces paramètres permet de les évaluer séparément pendant les roulages aléatoires prévus dans la procédure de validation et/ou compléter par des roulages dédiés à l'évaluation de certains paramètres. Nous devrons vérifier que ces évaluations alternatives permettent bien la convergence de l'estimateur de fiabilité sans biais.
Les probabilités de transition entre les cas d'usage peuvent par exemple être estimées à l'aide de roulages aléatoires réalisés avec le véhicule autonome mais également en utilisant un véhicule instrumenté capable d'enregistrer les différents scénarios rencontrés. En effet, les cas d'usage sont une décomposition de l'environnement de conduite indépendante du comportement du véhicule autonome. Leurs fréquences d'apparition, en première approche, sont identiques lorsque le véhicule est en mode autonome ou lorsque le véhicule est conduit par l'utilisateur. Les systèmes d'aide à la conduite, en cours de validation ou actuellement sur le marché, pourraient par exemple contribuer à la validation du véhicule autonome.
Nous imaginons la présence de cas d'usage plus rares qui peuvent mettre plus facilement en défaut le véhicule autonome. S'ils sont connus, il est possible d'intensifier les essais du véhicule autonome dans ces cas d'usage. La probabilité de défaillance plus grande sera vite précisée et ne sera plus un problème dans l'évaluation de la fiabilité.

Les méthodes bayésiennes utilisées pour estimer les paramètres de ce modèle peuvent introduire un biais si les *a priori* initiaux comportent des erreurs. Ce biais devrait s'atténuer puis disparaître avec les roulages de validation. Les erreurs devront cependant ne pas être trop importantes car elles pourraient alors freiner la convergence du modèle de fiabilité ce qui fait tout l'inverse de ce qui est souhaité. Nous devons maintenant déterminer la valeur de l'erreur maximale admissible dans le modèle pour ne pas pénaliser la vitesse de convergence de la fiabilité estimée. Les tests réalisés doivent être optimisés, moins coûteux et plus rapides que les tests dimensionnés par Kalra et Paddock [40]. Les erreurs doivent donc être détectées dans un temps raisonnable.

Nous allons par la suite analyser le comportement de ce modèle dans différents contextes pour étudier ses performances et ses limites. Des tests théoriques sont construits pour répondre à plusieurs objectifs que nous présentons dans le chapitre suivant.

Ce chapitre a fait l'objet de deux publications [45, 44]

Chapitre 8

Evaluation de la performance et des limites de l'approche sur cas tests

8.1 Introduction

La connaissance même partielle du système étudié et de son environnement participe au dimensionnement d'un plan de validation incrémental. Elle est supposée rendre la démarche de validation plus efficace que des essais purement aléatoires, i.e., pour un même objectif, la démarche choisie sera moins coûteuse. Le système n'est plus une boîte noire, il est alors possible de construire des roulages numériques ou sur piste, de rechercher des zones ciblées de l'environnement pour lesquelles le niveau de connaissance est encore trop faible. Ces nouvelles données sont intégrées au modèle de fiabilité au travers de distributions *a priori*.
Une méthode d'évaluation de la fiabilité fait le lien entre toutes ces informations. La modélisation du problème posé permet de dissocier la contribution de chaque cas d'usage caractérisée par la probabilité de survie du système dans ces cas d'usage. Les fréquences d'apparition de ceux-ci sont modélisées par une chaîne de Markov. L'ensemble des paramètres est donné *a priori* et est mis à jour par une inférence bayésienne. Si d'éventuels cas d'usage sont encore inconnus, un modèle de croissance de fiabilité, de "Goel Okumoto", prédit la probabilité d'occurrence d'un tel cas d'usage à partir des temps d'apparition des nouveaux cas d'usage détectés précédemment.
La démarche a pour objectif d'être moins coûteuse que les méthodes actuelles mais doit faire l'objet d'une étude approfondie pour vérifier dans quel contexte elle est réellement efficace. D'autant plus que la connaissance partielle peut entraîner un biais dans l'estimation des paramètres et ainsi amener à une estimation erronée de la fiabilité. Une erreur dans l'*a priori* doit être détectable pour ne pas arrêter trop tôt les roulages de validation.
Le choix d'un critère d'arrêt des essais de validation doit se faire par une analyse du comportement de ce modèle. D'une part, l'étude de la distribution de la fiabilité estimée et son évolution aide à la sélection d'un nouvel estimateur plus pertinent pour l'évaluation de la fiabilité ; cet estimateur peut par exemple être un quantile de la distribution. D'autre part, la convergence de cet estimateur peut différer en fonction du contexte choisi. En effet sa vitesse varie selon les caractéristiques du système et du niveau de connaissance. L'estimation peut être une valeur biaisée plus ou moins proche de la fiabilité réelle. Ce biais peut être favorisé par un plan de validation qui cible des scénarios de roulage mais omet des scénarios importants pour l'évaluation de la

fiabilité.
Les expérimentations réalisées dans ce chapitre ont pour but de mieux visualiser le comportement du modèle de fiabilité établi. En fonction du système étudié, de son environnement et du niveau connaissance en début de validation, la méthode d'évaluation peut être plus ou moins efficace et plus ou moins adaptée. Ce modèle est un prototype qu'il faudra réajuster au système étudié en fonction de l'influence de chaque paramètre qui le compose sur l'estimation de la fiabilité. Nous nous proposons de donner des exemples d'analyses réalisables avec le modèle sur des systèmes fictifs. Ces études ont pour but de donner un premier élément de réponse aux objectifs listés ci-dessous :

1. Choisir un nouvel estimateur qui caractérise plus fidèlement la fiabilité du système.
2. Etudier l'influence des parcours possibles pendant le processus de validation.
3. Etudier la convergence de l'estimateur vers la fiabilité du système dans différents cas de connaissance.
4. Quantifier l'impact sur la vitesse de convergence d'un biais sur les distributions *a priori* des probabilités de transition et de survie et estimer le temps de détection d'un tel biais.
5. Caractériser le domaine de validité de la méthode, *i.e.* trouver :
   — des systèmes pour lesquels la méthode est inefficace
   — des systèmes pour lesquels la méthode est efficace
   — des erreurs sur l'*a priori* à ne pas dépasser.
6. Etudier le comportement du modèle lorsque des cas d'usage sont inconnus et analyser la prévision du modèle de Goël Okumoto en fonction des apparitions de nouveaux cas d'usage.
7. Chercher l'existence d'une accélération de la convergence de l'estimateur par l'utilisation de roulages guidés.

La première partie présentera la procédure d'essais mise en place dans ces études, les parties suivantes analyseront les résultats de ces essais sélectionnés.

8.2 Description des cas tests choisis

La méthode est appliquée à plusieurs systèmes qui sont des cas d'études simplifiés simulés numériquement. Ils ont un comportement vérifiant les hypothèses choisies pour la construction du modèle de fiabilité. L'enchaînement des scénarios suit bien des chaînes de Markov et l'état des systèmes confrontés à ces scénarios suit bien une loi de Bernoulli. Pour chaque système étudié, les valeurs des variables suivantes sont précisées :

— le nombre de cas d'usage dans le domaine de fonctionnement, N_{uc},
— les probabilités de survie S_i du système dans chaque cas d'usage u_i regroupées dans une matrice diagonale de taille $N_{uc} \times N_{uc}$ notée S,
— les probabilités de transition entre les cas d'usage également présentées sous forme matricielle de même taille que S notée P,
— les probabilités du cas d'usage initial, débutant la séquence de validation, rangées dans un vecteur de taille initiale N_{uc}, Π_0.

Les scénarios possèdent tous la même durée D_{sc} (2 minutes). Une heure de roulage correspond à une séquence de h scénarios (30 scénarios dans le cas d'étude). La fiabilité de ce système dite "fiabilité réelle" est alors calculée selon l'expression (7.10), pour h scénarios.
On peut avoir une connaissance plus ou moins précise du système représentée par les paramètres décrivant le niveau de connaissance :

— le nombre de cas d'usage connus en début de validation
— les distributions *a priori* des probabilités de survie
— les distributions *a priori* des probabilités de transition

Les distributions initiales des cas d'usage, Π_0, sont supposées connues et fixé pour chaque essai. En effet l'ensemble des cas d'usage initiaux est une partie de l'ensemble des cas d'usage connu. Ce vecteur sera complété par des 0 à chaque identification d'un nouveau cas d'usage.

8.2.1 Paramètres qualifiant la connaissance

Les probabilités de survie *a priori* suivent des lois bêta de couples de paramètres $\{(\alpha_i, \beta_i)\}_{i\in\{1,\dots,N_{uk}\}}$ pour les N_{uk} cas d'usage connus et les probabilités de transition *a priori* des lois de Dirichlet de paramètres $\{(\alpha_{i1}, \cdots, \alpha_{iN})\}_{i\in\{1,\dots,N_{uk}\}}$. Les valeurs des paramètres *a priori* sont difficilement interprétables. Le niveau de connaissance n'est alors pas facilement quantifiable. Les faire varier directement rendra les interprétations confuses. Pour mieux caractériser le niveau de connaissance, chaque distribution sera caractérisée par deux autres types de paramètres :

— les erreurs sur la moyenne des distributions *a priori* :
Une erreur d'estimation de quelques pourcents sur la fiabilité du système n'a pas d'impact sur la validation en sûreté de fonctionnement, car l'ordre de grandeur est respecté. Par contre une erreur sur l'ordre de grandeur de la valeur de la fiabilité est bien plus pénalisante.
Pour exprimer ce type d'erreur, on définit une erreur sur la puissance entre la valeur du paramètre réel et la valeur supposée de ce dernier. On note ϵ_s les erreurs des probabilités de survie et ϵ_t celles sur les probabilités de transition.
Par exemple, pour la probabilité de survie S_i, dans le cas d'usage u_i, la valeur *a priori* initiale $\widehat{S}_i$ est donnée en fonction de l'erreur ϵ_s^i selon l'équation (8.1).

$$\widehat{S}_i = 1 - 10^{(1-\epsilon_s^i)\times \mathrm{Log}_{10}(1-S_i)} \tag{8.1}$$

Ainsi l'expression (8.1) exprime bien une erreur sur l'ordre de grandeur. En effet, une erreur de $\pm 20\%$ autour d'une probabilité de survie valant $1 - 10^{-5}$ sera caractérisée par l'intervalle $[1 - 10^{-4}; 1 - 10^{-6}]$. Cet intervalle est un encadrement entre deux ordres de grandeur.
L'effet de cette erreur n'est pas symétrique : l'écart avec la borne inférieure est bien plus grand qu'avec la borne supérieure. Pourtant une surestimation de le probabilité de défaillance aura plus de conséquences néfastes qu'une sous-estimation. Elle pourrait entraîner un arrêt précoce de la démarche de validation alors que la fiabilité du système est mal estimée. Nous analyserons la convergence de l'estimateur dans ces deux cas de figure.

— les poids caractérisant la confiance que l'on peut accorder à la valeur moyenne de la distribution supposée :

Ces poids ont été présentés dans les sections 7.4.1 et 7.4.2. w_s désigne les poids des probabilités de survie et w_t les poids des probabilités de transition. Par exemple pour la distribution *a priori* de la probabilité de survie S_i, nous posons $\alpha_i^{(0)}$, $\beta_i^{(0)}$ et w_s^i tels que :

$$\alpha_i^{(0)} = w_s^i(1-\widehat{S}_i) \qquad \text{et} \qquad \beta_i^{(0)} = w_s^i\widehat{S}_i \tag{8.2}$$

La valeur du poids w_s^i influence l'étendue de la distribution *a priori* et l'importance de l'espérance *a priori* sur l'estimation de l'espérance *a posteriori*. Le choix de cette valeur se fait en analysant l'expression :

$$E\left[1-\widehat{S_i^{(1)}}|X_i = x_i^{(1)}\right] = \frac{N_i^{(1)}}{(N_i^{(1)}+w_s^i)} \times \frac{x_i^{(1)}}{N_i^{(1)}} + \frac{w_s^i}{(N_i^{(1)}+w_s^i)} \times (1-\widehat{S}_i)$$

avec $N_i^{(1)}$ le nombre de scénarios issus de u_i observés pendant l'étape 1 et $x_i^{(1)}$ le nombre de fois où le système AD s'est bien comporté pendant les $N_i^{(1)}$ observations. Cette expression montre que w_s^i sert de poids pour le calcul de l'espérance d'une distribution *a posteriori*. Pour que ce poids ait un véritable effet au cours des itérations, il doit être du même ordre de grandeur ou plus important que le nombre de scénarios observés $N_i^{(1)}$ sinon il risque d'être négligeable.

8.2.2 Choix du processus de validation

Pendant un roulage de validation plusieurs véhicules munis du système autonome seront testés en parallèle. A la fin d'une étape, l'ensemble des scénarios observés par tous les véhicules sont collectés et analysés en post-traitement.
Le processus de validation dépend du nombre de véhicules prototypes N_v à faire tester, du nombre d'heures de roulage N_h dans la semaine et du nombre de semaines à réaliser N_w. Ces paramètres donnent le nombre de scénarios N_{sc} observés par le système pendant une étape de validation. Imaginons que les véhicules soient conduits par une équipe d'opérateurs travaillant 35H par semaine ($N_h = 35$) ou par deux équipes d'opérateurs en alternance pour les tester 70H par semaine chacun ($N_h = 70$). On suppose qu'après chaque semaine, le comportement du véhicule dans les scénarios observés est analysé et les estimations des paramètres servant aux calculs de la fiabilité sont mis à jour.
Ce déroulement est reconstruit numériquement pour le cas d'étude. Pour analyser la variation des estimations liées aux séquences des cas d'usage observées, nous proposons de simuler pour un même système et un même niveau de connaissance plusieurs roulages de validation différents générés aléatoirement. Pour chaque roulage, des séquences des cas d'usage (d'une semaine) sont tirées aléatoirement à partir du modèle de Markov découlant des transitions générées lors de la création du système. Ensuite l'état non défaillant ou défaillant du système est tiré aléatoirement pour chaque scénario issu de chaque cas d'usage i observé pendant les séquences de validation en suivant une loi binomiale de paramètre s_i.

8.2.3 Description de l'algorithme construisant les essais

Pour réaliser les essais de validation par simulation numérique, un algorithme est décomposé en quatre parties comme le schématise la figure 8.1.

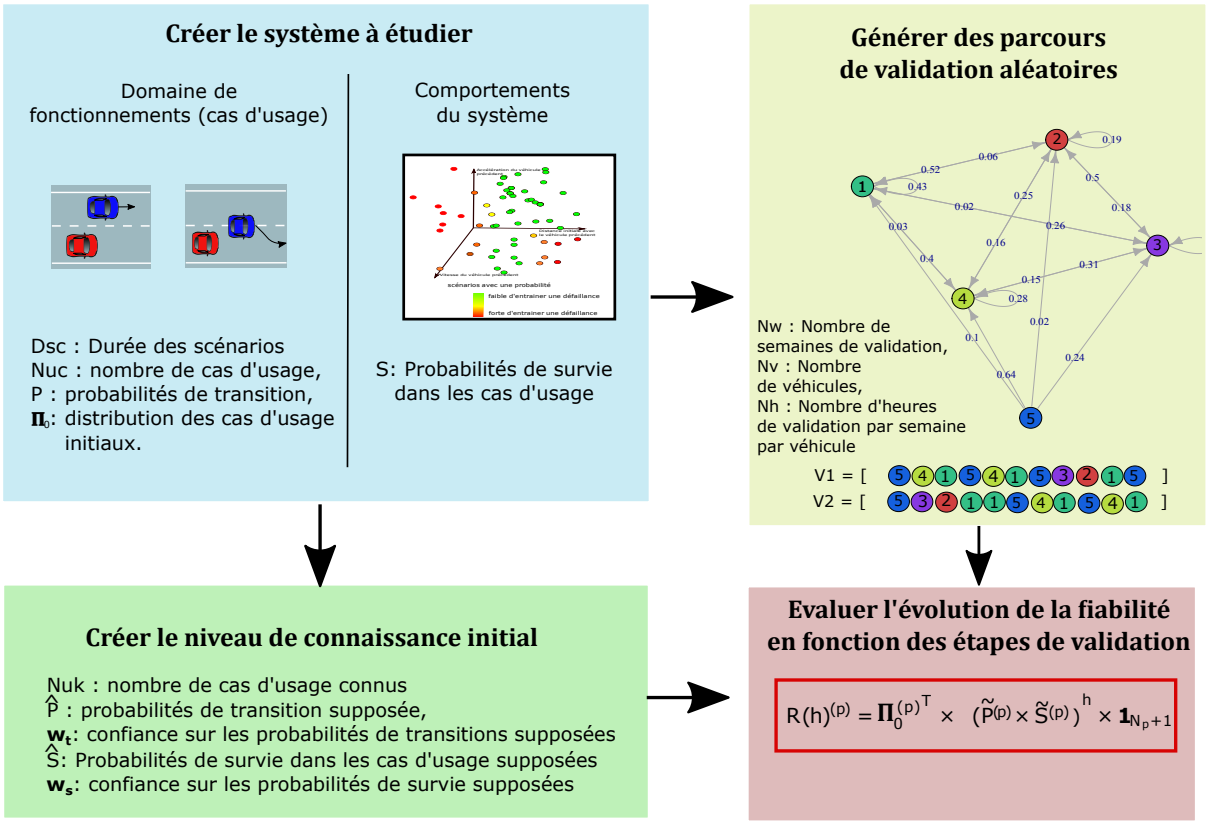


FIGURE 8.1 – Les quatre parties de l'algorithme de tests

La première partie génère les paramètres du système étudié et de son environnement, c'est-à-dire les paramètres décrivant les cas d'usage qui le composent et la réaction du système dans ces cas d'usage, caractérisée par la matrice S.
La seconde partie construit numériquement les roulages de validation effectués avec le système. Plusieurs parcours différents, que l'on appelle des séquences de validation $\{V_k\}_{k\in\mathbb{N}}$, peuvent être tirés selon les mêmes conditions pour simuler la succession de scénarios en tirant aléatoirement des trajectoires du processus de Markov de matrice P. L'état de défaillance ou de survie du système dans chaque cas d'usage observé u_i est obtenu selon des lois de Bernoulli avec la probabilité S_i.
La troisième partie consiste en l'ajout du niveau de connaissance initial selon les paramètres présentés dans le paragraphe 8.2.1.
Enfin le dernier bloc construit la distribution de la fiabilité estimée à chaque pas de temps pour chaque roulage de validation selon l'expression :

$$R(h)^{(p)} = {\Pi_0^{(p)}}^T \times \left(\widetilde{P^{(p)}} \times \widetilde{S^{(p)}}\right)^h \times \mathbb{1}_{N_p+1} \tag{8.3}$$

$\widetilde{S^{(p)}}$, $\widetilde{P^{(p)}}$ sont des variables aléatoires dont les distributions sont estimées *a posteriori* à l'étape de validation p. $R(h)^{(p)}$ est, par conséquent, une variable aléatoire. Sa fonction de répartition est estimée empiriquement par la méthode de Monte Carlo en extrayant un échantillon de $N_{echantillon}$ points des paramètres du modèle de fiabilité selon les distributions mises à jour à l'étape de validation étudiée. h est le nombre de scénarios sur une heure.

Ce découpage en 4 blocs permet de mieux comparer les influences de chaque groupe de paramètres pour un même système et une même séquence de validation. Nous pouvons voir l'influence du niveau de connaissance. Nous pouvons également, pour un même système et un même niveau de connaissance, analyser l'effet de plusieurs parcours de validation. Nous présentons des exemples d'expérimentations et d'analyse dans les sections suivantes.

8.3 Choix de l'estimateur et première étude du comportement du modèle de fiabilité

Le premier essai a pour but de visualiser le comportement du modèle de fiabilité. Seulement trois cas d'usage composent le domaine de fonctionnement du système étudié. Ce domaine de fonctionnement est réduit par rapport aux domaines envisagés pour le véhicule autonome composés de plus de 200 cas d'usage actuellement. Il permet cependant de mieux identifier l'importance et les effets de chaque paramètre du modèle. Nous supposons qu'initialement les roulages débutent toujours par le cas d'usage n°1 que ce soit pendant les séquences de validation ou pour un usage en clientèle. Le vecteur des probabilités du cas d'usage initial est donc $\Pi_0 = [1 \quad 0 \quad 0]$. Nous choisissons deux cas d'usage fréquents et un cas d'usage rare. Les probabilités de survie du système dans les cas d'usage fréquents sont très fortes alors que celle dans le cas d'usage rare est faible. En effet le modèle de fiabilité et la démarche de validation ont été conçus suivant cette hypothèse. Les défaillances ne sont pas réparties de manière homogène dans tout l'espace des paramètres mais elles sont supposées être concentrées dans certaines zones rares mal connues pour lesquelles la mise au point du système présente des lacunes. Trop peu de scénarios ont été collectés provenant de cette zone. Nous donnons les matrices P et S.

$$P = \begin{bmatrix} 0.15 & 0.849 & 0.001 \\ 0.10 & 0.900 & 0.000 \\ 0.30 & 0.600 & 0.100 \end{bmatrix} \quad (8.4) \qquad S = \begin{bmatrix} 0.99999 & 0 & 0 \\ 0 & 0.999999 & 0 \\ 0 & 0 & 0.99 \end{bmatrix} \quad (8.5)$$

Chaque scénario dure 2 minutes. Pendant une heure de roulage, 30 scénarios sont donc observés par le véhicule. La fiabilité de ce système après une heure de roulage est alors de $R(h) = 0.9998958$ et nous souhaitons la comparer avec la fiabilité estimée à partir du modèle proposé. Ici la fiabilité du système est très petite par rapport à la fiabilité du véhicule autonome attendue de $1 - 10^{-9}$ après une heure de roulage. Cependant on peut envisager que, parmi les 200 cas d'usage répertoriés, seulement un petit sous-ensemble peut entraîner des défaillances du système et est le seul ou le plus grand contributeur dans le calcul de la fiabilité. Les études peuvent être alors menées dans un domaine restreint, composé de ces uniques cas d'usage, dans lequel la fiabilité est plus faible et donc plus facile à estimer.
Un parcours de validation est généré. Il dure 400 semaines. Pendant chaque semaine, 10 véhicules sont testés 35 heures chacun. Les scénarios observés sont analysés chaque semaine. Ainsi à chaque étape de validation 10500 scénarios sont observés.
En début de validation, les 3 cas d'usage sont supposés connus. Le niveau de connaissance initial est donné par :

— Les probabilités supposées de transition entre les cas d'usage, présentées dans la matrice $\widehat{P}$, et le niveau de confiance associé à chaque ligne de cette matrice dans la matrice w_t. Plus le cas d'usage est rare et moins les probabilités de transition supposée sont des données certaines.

$$w_t = \begin{bmatrix} 1120 & 9539 & 2 \end{bmatrix} \quad (8.6) \qquad \widehat{P} = \begin{bmatrix} 0.15 & 0.849 & 0.001 \\ 0.099 & 0.901 & 0 \\ 0.21 & 0.735 & 0.055 \end{bmatrix} \quad (8.7)$$

— Les probabilités supposées de survie dans les cas d'usage sont sans erreur $\epsilon_s = 0$ et sont donc identiques aux probabilités de survie du système. Le niveau de confiance est quant à lui très bas $w_s = 1$.

Après chaque semaine de validation, la variable aléatoire caractérisant la fiabilité estimée est analysée. Sa distribution est observée en tirant un échantillon de taille 1000 à chaque étape. La Figure 8.2 donne les histogrammes de ces distributions à l'étape initiale, après 10 semaines et après 20 semaines. Entre l'étape initiale et 10 semaines, la distribution s'est resserrée vers la fiabilité vraie du système. Entre 10 semaines et 20 semaines, aucune différence ne semble notable. La distribution de la fiabilité estimée ne semble présenter qu'un seul mode prépondérant et garde la même forme au fil des itérations, présentant un pic très marqué décentré proche de la fiabilité réelle du système. Cependant des valeurs très rares restent dispersées et assez éloignées de la fiabilité réelle. Ce qui entraîne une mauvaise estimation d'un intervalle de crédibilité construit par des quantiles choisis. Un intervalle de crédibilité est en statistique bayésienne une étendue des valeurs probables autour de l'estimation centrale d'un paramètre, avec un risque d'erreur donné. La Figure 8.3 présente l'évolution de la valeur moyenne de la fiabilité estimée, du quantile à 2.5%, notée borne inférieure et du quantile à 97.5% notée borne supérieure en fonction des semaines de validation. La moyenne empirique de la fiabilité estimée se rapproche, au fil des itérations, de la fiabilité du système par saut et croît par morceaux. Chaque saut est dû à l'apparition d'une défaillance dans les cas d'usage observés. L'estimation croît avec les itérations tant qu'aucune défaillance n'est constatée. Les sauts et la croissance sont au départ de grandes ampleurs avant de devenir moins importants autour de la vraie fiabilité du système. Les deux quantiles réagissent de la même façon par croissance par morceaux et sauts successifs. Ils encadrent l'espérance avec

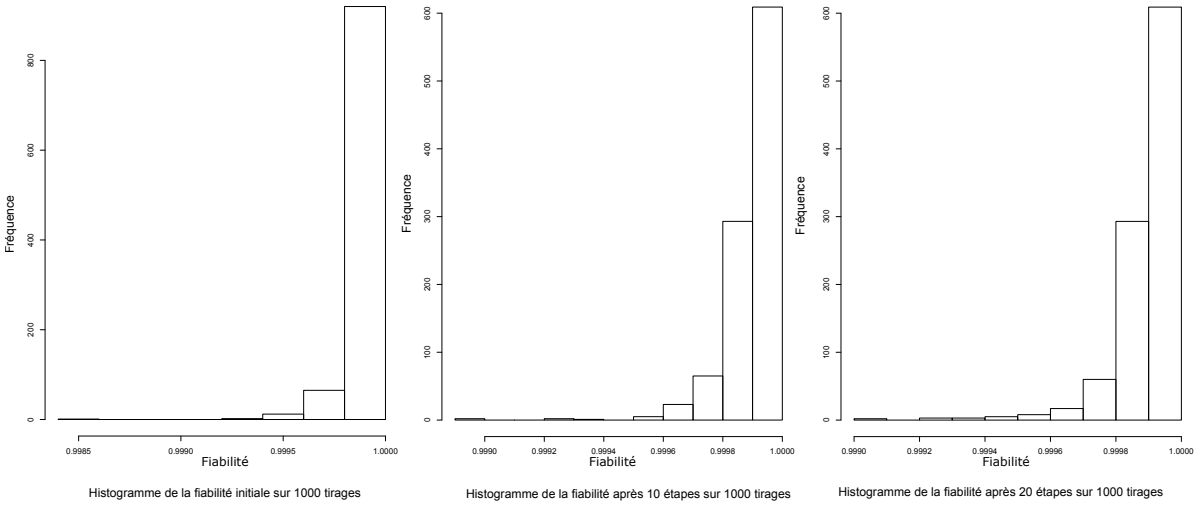


FIGURE 8.2 – Histogrammes de la fiabilité initiale, après 10 et 20 étapes

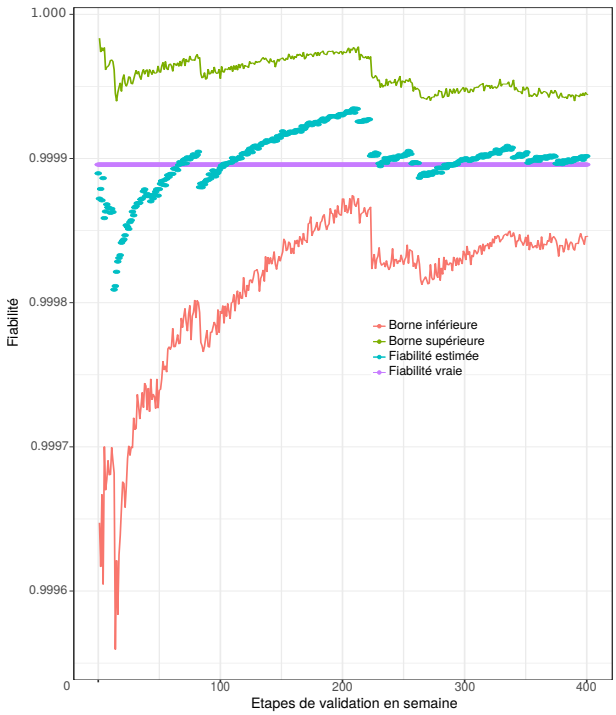


FIGURE 8.3 – Evolution de la fiabilité pendant les étapes de validation

un écart élevé en début de validation et l'écart se réduit faiblement au cours des itérations pour se stabiliser vers la $300^{\text{ème}}$ semaine. Un intervalle de crédibilité pour encadrer la fiabilité "vraie" du système encore inconnue ne semble pas une information pertinente avec les distributions *a priori* choisies. Quelle que soit la confiance initiale donnée, il reste autour de l'espérance. Sa largeur reste de grande taille. Quand cette espérance est initialement très biaisée, l'intervalle de crédibilité peut ne pas encadrer la vraie fiabilité. Si l'étendue des distributions *a priori* des paramètres est choisie de grande ampleur, cet intervalle ne semble pas fluctuer et reste large. La variation de l'espérance, quant à elle, semble un bon indicateur pour l'évaluation de la fiabilité. La réduction de l'ampleur des sauts est un indicateur de la convergence de l'estimation.
Entre les sauts, la croissance de l'espérance et des quantiles est bruitée, fortement au début puis les bruits s'estompent au cours des itérations. Ceci est dû en grande partie à la taille d'échantillonnage des probabilités estimées de transition et de survie pour l'estimation de l'espérance et des quantiles de la fiabilité. En analysant la convergence de l'estimation de ces trois valeurs en fonction de la taille de l'échantillon, il convient de choisir un échantillon d'au moins 40000 points pour ces estimations.

Ce premier exemple semble montrer que la moyenne empirique de la fiabilité estimée converge vers la fiabilité réelle du système. Pour les essais suivants, nous étudierons la convergence de cette moyenne empirique qui sera appelée pour simplifier l'estimateur de la fiabilité.

8.4 Influence des parcours possibles pendant le processus de validation

Dans cette étude le système étudié a toujours 3 cas d'usage. On souhaite faire une première analyse sur l'effet des différentes séquences de validation sur la convergence de l'estimateur de la fiabilité. Ici deux cas d'usage sont parfaitement connus et leurs paramètres bien caractérisés. L'existence du cas d'usage 3 est connue mais ses paramètres sont imprécis. Nous donnons la matrice P et S.

$$P = \begin{bmatrix} 0.8 & 0.199 & 0.001 \\ 0.6 & 0.399 & 0.001 \\ 0.7 & 0.299 & 0.001 \end{bmatrix} \quad (8.8) \qquad S = \begin{bmatrix} 0.999999 & 0 & 0 \\ 0 & 0.99999 & 0 \\ 0 & 0 & 0.9999 \end{bmatrix} \quad (8.9)$$

La fiabilité de ce système est plus faible que le précédent et vaut $R = 0.9703691$.
L'erreur, ϵ_s, sur la probabilité de survie du cas d'usage 3 est de $0,2$ de même que pour l'erreur sur la probabilité de transition vers le cas d'usage 3, ϵ_t. La confiance pour la probabilité de survie dans le cas d'usage 3 est très grande : $w_s = 100000$. Les indices de confiance sur chaque ligne de la matrice de transition valent tous w_t, qui vaut 10000.

10 séquences différentes de validation sont tirées aléatoirement. Elles durent toutes 100 semaines, comportent 10 véhicules qui roulent 70 heures par semaine. L'évolution de l'estimation de la fiabilité est donnée toutes les 5 semaines sur la Figure 8.4 ainsi que l'erreur relative. Initialement la fiabilité *a priori* sous-estime la fiabilité du système. La fiabilité estimée augmente au fur et à mesure et semble converger vers la fiabilité du système.
Dans cet exemple nous remarquons que la séquence de validation a bien une influence sur la convergence de l'estimation de la fiabilité. En effet chaque roulage entraîne une estimation dif-

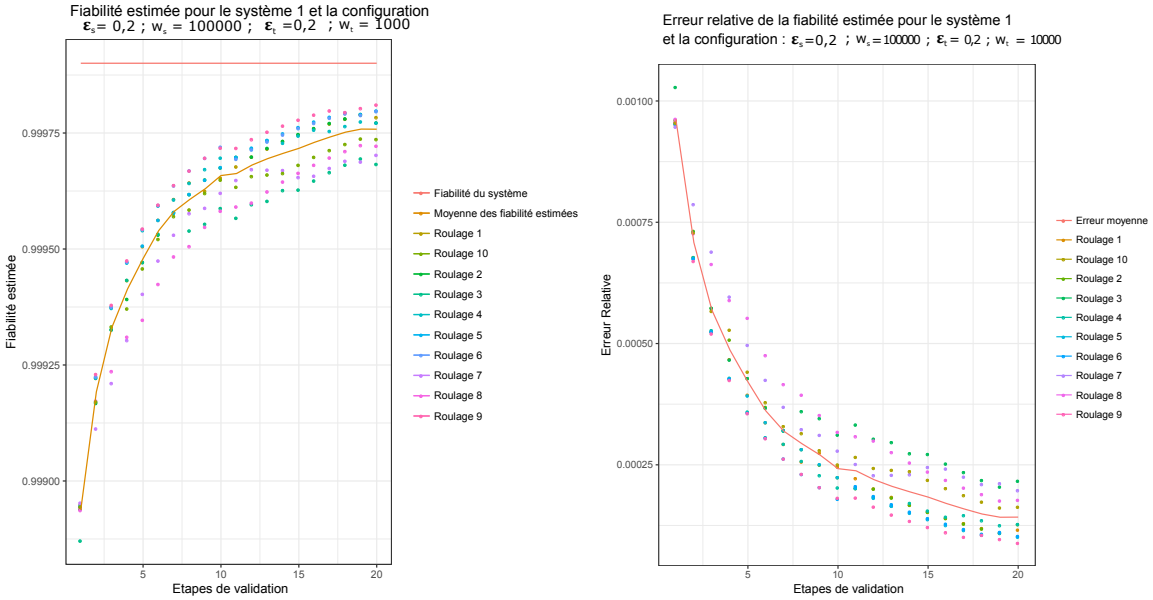


FIGURE 8.4 – Evolution de la fiabilité estimée sur 10 séquences de validation différentes dans le cas où la fiabilité *a priori* est plus faible que la fiabilité du système

férente de la fiabilité à chaque pas de temps et la vitesse de convergence de l'estimateur diffère. De plus, nous remarquons que l'écart entre les estimations de chaque parcours ne diminue pas mais semble augmenter avec les itérations dans la fenêtre d'observation. Normalement, pour un temps de validation très long ces estimations devraient être identiques entre les roulages. Cela signifie que la fenêtre de temps est encore trop courte pour atteindre la même évaluation entre tous les parcours.

Nous présentons un second exemple avec le système mais un niveau de connaissance différent sur la Figure 8.5. Dans cet exemple, l'erreur sur la probabilité de transition et de survie du cas d'usage 3 est de 0. Les coefficients de confiance sont de 10000 pour w_s et de 1000 pour w_t. la fiabilité *a priori* est donc égale à la fiabilité du système.

Nous remarquons que pour des erreurs très faibles, l'estimateur continue de faire des sauts autour de la fiabilité du système. Certains parcours peuvent entraîner une surestimation de la fiabilité, d'autres une sous-estimation.

Enfin nous présentons un dernier cas de paramètres de connaissance $\{\epsilon_s = -0,2; w_s = 100000; w_t = 1000; \epsilon_t = 0\}$ sur la Figure 8.6. La fiabilité *a priori* est dans ce dernier cas plus grande que la fiabilité du système. On observe ici une erreur très basse dès la première itération mais nous observons que les résultats obtenus entre les différentes séquences de validation sont très différents. Contrairement au premier cas des sauts très marqués sont constatés. Lorsque la fiabilité est surestimée, ces sauts correspondent à l'apparition d'une défaillance par le système étudié. Lorsque la fiabilité devient sous-estimée, l'évolution de la fiabilité estimée est moins régulière. La forme des courbes d'évolution diffère beaucoup entre les différentes séquences.

La différence entre les erreurs relatives maximales des deux derniers niveaux de connaissance est significative en début de validation ($4 \cdot 10^{-4}$ contre $1 \cdot 10^{-4}$). Alors que dans le dernier exemple l'indice de confiance est plus important et les probabilités initiales comportent des erreurs. En fin

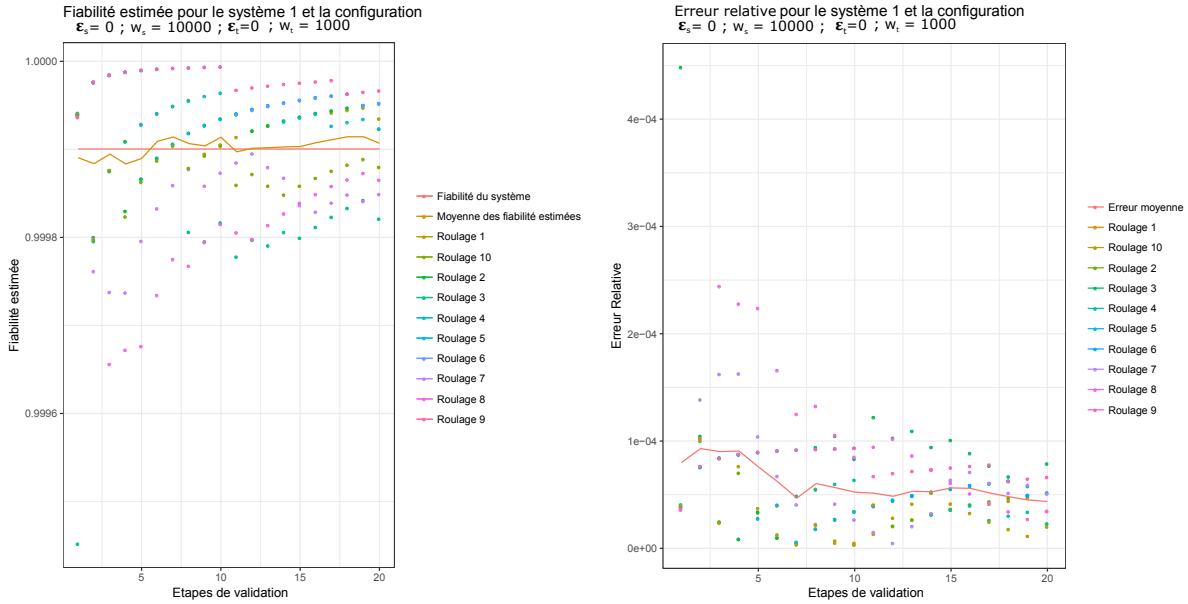


FIGURE 8.5 – Evolution de la fiabilité estimée sur 10 séquences de validation différentes dans le cas où la fiabilité *a priori* est égale à la fiabilité du système

de validation, les erreurs relatives maximales sont du même ordre de grandeur et valent $7 \cdot 10^{-5}$. Cela semble montrer que l'apport d'information même erronée peut accélérer la convergence de l'estimateur. Une comparaison quantitative des évolutions de la fiabilité estimée, en faisant varier les paramètres du système et de la connaissance, ne semble en première approche pas réalisable. Pour comparer deux cas de manière quantitative, il faut une grandeur mesurée qui caractérise ces deux courbes comme par exemple un coefficient d'un modèle représentant les résultats obtenus. Les courbes d'évolution sont très différentes en fonction des cas. Il est difficile de distinguer un modèle universel entre toutes les courbes pour comparer les valeurs des coefficients. De même une comparaison de l'estimation après une étape de validation donnée ne tiendra pas compte des nouveaux sauts possibles de l'estimateur après cette étape. Nous proposons dans cette étude de ne réaliser que des études qualitatives en comparant visuellement l'évolution des fiabilités estimées en fonction du cas. L'étude suivante compare la convergence de la fiabilité estimée pour différents systèmes, dans différents états de connaissance.

8.5 Etude de la convergence de l'estimateur vers la fiabilité du système en fonction de l'état de connaissance et du système choisi

Dans cette section la convergence de l'estimateur est évaluée sur plusieurs systèmes et plusieurs états de connaissance mélangeant biais et niveau de confiance sur les valeurs *a priori*. Pour ce faire, nous reprenons le système précédent et nous faisons varier la probabilité de transition vers le cas d'usage 3, notée P_3, et la probabilité de défaillance dans le cas d'usage 3 notée D_3. Les matrices de transition et de survie sont exprimées dans les équations (8.10) et (8.11).

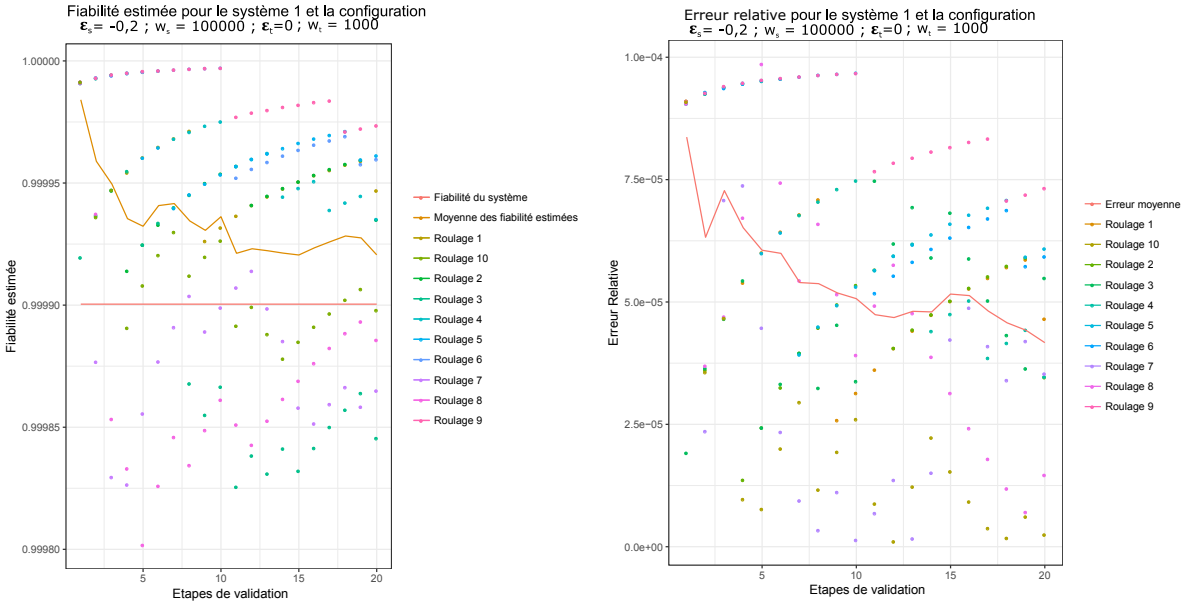


FIGURE 8.6 – Evolution de la fiabilité estimée sur 10 séquences de validation différentes dans le cas où la fiabilité *a priori* est plus grande que la fiabilité du système

$$P = \begin{bmatrix} 0,8 & 0,2 - P_3 & P_3 \\ 0,6 & 0,4 - P_3 & P_3 \\ 0,7 & 0,3 - P_3 & P_3 \end{bmatrix} \quad (8.10) \qquad S = \begin{bmatrix} 0,999999 & 0 & 0 \\ 0 & 0,99999 & 0 \\ 0 & 0 & 1 - D_3 \end{bmatrix} \quad (8.11)$$

Comme l'étude précédente, 10 séquences différentes de validation sont tirées aléatoirement. Elles durent toutes 100 semaines et comportent 10 véhicules qui roulent 70 heures par semaine. L'évolution de l'estimation de la fiabilité est donnée toutes les 5 semaines. L'estimateur est toujours l'espérance de la variable aléatoire obtenue par inférence bayésienne à l'aide d'une méthode de Monte Carlo avec un tirage de 40000 points. Pour un système donné, les 10 séquences de validations restent les mêmes quel que soit le niveau de connaissance étudié. Ainsi leurs influences ne sont pas prises en compte lorsque l'on compare l'évolution de l'estimateur de fiabilité pour le même système avec des états de connaissance différents.

Les valeurs choisies par les variables D_3 et S_3 sont représentées dans la table 8.1. Le cas d'usage 3 peut ainsi être plus ou moins rare avec une probabilité de défaillance plus ou moins forte. Pour les essais, nous choisissons de réaliser le plan complet qui est également décrit dans la table 8.1.

Pour chaque système nous appliquons différents niveaux de connaissance. Nous proposons de faire varier les paramètres de la connaissance selon la table 8.2.

Nous réalisons alors le plan complet pour ces 4 paramètres à 3 niveaux. 81 expériences sont réalisées et numérotées suivant la table 8.3.

Au total 729 expérimentations sont analysées dans cette section. Dans un premier temps, pour un même système, nous présentons l'influence qualitative de chaque paramètre caractérisant la connaissance. Dans un second, nous donnons une comparaison des évolutions de l'estimation de la fiabilité en fonction des systèmes étudiés.

P_3	D_3
0,100	1e-02
0,010	1e-03
0,001	1e-04

Système	P_3	D_3	R
1	0,001	0,0001	0,9999
2	0,01	0,0001	0,99988
3	0,001	0,001	0,99987
4	0,1	0,001	0,99694
5	0,1	0,0001	0,9996
6	0,1	0,01	0,97
7	0,01	0,01	0,99691
8	0,01	0,001	0,99961
9	0,001	0,01	0,99960

TABLE 8.1 – Ensemble des niveaux des variables P_3 et D_3 et présentation du plan complet réalisé

ϵ_s	w_s	ϵ_t	w_t
-0.2	1e+03	-0.2	1e+03
0.0	1e+04	0.0	1e+04
0.2	1e+05	0.2	1e+05

TABLE 8.2 – Niveaux des paramètres de la connaissance

8.5.1 Comparaison pour un même système à différents niveaux de connaissance

Pour le système 1 du plan complet, la Figure 8.7 présente l'évolution de l'erreur relative de l'estimateur sur les 81 configurations de connaissance étudiées. Certaines courbes se superposent presque parfaitement. Après étude au cas par cas, les paramètres w_t et ϵ_t caractérisant la connaissance de la probabilité de transition vers le cas d'usage 3 sont considérés peu influents dans la convergence de l'estimateur. Nous reprenons l'étude en ne tenant plus compte de ces deux paramètres et nous obtenons le deuxième graphe de la Figure 8.7. Les barres horizontales à chaque étape de validation représentent les estimations maximales et minimales des dix parcours. En règle générale, au fil des itérations, l'écart entre les séquences de validation se réduit. En fin de la séquence une très faible erreur persiste. La moyenne des parcours ne semblent pas converger vers la fiabilité "vraie" du système. Cependant cette erreur est acceptable, l'ordre de grandeur est bien estimé. Nous remarquons que lorsque w_s vaut 1000, l'erreur sur la probabilité de survie a très peu d'influence sur la convergence de l'estimateur. Ce niveau de confiance est trop faible et l'estimation obtenue est très proche de l'estimation fréquentiste. Les surestimations ou sous-estimations de la probabilité de survie dans le cas d'usage n'ont pas un effet symétrique. Dans le cas d'une sous estimation l'apparition d'une défaillance semble moins perturber l'évolution de la fiabilité qui semble avoir une croissance exponentielle. Alors qu'à l'inverse des sauts fréquents sont observés. Cependant dans notre cas, les probabilités de défaillance sont très élevées et des défaillances sont observables pendant les roulages de validation. Pour des cas d'usage de probabilités de défaillance plus petites, cette réévaluation de la fiabilité surestimée peut prendre plus de temps. La fiabilité estimée croît jusqu'à l'apparition d'une défaillance (plus rare) et la fiabilité sera mieux évaluée à partir de cet instant.
Dans le cas où la probabilité de survie *a priori* est égale à la probabilité de survie réelle avec un

K	ϵ_s	w_s	ϵ_t	w_t
1	0,2	100000	0,2	10000
2	0	10000	0,2	10000
3	0,2	1000	0,2	1000
4	0,2	1000	0	100000
5	0	100000	0,2	100000
6	-0,2	100000	0	100000
7	0	10000	0,2	1000
8	0,2	1000	0	10000
9	0,2	10000	-0,2	10000
10	0,2	100000	0,2	1000
11	0,2	10000	0	10000
12	-0,2	1000	0,2	1000
13	-0,2	10000	0,2	10000
14	-0,2	100000	0,2	1000
15	0	10000	0	1000
16	0,2	1000	-0,2	1000
17	0,2	10000	-0,2	1000
18	-0,2	10000	-0,2	10000
19	0,2	100000	0	10000
20	-0,2	10000	0	10000
21	0	10000	0	10000
22	0	1000	-0,2	100000
23	0	100000	0	100000
24	0	1000	0	1000
25	0	1000	0,2	1000
26	0,2	10000	0,2	10000
27	0	100000	0	1000
28	-0,2	10000	0,2	1000
29	0,2	10000	0	100000
30	0	10000	-0,2	1000
31	0	1000	0	10000
32	0,2	10000	-0,2	100000
33	0	10000	-0,2	10000
34	-0,2	100000	0,2	100000
35	-0,2	100000	0,2	10000
36	-0,2	1000	0	10000
37	0,2	100000	0	1000
38	0	10000	-0,2	100000
39	0,2	10000	0	1000
40	-0,2	100000	-0,2	1000
41	0	100000	-0,2	100000
42	0	1000	-0,2	10000
43	0	100000	0,2	1000
44	-0,2	10000	-0,2	1000
45	-0,2	1000	0	100000
46	0,2	1000	0,2	100000
47	-0,2	100000	0	1000
48	0	100000	0,2	10000
49	-0,2	10000	-0,2	100000
50	0	10000	0,2	100000
51	0	1000	0,2	100000
52	0,2	1000	0	1000
53	-0,2	10000	0	100000
54	0,2	100000	-0,2	1000
55	-0,2	100000	0	10000
56	0	100000	-0,2	1000
57	-0,2	100000	-0,2	10000
58	-0,2	1000	-0,2	1000
59	0	100000	0	10000
60	0,2	1000	-0,2	100000
61	-0,2	10000	0,2	100000
62	-0,2	1000	-0,2	100000
63	0,2	100000	0	100000
64	0,2	1000	-0,2	10000
65	-0,2	1000	-0,2	10000
66	-0,2	10000	0	1000
67	-0,2	100000	-0,2	100000
68	0	100000	-0,2	10000
69	0,2	100000	-0,2	100000
70	0,2	1000	0,2	10000
71	0,2	100000	-0,2	10000
72	0	1000	0	100000
73	0,2	10000	0,2	1000
74	0,2	100000	0,2	100000
75	0	10000	0	100000
76	-0,2	1000	0,2	100000
77	0,2	10000	0,2	100000
78	-0,2	1000	0	1000
79	-0,2	1000	0,2	10000
80	0	1000	0,2	10000
81	0	1000	-0,2	1000

TABLE 8.3 – Plan d'expériences sur les paramètres caractérisant le niveau de connaissance pour tous les systèmes

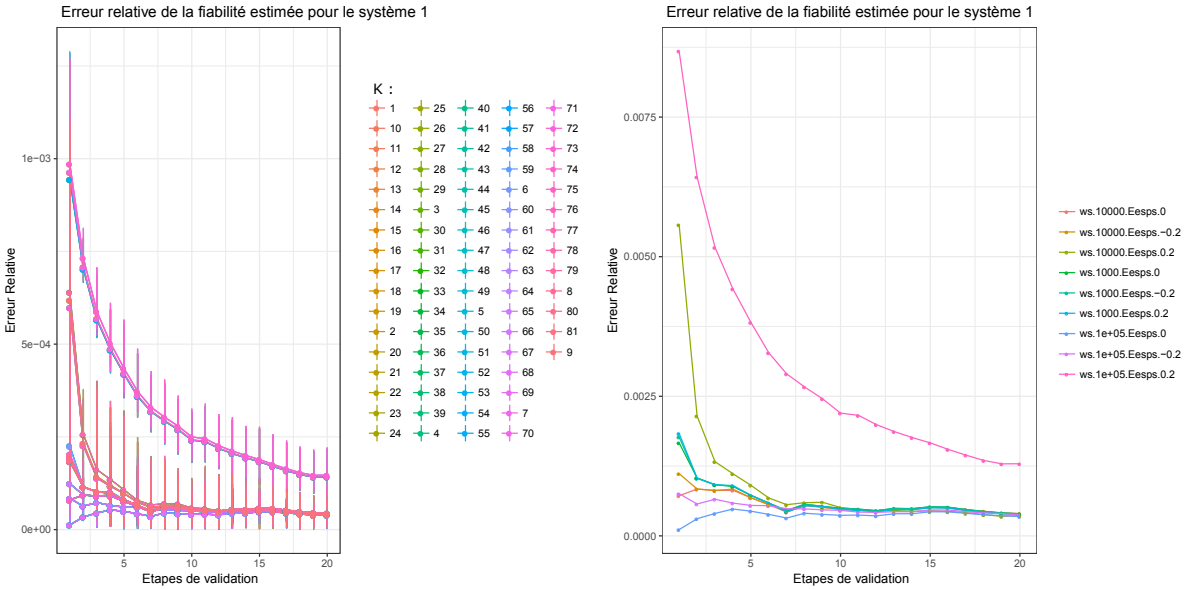


FIGURE 8.7 – Evolution de la fiabilité estimée du premier système pour 81 niveaux de connaissance différents puis en omettant les variations de w_t et ϵ_t

très haut niveau de confiance, l'erreur relative croît relativement peu et se stabilise assez vite. En conclusion, pour le système 1, les paramètres, qualifiant la connaissance ont une vraie influence pendant les 50 premières semaines (étape 10 sur la figure). Après ce laps de temps, l'ensemble des estimations moyennes ont toutes la même erreur. À l'exception du cas avec $w_s = 1e + 05$ et $\epsilon_s = 0,2$, l'erreur est alors trop importante pour se stabiliser au bout des 100 semaines.

La Figure 8.8 présente le même type d'analyse pour le système 9. A la différence du système 1, les paramètres w_t et ϵ_t sont influents. Ils ont pourtant beaucoup moins d'effets sur la convergence de l'estimateur que les paramètres caractérisant la probabilité de survie. De plus une erreur sur la probabilité de survie est influente même avec un indice de confiance w_s de 1000.

Ces exemples démontrent que des roulages ciblant certains cas d'usages peuvent réduire la durée de validation pour un même objectif de fiabilité. Pour le système 1, un roulage n'est nécessaire que pour quelques semaines. Une fois la probabilité de transition suffisamment bien estimé, elle n'influe plus sur l'estimation de la fiabilité. Les roulages de validation peuvent alors tester le système uniquement dans le cas d'usage 3 pour mieux évaluer la probabilité de survie. En une semaine, le nombre de tests dans le cas d'usage est ainsi en moyenne multiplié par 100. Pour le système 9, Une durée plus importante de roulages aléatoires est nécessaire avant de procéder à un roulage ciblé sur le cas d'usage 3. Une analyse de sensibilité sur l'estimation de la fiabilité faisant varier les paramètres de la connaissance pourrait ainsi aider et guider les roulages de validation.

8.5.2 Comparaison à mêmes niveaux de connaissance du comportement de la fiabilité estimée pour différents systèmes

Le niveau de connaissance est dorénavant figé pour tous les systèmes. La convergence de la fiabilité est comparée entre les systèmes. Sur la Figure 8.9, nous observons trois états de

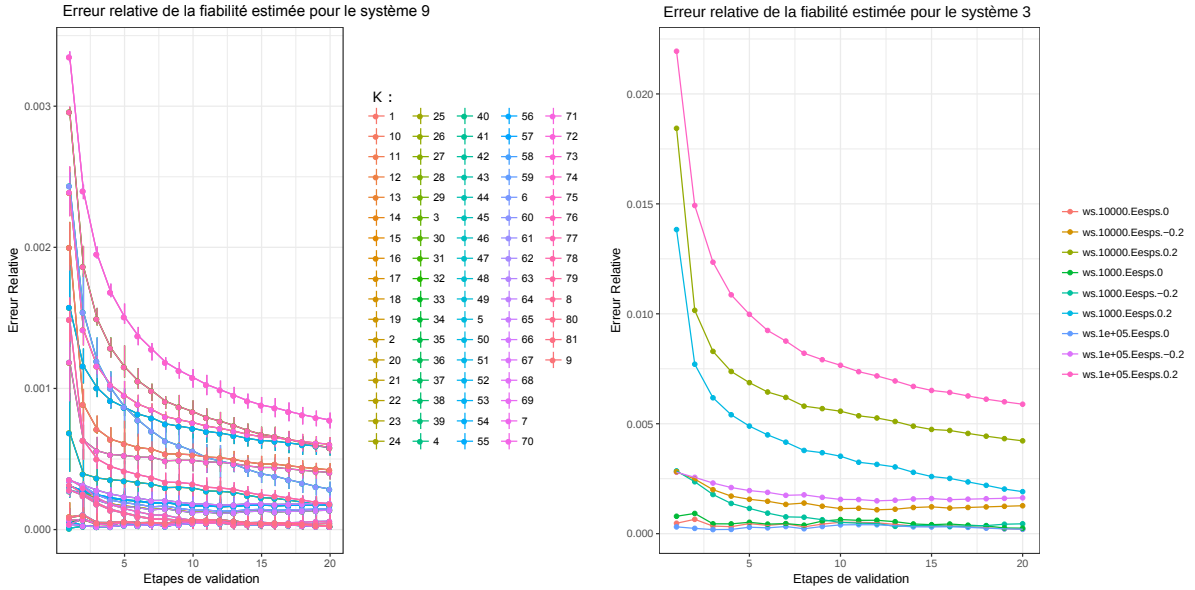


FIGURE 8.8 – Evolution de la fiabilité estimée d'un second système pour 81 niveaux de connaissances différents puis en omettant les variations de w_t et ϵ_t

connaissances avec une forte influence pour lesquels la probabilité de transition initiale est bien connue $\epsilon_t = 0$, mais avec peu de confiance $w_t = 1000$ et les niveaux de confiance de la probabilité de survie sont très élevés $w_s = 100000$ pour une erreur ϵ_s qui varie :

- Dans l'état de connaissance $K = 27$, ϵ_s vaut 0.
- Dans l'état de connaissance $K = 37$, ϵ_s vaut $0,2$.
- Et dans l'état de connaissance $K = 47$, ϵ_s vaut $-0,2$.

En analysant ces trois figures, nous remarquons que nous ne pouvons pas comparer les erreurs relatives de la fiabilité estimée. L'erreur initiale diffère beaucoup entre les systèmes parce que les ordres de grandeurs ne sont pas les mêmes. Le système 6 pour lequel la fiabilité est la plus faible se retrouve avoir l'erreur la plus élevée en fin validation. Pour une meilleure analyse de la convergence de l'estimateur en fonction du système étudié, la valeur de la fiabilité du système réel ne doit pas perturber les conclusions. Nous proposons alors d'étudier l'évolution des erreurs relatives de la probabilité de l'événement contraire c'est-à-dire la probabilité qu'une défaillance se produise avant une heure $F(h\Delta t) = 1 - R(h\Delta t) = Pr(T < h\Delta t)$, avec T le temps de la première défaillance.

La Figure 8.10 représente cette erreur relative. Lorsque que la fiabilité est sous estimée, l'erreur relative décroît pour l'ensemble des systèmes. L'erreur initiale entre les systèmes n'est pas la même, cela provient de l'expression (8.1) qui implique une erreur plus impactante pour les systèmes plus fiables. Ce qui entraîne ce décalage entre les systèmes. Pour des erreurs de même valeur, les vitesses de convergence diffèrent entre les systèmes. Que ce soit avec le niveau de connaissance 37 ou 47 ; le système 8 conserve une grande erreur relative de la probabilité de défaillance après 100 itérations. Pourtant ce système n'est pas le plus fiable. La vitesse de convergence de la fiabilité estimée semble dépendre de trois facteurs :

- La valeur des paramètres à estimer ; plus les probabilités sont faibles et plus une estimation précise de la fiabilité requerra de points.

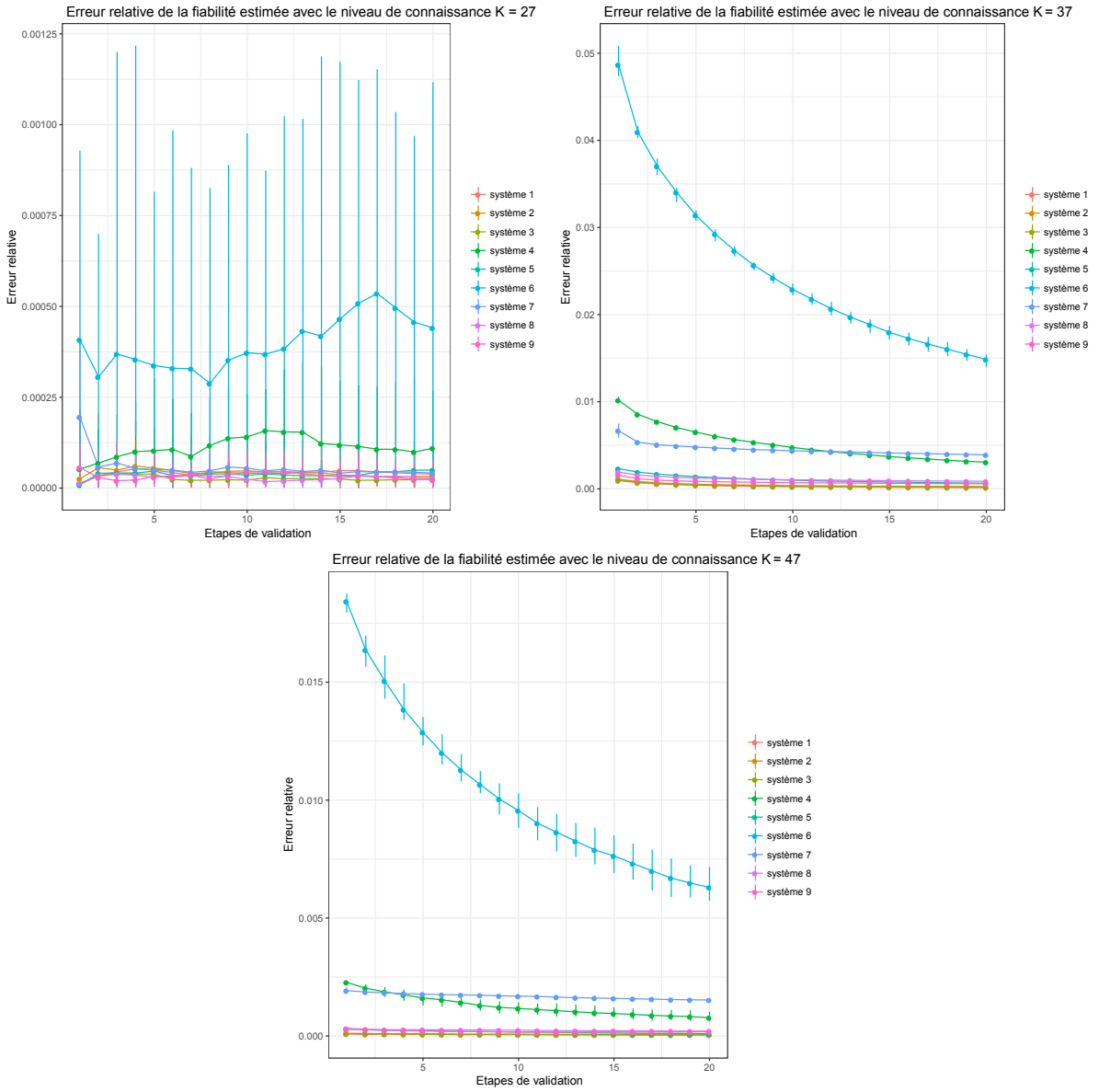


FIGURE 8.9 – Erreur relative de la fiabilité estimée pour les niveaux de connaissance 27,37 et 47 avec différents systèmes

— La valeur des paramètres initiaux de la connaissance associés à ces valeurs
— L'influence des paramètres à estimer sur le calcul de la fiabilité totale. L'imprécision d'un paramètre peut ne plus avoir d'effet lorsque celle-ci devient suffisamment petite pour être négligeable dans le calcul de la fiabilité.

Lorsque l'erreur est initialement nulle ou assez faible (par exemple dans le cas de la surestimation de la probabilité du survie) ; la décroissance est difficilement visible ou inexistante. L'estimation de la fiabilité est instable. Le comportement du modèle de fiabilité dans le K27 devra être analysé plus en détail. Le critère d'arrêt devra prendre en compte cette instabilité de l'estimateur lorsque celui-ci est très proche de la fiabilité du système.
Ces premières expérimentations montrent l'influence des distributions *a priori* sur la convergence de l'estimateur de la fiabilité pour différents systèmes. Cependant elles ne tiennent pas compte d'éventuels cas d'usage inconnus. La section suivante propose une nouvelle étude pour analyser le comportement du modèle de fiabilité lorsque des cas d'usage sont inconnus.

8.6 Etude de la convergence de l'estimateur vers la fiabilité du système lorsque des cas d'usages sont inconnus

L'objet de cette étude est un système à cinq cas d'usage. Trois sont connus mais leurs paramètres sont mal caractérisés. Les deux derniers sont inconnus. La procédure de validation est inchangée de celle de l'étude précédente. Dès qu'un scénario inconnu apparaît dans la séquence de validation, il est immédiatement détecté et bien classé dans une nouveau cas d'usage. La matrice de transition et la matrice de survie sont exprimées par les équations (8.12) et (8.13).

$$P = \begin{bmatrix} 0,8 & 0,2-(10+1+0,1)\times P_u & 10\times P_u & 1\times P_u & 0,1\times P_u \\ 0,6 & 0,4-(10+1+0,1)\times P_u & 10\times P_u & 1\times P_u & 0,1\times P_u \\ 0,7 & 0,3-(10+1+0,1)\times P_u & 10\times P_u & 1\times P_u & 0,1\times P_u \end{bmatrix} \tag{8.12}$$

$$S = \begin{bmatrix} 0,999999 & 0 & 0 & 0 & 0 \\ 0 & 0,99999 & 0 & 0 & 0 \\ 0 & 0 & 1-0,01\times D_u & 0 & 0 \\ 0 & 0 & 0 & 1-0,1\times D_u & 0 \\ 0 & 0 & 0 & 0 & 1-D_u \end{bmatrix} \tag{8.13}$$

P_u et D_u sont des variables qui permettent de générer différents systèmes. Les niveaux choisis et le plan complet généré sont présentés dans la table 8.4. Pour les trois cas d'usage connus, les erreurs des probabilités de transition et de survie *a priori* sont les mêmes et sont respectivement appelées ϵ_s et ϵ_t ainsi que les indices de confiance nommés w_s et w_t. Leurs valeurs et plan d'expériences sont identiques aux expérimentations précédentes données dans les tables 8.2 et 8.3.
Aucune connaissance *a priori* n'est donnée pour les cas d'usage inconnus. Les paramètres des distributions valent initialement zéro et sont mis à jour avec l'ensemble des données capitalisées pendant les semaines précédant leur instant de détection.

Le modèle de Goel Okumoto s'est révélé peu pertinent pour les systèmes 1, 3 et 9 car les temps d'apparition comptés en nombre de scénarios observés étaient trop grands, une autre échelle doit être choisie quand les apparitions se font rares. Pour les autres systèmes les expérimentations

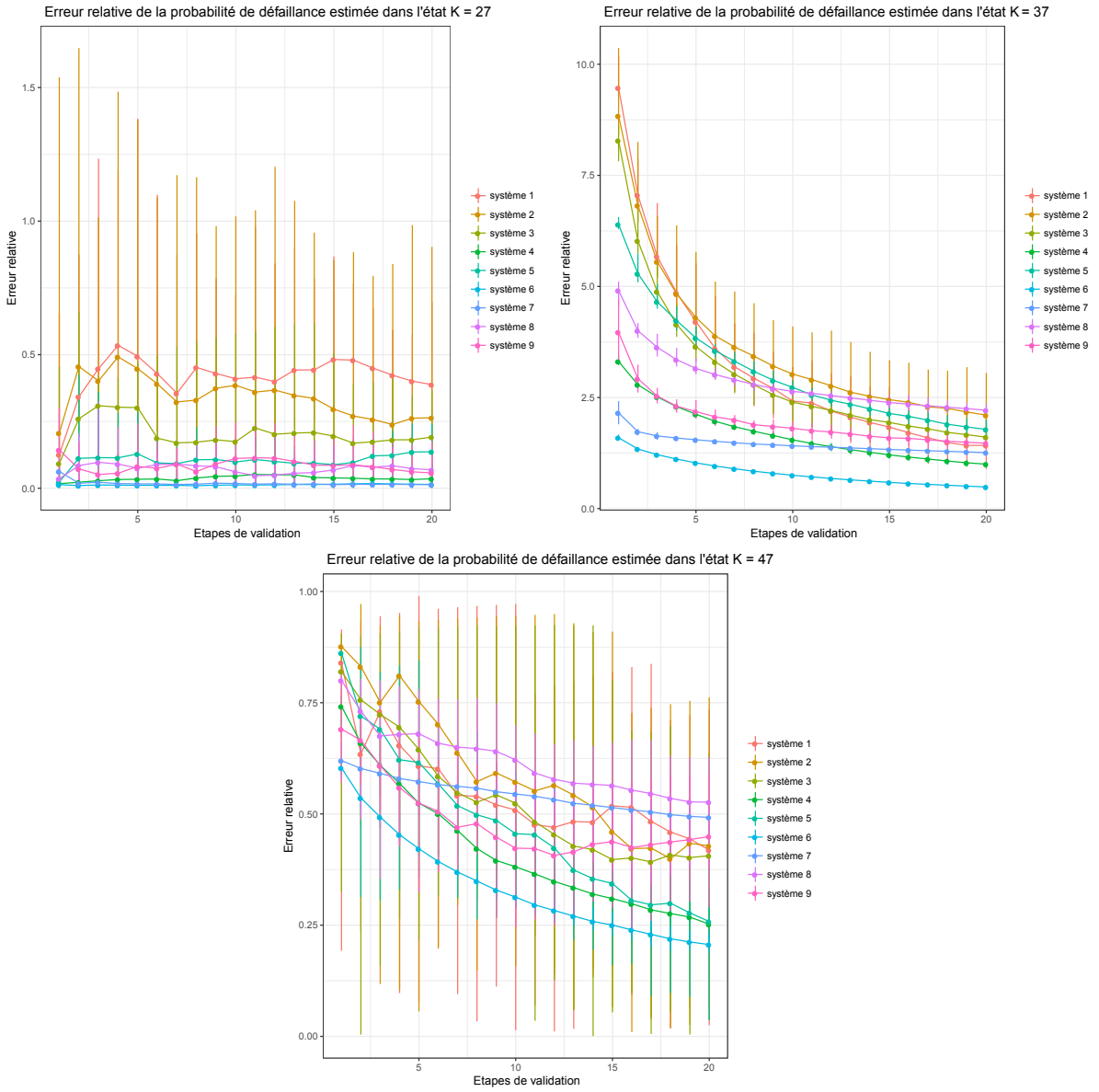


FIGURE 8.10 – Erreur relative de la probabilité de défaillance avant une une heure de roulage estimée pour les mêmes niveaux de connaissance 27,37 et 47 avec différents systèmes.

P_3	D_3
1e-02	1e-02
1e-03	1e-03
1e-04	1e-04

Système	P_3	D_3	R
1	0.0001	0,0001	
2	0.001	0,0001	0,99990
3	0.0001	0.001	
4	0.01	0.001	0,99904
5	0.01	0,0001	0,99985
6	0.01	0.01	0,99100
7	0.001	0.01	0,99901
8	0.001	0.001	0,99982
9	0.0001	0.01	

TABLE 8.4 – Valeurs et plan complet des paramètres des systèmes à 5 cas d'usage

ont bien fonctionné. Cependant les deux cas d'usage ont été détectés dés la première semaine d'observation. Le modèle de Goel Okumoto prédit la probabilité d'apparition d'un futur nouveau cas d'usage et reste inchangé pendant le reste de la séquence de validation. Le nombre de cas d'usage de l'expérimentation est insuffisant pour bien analyser le comportement du modèle à l'arrivée de cas d'usage nouveau. Nous présentons néanmoins les résultats obtenus pendant cette étude.

8.6.1 Comparaison de l'évolution de l'estimateur de la fiabilité entre plusieurs séquences de validation

Quelque soit le système étudié et l'état de connaissance choisi, l'évolution de la fiabilité estimée se présente comme la Figure 8.11 même lorsque les paramètres des cas d'usage connus sont surestimés initialement. Sur cette figure, nous pouvons voir que l'effet de la séquence est moins important. Les courbes d'évolution ont toutes la même forme, les sauts sont plus atténués que dans l'étude précédente. L'estimation du roulage 3 est décalée par rapport aux autres roulages. Ceci est en grande partie dû à la mauvaise prédiction de la probabilité de ne pas rencontrer un scénario inconnu, $\bar{P}_{uk}$, comme le montre la table 8.5. Ainsi pour le roulage 3, la valeur de l'estimation de $\bar{P}_{uk}$ est plus petite que celle des autres roulages. Or tous les nouveaux cas d'usage ont été rencontrés, cette probabilité devrait être égale à 1. Le modèle de Goel Okumoto ne semble pas pertinent pour un si petit nombre de cas d'usage encore inconnus. Il faudrait voir comment ce modèle se comporte pour plus de cas d'usage.

8.6.2 Comparaison de l'évolution de l'estimateur de la fiabilité entre différents états de connaissance

Pour le système 2, la Figure 8.12 présente les évolutions de l'estimateur de fiabilité en fonction des étapes d'avancement pour différents états de connaissance. Ici la connaissance initiale ne semble pas avoir beaucoup d'effet sur le comportement du modèle de fiabilité. Initialement les estimations de la fiabilité diffèrent. Elles sont très proches dès la seconde étape, sauf lorsque la connaissance est caractérisée par les valeurs de paramètres : $\epsilon_s = 0,2$ et $w_s = 100000$. Au fur et à mesure des itérations l'estimation de la fiabilité minimale et maximale des séquences de

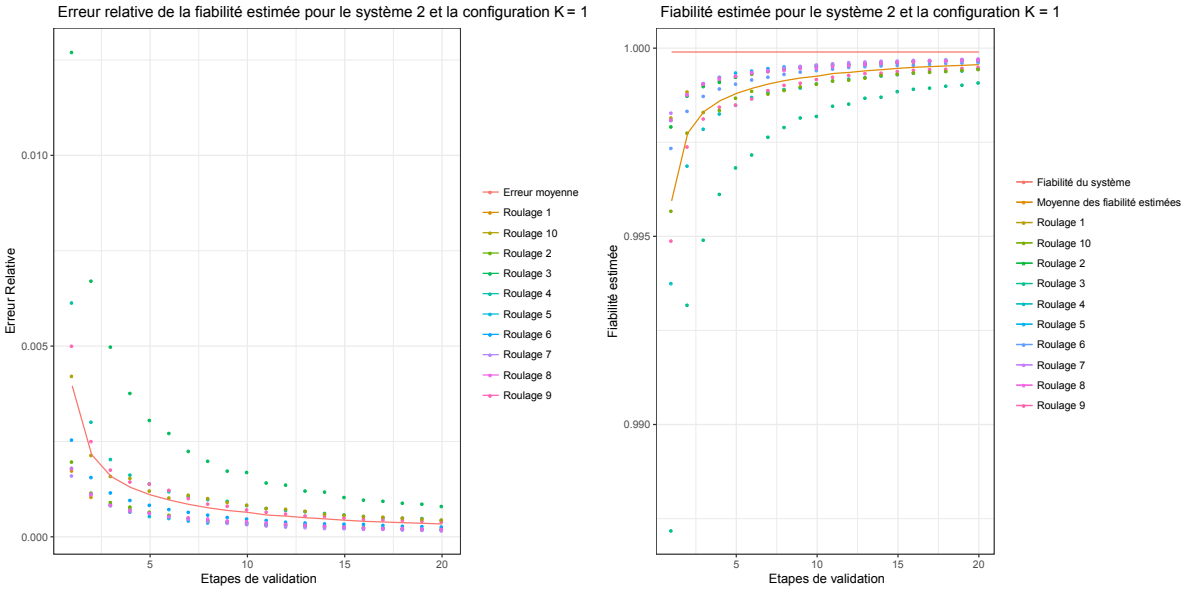


FIGURE 8.11 – Evolution de la fiabilité estimée du système 2 et le niveau de connaissance K = 1

Roulages	$\bar{P}_{uk}$
Roulage 1	0,999970
Roulage 2	0,999895
Roulage 3	0,997403
Roulage 4	0,999079
Roulage 5	0,999712
Roulage 6	0,999995
Roulage 7	0,999973
Roulage 8	0,999949
Roulage 9	0,999352
Roulage 10	0,999390

TABLE 8.5 – Prédiction de la probabilité de ne pas rencontrer de scénarios inconnus pour les différentes séquences de validation

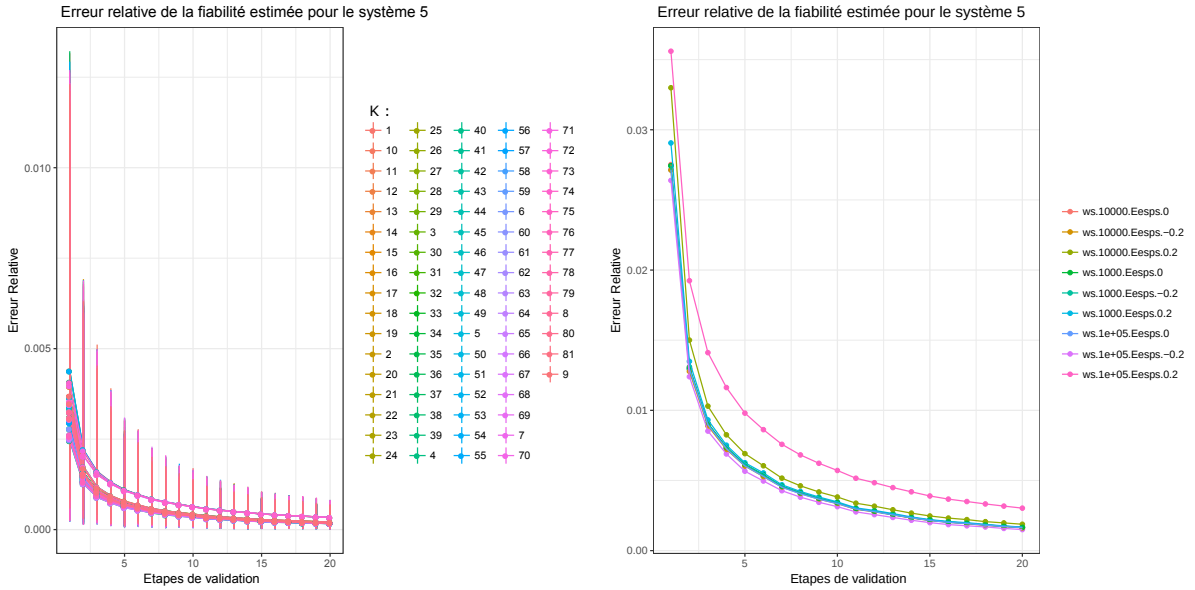


FIGURE 8.12 – Evolution de l'erreur relative de la fiabilité estimée pour le système à cinq cas d'usage dans tous les états de connaissance

validation représentées par des barres horizontales sur la figure de gauche se réduisent. L'impact de la séquence de validation a beaucoup moins d'effet avec les itérations.

8.6.3 Comparaison de l'évolution de l'estimateur de la fiabilité entre différents systèmes pour un même état de connaissance

Le graphe 8.13 présente l'évolution de l'estimation de la fiabilité pour différents systèmes. Initialement l'erreur est très grande pour les systèmes 5, 2 et 8 et se réduit très rapidement. Ce sont les trois systèmes ayant la plus grande fiabilité. Par conséquent l'obtention d'une estimation précise requiert plus d'étapes de validation que pour les autres systèmes.

Le modèle de Goël Okumoto ne prend pas en compte le temps à l'issue de la dernière apparition d'un nouveau cas d'usage. Pourtant cette information met en évidence que la prédiction donnée est incohérente. En effet, 99 semaines se sont écoulées sans nouvelle apparition d'un cas d'usage inconnu. 2079000 scénarios ont été observés pendant ce laps de temps. Supposons que l'observation d'un nouveau cas d'usage suit une loi de Bernoulli, de paramètre la probabilité estimée par le modèle Goël Okumoto. Prenons par exemple, la probabilité de non occurrence $\bar{P_{uk}}$ prédite par le modèle lors du roulage 1 pour le système 1, égale à $0,999970$. Après 2079000 scénarios la probabilité de n'observer aucun nouveau cas d'usage selon cette hypothèse est donc de 8.10^{-28}. Ce qui signifie que cette séquence de non occurrence est extrêmement rare voire non réaliste.
Nous recherchons une probabilité telle que la probabilité de rencontrer cette séquence soit au moins égale à 5%. Nous obtenons alors $\bar{P_{uk}} = 0,9999986$.

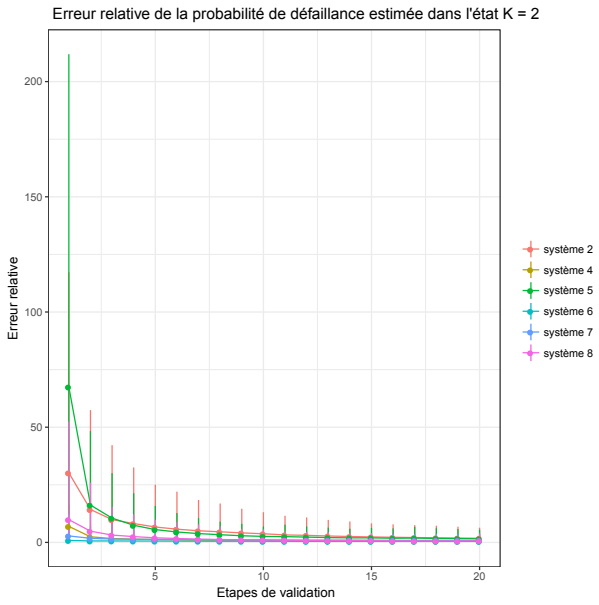


FIGURE 8.13 – Evolution de l'erreur relative de la probabilité de défaillance dans l'état de connaissance K2 pour tous les systèmes

8.7 Conclusion

La méthode d'estimation de la fiabilité fournit un cadre général permettant de mieux comprendre comment s'articule la validation du véhicule autonome. Elle a pour but de visualiser comment les séquences de scénarios observés, issus de cas d'usage mal caractérisés ou inconnus, influencent notre perception du comportement du véhicule autonome et l'organisation des roulages de validation. De nombreux objectifs ont été listés et les expérimentations réalisées dans une configuration prototype permettent d'en atteindre quelques uns partiellement :

1. **Choisir un nouvel estimateur qui caractérise plus fidèlement la fiabilité du système**

   La moyenne empirique de la variable aléatoire exprimée par l'équation (7.51) semble être un bon estimateur de la fiabilité du système. Dans de nombreuses configurations son évolution au fil des itérations de la validation apporte une information sur la valeur de la fiabilité du système. La moyenne de l'estimateur sur plusieurs séquences de validation a été étudiée dans plusieurs états de connaissance sur plusieurs systèmes.

2. **Etudier l'influence des parcours possibles pendant le processus de validation**

   En fonction des séquences de validation, l'estimateur converge plus ou moins rapidement. Suivant les systèmes et les paramètres de connaissance l'écart entre les estimations de chaque séquence de roulage peut être plus ou moins important et diminue au fil des itérations.

3. **Etudier la convergence de l'estimateur vers la fiabilité du système dans différents cas de connaissance et l'impact sur la vitesse de convergence d'un biais sur les distributions *a priori* des probabilités de transition et de survie**

   En moyenne, lorsque les distributions *a priori* initiales entraînent une sous-estimation de la fiabilité, l'estimateur croît régulièrement vers la fiabilité du système.
   Lors d'une sur-estimation initiale de la fiabilité l'estimateur croît par morceaux et décroît par sauts successifs. L'estimateur croît tant qu'aucune défaillance n'est observée et décroît à l'apparition d'une défaillance. Plus l'estimateur s'approche de la valeur de la fiabilité du système et plus l'impact de ces sauts se réduit. De même la croissance entre ces sauts est plus faible avec les itérations. Si la fiabilité du système étudié est élevée et qu'aucune défaillance n'est observée pendant les essais de validation, l'estimation de la fiabilité risque de rester erronée. Des roulages aléatoires ne seront peut être pas pertinents dans ce contexte.
   Enfin lorsque la fiabilité est initialement bien estimée une instabilité de l'estimateur est observée.
   La construction d'un critère d'arrêt ne semble pas évidente. Les roulages de validation peuvent être arrêtés trop tôt avant l'apparition d'un saut de l'estimateur. Des études complémentaires doivent être menées.

4. **Étudier l'efficacité de la méthode en fonction du système à valider**

   L'efficacité de la méthode varie selon les systèmes étudiés. Étonnamment, la vitesse de convergence a été constatée plus lente pour un système qui n'était ni le plus fiable, ni avec le cas d'usage influent le plus rare. Une erreur simultanée des deux probabilités semble avoir un fort impact sur le calcul de la fiabilité.

5. **Étudier le comportement du modèle lorsque des cas d'usage sont inconnus et analyser la prévision du modèle de Goël Okumoto en fonction des apparitions de nouveaux cas d'usage**

   Le modèle de Goël Okumoto permettant de prédire la probabilité d'occurrence d'un cas d'usage inconnu n'a pas été adapté au cas d'étude proposé. Le modèle n'a pas pu estimer cette probabilité lorsque les nouveaux cas d'usage sont apparus très tardivement. De plus les estimations étaient mauvaises dans les autres cas, impactant le reste de l'analyse. Un autre modèle de croissance de fiabilité, ne tenant pas compte du temps passé sans nouvelle apparition d'un cas d'usage inconnu, n'aurait pas été plus pertinent. Ces modèles sont pertinents dans le contexte de la fiabilité d'un logiciel car de nombreux bugs sont détectés pendant la phase de débogage et leur nombre en phase de validation est beaucoup plus important que le nombre de cas d'usage présent dans le cas académique traité. Pour mieux savoir si ce modèle sera adapté au contexte du véhicule autonome, il faudrait analyser les temps d'apparition des nouveaux cas détectés pendant la phase de conception du système autonome.

6. **Chercher l'existence d'une accélération de la convergence de l'estimateur par**

l'utilisation de roulages guidés.

Les premières analyses ont démontré que dans un cas très simple, un roulage réduisant le temps de validation était possible pour l'estimation de la fiabilité de certains systèmes. Une analyse de sensibilité de la fiabilité faisant varier les paramètres caractérisant la connaissance semble donner une indication des roulages nécessaire pour préciser l'estimation de la fiabilité.

Les résultats d'expérimentations ont montré que l'efficacité de la méthode dépendait du système étudié. Ils n'ont pas permis d'identifier dans quel contexte cette méthode était efficace. D'autres expérimentations faisant varier plus largement le nombre de cas d'usage, ainsi que les probabilités de transition et de survie de nouveaux systèmes pourront éclaircir ce point.
Pour le moment, les expérimentations ont été réalisées sur des systèmes dont les domaines de fonctionnement comportent peu de cas d'usage. Elles sont des exemples d'expérimentations possibles pour prédire les différents déroulements des essais de validation observables. Cet exemple numérique peut aider dans la sélection et le dimensionnement des roulages de validation. Les essais peuvent être complétés par des analyses virtuelles des comportements possibles du système étudié en faisant varier le niveau de connaissance. Ainsi ces analyses indiqueront les erreurs possibles de jugement et d'estimation avec les données recueillies pendant les étapes de validation. L'ensemble des perspectives et des améliorations à réaliser sont développées dans le chapitre 9.

Chapitre 9

Conclusion et perspectives

Le nombre, la diversité et l'arrivée très rapide des nouvelles technologies entraînent une méconnaissance du comportement des nouveaux véhicules AD et ADAS pendant la phase de validation. Une méthode de validation de la fiabilité itérative a été proposée dans ce document pour compléter les méthodes traditionnelles de sûreté de fonctionnement et aider dans la planification et la décision des essais de validation.

Au lieu de traiter le problème en supposant que le système est une boîte noire, dont la seule information disponible est l'objectif de fiabilité à atteindre, notre étude tire partie de l'ensemble des informations accessibles sur le système et son environnement. De plus tous les outils de validation sont mis à contribution pour estimer la fiabilité du véhicule autonome. Les roulages aléatoires sur route ouverte sont beaucoup trop longs pour valider le système à la date de lancement attendue. La connaissance même partielle du comportement du véhicule autonome permet d'une part de simuler le comportement du véhicule autonome numériquement ou sur des pistes contrôlées et d'autre part de cibler les zones de l'espace des scénarios dans lesquels le comportement du véhicule autonome est le plus incertain. La méthode d'estimation de la fiabilité a été choisie en faisant l'hypothèse que les scénarios entraînant des défaillances du système ne sont pas réparties de manière homogène dans l'espace des paramètres qui caractérisent le domaine de fonctionnement. Ils sont supposés être situés dans des zones de cet espace plus rares. Ces zones pénalisent la fiabilité du véhicule autonome.

L'organisation générale des procédures d'essais proposée ne peut s'effectuer que par le biais d'une méthode d'estimation de la fiabilité qui calcule séparément la contribution de chaque zone. Pour ce faire, les parcours réalisés avec ce véhicule sont vus comme des séquences de scénarios, courtes séquences temporelles contenant des actions des automobilistes, regroupés en cas d'usage. Le modèle de fiabilité choisi évalue d'une part la probabilité d'apparition des différentes séquences de scénarios et d'autre part la probabilité de survie du véhicule dans chaque cas d'usage. Les paramètres du modèle de fiabilité sont au préalable estimés *a priori* et sont mieux qualifiés par une mise à jour bayésienne. Certains cas d'usages ont été omis pendant la phase de conception et seront identifiés pendant les roulages de validation. Pour prendre en compte leur non connaissance dans le calcul de la fiabilité, une méthode de croissance de fiabilité, utilisée actuellement pour la fiabilité des logiciels, prédit la probabilité d'apparition d'un futur cas d'usage.

Cette méthode d'évaluation a été testée sur des cas d'étude académiques, composés de quelques cas d'usage. Bien qu'assez éloignés des systèmes autonomes conçus dans l'entreprise comportant plus de 200 cas d'usage, leurs analyses montrent les avantages d'utiliser une telle méthode.

Ce type d'analyse peut aider à la décision tout au long de la phase de validation. Nous listons un ensemble d'étude possible avec le modèle.

— **Donner un premier ordre de grandeur sur la durée des tests nécessaires**
Avec la connaissance acquise pendant la phase de conception des déroulements possibles de validation peuvent être simulés. Ainsi, la variation des niveaux de connaissance et des erreurs possibles sur les paramètres du modèle de fiabilité peuvent donner une durée majorante de la validation pour organiser le plan de validation.

— **Mettre en évidence les paramètres les plus influents et identifier les actions à réaliser en priorité**
Pour aider dans le choix des *a priori*, les données obtenues aux essais de validation peuvent être confrontées à des résultats obtenus en simulation numérique. Par des analyses de sensibilité, l'étude de la variation de la fiabilité associée aux variations des paramètres du système et des paramètres de la connaissance peut mettre en évidence les paramètres fortement influents. Les efforts seront mis en priorité pour construire un bon *a priori* à ces paramètres et les essais devront se concentrer sur leur précision.

— **Donner un encadrement aux résultats obtenus**
La séquence de cas d'usage observés lors du roulage de validation a une influence sur les résultats obtenus. Pour rajouter un niveau de sécurité supplémentaire ces résultats peuvent être encadrés par des estimations réalisées par simulation numérique.

Le modèle présenté est une première proposition mais doit être appliqué au comportement réel du véhicule autonome. Tout au long de cette thèse, sa construction a permis de mettre en évidence les difficultés liées à la validation du véhicule autonome. Il sert d'illustration, et initie la mise en place d'une méthode de validation dédiée au système très innovant. Son caractère modulaire permet de l'adapter au contexte et à l'améliorer sans abandonner toute la méthode décrite dans cette partie. Il ouvre sur un vaste champ de perspectives.

— **Evaluer le niveau de réalisme des roulages numériques pour le choix d'un niveau de confiance des résultats obtenus**
Tout au long de ce document, le manque de réalisme des roulages numériques a été signalé.
D'une part, l'existence de certains scénarios numériques est discutable, car leurs probabilités de survenir sont extrêmement faibles et leur combinaisons de paramètres de l'environnement associées ne sont pas réalisables. D'autre part, beaucoup de paramètres de l'environnement et l'effet de leurs variabilités ne sont pas pris en compte dans l'estimation de la probabilité de défaillance du système dans chaque cas d'usage.
Ce manque de réalisme doit être pris en compte dans la sélection du niveau de confiance à accorder aux résultats obtenus en simulation pour débuter la phase de validation. Ce-

pendant aucune stratégie de sélection n'a été présentée dans ce document et peut être le sujet d'une nouvelle étude. Un niveau de réalisme élaboré à l'aide d'une comparaison entre les résultats obtenus en simulation et ceux recueillis par des essais sur piste ou sur route ouverte peut être une piste à investiguer.

— **Définir un critère d'arrêt pour la recherche numérique des zones de défaillances dans chaque cas d'usage**
Tout comme les essais physiques, les essais numériques se font par itération successive pour rechercher les zones entraînant des défaillances. Ces essais se réalisent séparément, cas d'usage par cas d'usage. Tout comme les essais physiques, les cas d'usage peu influents n'auront pas besoin d'une recherche aussi fine des défaillances.
Un critère d'arrêt global sur l'ensemble des essais, numériques ou physiques doit être trouvé pour faire un compromis entre finesse des résultats et durée des essais à chaque étape de validation.

— **Réaliser des études avec un nombre de cas d'usage du même ordre de grandeur que le véhicule autonome étudié**
Les applications effectuées sur le modèle de fiabilité ont été choisies volontairement avec un nombre réduit de cas d'usage pour faciliter l'analyse. En effet l'influence de chaque cas d'usage est dans ce cadre plus facile à maîtriser. Cependant plus de 200 cas d'usage sont actuellement répertoriés pour le véhicule autonome. Plus ce nombre est grand et plus il risque d'y avoir de cas d'usage influents. Cela peut réduire l'efficacité de la méthode. De nouvelles études avec des exemples académiques comportant un très grand nombre de cas d'usage permettront de vérifier l'applicabilité et l'efficacité de la méthode dans ce contexte et orienter les prochaines analyses à mener dans le cas contraire.

— **Vérifier l'adéquation de la modélisation avec un système autonome**
Les exemples d'application ont été imaginés suivant les hypothèses adoptées pour la conception du modèle. Pourtant rien n'assure que ces hypothèses représentent bien le système autonome. Des tests d'adéquation sont nécessaires avant d'appliquer la méthode sur de réels systèmes. Parce que le modèle est modulaire il pourra être amélioré pour s'adapter au contexte.

— **Sélectionner un modèle de croissance de fiabilité qui tient compte du temps sans défaillance**
Les essais avec des cas d'usage inconnus n'ont pas donné de résultats très satisfaisants. Le nombre de cas d'usage à identifier était trop petit pour que la prédiction du modèle de Goel Okumoto soit pertinente.
L'approche des modèles de croissance de fiabilité n'est peut être pas la plus adéquate pour répondre à ce type de problème. En effet le nombre de bugs dans un algorithme est souvent très élevé en phase de conception alors que les nouveaux cas d'usage sont moins nombreux et plus longs à survenir dans le temps. De plus le parcours d'un algorithme pendant la phase de test permet de diversifier les usages et ainsi de trouver plus rapidement les bugs. Pour la recherche de nouveaux cas d'usage, l'absence complète de connaissance sur les cas inconnus retarde leur identification. Enfin, l'hypothèse d'une vitesse de détection proportionnelle au nombre de cas d'usage restant n'est sans doute pas vérifiée.

Une méthode de croissance de fiabilité bayésienne tenant compte du temps sans défaillance pourrait apporter de meilleurs résultats.

Les essais n'ont pas non plus permis d'étudier le choix de la probabilité de survie du système dans les cas d'usage inconnus. Nous avons pu constater que la fiabilité était largement sous-estimée quelque soit le niveau de connaissance. Ce choix doit avoir un impact sur l'évaluation de la fiabilité mais il était négligeable comparé à l'influence de l'estimation erronée de la probabilité d'apparition d'un cas d'usage inconnu.

— **Donner un critère d'arrêt des essais de validation**
Nous avons observé trois comportements distincts de l'estimateur de fiabilité. Si la fiabilité est sur-estimée, l'estimateur croît par morceau et décroît par saut. Lorsque la fiabilité est bien estimée, l'estimateur est instable. Enfin, si la fiabilité est sous-estimée, l'estimateur croît. Dès-lors, il n'est pas facile d'identifier un critère d'arrêt des validations applicable dans toutes ces situations. Ce critère pourrait s'établir par simulation. La recherche de l'ensemble des systèmes (de probabilités de transition et probabilités de survie différentes) pouvant conduire aux mêmes observations pendant la phase de validation (même enchaînement de scénarios, même nombre de défaillances) donne une indication sur les erreurs possibles d'analyse avec une probabilité associée.

— **Donner un meilleur encadrement de la fiabilité**
La méthode par inférence bayésienne, avec les distributions *a priori* des probabilités de transition entre chaque cas d'usage et de survie, n'ont pas permis de construire un intervalle de crédibilité exploitable pour les études de fiabilité. Le choix d'autres distributions ou la création d'un intervalle par une méthode non probabiliste pourrait contribuer à l'élaboration d'un nouvel intervalle. Celui-ci encadrerait mieux la fiabilité du système autonome. Une information plus robuste et moins instable que l'estimation de la fiabilité actuelle serait apportée.

— **Identifier les configurations pour lesquelles la méthodologie est efficace ou non**
Les applications réalisées sont juste des exemples qui n'ont pas permis de mettre en évidence les conditions pour lesquelles la méthode est efficace. En effet le nombre de paramètres à faire varier était bien trop important pour obtenir de telles conclusions. Le système n'était pas assez mature pour réduire la dimension du problème en ne sélectionnant que quelques paramètres. Certains paramètres, tels le nombre de cas d'usage, la fréquence des cas d'usages ou les probabilités du système, peuvent être orientés par les premières analyses du système à tester. Ainsi lorsque les premières connaissances seront exploitables pour réaliser ce type d'étude il sera plus facile d'en déduire des configurations à privilégier pour garantir l'efficacité de la méthode.

— **Accélérer les roulages de validation**
Les expérimentations réalisées dans le chapitre précédent laisse penser qu'un roulage de validation qui favorise l'apparition de certains cas d'usage, dont l'incertitude influence le plus l'estimation de la fiabilité, pourrait entraîner une convergence plus rapide de l'estimateur vers la fiabilité du système. Une analyse de sensibilité de la fiabilité face aux variations des paramètres caractérisant la connaissance peut identifier les cas d'usage les

plus influents. Les algorithmes proposés peuvent aider dans l'élaboration d'une méthode d'accélération en sélectionnant la méthode de sensibilité adéquate. Celle-ci guidera les roulages de validation pour accélérer la convergence de l'estimation sans introduire de biais.

— **Construire un nouvelle classification afin de sélectionner les cas d'usage qui rendent la méthode de validation plus efficace**
Les expérimentations ont montré que pour des systèmes de valeurs de fiabilité presque similaires, la vitesse de convergence de l'estimateur vers la fiabilité du système diffère alors que l'état de connaissance est le même. Il faut donc bien choisir la classification en cas d'usage pour augmenter l'efficacité de la méthode d'estimation. Actuellement la classification en cas d'usage est indépendante du comportement du système. Ainsi la contribution de chaque cas d'usage sur la fiabilité n'est pas contrôlée. Cependant il est possible d'envisager de redécouper ces cas d'usages en découpant les intervalles de valeurs de chaque paramètre. Par exemple si dans un cas d'usage, une zone dans l'espace des paramètres entraîne une défaillance du système avec une plus grande probabilité, cette zone pourra être isolée en un nouveau cas d'usage car la convergence des estimations de ces paramètres sera plus rapide (la défaillance apparaîtra plus vite car la probabilité est plus grande). Les zones bien caractérisées du cas d'usage peuvent être également isolées car leur niveau de connaissance est suffisant et leurs observations ne sont plus nécessaires pendant les essais de validation. Il faut toutefois faire attention. Si le nombre de cas d'usage est élevé, avec des probabilités de défaillances du même ordre de grandeur, cela risque de retarder la précision des estimations de leurs paramètres pris indépendamment et par conséquence de ralentir la convergence de l'estimateur de la fiabilité. Il faut donc trouver un compromis entre redécoupage des cas d'usage et nombre de cas d'usage.
Une nouvelle méthode de classification est donc à construire pour sélectionner les meilleurs cas d'usage et garantir ainsi une convergence rapide de l'estimateur de fiabilité.

Conclusion Générale

Les systèmes d'aide à la conduite et le véhicule autonome vont garantir une plus grande sécurité routière dans les années à venir. Les fonctionnalités de ces systèmes s'enrichissent continuellement pour, à terme, remplacer l'être humain dans l'ensemble de ses actions de conduite.
La certification de la fiabilité est un enjeux majeur pour assurer cette sécurité. Cependant le contexte actuel rend cette tâche complexe à réaliser. Ce sont des systèmes très innovants dont les diverses technologies évoluent sans cesse pour améliorer leurs performances et fonctionnalités. Les méthodes de sûreté de fonctionnement actuelles sont insuffisantes pour concevoir un plan de validation final de durée réduite afin de respecter le temps de mise sur le marché.

Dans une première partie l'ensemble des méthodes et outils disponibles dans le contexte des ADAS et du véhicule autonome au sein de l'entreprise a été revu. Ces méthodes prises indépendamment ne sont pas suffisantes pour construire un plan adapté à la validation des véhicules autonomes. Les essais de différents types, numériques et physiques doivent être combinés pour atteindre cet objectif. Cette stratégie semble être adoptée par la plupart des concurrents.
Pour organiser les différents essais à réaliser, la bonne connaissance de l'environnement du véhicule est un atout. Grâce à cette connaissance, les essais sont sélectionnés pour tester le véhicule dans les scénarios de conduite qui sont susceptibles de mettre en défaut ce dernier. Cependant la méconnaissance de ces événements rend la conception d'un tel plan impossible au début de la phase de validation. Le système ne sera attesté fiable que lorsque la base de connaissance aura été jugée "complète" ou suffisamment représentative de son environnement et que le bon fonctionnement du système aura été validé dans cette base.
Une étude bibliographique est réalisée dans le but d'identifier une méthode statistique qui permet d'évaluer la fiabilité du véhicule autonome en tenant compte des incertitudes épistémiques avec une procédure d'échantillonnage efficace.
La modélisation de la fiabilité doit reproduire l'évolution dynamique du système pendant son utilisation. La forte variabilité de l'environnement empêche la collecte d'une base de données exhaustive. Les estimations des paramètres sont par conséquent entâchées d'incertitudes qui se réduisent avec l'accroissement de connaissance. Enfin ce modèle doit tenir compte des incertitudes épistémiques liées à la non connaissance de certains scénarios.

La seconde partie propose une méthode de validation de la fiabilité itérative pour compléter les méthodes traditionnelles de sûreté de fonctionnement et aider dans la planification et la décision des essais de validation.
Elle part de l'hypothèse que la durée des tests de roulage est partitionnée en séquences de scénarios. Ceux-ci sont de courtes séquences temporelles de quelques minutes qui décrivent les actions

observées par le véhicule et son environnement. Ils sont regroupés en cas d'usage selon une classification choisie. Chaque cas d'usage influence la fiabilité du véhicule autonome. Leur contribution respective s'évalue selon deux composantes : les fréquences de chaque enchaînement de cas d'usage et les probabilités de défaillance du système dans ces cas d'usage. De cette manière, la démarche de validation peut combiner l'ensemble des moyens disponibles dans l'entreprise.
Une première organisation a été détaillée pour sélectionner les essais à réaliser. Les essais numériques et les essais ciblés sur piste ou sur route ouverte servent à évaluer les probabilités de défaillance dans les cas d'usage. Les essais aléatoires sur route ouverte et les sources externes d'informations sont principalement utiles dans l'estimation de la probabilité d'occurrence des séquences de cas d'usage.
Pour chaque étape de la méthode proposée, des études de faisabilité ont été menées. Certaines étapes comme l'optimisation des roulages numériques ouvrent de nombreuses perspectives d'amélioration en proposant de nouveaux algorithmes plus adaptés à la problématique étudiée. Elle fait l'objet d'un nouveau sujet de thèse chez Renault. D'autres, comme les roulages ciblés et les roulages sur piste requièrent un travail plus approfondi.
La démarche de validation est itérative et s'associe à une méthode d'estimation de la fiabilité. Cette modélisation a pour objectif d'apporter une mesure de l'état d'avancement de la phase de validation. Elle évalue en effet la fiabilité du véhicule avec une erreur après chaque étape de validation grâce au niveau de connaissance acquis.
Nous avons présenté un cadre général et l'avons exposé au travers d'une configuration particulière comme preuve de faisabilité. Le modèle résultant est composé de plusieurs sous-parties :

- la chaîne de Markov qui représente l'enchaînement des cas d'usages,
- les distributions *a priori* des paramètres, bêta-binomiale pour les probabilités de survie et Dirichlet-multinomiale pour les probabilités de transition,
- le modèle de croissance de fiabilité de Goel-Okumoto pour évaluer la probabilité des cas d'usages inconnus avec une inférence bayésienne pour estimer ses paramètres.
- la plus faible des probabilités de survie dans les cas d'usages connus pour prédire la probabilité de survie du système dans le cas d'usage inconnu

Le caractère modulaire de ce modèle offre l'opportunité de modifier les sous-parties sans remettre en question toute la structure présentée.
Le chapitre 8 fait une première étude des performances de la méthode sur des cas d'études numériques et ouvre sur sa potentielle utilité pour aider à l'organisation des essais et la décision. Sur certains cas, la méthode s'est révélée efficace mais cela dépend beaucoup du contexte et du système étudié. D'autres expérimentations faisant varier plus largement le nombre de cas d'usage, ainsi que les probabilités de transition et de survie de nouveaux systèmes pourront éclaircir ce point.
Le chapitre 9 conclut et donne un grand nombre de perspectives pour continuer l'étude. En effet ce mémoire initie à peine les travaux à mener avant de valider un système aussi innovant que le véhicule autonome. Il conduit à de nombreuses questions. D'une part, la construction d'un modèle de fiabilité cohérent est primordial pour obtenir une bonne analyse pour un état de connaissance donné. D'autre part chaque étape de la démarche de validation nécessite un travail de recherche approfondi et peut remettre en cause son organisation.

Notons enfin que ce travail de thèse s'est réalisé en participant à de nombreuses discussions sur la stratégie de validation. Ces discussions ont contribué à l'initiation d'un POC à l'INRIA [68] pour la classification des scénarios. Toujours en collaboration avec l'équipe de projet ces

discussions ont abouti à une étude pour définir la fiabilité des algorithmes des capteurs et des algorithmes de fusion en termes d'erreurs admissibles. Un outil numérique ADValue est en cours de perfectionnement et d'industrialisation par le service d'accueil. Enfin le modèle de fiabilité est codé avec le langage R. Il est envisagé d'appliquer en premier lieu cette approche aux simulations numériques.

Bibliographie

[1] AFNOR, N. (1988). X60-500. *Terminologie relative à la Fiabilité-Maintenabilité-Disponibilité*, 988.

[2] auto innovations (2015). Simulation pour la sécurité du Véhicule Autonome : SystemX lance le projet SVA. `http://www.auto-innovations.com/communique/357.html`.

[3] Bergenhem, C., Johansson, R., Söderberg, A., Nilsson, J., Tryggvesson, J., Törngren, M., and Ursing, S. (2015). How to reach complete safety requirement refinement for autonomous vehicles. In *CARS 2015-Critical Automotive applications : Robustness & Safety*.

[4] Berk, M., Kroll, H.-M., Schubert, O., Buschardt, B., and Straub, D. (2017). Bayesian test design for reliability assessments of safety-relevant environment sensors considering dependent failures. Technical report, SAE Technical Paper.

[5] Berthomieu, B. and Diaz, M. (1991). Modeling and verification of time dependent systems using time petri nets. *IEEE transactions on software engineering*, 17(3) :259–273.

[6] Billingsley, P. (1961). Statistical methods in markov chains. *The Annals of Mathematical Statistics*, pages 12–40.

[7] Bird, F. E. and Germain, G. L. (1996). *Practical loss control leadership*. Det Norske Veritas (USA).

[8] Breiman, L., Friedman, J. H., Olshen, R. A., and Stone, C. J. (1984). Classification and regression trees, the wadsworth statistics and probability series, wadsworth international group, belmont california (pp. 356).

[9] Cerf, V. G. (2018). A comprehensive self-driving car test. *Communications of the ACM*, 61(2) :7–7.

[10] Chen, X., Wang, K., and Yang, F. (2013). Stochastic kriging with qualitative factors. In *Proceedings of the 2013 Winter Simulation Conference : Simulation : Making Decisions in a Complex World*, pages 790–801. IEEE Press.

[11] Cherfi, A., Arbaretier, E., and Zhao, L. (2016). Sécurité-innocuité des véhicules autonomes : enjeux et verrous. *6A-Risques liés aux nouveaux usages-architectures robustes 2*.

[12] Cocozza-Thivent, C. (1997). *Processus stochastiques et fiabilité des systèmes*, volume 28. Springer Science & Business Media.

[13] Der Kiureghian, A. et al. (2005). First-and second-order reliability methods. *Engineering design reliability handbook*, 14.

[14] Dingus, T. A., Klauer, S. G., Neale, V. L., Petersen, A., Lee, S. E., Sudweeks, J., Perez, M. A., Hankey, J., Ramsey, D., Gupta, S., et al. (2006). The 100-car naturalistic driving study, phase ii-results of the 100-car field experiment. Technical report.

[15] Driving, S. A. (2014). Sae international j3016.

[16] Duane, J. (1964). Learning curve approach to reliability monitoring. *IEEE transactions on Aerospace*, 2(2) :563–566.

[17] Dubois, D. and Prade, H. (2012). Possibility theory. In *Computational complexity*, pages 2240–2252. Springer.

[18] Dupuy, D., Helbert, C., Franco, J., et al. (2015). Dicedesign and diceeval : two r packages for design and analysis of computer experiments. *Journal of Statistical Software*, 65(11) :1–38.

[19] Duthon, P., Bernardin, F., Chausse, F., and Colomb, M. (2016). Methodology used to evaluate computer vision algorithms in adverse weather conditions. *Transportation Research Procedia*, 14 :2178–2187.

[20] Echard, B., Gayton, N., and Lemaire, M. (2011). Ak-mcs : an active learning reliability method combining kriging and monte carlo simulation. *Structural Safety*, 33(2) :145–154.

[21] Eenink, R., Barnard, Y., Baumann, M., Augros, X., and Utesch, F. (2014). Udrive : the european naturalistic driving study. In *Proceedings of Transport Research Arena*. IFSTTAR.

[22] Euro, N. (2010). Pedestrian testing protocol.

[23] Fancher, P. (1998). Intelligent cruise control field operational test. final report. volume i : Technical report.

[24] Farr, W. (1996). Software reliability modeling survey. *Handbook of software reliability engineering*, pages 71–117.

[25] Gaudoin, O., Ledoux, J., et al. (2007). *Modélisation aléatoire en fiabilité des logiciels*. Hermès Science.

[26] Geronimi, S., Abadie, V., and Becker, N. (2016). Methodology to assess and to validate the dependability of an advanced driver assistance system (adas) such as automatic emergency braking system (aebs). In *Energy Consumption and Autonomous Driving*, pages 125–131. Springer.

[27] Geronimo, D., Lopez, A. M., Sappa, A. D., and Graf, T. (2010). Survey of pedestrian detection for advanced driver assistance systems. *IEEE transactions on pattern analysis and machine intelligence*, 32(7) :1239–1258.

[28] Gettman, D. and Head, L. (2003). Surrogate safety measures from traffic simulation models. *Transportation Research Record : Journal of the Transportation Research Board*, (1840) :104–115.

[29] Gietelink, O., Ploeg, J., De Schutter, B., and Verhaegen, M. (2006). Development of advanced driver assistance systems with vehicle hardware-in-the-loop simulations. *Vehicle System Dynamics*, 44(7) :569–590.

[30] Gunst, R. F. (1996). Response surface methodology : process and product optimization using designed experiments.

[31] Hastings, W. K. (1970). Monte carlo sampling methods using markov chains and their applications. *Biometrika*, 57(1) :97–109.

[32] Hobbs, C. A. and McDonough, P. J. (1998). Development of the european new car assessment programme (euro ncap). *Regulation*, 44 :3.

[33] Hojjati-Emami, K., Dhillon, B., and Jenab, K. (2012). Reliability prediction for the vehicles equipped with advanced driver assistance systems (adas) and passive safety systems (pss). *International Journal of Industrial Engineering Computations*, 3(5) :731–742.

[34] Huang, Z., Lam, H., and Zhao, D. (2017). Sequential experimentation to efficiently test automated vehicles. In *Simulation Conference (WSC), 2017 Winter*, pages 3078–3089. IEEE.

[35] Hydén, C. (1996). Traffic conflicts technique : state-of-the-art. *Traffic Safety Work with Video-Processing, University Kaiserslautern, Transportation Department, Kaiserslautern, Germany.*

[36] Ismail, K., Sayed, T., Saunier, N., and Lim, C. (2009). Automated analysis of pedestrian-vehicle conflicts using video data. *Transportation Research Record : Journal of the Transportation Research Board*, (2140) :44–54.

[37] Iso, I. (2011). 26262 : Road vehicles-functional safety. *International Standard ISO/FDIS*, 26262.

[38] Jelinski, Z. and Moranda, P. (1972). Software reliability research, statistical computer performance evaluation, edited by w. freigerger.

[39] Jones, D. R., Schonlau, M., and Welch, W. J. (1998). Efficient global optimization of expensive black-box functions. *Journal of Global optimization*, 13(4) :455–492.

[40] Kalra, N. and Paddock, S. M. (2016). Driving to safety : How many miles of driving would it take to demonstrate autonomous vehicle reliability ? *Transportation Research Part A : Policy and Practice*, 94 :182–193.

[41] Koita, A. (2011). *Evaluation probabiliste de la dangerosité des trajectoires de véhicules en virages.* PhD thesis, Université Blais e Pascal-Clermont-Ferrand II.

[42] Kuo, L. and Yang, T. Y. (1996). Bayesian computation for nonhomogeneous poisson processes in software reliability. *Journal of the American Statistical Association*, 91(434) :763–773.

[43] Kusano, K. D. and Gabler, H. (2011). Method for estimating time to collision at braking in real-world, lead vehicle stopped rear-end crashes for use in pre-crash system design. *SAE International Journal of Passenger Cars-Mechanical Systems*, 4(2011-01-0576) :435–443.

[44] Lakomicki, P., Castanier, B., and Grall, A. (2017). How to assess the reliability in case of a scalable random environment. In *Safety and Reliability - Theory and Applications, the 27th European Safety and Reliability Conference (ESREL)*. CRC Press.

[45] Lakomicki, P., Castanier, B., and Grall, A. (2018). Incremental reliability modeling framework to optimize vehicle's validation tests. In *2018 Annual Reliability and Maintainability Symposium (RAMS)*, pages 1–7. IEEE.

[46] LeBlanc, D. (2006). Road departure crash warning system field operational test : methodology and results. volume 1 : technical report.

[47] Limnios, N. and Oprisan, G. (2012). *Semi-Markov processes and reliability*. Springer Science & Business Media.

[48] Littlewood, B. and Sofer, A. (1987). A bayesian modification to the jelinski-moranda software reliability growth model. *Software engineering journal*, 2(2) :30–41.

[49] Littlewood, B. and Verrall, J. L. (1973). A bayesian reliability growth model for computer software. *Applied statistics*, pages 332–346.

[50] Lv, J., Yin, B.-B., and Cai, K.-Y. (2014). On the asymptotic behavior of adaptive testing strategy for software reliability assessment. *IEEE transactions on Software Engineering*, 40(4) :396–412.

[51] Lyonnet, P., Thomas, M., and Toscano, R. (2012). *Fiabilité, diagnostic et maintenance prédictive des systèmes*. Éd. Tec & doc.

[52] Lyu, M. R. et al. (1996). Handbook of software reliability engineering.

[53] Mahmud, S. S., Ferreira, L., Hoque, M. S., and Tavassoli, A. (2017). Application of proximal surrogate indicators for safety evaluation : a review of recent developments and research needs. *IATSS research*.

[54] Marchau, V., Van der Heijden, R., and Molin, E. (2005). Desirability of advanced driver assistance from road safety perspective : the case of isa. *Safety Science*, 43(1) :11–27.

[55] Metropolis, N. (1989). Monte carlo method. *From Cardinals to Chaos : Reflection on the Life and Legacy of Stanislaw Ulam*, page 125.

[56] Micskei, Z., Szatmári, Z., Oláh, J., and Majzik, I. (2012). A concept for testing robustness and safety of the context-aware behaviour of autonomous systems. In *KES International Symposium on Agent and Multi-Agent Systems : Technologies and Applications*, pages 504–513. Springer.

[57] Moore, R. E. (1979). *Methods and applications of interval analysis*, volume 2. Siam.

[58] Murthy, S. K., Kasif, S., and Salzberg, S. (1994). A system for induction of oblique decision trees. *Journal of artificial intelligence research*, 2 :1–32.

[59] Niederreiter, H. (1992). *Random number generation and quasi-Monte Carlo methods*, volume 63. Siam.

[60] Niewöhner, W., Roth, F., Gwehenberger, J., Gruber, C., Kuehn, M., Sferco, R., Pastor, C.-H., Nagel, U., and Stanzel, M. (2011). Proposal for a test procedure of assistance systems regarding preventive pedestrian protection. In *Enhanced Safety of Vehicles (ESV) Conference, Washington, USA*.

[61] Norme, N. (2001). En 13306 : 2001,«. *Terminologie de la maintenance», Afnor*, 59.

[62] Ohsnman, A. (2016). Toyota's Robot-Car Line In The Sand : 8.8 Billion Test Miles To Ensure Safety. `https://www.forbes.com/sites/alanohnsman/2016/10/03/toyotas-robot-car-line-in-the-sand-8-8-billion-test-miles-to-ensure-safety/#78f41f4416f0`.

[63] Phadke, M. S. (1995). *Quality engineering using robust design*. Prentice Hall PTR.

[64] Pham, H. (2007). *System software reliability*. Springer Science & Business Media.

[65] Philippe Lesire, V. H. and Kröger, R. (2016). Véhicules à conduite déléguée, revue accidentologie. Technical report, LAB, CEESAR, IRTSystemX.

[66] Rau, P. S. (2005). Drowsy driver detection and warning system for commercial vehicle drivers : field operational test design, data analyses, and progress. In *19th International Conference on Enhanced Safety of Vehicles*, pages 6–9. Citeseer.

[67] Rausand, M. and Høyland, A. (2004). *System reliability theory : models, statistical methods, and applications*, volume 396. John Wiley & Sons.

[68] Reynaud, P. (2017). Iliad poc : Drive scenario categorization. Technical report, INRIA, Renault.

[69] Rivero, J. R. V., Tahiraj, I., Schubert, O., Glassl, C., Buschardt, B., Berk, M., and Chen, J. (2017). Characterization and simulation of the effect of road dirt on the performance of a laser scanner. In *Intelligent Transportation Systems (ITSC), 2017 IEEE 20th International Conference on*, pages 1–6. IEEE.

[70] Rocklage, E. (2017). Teaching self-driving cars to dream : A deeply integrated, innovative approach for solving the autonomous vehicle validation problem. In *Intelligent Transportation Systems (ITSC), 2017 IEEE 20th International Conference on*, pages 1–7. IEEE.

[71] Rokach, L. and Maimon, O. Z. (2008). *Data mining with decision trees : theory and applications*, volume 69. World scientific.

[72] Rubinstein, R. Y. and Kroese, D. P. (2016). *Simulation and the Monte Carlo method*, volume 10. John Wiley & Sons.

[73] Sachse, M., Reindl, J., and Krumbiegel, K. (2016a). Sensor tests proving ground (dynamic). Technical report, IAV.

[74] Sachse, M., Reindl, J., and Krumbiegel, K. (2016b). Sensor tests report (dynamic). Technical report, IAV.

[75] Sallak, M., Aguirre, F., and Schon, W. (2013). Incertitudes aléatoires et épistémiques, comment les distinguer et les manipuler dans les études de fiabilité ? In *QUALITA2013*.

[76] Saporta, G. (2006). *Probabilités, analyse des données et statistique*. Editions Technip.

[77] Shafer, G. (1976). *A mathematical theory of evidence*, volume 42. Princeton university press.

[78] Shalev-Shwartz, S., Shammah, S., and Shashua, A. (2017). On a formal model of safe and scalable self-driving cars. *arXiv preprint arXiv :1708.06374*.

[79] St-Aubin, P., Miranda-Moreno, L., and Saunier, N. (2013). An automated surrogate safety analysis at protected highway ramps using cross-sectional and before–after video data. *Transportation Research Part C : Emerging Technologies*, 36 :284–295.

[80] St-Aubin, P., Saunier, N., and Miranda-Moreno, L. F. (2015). Comparison of various time-to-collision prediction and aggregation methods for surrogate safety analysis. In *Transportation Research Board 94th Annual Meeting*, number 15-4629.

[81] Strelioff, C. C., Crutchfield, J. P., and Hübler, A. W. (2007). Inferring markov chains : Bayesian estimation, model comparison, entropy rate, and out-of-class modeling. *Physical Review E*, 76(1) :011106.

[82] Tesla, L. (2016). Toutes les Tesla produites jusqu'à aujourd'hui possèdent maintenant les capacités de conduite autonome. `https://www.tesla.com/fr_FR/blog/all-tesla-cars-being-produced-now-have-full-self-driving-hardware?redirect=no`.

[83] Tourbier, Y. (2017). Autonomous vehicle main validation algorithm. Technical report, Renault.

[84] Ulbrich, S., Menzel, T., Reschka, A., Schuldt, F., and Maurer, M. (2015). Defining and substantiating the terms scene, situation, and scenario for automated driving. In *Intelligent Transportation Systems (ITSC), 2015 IEEE 18th International Conference on*, pages 982–988. IEEE.

[85] Uschold, M., Provine, R., Smith, S., Schlenoff, C., and Balikirsky, S. (2003). Ontologies for world modeling in autonomous vehicles. In *18Th International Joint Conference on Artificial Intelligence, IJCAI*, volume 3.

[86] Walley, P. (1991). Statistical reasoning with imprecise probabilities.

[87] Yin, L. and Trivedi, K. S. (1999). Confidence interval estimation of nhpp-based software reliability models. In *Software Reliability Engineering, 1999. Proceedings. 10th International Symposium on*, pages 6–11. IEEE.

[88] Zadeh, L. A. (1999). Fuzzy sets as a basis for a theory of possibility. *Fuzzy sets and systems*, 100 :9–34.

[89] Zamansky, A. and Farchi, E. (2015). Helping the tester get it right : Towards supporting agile combinatorial test design. In *International Conference on Software Engineering and Formal Methods*, pages 35–42. Springer.

[90] Zhao, D., Lam, H., Peng, H., Bao, S., LeBlanc, D. J., Nobukawa, K., and Pan, C. S. (2017). Accelerated evaluation of automated vehicles safety in lane-change scenarios based on importance sampling techniques. *IEEE transactions on intelligent transportation systems*, 18(3) :595–607.

Annexe A

Essais sur piste pour construire des modèles d'erreur capteur

Pour le cas d'usage "suivi de véhicule", les essais sur pistes réalisés sont les suivants [73] :

— Essais n°1 : le véhicule autonome suit le véhicule de devant à la même vitesse à la distance de sécurité (Figure A.1). Ce test a été réalisé suivant trois vitesses $30km/h$, $50km/h$, $80km/h$.

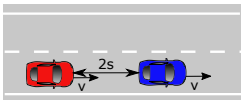


FIGURE A.1 – Essais n°1

— Essais n°2 : le véhicule autonome suit le véhicule de devant à la même vitesse à la distance de sécurité puis le véhicule décélère à $-2m \cdot^{-} 2$ (Figure A.2). Ce test a été réalisé suivant trois vitesses $30km/h$, $50km/h$, $80km/h$.

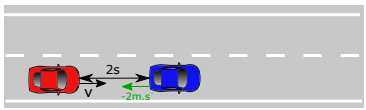


FIGURE A.2 – Essais n°2

— Essais n°3 : le véhicule autonome (ego) suit le véhicule de devant à la même vitesse à la distance de sécurité. Le véhicule de devant louvoie dans sa voie (Figure A.2). Ce test a été réalisé suivant trois vitesses $30km/h$, $50km/h$, $80km/h$.

Les résultats des essais sont fournis par IAV dans le document interne [74].

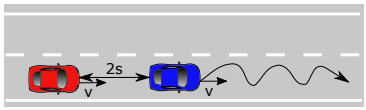


FIGURE A.3 – Essais n°3