“ Validations par Virtualisation et Simulation : de nouveaux champs méthodologiques et techniques pour une ingénierie de conception sûre des systèmes autonomes ”

Linda Zhao, Emmanuel Arbaretier, Mohamed Tlig

« Validations par Virtualisation et Simulation : de nouveaux champs méthodologiques et techniques pour une ingénierie de conception sûre des systèmes autonomes »

« Virtualization and Simulation Validations : New Methodological and Technical Fields for Safe Design Engineering of Autonomous Systems »

Linda Zhao
SECTOR
12 avenue du Québec
91140 Villebon sur Yvette
linda.zhao@sector-group.net

Emmanuel Arbaretier
APSYS
1 boulevard Jean Moulin
78996 Élancourt Cedex
emmanuel.arbaretier@apsys.eads.net

Mohamed Tlig[1]
IRT SystemX – Pôle transport autonome
Paris-Saclay
mohamed.tlig@irt-systemx.fr

Résumé

Dans le cadre d'un retour d'expérience concernant le processus de développement des fonctions de véhicules autonomes, cet article se propose d'identifier des éléments de réponse méthodologiques face aux bouleversements scientifiques présentés par les cycles de validation des systèmes autonomes et s'inscrivant dans un environnement « ouvert » et « changeant », que ce soit au niveau du référentiel d'ingénierie système applicable, à la définition des métriques ou performances de sécurité susceptibles de leur être appliquées, ou encore au type de couverture assurantielle qu'il est possible de produire au cours de leur processus de développement.
Dans ce travail, nous exposons une réflexion sur un référentiel d'outils et méthodes liés au domaine de la « validation par virtualisation et simulation » susceptible d'apporter une solution pluridisciplinaire à la problématique d'ingénierie de conception sûre des systèmes autonomes.

Mots clés

Système autonome, Sécurité, Fonctionnel sûr, SOTIF, Simulation, Validation, Ingénierie Système, MBSE, MBSA, Model checking

Summary

In the context of a methodological cooperation achieved through an IRT Research project, which concerned design, safety assessment and validation of autonomous vehicles, some scientific and technical material has been produced and collected about how to provide some assurance about autonomous systems and how it has to change the way we conceptualize knowledge about such systems and we produce evidence about how they will behave and how far they will be exposed to critical situations able to cause human damages. We try to describe the corner stones of an incremental engineering framework, which has already begun in new technology application development, and where close interaction between operational deployment field analysis and front-end design optimization process is fostered, at the same time whilst multiple simulation technics are pushed forward to substitute with real experimentation of the system.

Index Terms

Autonomous systems, Safety, Functional safe, SOTIF, Simulation, Validation, System Engineering, MBSE, MBSA, Model checking

Contexte

Le développement accéléré des innovations technologiques, notamment en ce qui concerne la généralisation digitale, remet en question les référentiels existants des méthodes, techniques et normes associées, communément admises dans le domaine de la maîtrise des risques ; à la lumière de plusieurs années consacrées au développement des véhicules autonomes, ce papier fait le point sur la nature des remises en question des concepts et approches mises en œuvre jusqu'à présent dans les divers domaines tels que aéronautique, ferroviaire, automobile et énergie, et tente de dessiner le contour d'un nouveau référentiel d'ingénierie système intégrant plus spécifiquement les caractéristiques de ces innovations technologiques qui imposent un certain nombre de ruptures avec les savoirs, savoir-faire et pratiques déployés dans la plupart des domaines industriels.

Les spécificités des systèmes autonomes

Dans une première partie nous identifions de nombreuses différences de contexte méthodologique et enjeux scientifiques présentés par les innovations technologiques, en particulier celles présentées par les systèmes autonomes, en les illustrant par des exemples concrets :

- Non finitude du nombre d'exigences fonctionnelles et opérationnelles : comme l'univers des cas d'usage est

[1] *Les travaux sont réalisés dans le cadre du projet SVA piloté par l'IRT-SystemX et donc financés dans le cadre du programme "Investissements d'avenir". Les partenaires industriels sont : Apsys, Sector, Valeo, Continental, Renault, PSA, AV Simulation, Assystem, All4Tec, Optis. Les partenaires académiques sont : CEA, ENS-CACHAN/LSV, Université Paris-Saclay, LNE.*

infini, les performances fonctionnelles et opérationnelles peuvent présenter une variabilité infinie correspondant à un « continuum » de contextes environnementaux et opérationnels aux multiples variantes et configurations possibles ;

- Non stationnarité des profils de performance, voire instabilité récurrente des régimes d'utilisation : les exigences opérationnelles s'inscrivent pour la plupart dans de multiples contextes de bouclages enchevêtrés avec la dynamique de l'environnement en changement quasi permanent et conduisant à des trajectoires d'évolutions plutôt « mouvementées », auxquelles s'ajoutent les interactions de nombreux acteurs, voire entités/éléments au sens large (véhicules, acteurs, objectés connectés, …) ;
- Non linéarité de la dynamique temporelle : les cas d'usages « critiques » pour lesquels des enjeux de « sécurité » doivent ou devraient être clairement adressés, sont associés pour la plupart à des échelles extrêmement étroites (quelques minutes, voire quelques secondes) dans lesquelles des événements concomitants peuvent cascader et superposer de nombreux effets imprévisibles sur l'ensemble des phénomènes, qui sont eux-mêmes difficiles à décrire précisément ;
- Non systématisme éventuel, voire instabilité, des scénarios de comportement du système (au sens strict autour du véhicule autonome analysé ou large en incluant une population de véhicules interagissant avec le véhicule autonome - ego) dans certains cas d'usage : il s'agit des nombreux types d'incertitudes présentées par les moyens de détection de l'environnement et de l'interprétation du contexte opérationnel en temps réel, ainsi que celles présentées par les logiques de décision et d'arbitrage des systèmes autonomes.

En fait, la complexité d'analyse des systèmes autonomes est liée notamment au constat suivant : la production d'une situation dangereuse pour le système autonome, dans le cadre d'un scénario qui est toujours fortement dynamique, peut procéder de la combinaison, l'intrication ou la concomitance de multiples facteurs. Ces facteurs sont traditionnellement analysés séparément :

- Sortie du périmètre d'applicabilité des performances fonctionnelles acceptables,
- Intrusion d'un phénomène optique (par ex éblouissement) ou CEM (en particulier vis-à-vis des systèmes électriques et de communication),
- Difficultés techniques de mise en œuvre de fonctions de sécurité (par ex le freinage) en raison de l'apparition de conditions environnementales ou opérationnelles défavorables, ou de contraintes supplémentaires rendant l'arbitrage difficile ;
- Mise en échec de capacité de réaction à une situation dangereuse, notamment en raison d'une exposition à une vulnérabilité de type cyber sécurité, que ce soit au niveau de l'intégrité de l'information utile, ou à un niveau de son transport et de son traitement.

L'ensemble de ces facteurs peut avoir comme résultante la mise en échec de la performance du système.

On ne peut plus donc superposer ou empiler les aspects traités selon une démarche « cartésienne ». La prise en compte de l'enjeu de sécurité nécessite une nouvelle discipline bien au-delà de la Sûreté de Fonctionnement (science des défaillances), Au sens restrictif, on peut parler de la maîtrise des risques (science du danger au sens large), qui consiste :

- En l'identification des situations insidieuses ou dangereuses de quelque nature que ce soit, dues par exemple à l'apparition des défaillances et/ou des perturbations (passage d'animaux sur route),
- En la vérification de l'acceptabilité des performances de type « fonctionnel sûr » en présence de ces situations.

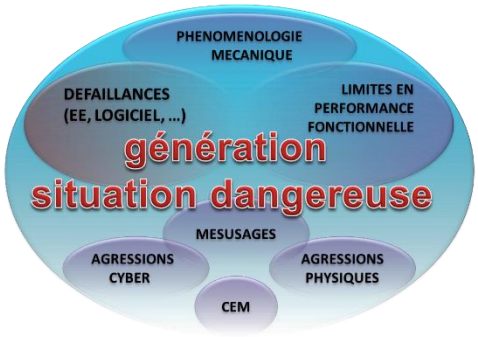

Figure 1. Cartographies des sources d'influence

En particulier, il apparaît que pour de nombreux systèmes autonomes, la séparation classique des notions de « Safety » et de « Security » s'avère de plus en plus artificielle, due à la généralisation des technologies de l'information, voire « contre-productive », et qu'il serait urgent d'intégrer la « Security » à la « Safety » pour une approche vraiment globale de la maîtrise des risques : l'apparition de directives « Cyber Security » souligne clairement la nécessité d'intégrer explicitement cette composante dans les enjeux de « Sécurité innocuité » ou « Safety ».

Par ailleurs, la notion de mésusage doit être reconsidérée à la lumière des systèmes autonomes : dans la mesure où un système autonome est sensé maîtriser complètement l'analyse d'une situation pour juger de sa capacité à y développer un comportement pertinent, ou à y renoncer en se repliant sur une reconfiguration de secours, cette notion apparaît obsolète car l'usager est clairement « sorti » de cette boucle de jugement et de décision ! Le besoin de prendre en compte ces contraintes opérationnelles de pleine connaissance du périmètre d'utilisation possible du système est encore une fois déportée sur le système.

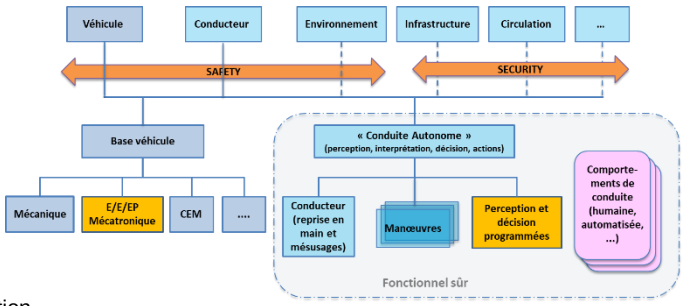

Figure 2. Champs d'investigation pour les conduites autonomes

Enfin, la difficulté principale consiste à définir un référentiel de comportement « souhaité » de la conduite autonome, ou encore « acceptable » : comment en effet décrire les frontières entre un espace critique de « conditions limites », anticiper les modalités de « passages » entre les situations « normales » et « critiques », voire dangereuses ? Ces marges successives de comportement ne sont plus évidentes à définir comme dans nos démarches habituelles qui se ramenaient souvent à des approches binaires ou discrètes, « ultra » confortables : comment en outre prendre en compte les mécanismes de déclenchement par les dysfonctionnements (défaillances), les phénomènes perturbants ou les règles utilisées pour la prise de décision à travers ces différentes zones de franchissement vers ces espaces critiques ?

En fait, l'idéal serait de pouvoir générer l'espace des phases du système global constitué par l'ego et les autres constituants

mobiles de la scène, au sens de la mécanique hamiltonienne, (utilisée en mécanique quantique) et à chaque instant de pouvoir identifier les zones d'évolution critiques intermédiaires et les zones catastrophiques d'accès absolument interdit, assimilables à la production d'accidents. En définissant une topologie sur cet espace, on se rendrait compte que ces zones varient en fonction du temps, et peuvent présenter des propriétés de non linéarité, non connexité et même discontinuité !

La démarche actuelle en automobile

Le référentiel actuel ISO 26262 et son évolution récente utilisés dans le domaine automobile illustrent la démarche applicable dans le processus de développement.

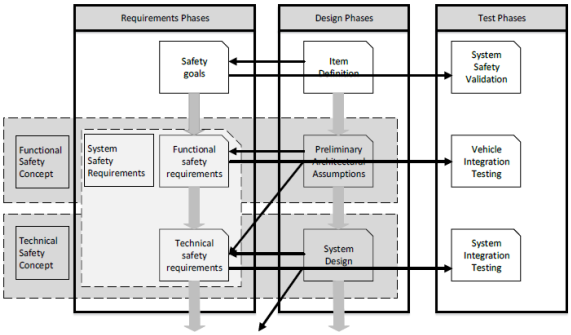

Figure 3. Processus de développement en automobile

Dans ce référentiel, il s'agit classiquement de traduire des « Safety Goal » en « Functional et System Safety Requirements », puis en « Technical Safety Requirements », en mettant en évidence des « Functional Safety Concept », mais aussi éventuellement des « Technical Safety Concept ».

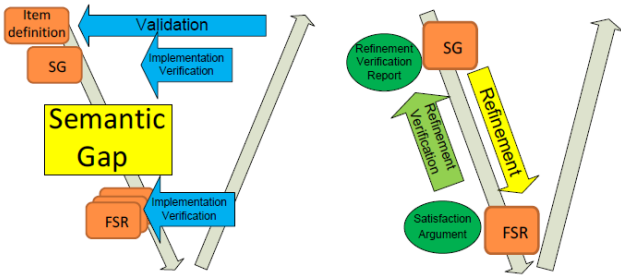

Figure 4. Bouleversement de la démarche lié au changement sémantique

Dans la démarche de raffinement permettant de passer des Safety Goal aux Functional Safety Concept, on observe ce que Rolf Johansson appelle un « gap sémantique » (Réf. [4]). En effet, ce qui est significatif ou pertinent pour un système autonome, ce n'est pas le fait de pouvoir satisfaire à une liste de « Functional Safety Requirement » mis à plat de manière statique dans une liste énumérative ; c'est une aptitude à adopter un comportement pertinent dans des scénarios dynamiques, en interaction avec de nombreux autres acteurs, ce qui ouvre la voie à un champ beaucoup plus vaste de possibles, où l'exigence sécuritaire devra se décliner suivant des modalités aux degrés de liberté beaucoup plus nombreux…

Une réflexion en cours est mise en œuvre par un ensemble de constructeurs en introduisant la notion de SOTIF (Safety of the Intended Functionality). Il s'agit d'un complément indispensable à l'ISO 26262 pour la conception des fonctions ADAS et véhicules autonomes.

À travers les constats identifiés dans le paragraphe précédent, apparait la prévalence des enjeux de « Fonctionnel Sûr » par rapport aux dimensions de Sûreté de Fonctionnement en ce qui concerne l'aspect « Sécurité » :

- L'enjeu n'est pas tant de se protéger contre l'irruption de modes de défaillance, que de réagir avec pertinence à des sollicitations du contexte environnemental et opérationnel.

Un ensemble de phénomènes sont à détecter, à interpréter, à comprendre et doivent conditionner une prise de décision cohérente avec la situation contextuelle. Nous citons à titre d'exemple :

- La capacité d'interprétation des phénomènes physico-chimiques dépend étroitement des solutions technologiques et des moyens de traitement dont les performances sont en constante progression ;
- La prise en compte des interactions avec d'autres systèmes mobiles (véhicules, vélos, camions, …) et de multiples objets fixes ou mobiles accentue la richesse des facteurs, qui nécessitent d'aller au-delà du périmètre d'applicabilité initialement envisagé.

De ce fait, on se confronte aux limites fonctionnelles avec les performances associées.

La prise de décision « avec pertinence » constitue aussi un véritable champ de réflexion en soi :

- Chercher une représentation avec un certain de niveau de précision ;
- Comment prendre en compte des règles de bonnes pratiques, des limites sécuritaires (par exemple MRM - Minimum Risques Manœuvre) et de viabilité de situation de confort acceptable ;
- En matière d'évaluation, suffit-il de ne pas produire de situation « dangereuse » ou doit-on en plus, pour chaque scénario, se conformer à des courbes ou surfaces de références (position, vitesse, accélération) définies pour chaque cas d'usage ?

Les besoins industriels

Compte tenu de la complexité à laquelle sont confrontés les systèmes autonomes, le premier besoin de plus haut niveau, exprimé sous une forme générale, est celui de ce que l'on pourrait appeler l'« Assurance Performancielle » vis-à-vis :

- De la population des usagers : tout d'abord la « Safety » (appelée aussi sécurité innocuité), la continuité de service (disponibilité/fiabilité), le confort, voire la Cybersécurité, … ;
- De la société : l'acceptabilité, la couverture juridique des usages, la compatibilité environnementale ;
- Des enjeux RSE de plus haut niveau : « sustainability », … ;
- Des infrastructures, plus particulièrement dans le domaine du transport routier ; il s'agit de la sécurité routière ;
- Du processus de fiabilisation du système autonome lui-même.

Les différents positionnements méthodologiques illustrés par les référentiels d'Ingénierie Système existants, ainsi que le type de légitimité développé autour des couvertures assurancielles peuvent toutefois se ramener aux fondamentaux suivants :

- Apport d'« aide à la conception » visant à interagir directement avec les bureaux d'étude et concepteurs pour les aider à identifier des choix d'architectures robustes et efficients : les différentes activités et processus de tâches associés doivent alors s'inscrire dans le cadre de l'Ingénierie Système ;
- Production de différents systèmes d'« Assurance Sécurité » évoluant à travers des modalités très diverses depuis le simple « Argumentaire de Sécurité »

jusqu'à de véritables « Démonstration de Sécurité » en lien avec un référentiel communément accepté ;

- Mise en relation des exigences avec des Plans de Validation et Démonstration Opérationnelle impliquant des métriques de couverture des exigences listées dans un référentiel, ainsi qu'une faisabilité et une validation possible des campagnes d'essais pratiques mis en œuvre.

Le point d'entrée par rapport à ces différents enjeux demeure la connaissance des contextes opérationnels où le système autonome est déployé : il s'agit de la notion de « cas d'usage » ou plus concrètement de scénarios incluant une définition complète de l'environnement au sens large, et qui constitue le sujet de préoccupation principal des constructeurs de véhicule autonome.

Par ailleurs, la caractéristique fondamentale du comportement des systèmes autonomes est la notion d'incertitude multi factorielle intervenant à différents niveaux :

- Incertitude épistémique de prise en compte des différents éléments de connaissance décrivant l'environnement ;
- Incertitudes de mesures liées à la détection des différents capteurs ;
- Incertitudes d'interprétation générées par les algorithmes de fusion des capteurs et associant des niveaux de confiance aux différents objets ;
- Incertitudes de décision issues des différents arbitrages éventuellement contradictoires parmi lesquels le système doit trancher, pour des scénarios « sensibles » ;
- Incertitudes liées à la dynamique d'évolution du système et de l'environnement et à la difficulté de rendre compatibles entre elles les différentes modalités de représentation de la synchronicité ou de l'asynchronicité et de l'échantillonnage du temps.

En tout état de cause, et malgré ces deux contraintes ou verrous (infinité de l'univers des cas d'usage et omni présence des incertitudes, Réf [3]), comme pour tout système technologique, la démarche de validation par roulage ne suffit plus. Pour autant, l'ingénierie système doit inventer une nouvelle méthodologie ayant recours à des *plateformes numériques* pour orchestrer l'ensemble des différents processus d'activités afin de construire un référentiel de « validation » applicable au système autonome.

Problématique préalable à la validation

Comme rappelé précédemment la notion de « cas d'usage » est centrale pour le processus de représentation et puis de validation.

Elle s'inscrit dans le cadre de la problématique classique de description ou représentation du « Réel » observable. Celle-ci ne peut échapper à ce que Kant désigne par « consensus intersubjectif ». Selon Kant l'objectivité scientifique est constituée de consensus intersubjectifs concernant des apparences phénoménales qui au départ sont foncièrement subjectives, mais qui sont par la suite « légalisées », notamment selon des méthodes scientifiques (Réf [5]).

Tous les outils et techniques déployés dans les démarches de description, formalisation, modélisation ou simulation des cas d'usages et scénarios répondent à cette contrainte : il n'y a jamais équivalence possible avec la représentation et le référent appartenant à la réalité, et toute représentation est nécessairement *« orientée »* à travers le choix sélectif de caractéristiques ou traits jugés pertinents par rapport à l'usage scientifique, ou disons plus communément « calculatoire » auquel on désire soumettre ces représentations ou modèles.

Par ailleurs, l'omniprésence de la notion d'incertitude citée au paragraphe précédent est également une difficulté spécifique supplémentaire à l'utilisation pertinente de ces modèles ou représentations.

A travers ces constats, le développement des activités d'ingénierie pour les systèmes autonomes s'oblige à adopter un référentiel de *processus progressif et itératif*, ceci également pour les raisons suivantes :

- L'univers des cas d'usage est infini ;
- Les systèmes autonomes intègrent souvent des briques d'Intelligence Artificielle, dont la mise au point obéit à des cycles d'expérimentation et de validation incrémentales ;
- Comme, par rapport à la complexité opérationnelle, le couplage avec le Retour d'Expérience est central, on n'échappe pas à un processus itératif entre l'exploitation de cas d'utilisation réels enregistrés et documentés par de nombreuses informations encadrées dans le cadre d'une démarche « Big Data », et la simulation virtuelle de cas d'usages complémentaires ou dérivés permettant de s'affranchir du coût de mise en œuvre réelle de ces cas pour les tests de vérification/validation.

On aboutit à un processus d'Ingénierie Système plus proche de méthodes agiles, dites « scrum » ou encore « Minimum Value Product » pour lesquelles les phases de déploiement opérationnel contribuent à l'amélioration continue de la performance du système, voire à la spécification de nouvelles fonctionnalités.

Dans la mise en œuvre d'approches par simulation virtuelle, et plus précisément dans la production des modèles, il faut être conscient des enjeux pluridisciplinaires et multi-physiques à traiter : mécanismes de fonctionnement, de dysfonctionnement, aspects cyber sécurité, spécification des cas d'usages « aux limites ». D'autre part, il est important d'introduire un point de vue du type « Facteurs Humains », notamment pour traiter les capacités de reprise de conduite et des mésusages ; ceci est important pour la simulation des décisions prises par un système autonome, de manière à pouvoir la comparer au comportement d'un automobiliste.

L'exploitation des modèles quant à elles peut s'examiner à la lumière des référentiels suivants :

- Référentiel absolu : simulation des cas d'usage, et évaluation d'un taux d'accidents,
- Application du principe GAME (Globalement Au Moins Équivalent) appliqué au monde habituel (transports, accidents domestiques, modèles accidentels, …),
- Référentiel lié à la notion de « fiabilisation de système global » associant les deux notions de sécurité routière et sécurité de roulage individuelle dans une approche même croisée,
- L'ISO 26262 pour la sécurité des fonctions de roulage impliquant des systèmes mécatroniques,
- La « norme » SOTIF pour l'enjeu plus global de sécurité de roulage, qui traite plus largement du « fonctionnel sûr », c'est-à-dire du contrôle du périmètre opérationnel de la performance fonctionnelle.

Pour rappel, dans le référentiel aéronautique, les approches « MBSE » (Model Based System Engineering) et « MBSA » (Model Based Safety Assessment) s'intéressent à comprendre et à quantifier en gravité et en probabilité une liste de situations critiques ou catastrophiques, pour, le cas échéant, être à même d'allouer des objectifs de probabilités ou de niveau DAL (Design Assurance Level) aux différents contributeurs respectivement physiques et logiciels ; l'avantage de ce domaine, c'est que cette liste de situations est en quelque sorte « déposée au pavillon des poids et mesures » (normes ARP 4754 et 4761) et qu'elles sont définies de manière stationnaire et en relation avec des configurations de pannes qui sont également clairement explicitées. Plus généralement, cette « hypothèse de base » constitue le postulat pour l'application de la Sûreté de Fonctionnement et dans tous les domaines industriels.

Dans le cas des systèmes autonomes, ce référentiel stable et absolu des situations redoutées n'existe pas : les contextes opérationnels sont extrêmement divers et fortement dynamiques, et il est difficile de concevoir des critères et règles de dépassement de limites pour la sécurité : comment caractériser, qu'en accédant à une zone de transition critique, le système évolue dans une zone de mise en danger, et ce, à travers des critères universels ? La notion de « golden case » doit permettre à termes de recenser et conceptualiser des contextes opérationnels limites et emblématiques constituant une jauge d'évaluation des performances de sécurité d'une architecture de système autonome.

C'est tout l'objet des champs de réflexion actuels concernant les cas d'usage que de savoir comment on sera à même d'exhiber différentes familles de scénarios ou cas d'usage emblématiques du point de vue de la sécurité qui suffiront à servir de « benchmarks » d'évaluations pour les architectures.

Validation par Simulation : techniques et apports

Face à ces multiples remises en question, émergent des perspectives prometteuses de « Validation par Simulation », que nous allons développer dans ce paragraphe, et étendre à la notion de « Validation par Virtualisation » qui semblent a priori présenter de multiples avantages, d'autant plus qu'elles peuvent encore se décliner à travers de nombreuses variantes dont nous allons qualifier les apports respectifs :

- S'affranchir des coûts prohibitifs des campagnes d'essais opérationnels, devant être de plus liées à une infinité de cas d'usages ;
- Traiter le verrou de l'« univers infini des cas d'usages » à travers des possibilités techniques de parallélisation, « réduction », analyses de sensibilité ;
- Utiliser la puissance et la richesse de cadres de conceptualisation mathématique de la réalité (chaînes de Markov, topologies algébriques, …) afin de les soumettre à des traitements ou des questionnements à forte valeur ajoutée ;
- « Reprendre la main » sur la problématique de l'univers infini des cas d'usage en y associant la notion d'exploration sélective et représentative, avec des critères scientifiques de pertinence d'échantillonnage, utilisant ce qu'on pourrait appeler « les outils mathématiques de représentation et de traitement de l'infini » (espaces de phase hamiltoniens, cartographies ou champs probabilistes de ces espaces d'états, …).

Ces approches de description formalisée et de traitement informatique des scénarios de simulation peuvent ainsi servir de support à un référentiel de validation basé sur des processus itératifs de virtualisation et modélisation visant à la fois :

- à explorer des univers infinis de cas d'usage modélisés dynamiquement, qualifiés et structurés ;
- à les mettre en relation avec des scénarios de simulation du comportement du système analysé dont les différentes couches peuvent apparaître dans les traitements de manière réelle (simulation hybride) ou abstraite privilégiant des points de vue complémentaires (multi-physique, fonctionnel, événementiel,…) ou transverses.

1. Postulat de l'univers infini des cas d'usage : non dépendant de la démarche de simulation

D'emblée, des travaux d'ontologie se sont imposés pour décrire, structurer et cartographier cet univers de cas d'usage (Réf [6] et [7]) : les langages Open Scenario et Open Drive proposent dans la communauté automobile européenne une structure pour accueillir ces ontologies.

Cependant, tout type de formalisation et de classification traduit une vision particulière de structuration et exploitation de différentes familles de cas d'usage.

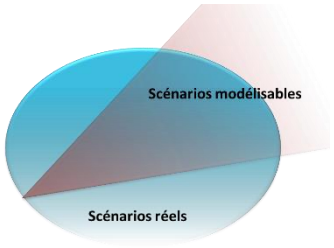

Figure 5. Regard orienté implicite/explicite

Dans cette schématisation des zones de couvertures respectives de l'univers des scénarios envisageables et celui des scénarios modélisables, on constate :

- Que certains scénarios réels ne pourront correspondre à aucun scénario modélisable ;
- Que certains scénarios modélisables ne correspondront jamais à aucun scénario réel.

Il est donc apparu très tôt la nécessité de coupler les essais réels (plans d'expérience, campagnes de roulage…) avec les modèles de scénarios issus de ces ontologies.

Ces ontologies mettent en évidence des facteurs critiques ou paramètres de haut niveau qui structurent les différents scénarios : infrastructure, obstacles fixes, mobiles, conditions météorologiques, conditions atmosphériques, circulation, événement (considéré comme une perturbation à laquelle le système est appelé à réagir), action (décrit un comportement élémentaire du système en réponse à l'événement) …

2. Représentations

Les modèles de scénarios reposent sur des consensus de règles de conceptualisation communément acceptées et partagées : cela constitue la base de constitution des connaissances humaines ; et c'est peut-être la seule manière qu'une perception du réel puisse se traduire en élément de connaissance conceptualisée et donc objectivables entre plusieurs observateurs.

Cependant, tout système de représentation conceptualisé (conventions, langages semi formels ou formels) constitue un goulet d'étranglement des champs possibles de perception de la réalité, et cela fonctionne comme un entonnoir, ou une succession de filtres simplificateurs.

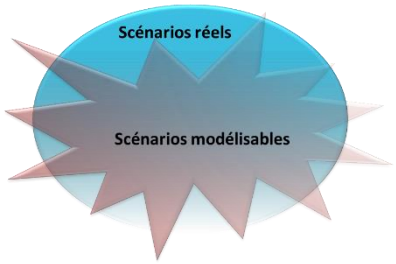

Figure 6. Pouvoir de représentation mathématique

Le schéma ci-dessus est une tentative d'évoquer les notions de variabilité et structuration discrète (étoile accidentée en rouge) induite par les langages et formalismes qui retranscrivent une logique de perception humaine mais brisent artificiellement un continuum environnemental non discriminé à l'origine. Se posent alors les deux questions suivantes :

- Comment éliminer les scénarios fictifs ?
- Comment réintégrer les scénarios réels non couverts par la structuration ?

Une part d'incertain présente de manière diffuse dans cette démarche de modélisation est donc également représentée par la difficile maîtrise de couverture entre la réalité à représenter et les représentations générées.

On subit donc une superposition de biais générés par une difficile correspondance entre la réalité des scénarios visés, les représentations conceptualisées de ces scénarios, puis les modèles de différentes natures (environnement routier, manœuvres de véhicule, multi-physique…) qui vont constituer la plateforme de virtualisation finale.

Se combine à cette incertitude fondatrice de non correspondance exacte entre les échantillons de réalité et les conceptualisations un enjeu de complétude et exhaustivité qu'on doit traiter.

Cet enjeu de complexité combinatoire, dont l'ampleur est difficile à maîtriser, a conduit à progresser de manière incrémentale à travers des périmètres de restriction de scénarios successifs et donc les fonctions et les périmètres associés dans le développement.

Pour gérer ces différents niveaux d'incertitudes concernant l'exploration du champ des scénarios réels, on s'est intéressé à « calibrer » différentes sources de « retour d'expérience » ainsi que les jeux de données associés, pour concevoir et valider, voire tester les performances du système, dans un cadre de boucle itérative permanent :

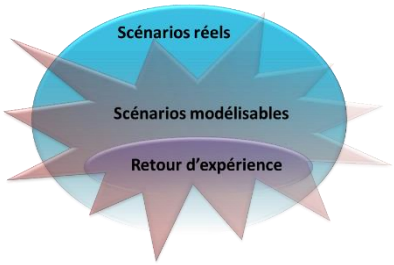

Figure 7. Apport du retour d'expérience

Dans les domaines industriels traditionnels, le retour d'expérience injectait de l'Analyse Dysfonctionnelle au niveau des modèles, à travers la connaissance de nouveaux modes de défaillance ou de nouveaux mécanismes de propagation de ces défaillances et de productions d'effets finaux : maintenant c'est l'accidentologie, et sans doute également l'incidentologie qui contribuent à initialiser certains cas dysfonctionnels et à enrichir voire compléter la connaissance issue de l'expertise « ingénierie ».

Par ailleurs, les roulages enrichissent la validation des performances et permettent de compléter la description de scénarios particuliers.

D'autres sources théoriques de génération de cas d'usages peuvent être envisagées, grâce à l'utilisation d'outils théoriques associés aux formalismes de représentation.

La Réf [8] utilise les différents degrés de liberté d'un scénario en considérant successivement les contraintes géométriques des trajectoires, les critères dynamiques d'évolution de ces trajectoires, et enfin les possibilités d'interaction des composantes de l'environnement (autres usagers de la route pour un véhicule autonome) pour générer les différentes classes de scénarios à simuler.

La Réf [9] montre comment un système de tableaux du type « Analyses Préliminaires de Risques » permet, à partir du parcours de cas d'usages emblématiques (Tracking, Cut In, Zip In) de faire varier certains facteurs critiques pour faire émerger des situations dangereuses susceptibles de provoquer un accident.

La Réf [10] illustre avec l'utilisation des réseaux de Pétri comment on peut explorer de nombreuses variantes de cas d'usages pour soumettre un applicatif de décision de système autonome à une validation de type « Model Checking ».

La Réf [11] quant à elle, grâce à des chaînes de Markov, déroule la combinatoire des critères caractéristiques des cas d'usage pour obtenir des variantes ou configurations pertinentes, en prenant en compte les contraintes de cohérence.

Tous ces moyens de génération théorique augmentent en volume le périmètre des cas simulés et étend le champ exploratoire des scénarios à simuler.

En tout état de cause, la capitalisation et le partage des cas de référence constructeurs / métiers permet d'une part d'augmenter l'espace des scénarios couverts dans l'univers des cas d'usage, et d'autre part de confirmer l'applicabilité des scénarios modélisés générés de manière théorique.

Cette validation croisée associée à un enrichissement permanent des scénarios et cas d'usage contribue à l'augmentation de la zone de couverture sur les cas réels susceptibles d'être rencontrés ou avérés, ainsi que de la pertinence des modèles et évolution des critères.

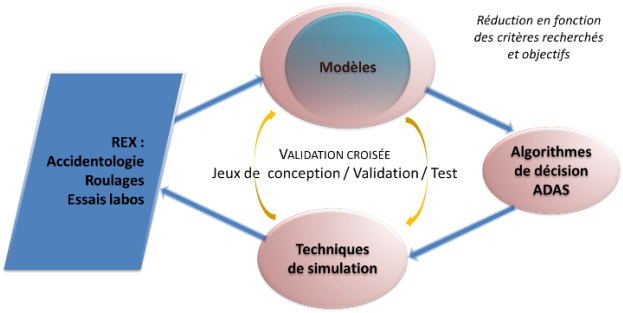

Figure 8. Méta-heuristique de validation

3. Types de modèles et phénoménologie associée

Nous allons voir que, de manière connexe aux enjeux de validation, la question incontournable des progiciels et des différents outils de modélisation, simulation, évaluation susceptibles d'accompagner ce processus de validation ouvre la porte à de multiples défis de mise en œuvre technique et scientifique, mais également de couplage et d'interopérabilité pour utiliser de manière harmonieuse des « contenus virtualisés » issus de langages différents, exprimés à travers des formats multiples et obéissant souvent à des hypothèses de modélisations hétérogènes.

De nombreuses briques logicielles sont envisagées pour contribuer à la simulation des scénarios :

- Simulation du trafic routier et de la distribution physique de l'infrastructure (par exemple SCANeR, Prescan ou Carmaker…),
- Simulation des capteurs (par exemple Matlab ou Simulink),
- Simulation des fonctions ADAS (Matlab ou Simulink),
- Simulations de type comportemental, événementiel, fonctionnel et dysfonctionnel (par exemple avec le langage Altarica),
- …

Si la plateforme ne contient que des logiciels de simulation et des modèles des différents systèmes en présence, on parlera de simulation de type « MIL » (« Model In the Loop »).

Si l'on introduit dans la plateforme les vrais logiciels de fusion de données et de décision, on parlera de simulation de type « SIL » (« Software In the Loop »), ce qui présente l'avantage de disposer d'un environnement de test qui émule les vraies briques à tester.

Enfin, si l'on introduit les vrais capteurs physiques sur la plateforme, il s'agira de simulations de type (« HIL » ou

« Hardware In the Loop »), avec la possibilité d'utiliser un environnement de synchronisation (comme RTMaps) pour pouvoir rendre compte de la temporisation des flux de données au plus juste : les simulations paraissent alors plus réalistes mais sont plus coûteuses.

Les modèles comportementaux quant à eux (Réf [12]), fournissent une autre heuristique de mise en évidence de cas de tests réels pertinents : grâce à des contenus de modélisation comportementale synthétisés et orientés, des traitements de type « model checking » permettent d'explorer des classes de cas d'usages jugés « a priori » critiques ; ces classes sont alors susceptibles d'être validées par instanciation sur une plateforme de simulation, où l'on analyse leur criticité théorique avant de pouvoir la tester et la mettre en évidence sur des cas de test réels, sur lesquels le concepteur pourra travailler en « vraie grandeur ».

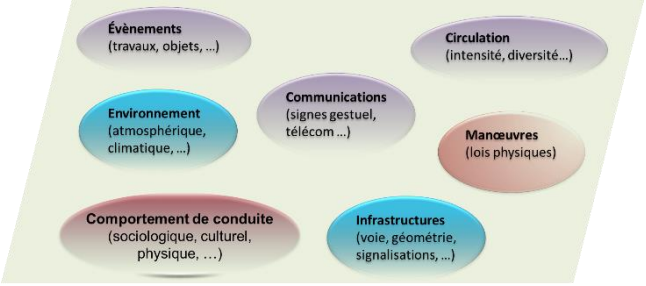

Figure 9. Complexité des interactions à prendre en compte

Néanmoins, la mise en œuvre de ces simulations dynamiques et interactives, impliquant des modèles de comportement de multiples acteurs représente de vrais défis, notamment des points de vue suivants :

- Échantillonnage des temporisations des différents flux de données, traitements d'information et phénomènes physiques ;
- Propagation, réflexion et perturbation électromagnétiques ;
- Fonctions de transfert des capteurs (si la simulation n'est pas « HIL ») ;
- Informations optiques et électromagnétiques en entrée des capteurs prenant en compte les conditions météorologiques et atmosphériques de l'environnement ;
- Dynamique d'évolution de toutes les composantes du scénario et gestion de la cohérence ;
- Facteur humain (comportement de conduite, capacité d'appréhension de danger immédiat ou à venir, capacité d'autoadaptation, …), stratégies de décision des acteurs ;
- Lois mécaniques de comportement des véhicules ;
- Propagation des incertitudes.

C'est pourquoi les enjeux suivants seront déterminants pour faire progresser la pertinence et « l'exploitabilité » des modèles :

- Simulation multi-physique de l'environnement : la lumière (optique : diffusion, diffraction, réfraction…), les champs électromagnétiques (interactions CEM) ;
- Compatibilité des points de vue, niveaux d'abstraction, pouvoirs d'expression supportables par les langages et dispositifs de conceptualisation mis en œuvre ; il est important de pouvoir maîtriser le juste niveau de détail nécessaire pour ne pas se noyer dans une inflation d'informations et de contenus mathématiques complexes ;
- Incertitudes multiples du comportement du système et de l'aptitude d'un contenu modélisé à en rendre compte : incertitudes possibles liées à la détection et l'interprétation de l'environnement, incertitudes liées à la logique de décision ; le recours systématique à des algorithmiques de gestion et propagation des incertitudes permettra de conduire les analyses de robustesse requises ;
- Enjeux de modélisation de fonctions de transfert d'un capteur (radar, laser, lidar, caméra…) rajoutée à la difficulté de mettre en œuvre les simulations phénoménologiques (optiques, électromagnétiques, …) rendant vraiment compte de leur comportement : sur ce sujet les démarches actuellement mises en œuvre sont extrêmement « approchantes », et il importera soit d'aller outre les contraintes de confidentialité absolue au niveau des modèles de conception des fournisseurs de capteur, soit à travers la notion de « blockchain » d'être en mesure de simuler un contenu de simulation sans en connaître précisément les composantes ;
- Complexité de traitement calculatoire des modèles impliqués : la mise en œuvre de démarches de réduction de modèle semble être une piste envisageable déjà mise en œuvre par les concepteurs de Matlab ;
- Complexité de mise en cohérence des différents contenus de modélisation du point de vue compatibilité des interfaces et formats d'informations associées : il importera de gérer également la configuration de ces contenus dans des environnements de gestion de méta données plus large, en rapport avec l'ensemble des contenus de modélisation.

4. « Métriques »

Comme on l'a déjà vu précédemment, dans les domaines industriels, les métriques apparaissent naturellement et sont liées à l'existence d'un référentiel stable de situations redoutées à considérer.

Dans le cas du véhicule autonome par exemple, le contexte opérationnel potentiel est de nature infinie multidimensionnelle pour lesquels les principes d'agrégations ne sont pas encore connus à ce jour : culturel, géographique, pratiques du code de la route, nature des infrastructures…

De plus, à chaque fois qu'on considère une famille de scénarios, on ne peut la détacher des considérations restrictives qui nous ont permis de l'instancier, en effet, pour tout scénario réel (une ou plusieurs portions de route particulières dans un territoire géographique donné), on a affaire à un environnement culturel routier, et à des comportements de conducteurs spécifiques à des pays particuliers, susceptibles d'être remis en cause d'un pays à l'autre…

On ne peut plus considérer qu'une « fonction technique » ou un « scénario technique élémentaire » a été validé une fois pour toute dans l'état actuel des pratiques : c'est la principale remise en cause de la notion traditionnelle de validation qui constitue ce principal verrou.

D'autre part, la virtualisation ne permet pas de lever ce verrou de manière satisfaisante pour l'instant : les environnements virtualisés ne font en effet que disposer d'un ou plusieurs « décors » simplifiés générés par des environnements softs de simulation de roulage où les interfaces de flux d'informations (optiques, électromagnétiques, acoustiques …) cascadent de multiples hypothèses de simplification de la réalité physique.

Avec les incertitudes ou imprécisions issues de la perception, la prise de décision évolue continuellement dans la plage d'ambiguïté bornée par les situations extrêmes d'erreurs Faux Positif (FP) et Faux Négatif (FN).

Les FP correspondent à la détection des objets non justifiés pour une manœuvre ; les FN à une échec de détection qui aurait dû générer une action de sécurité.

Les FN sont plus graves que les FP, mais les FP trop fréquents nuisent au confort et à la continuité de service du véhicule.

On retrouve ce fameux dilemme entre la sécurité et la disponibilité. La question consiste à :

- Connaître le domaine de distribution des statuts FP et FN (surface de réponse) ;
- Savoir doser la marge de sévérité versus permissivité dans les algorithmes de la chaîne de traitement en face des incertitudes.

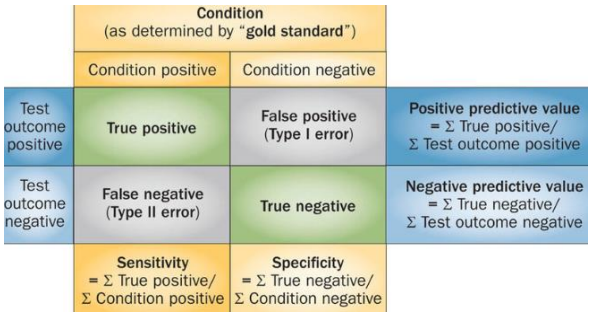

Figure 10. Utilisation de la métrique issue des Data Science

En attendant, des métriques quantitatives (Time To Collision, Deceleration to Safety Time, Time To React, Collision Rate…) ou qualitatives permettent d'exploiter les résultats de simulation et de comparer différents choix de conception, par rapport à l'identification et au diagnostic pertinent ou non pertinent des situations dangereuses.

Ces métriques sont en cours d'élaboration et elles ne peuvent pas être assimilées à des estimateurs théoriques ou statistiques habituellement utilisés en Analyse de Risque. Elles permettent néanmoins :

- De discriminer des scénarios en fonction de la criticité de comportement d'une architecture de véhicule donnée ;
- De fournir une échelle de confiance sur une fonction donnée représentée sous forme de modèle et rapportée à un ensemble de conditions très définies.

Les travaux présentés dans Réf [4] et Réf [13] utilisent des techniques d'« importance fault sampling » (ou simulation d'événements rares) afin de simuler les erreurs de décision qu'aurait pu effectuer un vrai conducteur et de les injecter dans les scénarios de simulation issus de l'accidentologie.

Plus spécifiquement, l'algorithme de Gibbs est une autre manière de quadriller l'univers théorique des scénarios en calibrant un échantillonnage sur un référentiel de probabilités d'états stationnaires calé sur un retour d'expérience (Réf [11]).

5. « Approche incrémentale »

Si l'on se situe dans un contexte d'ingénierie purement incrémentale, telle que les Data Science et l'IA (Réf [14]) nous en donne de multiples exemples, alors certains tableaux de bord permettent de piloter les différentes itérations de cette ingénierie incrémentale, sans qu'aucune signification de performance de Sûreté de Fonctionnement ne puisse être reliée à ces indicateurs.

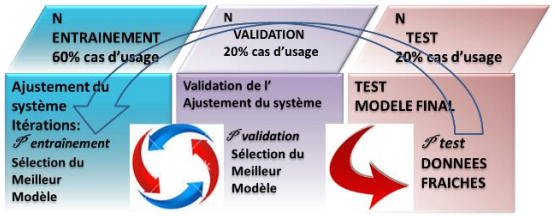

Figure 11. Processus de validation croisé au sens « Data Science »

Il s'agit de l'apprentissage pour la construction d'un modèle, la correction possible du modèle via la validation, et son évaluation par la campagne de tests. Des jeux d'essais dans les étapes de validation et de test peuvent être réinjectés dans les modèles précédents.

On distingue alors un jeu de scénarios d'entrainement N1, un jeu de scénarios de validation N2 qui va être utilisé pour tester les différents modèles paramétrés sur N1 et un jeu de scénarios de test N3 qu'on laisse de côté afin de tester le plus honnêtement possible la performance du système. Des approches de validation croisée plus sophistiquées peuvent être mises également en œuvre à travers ces différentes familles de jeux d'essais.

Ce référentiel de processus de production de modèles et contenus virtualisés, à la fois « emboîté » et croisé avec un relevé massif et systématique de cas d'usage et scénarios de comportement réels enregistrés au fil de l'eau, notamment dans le cadre des premières campagnes d'essais ou de déploiement réel du système, est déjà partiellement à l'œuvre dans les approches actuelles de production de technologies innovantes (« Minimum Value Product », outillage et généralisation de la méthode STAMP, …), tel que nous le présente ce schéma :

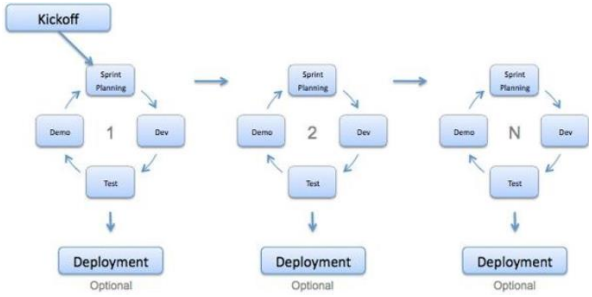

Figure 12. Enchaînement des itérations dans l'approche incrémentale

Chaque famille restrictive de cas d'usages « théorique » donne lieu à une campagne de simulation qui pourra être mise en relation avec une campagne de plans d'expérience ou d'essais opérationnels, afin de s'assurer un périmètre de couverture assurancielle dûment qualifié avec une caractérisation précise de la famille de cas d'usage et des différentes conditions restrictives associées.

Conclusion

Compte-tenu des spécificités des systèmes autonomes, nous avons constaté que :

- Le développement et la validation reposent en grande partie sur les maquettes numériques ;
- Tout modèle est une représentation orientée ;
- Le pouvoir d'expression et représentation devient une étape fondatrice nécessitant un investissement scientifique majeur ;
- L'exploitation des modèles permettent d'itérer de manière vertueuse avec le retour d'expérience (cas de roulage, accidentologie, méta testeurs, …) ;
- La question d'identifier les métriques pertinentes reste ouverte à tout niveau de modélisation.

C'est déjà beaucoup de pouvoir affirmer que dans un tel contexte, l'approche basée sur les modèles est incontournable ; mais c'est encore plus audacieux de reconnaître que les modèles nous servent tout autant, sinon moins, à tenter d'approcher une réalité continue aux contours et aux contenus infiniment variables et renouvelés, que de savoir reboucler avec pertinence sur un réel mieux caractérisé et qualifié.

Nous avons constaté également comment différentes modalités de « virtualisation » (maquettage informatique ou représentation mathématique…) permettent de compléter massivement le retour d'expérience et les campagnes d'essais en vraie grandeur, quel que soit le type de virtualisation adopté (MIL, HIL, SIL…).

Ces différents niveaux de « virtualisation croisée » démultiplient la notion de « Réel », « Perçu », « Simulé », « Virtuel » et fournissent autant de moyens de maîtrise et connaissance anticipée du « réel » observable à travers différents niveaux de perception de ce même « réel » : à partir d'une phénoménologie constatée et mesurable, il s'échelonne à travers des grilles et des champs d'interprétation calibrés sur des ontologies orientées, faisant toutes plus ou moins l'objet d'un consensus formel et cognitif.

L'ensemble des nouvelles techniques de numérisation / digitalisation applicables à des cas d'usages observés ou raisonnablement prévisibles et issus de retour d'expérience opérationnels devront compléter ces approches absolues et théoriques de virtualisation pour en contrôler le périmètre « spatio-temporel » de déploiement ; et c'est ce processus vertueux de couplage entre des univers concrets et digitalisés d'observations de la réalité « multi dimensionnelle » entourant les trajectoires d'évolution de systèmes autonomes réellement observés et des univers représentés et informatisés de conceptualisations « dirigées » et « sélectives » nécessaire-ment « orientées » en fonction des objectifs recherchés, qui fournira le support rationnel d'organisation et de contrôle de leur développement, en association avec des tableaux de bord d'indicateurs maitrisés et des critères de restriction clairement formulés et acceptés.

Références

[1] ISO/WD PAS 21448, "Road vehicles – Safety of the intended functionality," International Organization for Standardization, Standard, Under development

[2] ISO26262. « Véhicules routiers - Sécurité fonctionnelle ». Organisation internationale de normalisation.

[3] Cherfi Abraham, Emmanuel Arbaretier et Linda Zhao, 2016. « Sécurité-innocuité des véhicules autonomes : enjeux et verrous ». Lambdamu 20, Saint Malo.

[4] Rolf Johansson, Samieh Alissa, Staffan Bengtsson, Carl Bergenhem, Olof Bridal, Anders Cassel, De-Jiu Chen, Martin Gassilewski, Jonas Nilsson, Anders Sandberg, Stig Ursing, Fredrik Warg, Anders Werneman, 2011. « A Strategy for Assessing Safe Use of Sensors in Autonomous Road Vehicles ». © Springer-Verlag Berlin Heidelberg

[5] Mioara Mugur Schaechter, 2016. « Sur le tissage des connaissances ». Lavoisier

[6] Ofaina Taofifenua, Hugo Chalé, Thierry Gaudré, Alexandra Topa, Nicole Lévy, Jean-Louis Boulanger, 2011. « Reducing the Gap Between Formal and Informal Worlds in Automotive Safety-Critical Systems ». 21th annual INCOSE International Symposium, Denver, United States

[7] Wei Chen, 2017, « L'infrastructure routière en France, proposition d'une ontologie ». Document interne IRT

[8] Stéphanie Lefèvre, Dizan Vasquez, Christian Laugier, 2014. « A survey on motion prediction and risk assessment for intelligent vehicles ». ROBOMECH Journal, Springer

[9] A. De Galizia, A. Bracquemond, E. Arbaretier, 2018. « A scenario-based risk analysis oriented to manage safety critical situations in autonomous driving ». ESREL 2018, Trondheim, Norway

[10] Benoît Barbot, Béatrice Bérard, Yann Duplouy, and Serge Haddad, 2018. « Integrating Simulink Models into the Model-Checker Cosmos ». 39th International Conference on Applications and Theory of Petri Nets and Concurrency, Bratislava, Slovakia

[11] Laurent Raffaelli, Frédérique Vallée, Guy Fayolle, Philippe De Souza, Xavier Rouah, Matthieu Pfeiffer, Stéphane Géronimi, Frédéric Pétrot, Samia Ahiad, 2016. « Facing ADAS validation complexity with usage oriented testing ». Proceeding of the 8th European Congress - ERTS 2016, Toulouse

[12] Mohamed Tlig, Mathilde Machin, Romain Kerneis, Emmanuel Arbaretier, Linda Zhao, Florent Meurville, Jean Van Franck, 2018. « Autonomous Driving System : Model Based Safety Analysis ». 48th International Conference on Dependable Systems and Networks (DSN-2018), Luxembourg

[13] Ding Zhao, Henry Lam, Huei Peng, Shan Bao, David J. LeBlanc, Kazutoshi Nobukawa, and Christopher S. Pan, 2017. « Accelerated Evaluation of Automated Vehicles Based on Importance Sampling Techniques ». IEEE Transactions on Intelligent Transportation Systems (Volume 18, Issue 3)

[14] Eric Biernat, Michel Lutz, 2015. « Data Science : fondamentaux et études de cas ». Eyrolles