



**HAL**  
open science

# Contribution à la démonstration de la sécurité du véhicule autonome, basée sur une stratégie de génération de scénarios, modélisée par niveaux d'abstraction et orientée par la sensibilité du VA, pour une validation par simulation

Tchoya Florence Koné

## ► To cite this version:

Tchoya Florence Koné. Contribution à la démonstration de la sécurité du véhicule autonome, basée sur une stratégie de génération de scénarios, modélisée par niveaux d'abstraction et orientée par la sensibilité du VA, pour une validation par simulation. Automatique / Robotique. Université de Lorraine, 2021. Français. NNT : 2021LORR0182 . tel-03632822

**HAL Id: tel-03632822**

**<https://hal.univ-lorraine.fr/tel-03632822>**

Submitted on 6 Apr 2022

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



## AVERTISSEMENT

Ce document est le fruit d'un long travail approuvé par le jury de soutenance et mis à disposition de l'ensemble de la communauté universitaire élargie.

Il est soumis à la propriété intellectuelle de l'auteur. Ceci implique une obligation de citation et de référencement lors de l'utilisation de ce document.

D'autre part, toute contrefaçon, plagiat, reproduction illicite encourt une poursuite pénale.

Contact : [ddoc-theses-contact@univ-lorraine.fr](mailto:ddoc-theses-contact@univ-lorraine.fr)

## LIENS

Code de la Propriété Intellectuelle. articles L 122. 4

Code de la Propriété Intellectuelle. articles L 335.2- L 335.10

[http://www.cfcopies.com/V2/leg/leg\\_droi.php](http://www.cfcopies.com/V2/leg/leg_droi.php)

<http://www.culture.gouv.fr/culture/infos-pratiques/droits/protection.htm>

**Thèse**

**Présentée et soutenue publiquement pour l'obtention du titre de**

**DOCTEUR DE L'UNIVERSITE DE LORRAINE**

**Mention : AUTOMATIQUE, TRAITEMENT DU SIGNAL ET DES IMAGES,  
GENIE INFORMATIQUE**

**Par Tchoya Florence KONE**

**Sous la direction de Eric Levrat (CRAN) et Eric Bonjour (ERPI)**

**Contribution à la démonstration de la sécurité du véhicule autonome, basée sur une stratégie de génération de scénarios, modélisée par niveaux d'abstraction et orientée par la sensibilité du VA, pour une validation par simulation**

**Soutenance publique le 15/10/2021  
devant le jury d'examen :**

<b>Co-directeurs :</b>	M. Eric LEVRAT	Professeur, Université de Lorraine
	M. Eric BONJOUR	Professeur, Université de Lorraine
<b>Président :</b>	M. Frédéric KRATZ	Professeur, INSA Centre Val de Loire
<b>Rapporteurs :</b>	M. Abdessamad KOBI	Professeur, Polytech Angers
	M. Laurent PIETRAC	Professeur, SIGMA Clermont
<b>Examineurs :</b>	M. Frédéric KRATZ	Professeur, INSA Centre Val de Loire
	Mme Frédérique MAYER	Maître de Conférences, Université de Lorraine
<b>Membre invité :</b>	M. Stéphane GERONIMI	ADAS and ADS Functional Safety Expert, Stellantis, encadrant industriel

---

## Remerciements

---

Certes, le commun des mortels m'attribuera tout le mérite associé à ce travail de thèse, mais je sais au fond de moi que cela n'aurait jamais pu se faire sans votre aide. Ainsi, je prie chacun de vous, d'accepter ces quelques mots qui ne sauront exprimer suffisamment, toute ma profonde gratitude pour avoir accepté de m'accompagner dans ce parcours.

Tout d'abord, merci à vous M. Frédéric KRATZ, pour avoir montré votre intérêt pour ce travail et pour l'honneur que vous m'avez fait en acceptant d'examiner ce travail et de présider le jury de soutenance.

Mes remerciements s'adressent également à M. Laurent PIETRAC, qui a accepté de rapporter cette thèse. Vos retours et nombreuses questions lors de la soutenance ont montré votre engouement pour le sujet et ont permis d'avoir des échanges très enrichissants.

M. Abdessamad KOBI, comme vous l'avez dit cela fait environ cinq ans que vous m'accompagnez et me suivez dans mon parcours, d'abord en tant que professeur et responsable de master, puis en tant que membre de mon comité de suivi de thèse et enfin, en qualité de rapporteur de ladite thèse. Merci pour vos conseils, votre disponibilité et pour les échanges que nous avons pu avoir.

Je tiens à te remercier Frédérique M., d'avoir été examinatrice de cette thèse. Bien plus que ça, nos séances de travail ensemble m'ont permis de bénéficier de tes conseils et de tes connaissances qui ont été d'une grande aide à l'obtention de ce résultat final. Je n'oublie pas également ton soutien féminin (à la « Girl power » !) que tu m'as témoignée du début jusqu'à la fin.

Je ne saurais poursuivre sans te remercier Eric B. pour ces 3 années (cela fait un peu plus que 3 ans d'ailleurs) en tant que co-directeur de cette thèse. Cette expérience de travail avec toi a été riche et fructueuse tant sur le plan humain que sur le plan scientifique et technique. Ta disponibilité, ta pédagogie, ton esprit vif et ton soutien moral ont été d'un très grand apport dans l'accomplissement de cette thèse. J'ai été chanceuse de t'avoir pour encadrant. Comme je te l'avais dit, nos séances de travail ensemble me manqueront certainement. Mais je garde espoir que nos chemins se recroiseront à nouveau à d'autres occasions.

Cela est également valable avec toi Eric L. (j'avoue que le jeu de mots Eric L. et Eric B. entre vos deux noms me manquent déjà). Merci à toi pour ton implication, ta pédagogie et ton soutien tant sur le plan administratif que morale pendant la codirection de cette thèse. Il va sans dire qu'un directeur de thèse peut faire bien plus que diriger une thèse comme par exemple être de bon conseil (je me rappelle encore ce jour où tu me conseillais de passer mon permis de conduire). Merci pour cela car c'est une chance de pouvoir compter sur ses directeurs de thèse. Enfin (oui, parce qu'il y'a encore une personne clé à remercier), je te dis merci Stéphane G. pour l'encadrement industriel que tu as apporté à cette thèse. Ton expertise et ton professionnalisme sont à souligner. J'ai apprécié t'avoir comme responsable et je garde de très bons souvenirs de la qualité de nos échanges. Je sais déjà que nous serons amenés à nous

recroiser (et c'est déjà le cas !) vu que le monde de l'automobile et surtout du Véhicule Autonome n'est pas si grand en fin de compte.

Puisque je viens d'évoquer le monde de l'automobile, j'en profite pour remercier mes collègues de STELLANTIS (ex Groupe PSA). Merci à Anass GASSI qui s'est montré disponible et m'a apporté son aide pour la phase d'expérimentation menée dans la thèse. Merci à toute mon équipe pour l'intégration, les échanges et interactions que nous avons pu avoir ensemble, à la communauté des doctorants ainsi qu'à son équipe d'animation. Un grand merci à STELLANTIS et à l'ANRT pour le financement apporté. Sans ce financement cette thèse n'aurait certainement pas pu se faire.

Je ne peux me permettre d'oublier mes deux laboratoires de rattachement, le CRAN (Centre de Recherche en Automatique de Nancy) et l'ERPI (Équipe de Recherche sur les Processus Innovatifs). Je remercie leur directeur respectif M. Didier WOLF et M. Mauricio Camargo, ainsi que l'ensemble des professeurs et collègues doctorants. Je n'ai pas eu l'occasion de tous vous côtoyer. Cependant, je garde de très bons souvenirs de certains d'entre vous avec qui j'ai pu sympathiser et / ou échanger (Benoît IUNG, Alexis AUBRY, Jean-François PETIN (merci d'avoir été membre de mon comité de suivi de thèse), David GOUYON, Pascale MARANGE).

Enfin, j'adresse ces derniers remerciements à ceux qui de près (puisqu'ils m'ont vu grandir et évoluer) et / ou de loin (car certains et la plupart n'ont pas pu être là physiquement à ma soutenance) m'ont apporté leur soutien indéfectible. Merci à mes frères et sœurs qui malgré la distance ont su être présents à mes côtés. Un clin d'œil à mon acolyte qui a dû vivre l'expérience d'une thèse malgré lui. Merci pour ta patience et les weekends sacrifiés pour me tenir compagnie. Merci à mes ami (e) s, cousins, cousines, oncles et tantes qui m'ont toujours encouragée et qui ont su me témoigner leur fierté.

*Pour finir, merci à mon père et à ma mère à qui je dédie cette thèse. Vous m'avez toujours soutenu dans mes projets et aventures ! Je sais que vous auriez voulu me serrer dans vos bras mais j'ai pu ressentir toute votre joie et fierté à l'idée de me savoir docteur.*

*« Tout ce que l'esprit de l'homme peut concevoir et croire, il peut l'accomplir. »*

*Napoleon Hill*

---

## Sommaire

---

Remerciements .....	2
Sommaire .....	5
INTRODUCTION.....	9
CONTEXTE INDUSTRIEL ET PROBLEMATIQUE.....	9
HYPOTHESES DE RECHERCHE .....	11
QUESTIONS DE RECHERCHE ET CONTRIBUTIONS .....	12
ORGANISATION DU MEMOIRE .....	14
Chapitre 1. Démonstration de la ‘Safety’ du VA : Challenges et problématiques associés .	15
1.1    DEFINITIONS « SURETE DE FONCTIONNEMENT, SECURITE, SAFETY »	19
1.2    ARCHITECTURE DU VA ET PROBLEMATIQUES TECHNOLOGIQUES.....	20
1.2.1    Architecture fonctionnelle du VA .....	20
1.2.2    Problématiques technologiques du VA .....	21
1.3    ISO 26262 VS SOTIF .....	23
1.4    METHODES DE VALIDATION DE LA SECURITE DU VA.....	26
1.4.1    Approche traditionnelle de validation de la sécurité.....	26
1.4.2    Validation par simulation de la sécurité du VA .....	27
1.4.2.1    Définitions des types de simulation .....	27
1.4.2.2    Intérêt de la validation par simulation de la sécurité du VA.....	28
1.4.2.3    Exemples d’environnement de test et de chaines de simulation pour la validation de la sécurité du VA .....	29
1.5    IDENTIFICATION DES SCENARIOS POUR LA VALIDATION PAR SIMULATION DU VA .....	33
1.6    PRISE EN COMPTE DE L’INCERTITUDE.....	35
1.7    SYNTHESE DES CHALLENGES OBSERVES .....	36
1.8    CONCLUSION .....	37
Chapitre 2. Concepts clés de la génération de scénarios.....	39
2.1    ETAT DE L’ART.....	39
2.2    DEFINITION DES CONCEPTS LIES AU VA ET A SON USAGE DANS L’ENVIRONNEMENT .....	42
2.2.1    Définition du concept « ODD » .....	42

2.2.2	Définitions : Cas d'utilisation (Use case), Cas de test (Test case), Performance fonctionnelle et Limitation de performance .....	45
2.2.3	Définitions : Mode de fonctionnement et manœuvre opérationnelle du VA .....	47
2.3	DEFINITION DES CONCEPTS LIES AU SCENARIO .....	52
2.4	DETERMINATION DES PARAMETRES DE LA GENERATION .....	54
2.5	MODELE DE CONNAISSANCE POUR LA GENERATION DE SITUATIONS ET DE SCENARIOS .....	56
2.6	DISCUSSION .....	59
2.7	CONCLUSION .....	59
Chapitre 3. Structure et indicateurs de performance d'un système de génération de scénarios et de validation par simulation de la sécurité du VA .....		61
3.1	ETAT DE L'ART SUR LES INDICATEURS DE PERFORMANCE DE LA GENERATION DE SCENARIOS ET LA VALIDATION PAR SIMULATION DE LA SAFETY DU VA .....	62
3.2	STRUCTURE DU SYSTEME DE GENERATION DES SCENARIOS ET DE VALIDATION PAR SIMULATION DE LA SAFETY DU VA .....	64
3.3	DEFINITIONS ET MESURES DES INDICATEURS POUR LA GENERATION DES SCENARIOS ET LA VALIDATION PAR SIMULATION DU VA.....	68
3.3.1	Indicateur de couverture .....	68
3.3.2	Indicateur de représentativité des scénarios concrets générés.....	68
3.3.3	Indicateurs de criticité et de sensibilité .....	69
3.3.3.1	Estimation de la criticité (a priori) et sensibilité .....	69
3.3.3.1.1	<i>APR, facteurs de criticité et types d'évènements</i> .....	70
3.3.3.1.2	<i>Détermination de la sensibilité du VA à chaque plage de valeurs</i> .....	73
3.3.3.2	Evaluation de la criticité a posteriori .....	77
3.3.4	Incertitude et indicateur de confiance .....	81
3.3.5	Indicateur final de risque .....	82
3.3.6	Indicateur de gain de durée de validation.....	83
3.4	DISCUSSION .....	84
3.5	CONCLUSION .....	84
Chapitre 4. Méthodologie de génération de scénarios .....		86
4.1	PARAMETRES, TECHNIQUES ET STRATEGIES UTILISES DANS LA GENERATION DE SCENARIOS.....	86
4.1.1	La modélisation et la gestion des paramètres dans la génération des scénarios	87
4.1.2	Les techniques utilisées dans la génération (automatique) de scénarios de test	88
4.1.3	Les stratégies de génération de scénarios dans le contexte du VA .....	90



4.2	STRUCTURE DE LA METHODOLOGIE PROPOSEE POUR LA GENERATION DE SCENARIOS .....	93
4.3	AI : DEFINIR LE CONTEXTE D'UTILISATION DE LA FONCTION D'AUTOMATISATION.....	95
4.4	AII.1 GENERER LES SCENARIOS DE NIVEAU FONCTIONNEL.....	97
4.5	AII.2 GENERER LES SCENARIOS DE NIVEAU LOGIQUE .....	99
4.6	AII.3 : GENERER LES SCENARIOS DE NIVEAU CONCRET .....	102
4.7	AII.4 : Mettre en œuvre une stratégie d'exploration, estimer les indicateurs de la génération et valider la sécurité du VA .....	104
4.7.2	Analyse de la sensibilité du VA aux situations logiques .....	107
4.7.3	Fonction de distribution de la sensibilité ou fonction d'importance des situations logiques	110
4.7.4	Evènements et analyse de la sensibilité du VA, gradient de sensibilité et notion de voisinage.....	111
4.7.5	Fonction de distribution de la sensibilité des évènements .....	114
4.7.6	Estimation de l'indicateur final de risque.....	115
4.7.7	Heuristique de génération des scénarios concrets .....	120
4.8	DISCUSSION .....	125
4.9	CONCLUSION .....	126
Chapitre 5.	Application de la stratégie de génération sur un cas d'étude .....	127
5.1	DESCRIPTION DE LA FONCTION TJC .....	127
5.2	CADRE CONCEPTUEL ET SPECIFICATION DE LA FONCTION TJC .....	127
5.3	ILLUSTRATION DE LA GENERATION DES SCENARIOS AVEC LE TJC ..	130
5.3.1	La génération des scénarios fonctionnels.....	130
5.3.2	La génération des situations logiques.....	132
5.3.3	Phase d'analyse en amont de la génération des scénarios concrets .....	137
5.3.3.1	La sensibilité du VA aux situations logiques.....	137
5.3.3.2	Distribution de la sensibilité du VA aux situations logiques .....	141
5.3.3.3	Evènements logiques et leur sensibilité .....	142
5.3.3.4	Distribution de sensibilité sur les évènements .....	144
5.3.4	Génération des scénarios concrets et expérimentation.....	146
5.3.4.1	Environnement d'échantillonnage et de simulation.....	148
5.3.4.2	Phase d'échantillonnage et de simulation (expérimentation) .....	148
5.3.4.3	Analyse des résultats .....	149
5.4	DISCUSSION .....	150
5.5	CONCLUSION .....	150

CONCLUSION GENERALE ET PERSPECTIVES .....	152
SYNTHESE DES RESULTATS .....	152
PERSPECTIVES .....	153
REFERENCES BIBLIOGRAPHIQUES .....	155
LISTE DES FIGURES ET DES TABLEAUX.....	161
Liste de figures .....	161
Liste des tableaux .....	162
ACRONYMES.....	164
ANNEXE 1 : Liste des 48 situations logiques obtenues pour le cas d'étude et leurs sensibilités .....	165
ANNEXE 2 : Résultats de simulation pour le scénario logique 1 .....	178
ANNEXE 3 : Résultats de simulation pour le scénario logique 2 .....	181
RESUME.....	184
ABSTRACT .....	185

---

## INTRODUCTION

---

Ce travail de thèse est une contribution à la compréhension de la dimension sûre du déploiement des véhicules autonomes (VA). Il s'inscrit au cœur des préoccupations actuelles de la filière automobile, notamment en ce qui concerne la **sécurité** des fonctions automatisées au nominal (démonstration de la capacité d'une fonction automatisée à prendre la bonne décision dans chaque situation de vie, prévisible et imprévisible). En effet, la sécurité d'un VA est une dimension critique lors de sa conception, son déploiement et pour son acceptation future par les clients. Les constructeurs automobiles en introduisant les VA seront garants de la sécurité des utilisateurs et des usagers de leur environnement. Ils devront démontrer que la spécification et la démonstration de cette sécurité sont satisfaisantes et au niveau requis. Le terme « sécurité » employé dans ce mémoire, fait référence à la correspondance « Safety » en anglais qui est un attribut de la sûreté de fonctionnement. Aussi, il est à noter que lorsque nous parlons de VA dans ce mémoire, il s'agit d'un système doté d'une fonction d'automatisation conditionnée, fortement automatisée ou totale (niveau 3 à 5). Ainsi, l'usage fait du terme « fonction d'automatisation », fait référence au VA et inversement. Nous reviendrons sur la définition de ces deux concepts, « sécurité » et « VA », dans le chapitre 1 de la thèse.

Ce chapitre introductif entend délimiter le périmètre des activités menées dans le cadre de cette thèse. Il s'agira d'abord, de définir le contexte industriel ainsi que la problématique ayant suscité la réalisation de ces travaux. Ensuite, les hypothèses et questions de recherche, puis, les contributions scientifiques proposées dans ce travail seront énoncées. Enfin, en conclusion de cette partie, un aperçu de l'organisation du mémoire sera donné afin d'explicitier l'enchaînement des chapitres.

## CONTEXTE INDUSTRIEL ET PROBLEMATIQUE

Les problématiques posées par la conception d'un VA sont nombreuses. En premier lieu, la conception doit assurer la question de la sécurité des êtres vivants (des passagers, des piétons, des autres conducteurs, des animaux errants...) et l'intégrité de l'environnement. Dans une démarche d'ingénierie traditionnelle (d'un véhicule avec un conducteur), le concepteur n'intègre pas ou peu les écarts de comportement des autres usagers de la route (autres véhicules, piétons, animaux... que le véhicule peut rencontrer sur la route), ou de l'environnement en général. Avec de tels véhicules « traditionnels » (non automatisés), la responsabilité de contrôle (du véhicule) est allouée au conducteur (« external measures » de sécurité dans l'ISO 26262). Dans ce cadre, la définition et la validation des exigences de sécurité sont à réaliser par le constructeur. Cela revient essentiellement à démontrer que les défaillances (principalement

portées par les composants hardware et software) du véhicule ne peuvent pas engendrer de phénomènes redoutés critiques.

Dans le cadre de l'ingénierie d'un VA (Hellestrand, 2013), la démonstration de sécurité et la certification du véhicule deviennent critiques : la responsabilité de contrôle du véhicule revient en tout ou partie (selon le niveau d'autonomie) au constructeur qui doit démontrer un niveau de sécurité acceptable, voire supérieur à celui obtenu avec le contrôle humain (véhicule « traditionnel »). En effet, pour attribuer au VA la capacité d'effectuer la tâche de conduite, les constructeurs utilisent des technologies spécifiques telles que les capteurs de perception de l'environnement. Ces technologies embarquées sont parfois nouvelles et difficiles à spécifier. Bien que les dysfonctionnements électriques et électroniques auxquels elles peuvent être confrontées et qui peuvent affecter la sécurité du véhicule soient déjà pris en compte dans le cadre de la norme de sécurité fonctionnelle automobile ISO 26262, certaines limitations de performance peuvent survenir (même si le véhicule est exempt de pannes électriques ou électroniques) : perception limitée de la situation, décision erronée due à la mise en œuvre d'une mauvaise heuristique, ...

La norme ISO 26262 ne prenant pas en compte ces limitations, une norme complémentaire est en cours d'élaboration. Une dernière version préliminaire de cette future norme est disponible sous le nom « ISO PAS 21448 (Publicly Available Specification 21448) » (ISO/PAS 21448, 2019). Cette norme, aussi appelée plus communément SOTIF (Safety of The Intended Functionality), vise à fournir un complément à la norme ISO 26262 en se focalisant sur les limitations de performances fonctionnelles du VA.

L'implémentation du SOTIF entend répondre à deux catégories de challenges encore difficiles à relever. D'une part, les exigences de performances du VA en termes de sûreté de fonctionnement sont très élevées. En effet, l'environnement opérationnel est difficile à définir dans le cadre de l'ingénierie mis en œuvre pour le VA et doit être considéré comme ayant des états potentiellement complexes pour les organes de perception et de décision embarqués dans le VA. Celui-ci peut se retrouver dans des situations non reconnues, non identifiées dans la spécification, pour lesquelles il devra soit solliciter le conducteur, soit passer en mode de minimisation de risque (par exemple, arrêter le véhicule en toute sécurité). Ainsi, une telle problématique dépasse le cadre habituel du traitement de la sécurité qui consiste à se focaliser exclusivement sur l'étude des défaillances matérielles du véhicule. Garantir la sécurité globale du VA impose, désormais, que les études s'étendent à plusieurs autres facteurs, notamment la multiplicité des situations réelles que rencontrera le VA (Conditions de trafic, météo, infrastructure...), la multitude de « déviations » difficilement prévisibles pour chaque situation opérationnelle et les performances réduites des fonctions du VA sous certaines conditions extrêmes.

D'autre part, les méthodes classiques de validation sont insuffisantes pour le contexte du VA. En effet, l'environnement opérationnel du VA et la multiplicité des composants du VA rendent complexes et nombreuses les exigences auxquelles il doit répondre. De plus, la présence potentielle d'algorithmes d'apprentissage et l'absence du conducteur dans la boucle de décision dans certains cas, rajoutent des contraintes de sécurité supplémentaires qui empêchent de se limiter exclusivement aux préconisations de la norme ISO 26262 pour la conception et/ou la validation du VA. Enfin, il est impossible de réaliser uniquement la validation par roulage à cause du nombre de kilomètres très élevé que cela impliquerait. En effet, ce nombre est fixé au regard de l'accidentologie, et donc assurer de ne pas avoir d'accident nécessiterait de parcourir des milliards de kilomètres (Kalra & Paddock, 2016).

## **Les travaux présentés dans ce mémoire concernant la sécurité du VA s'inscrivent dans le cadre de la norme SOTIF.**

Compte tenu de la difficulté qu'il y a à prédire toutes les situations réelles en raison des variations des conditions environnementales, et d'autre part, de l'impossibilité de concevoir de manière expérimentale l'exhaustivité des tests physiques (Kalra & Paddock, 2016) à cause de cette explosion combinatoire de situations potentiellement chaotiques, le standard SOTIF préconise l'exploration de l'univers des situations critiques pour le VA avec d'autres stratégies, et en particulier via l'utilisation systématique de la simulation massive.

Toutefois, le recours à la simulation ne résout pas le problème du nombre de cas de test élevé ou encore celui de la variabilité des situations qu'il va falloir tester. De ce fait, il apparaît important de fournir un travail préalable visant à définir le cadre général associé au VA en s'intéressant plus particulièrement à la spécification des situations et des scénarios d'usage avant d'aborder leur génération pour la validation par simulation de la sécurité du VA.

### **HYPOTHESES DE RECHERCHE**

L'hypothèse de recherche adoptée pour ce travail de thèse est qu'une approche globale, basée sur les situations et scénarios d'usage et sur la simulation, est nécessaire pour redonner une cohérence à l'ensemble des travaux spécialisés, mais partiels, existant déjà aujourd'hui autour de la validation de la sécurité du VA.

Cette hypothèse globale a été soutenue par d'autres hypothèses que nous allons expliquer et justifier à travers ce mémoire.

D'abord, nous faisons l'hypothèse de la nécessité de recourir à un processus itératif basé sur les résultats de simulation pour l'amélioration de la recherche des scénarios pertinents pour la validation de la sécurité du VA. En effet, malgré l'analyse indispensable faite en amont de la simulation pour mieux cibler ces scénarios, seule la simulation pourra confirmer leur pertinence (au travers du non-respect d'un critère d'évaluation). Nous estimons que l'exploitation de cette information fournie par la simulation, a une contribution importante dans l'obtention de l'ensemble des scénarios non testés et qui sont finalement nécessaires à la validation.

Une autre hypothèse, considérée dans ce travail, est que les lois de probabilités des valeurs des paramètres considérés dans la génération ont été déterminées à l'avance et nous sont fournies. Cela est possible grâce à l'exploitation statistique des données collectées par les concepteurs, notamment ceux en lien avec le profil de mission, c'est-à-dire, le type de missions auquel on prédestine le VA (le domaine de fonctionnement opérationnel, les attentes fonctionnelles, la durée d'utilisation du véhicule, ...).

Enfin, les experts des technologies et sous-systèmes embarqués sur le VA disposent d'une connaissance indispensable dans l'élaboration de la méthodologie de génération des scénarios. Ainsi, cette connaissance sera exploitée pour découper les espaces de variation des paramètres, en fonction de leurs impacts potentiels sur le VA. Cela permettra d'orienter la génération en favorisant les plages de valeurs identifiées pour lesquelles le VA aurait une sensibilité élevée.

Ces hypothèses ont été posées pour apporter des solutions aux questions de recherche adressées dans ce mémoire.

## QUESTIONS DE RECHERCHE ET CONTRIBUTIONS

Pour répondre à l'hypothèse globale ayant motivée ce travail de thèse, cinq questions de recherche seront traitées. Chaque question donne lieu à une contribution.

- La première question de recherche est la suivante :

***Question 1 : Quels sont les challenges et les problématiques associées à la démonstration de la 'safety' (ou sécurité) du VA ?***

Cette première question vise à analyser les éléments d'entrée qui ont favorisé ce travail de thèse. Il s'agit d'une part de s'interroger sur les concepts et dispositifs actuels : architecture fonctionnelle du VA, norme ISO 26262, norme ISO SOTIF, concept de sécurité et de « safety », méthodes de validation. D'autre part, il est question de porter un regard sur l'ensemble des problématiques qui rendent complexe la démonstration de la sécurité du VA notamment les problématiques technologiques et les incertitudes liées au VA et à son environnement opérationnel.

- La deuxième question de recherche est

***Question 2 : Comment spécifier les concepts clés de la génération des scénarios ?***

Après avoir cerné les dispositifs existants grâce à la question 1, la question 2 permettra d'établir le cadre conceptuel de la génération des situations et scénarios, en fixant l'ensemble des concepts clés qui seront employés à cet effet. En effet, des concepts clés ont été proposés dans la littérature (Geyer et al., 2013), (Ulbrich, Menzel, Reschka, Schuldt, & Maurer, 2015), (Bagschik, Menzel, & Maurer, 2018). Cependant, certains d'entre eux (par exemple, « scene or scenery ») créent de la confusion lors des échanges ou de l'ambiguïté qu'il convient de supprimer en définissant clairement les concepts que nous utiliserons dans le cadre de ce mémoire. Cette phase vise ainsi à définir un scénario et à modéliser ses éléments de variabilité.

- La troisième question à analyser, est définie ainsi :

***Question 3 : Quelle structure de système et quels indicateurs vont permettre de guider et de juger de la pertinence, voire de la performance, de la stratégie de génération et de validation par simulation de la sécurité du VA ?***

Des indicateurs ont été proposés par des auteurs dans le cadre de la validation du VA (Amersbach & Winner, 2019a), (Zhou & Re, 2017), (Jesenski, Stellet, Branz, & Zöllner, 2019)... Cependant, il n'existe pas à notre connaissance d'indicateur permettant d'identifier en amont de la simulation, les scénarios potentiellement critiques pour le VA. De plus, il faut une utilisation conjointe de plusieurs indicateurs, si l'on veut augmenter l'efficacité de la démonstration de la sécurité du VA.

La réponse à cette troisième question vise à identifier et définir les indicateurs que nous retiendrons dans notre stratégie de génération des scénarios. D'autre part, elle fournit une structure du système de génération des scénarios et de validation par simulation de la sécurité du VA, ainsi que la manière dont les indicateurs seront exploités dans cette structure.

- La question 4 permet d'apporter une réponse concrète à la problématique du SOTIF :

***Question 4 : Quelle stratégie utiliser pour la génération des scénarios nécessaires à la validation par simulation de la sécurité du VA ?***

Des stratégies existent pour générer les scénarios qui vont servir à la validation du VA. Toutefois, des manques (ou faiblesses) peuvent être relevés, comme par exemple le passage à l'échelle de la stratégie dans le cas d'un nombre de paramètres plus élevé (D. Zhao et al., 2017) ou la réutilisation de la stratégie notamment dans le cas où il est nécessaire de définir une fonction objectif (difficile à élaborer) (Feng et al., 2020a) (Feng et al., 2020b).

La réponse à cette question 4 a pour objectif d'apporter une solution à la génération des scénarios nécessaires à la validation par simulation de la sécurité du VA en s'appuyant sur le cadre conceptuel défini dans la question 2 ainsi que sur les indicateurs et la structure du système proposés dans la question 3. Cette phase va prendre en entrée les propositions obtenues à partir des questions précédentes. Elle consiste à définir une méthodologie permettant de générer un échantillon de scénarios représentatif du profil de mission souhaité pour le VA tout en remédiant aux manques relevés dans la littérature.

- La dernière question abordée porte sur la mise en application de l'ensemble des propositions faites dans ce mémoire.

***Question 5 : Comment appliquer les propositions faites pour la génération et la validation par simulation de la sécurité du VA ?***

La réponse à cette question sera fournie au travers d'un cas d'étude implémentant l'ensemble des propositions qui seront fournies dans les questions précédentes.

Pour résumer, ces cinq questions ont pour but de répondre à la question globale de la thèse qui peut être formulée de la manière suivante : **Comment assurer la validation par simulation de la sécurité du VA, au regard de ses limitations de performance ?**

## ORGANISATION DU MEMOIRE

Le tableau 1 permet de résumer les objectifs attendus ainsi que les propositions faites durant ce travail de thèse.

Chapitres	Objectifs visés	Propositions
Chapitre 1	Objectif 1 : S'interroger sur comment les dispositifs actuels ont été spécifiés et analyser l'ensemble des problématiques qui rendent complexe la démonstration de la sécurité du VA (Relatif à la question 1)	Positionnement et problématique de cette thèse, par rapport à l'état de l'art
Chapitre 2	Objectif 2 : Spécifier les concepts clés nécessaires à la génération des scénarios (Relatif à la question 2)	Cadre conceptuel de la génération
Chapitre 3	Objectif 3 : Définir la structure du système et les indicateurs qui vont permettre de guider et de juger de la pertinence, voire de la performance, de la stratégie de génération et de validation par simulation de la sécurité du VA (Relatif à la question 3)	Définition et construction de la structure du système et des indicateurs pour la génération des scénarios et la validation par simulation de la sécurité du VA
Chapitre 4	Objectif 4 : Définir une stratégie permettant de générer les scénarios nécessaires à la validation par simulation de la sécurité du VA (Relatif à la question 4)	Méthodologie d'obtention des scénarios de validation par simulation du VA (intégrant une heuristique et une estimation de l'indicateur de risque associé au VA)
Chapitre 5	Objectif 5 : Appliquer la méthodologie proposée sur un cas d'étude (relatif à la question 5)	Cas d'étude pour l'application des propositions précédentes.
Objectif global de ce travail de thèse : ce travail permettra de spécifier une stratégie de génération de scénarios permettant d'identifier et générer des scénarios critiques, que les concepteurs devront simuler pour vérifier le comportement du VA afin d'estimer sa sécurité.		

*Tableau 1 : Récapitulatif des objectifs et des propositions de la thèse par chapitre*

Chaque objectif et la proposition qui lui est associée, correspondent à des éléments qui seront développés dans un chapitre dédié. Ainsi, cinq chapitres seront présentés dans ce mémoire. Chacun d'eux entend contribuer à définir une partie de la réponse à la question globale de la thèse.

L'ensemble de ce travail permettra de spécifier une stratégie de génération de scénarios permettant d'identifier et générer des scénarios critiques, que les concepteurs devront simuler pour vérifier le comportement du VA afin d'estimer et valider sa sécurité.

**Cette thèse a été réalisée dans le cadre d'une bourse CIFRE (Convention Industrielle de Formation par la Recherche) avec STELLANTIS (ex GROUPE PSA) du 1/02/2018 au 31/03/2021.**



---

## CHAPITRE 1. DEMONSTRATION DE LA 'SAFETY' DU VA : CHALLENGES ET PROBLEMATIQUES ASSOCIES

---

Un véhicule automatisé (VA) est un véhicule qui, selon les conditions de son environnement opérationnel et son niveau d'automatisation, peut se déplacer avec ou sans intervention humaine. Le VA est considéré comme une solution technologique centrale pour de nouveaux schémas de mobilité, grâce aux avantages qu'il présente : une sécurité accrue en termes de vies sauvées ou de diminution des blessures, un gain économique et sociétal (par exemple, le VA aura une éco-conduite, le conducteur aura un gain de temps pour effectuer d'autres tâches), ou encore une amélioration de la mobilité (par exemple, meilleure fluidité du trafic) (NHTSA, n.d.). Pour encadrer le déploiement de cette technologie, la SAE (Society of Automotive Engineers) a défini six niveaux d'automatisation illustrés dans le tableau 2<sup>1</sup>: *No Driving Automation (Level 0)*, *Driver Assistance (Level 1)*, *Partial Driving Automation (Level 2)*, *Conditional Driving Automation (Level 3)*, *High Driving Automation (Level 4)*, and *Full Driving Automation (Level 5)*.

Cette classification signifie que, plus nous progressons dans les niveaux d'automatisation, moins le conducteur humain s'implique dans la tâche de conduite. Ainsi, le niveau 5 indique que la tâche de conduite incombe complètement au véhicule automatisé, qui devient le garant du contrôle du véhicule.

Dans le niveau 1 (conducteur assisté), le conducteur reste maître de la conduite mais un système d'aide à la conduite (ADAS<sup>2</sup>) utilise les informations sur l'environnement pour l'assister. Ce système d'aide assure soit le contrôle latéral, soit le contrôle longitudinal. Au niveau 2 (Automatisation partielle), un ou plusieurs systèmes d'aide à la conduite sont intégrés dans le véhicule pour assurer le contrôle latéral et longitudinal dans certaines situations de roulage. Le conducteur doit rester vigilant et superviser le système continuellement. Quant au niveau 3 (Automatisation conditionnée), le système assure toujours le contrôle longitudinal et latéral dans certaines situations et est à même d'identifier ses limites et de demander au conducteur de reprendre la main. Le conducteur n'a donc pas besoin de superviser continuellement le système mais doit être prêt à reprendre la main à tout moment. Pour le niveau 4 (Automatisation élevée), le système assure toutes les tâches de conduite dans des conditions opérationnelles bien définies. Le conducteur n'a alors pas besoin d'intervenir dans ces conditions. Enfin, le niveau 5 (Automatisation complète), permet au système d'être maître de la conduite et d'assurer toutes les tâches de conduite sans aucune intervention humaine. Ces niveaux sont souvent classés en deux catégories : la conduite assistée qui nécessite systématiquement donc l'intervention

---

<sup>1</sup> ADS: Automated Driving System. ODD: Operational Design Domain. DDT: Dynamic Driving Task. OEDR: Object and Event Detection and Response

<sup>2</sup> ADAS: Advanced Driver-Assistance System

humaine (niveaux 0, 1 et 2) et la conduite autonome (niveaux 3, 4, 5). Dans ce mémoire, nous nous intéressons essentiellement aux niveaux 3, 4 et 5 où la conduite est dite autonome. Nous utiliserons le terme usuel de "véhicule autonome", en parlant de VA.

Level	Name	Narrative definition	DDT		DDT fallback	ODD
			Sustained lateral and longitudinal vehicle motion control	OEDR		
<b>Driver performs part or all of the DDT</b>						
0	No Driving Automation	The performance by the <i>driver</i> of the entire DDT, even when enhanced by <i>active safety systems</i> .	Driver	Driver	Driver	n/a
1	Driver Assistance	The <i>sustained</i> and ODD-specific execution by a <i>driving automation system</i> of either the <i>lateral</i> or the <i>longitudinal vehicle motion control</i> subtask of the DDT (but not both simultaneously) with the expectation that the <i>driver</i> performs the remainder of the DDT.	Driver and System	Driver	Driver	Limited
2	Partial Driving Automation	The <i>sustained</i> and ODD-specific execution by a <i>driving automation system</i> of both the <i>lateral</i> and <i>longitudinal vehicle motion control</i> subtasks of the DDT with the expectation that the <i>driver</i> completes the OEDR subtask and <i>supervises</i> the <i>driving automation system</i> .	System	Driver	Driver	Limited
<b>ADS ("System") performs the entire DDT (while engaged)</b>						
3	Conditional Driving Automation	The <i>sustained</i> and ODD-specific performance by an ADS of the entire DDT with the expectation that the DDT fallback-ready user is <i>receptive</i> to ADS-issued requests to <i>intervene</i> , as well as to DDT performance-relevant system failures in other vehicle systems, and will respond appropriately.	System	System	Fallback-ready user (becomes the driver during fallback)	Limited
4	High Driving Automation	The <i>sustained</i> and ODD-specific performance by an ADS of the entire DDT and DDT fallback without any expectation that a user will respond to a request to <i>intervene</i> .	System	System	System	Limited
5	Full Driving Automation	The <i>sustained</i> and unconditional (i.e., not ODD-specific) performance by an ADS of the entire DDT and DDT fallback without any expectation that a user will respond to a request to <i>intervene</i> .	System	System	System	Unlimited

Tableau 2 : Niveaux d'automatisation d'un véhicule (SAE international J3016, 2016)

Pour son fonctionnement, le VA recueille des informations sur son environnement, les traite, planifie sa trajectoire et décide des actions à entreprendre. Pour ce faire, des technologies spécifiques telles que des capteurs et des systèmes de localisation, des systèmes de communication et des systèmes de contrôle intelligents, sont utilisés (La figure 1 donne un aperçu de la localisation de ces différentes technologies sur un véhicule automatisé).

**Les capteurs** : ils servent à identifier les éléments qui composent l'environnement du véhicule et à établir une cartographie en trois dimensions afin de pouvoir s'y déplacer. On retrouve principalement :

- les Lidars, systèmes de détection et parfois aussi de localisation par laser (ils utilisent la lumière pour la télémétrie des objets). Ils peuvent intégrer des algorithmes de reconstruction de l'environnement afin d'identifier les objets mobiles, les objets fixes, les éléments constitutifs de l'environnement de conduite.
- les caméras qui détectent les signalisations horizontales (lignes) et permettent de tracker et classifier les objets (piétons, cyclistes, voiture, camion, les feux tricolores et les panneaux de signalisation, ...).
- les capteurs radars détectent les objets (ceux originellement porteur d'éléments métalliques) ou cibles et mesurent leurs vitesses relatives par effet Doppler (décalage de fréquence d'une onde observé entre les mesures à l'émission et à la réception, lorsque la distance entre l'émetteur et le récepteur varie au cours du temps).
- les télémètres à ultrasons qui sont des capteurs et émetteurs d'ondes ultrasons permettant de mesurer la distance entre le télémètre et un objet. Ils ont une faible portée de deux (2) à six (6) mètres. A cause de leur faible portée, ces capteurs sont essentiellement utilisés pour l'aide au stationnement. Toutefois, dans les phases d'arrêt du VA (durée de l'arrêt < 2s), ils peuvent être utilisés pour vérifier l'absence d'obstacle et autoriser le redémarrage du véhicule.

**La cartographie et le positionnement** : il est essentiel pour le véhicule autonome de comprendre l'environnement dans lequel il se trouve. Pour cela, la perception de l'environnement grâce aux capteurs ne peut se suffire à elle seule. Une reconstruction de l'environnement en 3D est utilisée pour aider au positionnement du véhicule et faciliter sa navigation. Les cartographies proposées sont de plus en plus améliorées en vue d'obtenir des cartographies HD (Haute Dimension) qui intègrent de nombreuses informations telles que les panneaux, tunnels et objets en bord de route, mais aussi des valeurs plus précises (sur la largeur des voies, les dimensions des éléments...) contrairement aux premiers systèmes GPS qui se limitaient à indiquer la route et les directions à suivre.

**Les solutions de communication (V2X)** : les informations collectées ne proviennent pas uniquement de l'environnement mais aussi des serveurs du Cloud, des autres véhicules et des infrastructures. Des liens de communications sont alors créés entre le VA et les différentes sources : Véhicule-environnement (V2E), Véhicule-Cloud (V2C), Véhicule-véhicule (V2V), Véhicule-infrastructure (V2I).

**Les systèmes de contrôle-commande intelligents** : l'ensemble des données collectées est traité par l'informatique embarquée via des algorithmes et applications qui décident des actions à effectuer sur les commandes contrôlant les fonctions dynamiques du véhicule (contrôle latéral, contrôle longitudinal) ainsi que sur les commandes d'accessoires de conduite (comme l'éclairage, la signalisation ou l'essuyage).

**Les actionneurs** : ils réalisent les actions décidées par le système de contrôle-commande (Exemples : système de direction, système de freinage, système de propulsion...)

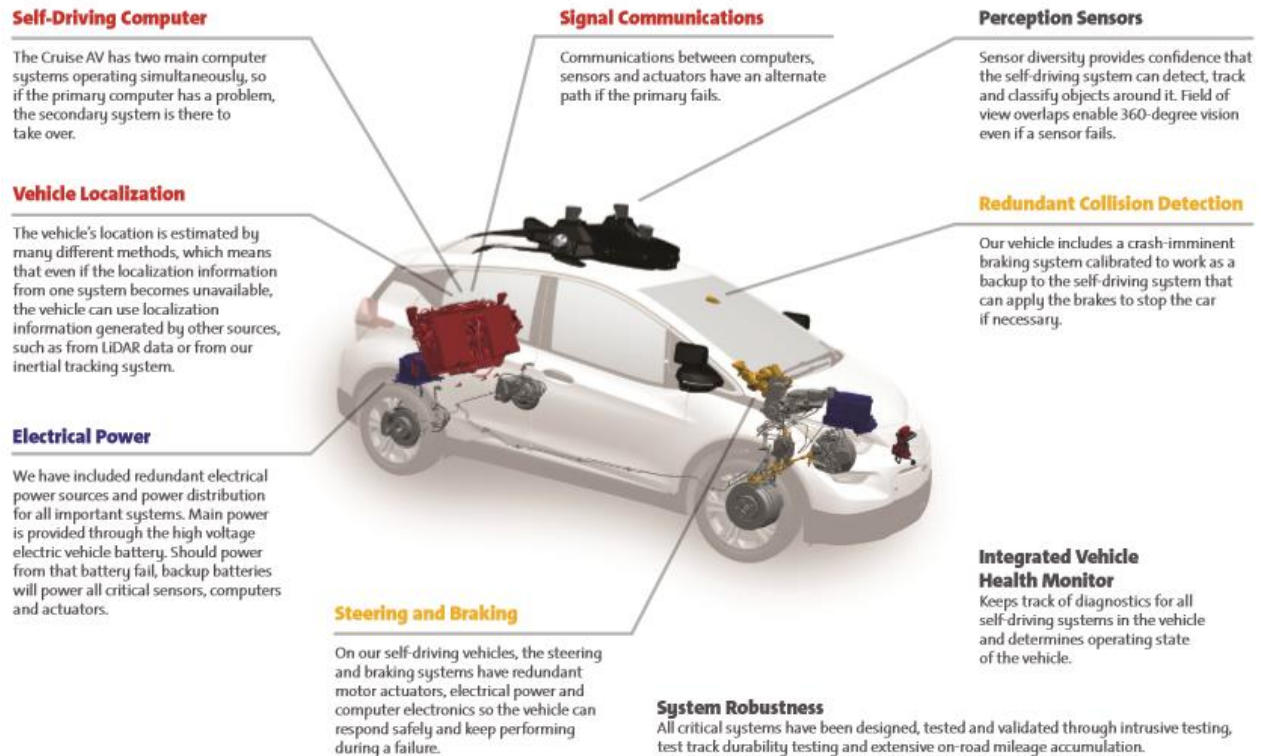


Figure 1 : Un exemple de l'emplacement des technologies embarquées sur un VA

**Ces technologies embarquées** (capteurs, systèmes de communication, de contrôle intelligents) bien que présentant une certaine maturité technique, **présentent des limites de performances fonctionnelles dans certaines conditions environnementales**. En effet, les limites de performances fonctionnelles observées proviennent de la difficulté à spécifier correctement de telles technologies pour les missions de perception de l'environnement et de navigation dans ce dernier, ainsi que d'interactions avec les acteurs qui y sont présents. **Cela affecte donc les procédures standards de validation de la sécurité d'un véhicule**, qui sont confrontées à de nouveaux défis et se retrouvent inadaptées. De ce constat, est né le besoin de distinguer les défis de sécurité engendrés par de telles limites fonctionnelles, de ceux qui sont dues aux défaillances matérielles. Ainsi, les premiers s'inscrivent dans le périmètre de la future norme ISO 21448 connue également sous l'appellation SOTIF (Safety of The Intended Functionality) tandis que les derniers sont quant à eux, liés à la norme ISO 26262. Pour bien comprendre les défis adressés par le SOTIF, il nous est apparu nécessaire de remonter aux origines du problème en répondant notamment à la question de recherche ci-dessous.

### **Quels sont les challenges et les problématiques associées à la démonstration de la 'safety' (ou sécurité) du VA ?**

Les réponses à cette question constituent l'objet de ce chapitre et notre première contribution. Nous commencerons d'abord, par préciser les définitions relatives aux concepts que nous utiliserons autour de la sécurité du VA. Ensuite, nous analyserons l'architecture du VA pour mettre en évidence, les problématiques technologiques associées. L'étape suivante consistera à porter un regard sur les principales différences entre les deux référentiels : ISO 26262 et ISO PAS 21448, en vue de distinguer les défis adressés par chacun. En outre, les différentes

méthodes de validation seront discutées avec une attention particulière sur la validation par simulation. La présence d'incertitudes dans l'environnement opérationnel du VA ainsi que les outils employés dans la démonstration de la sécurité, impactent l'ensemble du processus de génération et de validation par simulation. Cela fera donc l'objet de notre attention dans la section suivante. Enfin, à la lumière de tous les éléments analysés, la dernière section du chapitre sera dédiée au positionnement du travail de thèse par rapport à l'état de l'art.

## 1.1 DEFINITIONS « SURETE DE FONCTIONNEMENT, SECURITE, SAFETY »

Les définitions françaises des termes « Sûreté de fonctionnement », « Sécurité » et « Safety » sont très souvent ambiguës. Pour éviter toute confusion, nous proposons de fixer dans cette section, le sens que nous accorderons à chacun de ces termes dans la suite de la lecture de ce mémoire. Les définitions adoptées sont proposées par Avizienis et al. (Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, & Carl Landwehr, 2004).

« **La sûreté de fonctionnement** » ou « **Dependability** » en anglais, se définit comme suit :

« *dependability is an integrating concept that encompasses the following attributes:*

- *availability: readiness for correct service.*
- *reliability: continuity of correct service.*
- *safety: absence of catastrophic consequences on the user(s) and the environment.*
- *integrity: absence of improper system alterations.*
- *maintainability: ability to undergo modifications and repairs. »*

Comme nous pouvons le noter, la « **safety** » est une composante de la sûreté de fonctionnement qui s'intéresse particulièrement à l'absence de conséquences catastrophiques pour les usagers et l'environnement.

« **La sécurité** » est le terme qui crée le plus d'ambiguïté. En effet, traduit en anglais, il renvoie à deux notions totalement différentes.

- Sécurité pour « Safety ».
- Sécurité pour « **Security** » qui est défini en ces termes :

« *Security is a composite of the attributes of **confidentiality**, **integrity**, and **availability**, requiring the concurrent existence of 1) availability for authorized actions only, 2) confidentiality, and 3) integrity with “improper” meaning “unauthorized.” »*

**Chaque fois que nous emploierons le terme « sécurité » dans ce mémoire (comme dans la question de recherche précédente), nous ferons référence à la correspondance « Safety » en anglais qui est un attribut de la sûreté de fonctionnement :**

<p><i>Safety: absence of catastrophic consequences on the user(s) and the environment. (Algirdas Avizienis et al., 2004).</i></p>
---

## 1.2 ARCHITECTURE DU VA ET PROBLEMATIQUES TECHNOLOGIQUES

Comme évoqué en début de ce chapitre, le VA est doté de technologies spécifiques qui ont un impact sur ses performances et sur la démonstration de sa sécurité. Parmi les solutions qui sont analysées pour garantir le niveau de sécurité recherché, figure avant tout la définition d'une architecture fonctionnelle optimisée et bien structurée.

### 1.2.1 Architecture fonctionnelle du VA

Ulbrich et al (Ulbrich et al., 2017), ont proposé une architecture modulaire caractérisée par une séparation fonctionnelle et hiérarchique des différents blocs qui composent le VA. Dans l'architecture qu'ils ont proposée, Matthaei et Maurer (Matthaei & Maurer, 2015), ont également intégré la modularité, mais utilisent une approche descendante qui couvre les aspects suivants : la perception de l'environnement, les données cartographiques, la localisation, les aspects opérationnels de l'humain, l'accomplissement de la mission ainsi que la coopération avec les autres usagers. En outre, d'autres architectures comprennent explicitement des modules dédiés aux aspects de sécurité (Staplin et al., 2018). Enfin, après l'examen et la comparaison des différentes architectures, Kuhnt et al.(Kuhnt, Sahin, Kuhnt, Zöllner, & Stiller, 2016) ont mis en évidence quelques caractéristiques principales possédées par la plupart des architectures :

- elles sont distribuées,
- comprennent des systèmes de surveillance (monitoring system) qui supervisent l'état du système pour détecter des pannes,
- utilisent des capteurs redondants et complémentaires pour observer tout l'environnement du véhicule et tenir compte des incertitudes sur les données fournies par les capteurs,
- disposent d'un contrôleur (système de contrôle-commande) pour la navigation,
- intègrent une séparation et une redondance de certains modules,
- prévoient la dégradation potentielle des fonctions logicielles,
- et enfin, effectuent une comparaison des données des capteurs avec celles fournies par la cartographie pour connaître l'état du système.

A titre illustratif, la figure 2 montre une architecture simplifiée d'une fonction d'automatisation, composée de quatre modules (avec le respect de la modularité, comme évoqué précédemment) : Acquisition, Analyse, Décision et Action. Le module « Acquisition » permet au VA d'établir des interactions (via ses capteurs, la cartographie ou les communications V2X) avec les éléments de la situation pour collecter des informations. Ensuite, le module « Analyse » fusionne les informations collectées et les analyse en vue de faire une classification et identifier les éléments qui composent la scène. Cette étape permet au VA d'identifier son contexte. Le module « Décision » permet de décider de la stratégie à suivre pour le guidage du VA dans son environnement. C'est l'étape de la planification de la trajectoire. Enfin, le dernier module « Action » permet aux actionneurs de déployer l'effort requis pour appliquer la stratégie retenue par le module précédent.

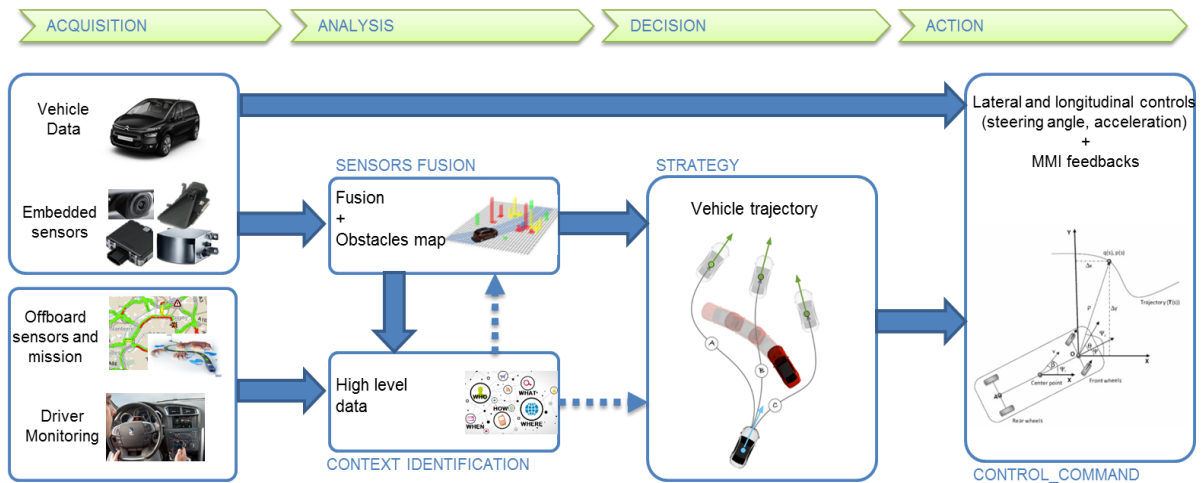


Figure 2 : Architecture simplifiée du VA (Source interne Stellantis)

Ces différentes alternatives d'architecture visent, en premier lieu, à rendre le service attendu « se déplacer en automatique / autonomie ». En deuxième lieu, elles contribuent à assurer un véhicule sûr. Cependant, elles engendrent d'autres difficultés telles que l'augmentation de la complexité et des ingénieries multidisciplinaires. Ainsi, pour faciliter les échanges entre tous les acteurs impliqués dans la conception du VA, Smaoui et al. (Smaoui & Liu, 2018) pensent que l'utilisation d'une approche MBSE peut s'avérer très utile. Par ailleurs, il apparaît pertinent aujourd'hui d'utiliser conjointement l'ingénierie des systèmes basée sur les modèles (MBSE) et l'évaluation de la sécurité basée sur les modèles (MBSA). C'est dans cette logique que, Mauborgne et al. (Mauborgne et al., 2016) ont proposé la définition d'exigences de sécurité de haut niveau (au niveau du véhicule) (appelées Safety Goals dans la norme ISO 26262) qui s'appuie sur un processus d'ingénierie des systèmes sûrs, basé sur des modèles.

Au-delà de l'architecture fonctionnelle, le VA est aussi confronté à des problèmes liés à des choix organiques, bien particuliers, concernant les technologies qu'il intègre.

## 1.2.2 Problématiques technologiques du VA

Comme évoqué, pour accomplir leur mission, les VA utilisent des technologies spécifiques telles que des capteurs, des systèmes de localisation, des systèmes de communication et des systèmes de contrôle intelligents (en intégrant potentiellement des algorithmes d'Intelligence Artificielle, IA). Malgré les nombreux travaux aidant à mieux spécifier et concevoir ces technologies, elles restent encore sujettes à des limitations.

Tout d'abord, subsistent des problèmes de perception inhérents à la qualité des capteurs. Cette qualité dépend de paramètres tels que la sensibilité, la linéarité, le bruit, la sélectivité, la saturation, la largeur de bande ou la résolution géométrique. Les performances et les limites des capteurs sont très variables. Certains capteurs sont plus adaptés à la détection d'objets proches comme le capteur ultrasonique et la caméra 3D mais sont limités en cas d'intempéries comme

la pluie. Le LIDAR est approprié pour la détection d'objets éloignés mais présente de mauvaises performances dans des conditions de brouillard et de neige. Quant au radar longue portée, il détecte également les objets éloignés et plus spécifiquement ceux qui sont métalliques. Toutefois, son angle de mesure peut s'avérer trop restreint. En plus des conditions météorologiques, les capteurs sont également sensibles à de nombreux autres facteurs comme la présence de sable, de sel ou de poussière. De plus, Li et al., (Li, Chen, Li, Shaw, & Nüchter, 2014) affirment que l'environnement est complexe et que des facteurs tels que l'alternance de routes structurées et non structurées, l'ombre prononcée sur la chaussée, la dégradation des chaussées, la saleté, les flaques, la courbure des routes, accentuent le défi de détection de l'environnement. Toutes ces limitations et variations de performances impactant la perception doivent être prises en compte dans la conception et aussi lors des tests de sécurité du VA. Le processus de validation doit s'assurer que le VA peut détecter des objets proches ou éloignés, s'assurer qu'il fonctionnera correctement dans de mauvaises conditions météorologiques ou dans des configurations d'environnement complexes et dégradées. La figure 3 illustre quelques difficultés de perceptions que l'on peut rencontrer avec les capteurs.



Figure 3 : Exemples de conditions difficiles de perception



Aussi, à l'instar de la perception, il peut arriver que le positionnement et la localisation du véhicule soient erronés. En effet, l'évolution constante de l'environnement impose que les cartes sur lesquelles reposent le positionnement et la localisation soient constamment mises à jour.

De plus, la planification de la trajectoire et la prise de décision sont des éléments qui méritent également notre attention. Le module de planification doit faire face à la fois à des contraintes dynamiques inhérentes à l'environnement et à un espace de planification restreint (Liu et al., 2015). En effet, la dynamique de l'environnement contraint le système à avoir une capacité de réaction rapide en prenant sa décision dans un temps limité. Sans cette capacité, le VA pourrait être dangereux ou en danger (en raison de son inertie) (Petti, Bank, & Fraichard, 2015). Ainsi, sa capacité à (ré)agir dans un environnement dynamique doit être testée pour la validation de sa sécurité.

Enfin, l'utilisation des communications V2X est envisagée pour le VA mais ces dernières peuvent également faire l'objet de divers dysfonctionnements ou menaces comme l'interception de données, le détournement de connexion, le brouillage des transmissions et les dénis de service. Ces menaces doivent être prises en compte dans la validation.

Au-delà des questions de conception, deux standards sont en jeu pour assurer l'atteinte des exigences de sécurité globale du VA et permettre ainsi sa validation au regard notamment des limites technologiques évoquées. Ces deux standards sont discutés dans la section suivante.

### 1.3 ISO 26262 VS SOTIF

**La norme ISO 26262** est une adaptation au monde automobile, de la norme internationale IEC 61508 proposée par la Commission électrotechnique internationale dans le but d'assurer la sécurité fonctionnelle des systèmes électriques, électroniques ou logiciels embarqués. C'est la norme de référence utilisée dans l'automobile en matière de sûreté de fonctionnement. Ainsi, elle traite de la sécurité d'un véhicule en termes **d'absence de risque déraisonnable dû à un dysfonctionnement des systèmes électriques et électroniques**. Elle vise à s'assurer que les défaillances soient efficacement évitées ou atténuées. La norme ISO 26262 utilise le cycle en V comme référence pour la spécification des exigences et des activités requises pour assurer la sécurité fonctionnelle d'un véhicule. Les objectifs et exigences de sécurité (« Safety goals » et « Safety requirements ») sont obtenus à l'issue d'une analyse de risque qui prend comme élément d'entrée la définition du système. En effet, la définition du système consiste à identifier ses différentes fonctions attendues et cela au niveau véhicule. Puis, une analyse de risque comme une HARA (« Hazard Analysis And Risk Assessment ») permet d'identifier l'ensemble des dangers et des événements dangereux associés au système. D'autres outils classiques tels que l'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC) ou encore l'HAZOP (HAZard and OPerability study) peuvent être utilisés pour évaluer les risques potentiels et les dangers dus au système.

Cette analyse se poursuit avec l'identification des niveaux de risques appelés ASIL (« Automotive Safety Integrity Level »), associés à chacun des événements dangereux identifiés et aux objectifs de sécurité requis (« Safety goals »). Il existe quatre niveaux ASIL (A, B, C et D) où A est le niveau le plus faible et D le plus élevé. On retrouve aussi la classe

QM (« Quality Management ») mais cette classe n'indique aucune exigence de se conformer à la norme ISO 26262. Les niveaux ASIL s'obtiennent grâce à trois composantes : l'exposition (Exposure) en termes de durée dans la situation ou de fréquence d'apparition de la situation, la contrôlabilité (Controllability) en termes d'aptitude de l'utilisateur (ou des participants à la situation) à éviter le danger et la sévérité (Severity) en termes de conséquence sur les personnes comme les blessures. Des exigences sont à satisfaire suivant chaque niveau ASIL tout au long du cycle de vie du système ainsi que de ses composants (hardware et software). Ainsi, parmi ces exigences, figurent des cibles quantitatives à respecter telles que le taux de défaillance limite associé à chaque ASIL. Par exemple, dans le cas des composants HW, on peut avoir :  $10^{-6}/h$  (ASIL A),  $10^{-7}/h$  (ASIL B),  $10^{-7}/h$  (ASIL C),  $10^{-8}/h$  (ASIL D).

Toutefois, dans le cas des systèmes automatisés, cette norme ne tient pas compte des manquements à la sécurité qui peuvent être causés par les limitations de performance et cela en l'absence de défaillance (Raffaëlli et al., 2016).

En outre, l'un des défis majeurs à prendre en compte désormais est le partage de la conduite entre le VA et le conducteur. Autrement dit, le conducteur n'est plus systématiquement dans la boucle décisionnelle. En effet, dans une approche d'ingénierie traditionnelle (d'un véhicule manuel), le constructeur prend peu en compte les écarts de comportement des autres usagers de la route et transfère cette responsabilité au conducteur. Une telle pratique ne sera pas acceptable pour le VA.

De nombreux autres défis existent et concernent entre autres la présence d'algorithmes non déterministes, d'algorithmes d'apprentissage inductif et de systèmes opérationnels défaillants, qui ne relèvent pas de cette norme. Une annexe existe dans la norme sur ces algorithmes.

En raison des défis évoqués précédemment, l'analyse de sécurité du VA ne peut se limiter à cette norme uniquement. La norme ISO PAS SOTIF a dû être envisagée pour prendre en compte les limitations de performance du VA en absence de défaillances.

**L'ISO PAS 21448 ou SOTIF (Safety Of the Intended Functionality)** est un référentiel qui vient en complément de la norme ISO 26262 en vue de traiter ou de tenir compte des comportements dangereux du système en l'absence de défaillances couvertes par l'ISO 26262. Ainsi, elle couvre les dysfonctionnements dus à des limitations de performances fonctionnelles ou à une mauvaise utilisation raisonnablement prévisible du véhicule. Le PAS 21448 cible des fonctionnalités pour lesquelles la connaissance appropriée de la situation est essentielle à la sécurité et particulièrement lorsque cette connaissance de la situation provient de capteurs complexes et d'algorithmes de traitement. Le terme SOTIF (Safety Of The Intended Functionality) se définit comme suit : *absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or from reasonably foreseeable misuse by persons* (ISO/PAS 21448, 2019).

La nécessité de l'ISO PAS SOTIF est apparue avec l'introduction de systèmes d'assistance aux conducteurs (ADAS). Ce sont les premiers systèmes qui ont initié le projet de conduite autonome. Ils appartiennent aux niveaux d'automatisation 1 et 2, selon la classification SAE. En raison de leur utilité, notamment pour la protection des usagers de la route et le confort du conducteur, ces systèmes ont rapidement suscité un intérêt croissant. Un tel intérêt a exigé de ces systèmes qu'ils soient robustes, fiables et, par conséquent, qu'ils n'affectent pas la sécurité du véhicule qui relève de la responsabilité du constructeur (Raffaëlli et al., 2016). Toutefois, comme ces systèmes sont également basés sur des systèmes de détection, ils sont sujets aux

limites de performance évoquées précédemment. Aussi, leur utilisation dans un environnement complexe, implique un grand nombre de paramètres à identifier au cours d'un profil de mission. Pour ces raisons, les méthodes conventionnelles se sont rapidement avérées insuffisantes ou obsolètes pour la validation des ADAS.

Ainsi, les activités identifiées et détaillées dans la norme ont pour but de définir un processus efficace d'identification et de traitement des scénarios qui seront critiques pour le VA lors de sa phase opérationnelle. De tels scénarios critiques concernent deux des catégories ou « areas » (voir figure 4) définies par la norme à savoir les « Area 2 » et « Area 3 ». L'« Area 2 » est relative aux scénarios dangereux connus (Known unsafe scenarios) et l'« Area 3 » regroupe les scénarios dangereux inconnus (Unknown unsafe scenarios).

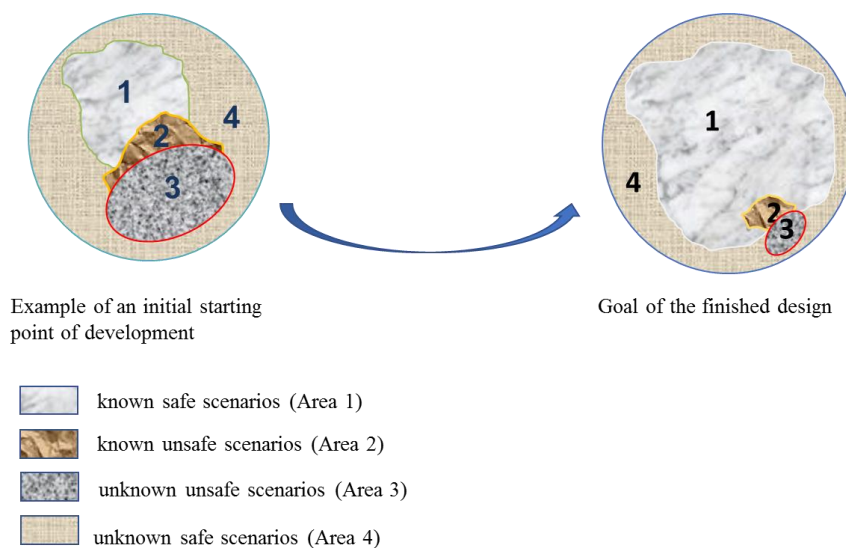


Figure 4 : Illustration des "Area" à prendre en compte dans les activités du SOTIF

Pour identifier ces deux catégories de scénarios et les réduire convenablement (de sorte à aboutir à l'obtention de la partie droite de la figure 4), le recours à la simulation massive apparaît aujourd'hui comme une nécessité, en complément de la validation par roulage.

Dans ce sens, le PAS SOTIF s'inscrit dans une perspective de définition d'un cycle de développement par améliorations itératives du fonctionnel nominal, en s'appuyant sur des analyses « Safety », basées sur la conception du système et la connaissance des scénarios d'usage habituel des clients.

En outre, de même que pour les défaillances matérielles, un niveau d'exigence ou cible de validation quantifiée ( $10^{-X}$ /heure de roulage) peut être utilisé pour garantir l'atteinte d'un niveau de sécurité acceptable pour le périmètre du PAS SOTIF. Selon le PAS 21448, la cible de validation peut être déterminée en tenant compte des réglementations ou normes en cours, au niveau industriel et gouvernemental, ainsi que du niveau de performance fonctionnelle requis pour garantir la sécurité. L'une des approches actuellement favorisées pour définir cette cible s'inspire de la preuve par l'usage. Il s'agit de se baser d'une part sur les données statistiques ou les données du trafic pour la clientèle visée (Target market) notamment via le profil de mission, et d'autre part, sur les cibles (de validation) préexistantes pour des fonctions similaires opérant sur le terrain.

Toutefois, il est à noter que les fonctions en jeu exigent des niveaux de sécurité élevés de telle sorte que le taux acceptable d'accident ou de blessures graves (et donc le niveau d'exigence quantifiée à atteindre), soit très faible (de l'ordre de  $10^{-7}/h$  à  $10^{-9}/h$ ).

## 1.4 METHODES DE VALIDATION DE LA SECURITE DU VA

Du calcul à l'expérimentation physique, en passant par le recours aux méthodes empiriques ou à la simulation, toutes les pistes sont aujourd'hui explorées pour mettre en place une procédure de validation de la sécurité du VA. Les paragraphes suivants présentent ces différentes possibilités.

### 1.4.1 Approche traditionnelle de validation de la sécurité

Dans les véhicules traditionnels, la validation de la sécurité a, jusqu'ici, été principalement assurée via la conformité avec la norme ISO 26262 et donc, était axée autour des défaillances matérielles et algorithmiques des systèmes électriques et électroniques. La validation de la sécurité revenait alors à s'assurer, grâce à des analyses et des tests, que le système est opérationnel et « safe » dans son environnement opérationnel (les « Safety goals » sont suffisants et ont été atteints).

Avec l'arrivée des ADAS, de nouveaux composants dotés de technologies particulières tels que les systèmes de vision, se sont rajoutés aux véhicules. De ce fait, ces ADAS et donc le SOTIF, induit de nouvelles « exigences » de sécurité et donc le besoin d'une stratégie de validation. Ainsi, le roulage est la première solution de réponse proposée (Raffaëlli et al., 2016). En effet, les roulages permettent de vérifier l'utilisation de la fonction et ses réponses aux exigences décrites dans les spécifications, sans considération du standard ISO 26262. En soit, c'est une raison valable d'admettre le besoin d'amélioration de la stratégie de test et de validation de ces systèmes. De plus, leur complexité et le nombre de paramètres, en lien avec le profil de mission, que les capteurs doivent considérer, sont d'autant plus importants que l'on tend vers des systèmes de plus en plus automatisés comme les ADS (Automated Driving Systems). Cela induit des niveaux d'exigences de sûreté de fonctionnement très élevés, avec une cible quantitative à atteindre qui est très faible. Cela signifie que les événements redoutés (les accidents) peuvent avoir des fréquences d'occurrence très faibles et peuvent correspondre à des situations dangereuses dont l'apparition en roulage est très peu probable. A l'inverse, le VA peut rouler, la plupart du temps au cours de l'expérimentation, dans des situations faciles à maîtriser et fréquemment rencontrées.

Par ailleurs, Kalra et Paddock (Kalra & Paddock, 2016) ont montré que la validation du VA par roulage nécessiterait de parcourir des milliards de kilomètres si l'on souhaite parvenir à l'obtention d'une base de connaissances, suffisante et acceptable, portant sur son environnement opérationnel. Ainsi, une telle cible de validation en termes de « kilométrage à parcourir » serait bien trop élevée et difficilement atteignable par roulage.

Etant donné les limites que présente la validation par roulage, d'autres stratégies de validation sont explorées dont notamment la validation par simulation qui fait l'objet de la section suivante.

## 1.4.2 Validation par simulation de la sécurité du VA

Dans cette section, la validation par simulation est analysée. Nous verrons les types de simulation existants, les avantages de la validation par simulation, les spécifications d'un environnement de simulation et des exemples de chaînes de simulation.

### 1.4.2.1 Définitions des types de simulation

Trois types de simulation sont principalement utilisés pour le test et la validation des ADS (Automated Driving Systems) (ISO/PAS 21448, 2019) (Staplin et al., 2018) :

- Software-In-the-loop (SIL) simulation
- Hardware-In-the-loop (HIL) simulation
- Vehicle-In-the-loop (VIL) simulation
- Model-In-the-Loop (MIL) simulation

La simulation SIL consiste à intégrer la totalité ou une partie des logiciels ADS dans le modèle du véhicule en vue de stimuler la réponse physique aux stimuli. Ensuite, la simulation HIL incorpore un certain niveau de matériel physique et d'équipements dans l'environnement de simulation pour fournir des entrées et un traitement de données réelles pour certaines parties du système. Enfin, avec la simulation VIL, le test et l'analyse sont plus intégrés car l'on incorpore le véhicule et les sous-systèmes destinés à la production. Le système de simulation peut être lié à un banc à rouleaux (sur lequel figure le véhicule) et au véhicule lui-même. L'actionnement physique des systèmes de direction, d'accélération et de freinage pour faire rouler et tourner les roues devient possible pour le VIL. L'injection de données de capteurs (pour simuler le terrain et les objets) et de données cartographiques (pour soutenir le routage et la prise de décision) se fait alors grâce à une interface avec le véhicule. Une autre interface avec le banc à rouleaux peut être utilisée pour simuler l'état de la chaussée (par exemple, rugosité, perte de traction). En outre, une infrastructure de communication, peut être intégrée à la simulation pour fournir un échange de données V2V ou V2I. Un tel dispositif, décrit par Staplin et al. (Staplin et al., 2018) n'est pas unique. D'autres configurations de VIL existent mais le cadre et le principe de base restent les mêmes.

Un autre type de simulation à savoir le MIL peut également être considéré. Cependant, il est utilisé avant de tester le logiciel avec la méthode SIL. En effet, il sert surtout à étudier certains comportements du modèle (dans lequel est intégré le logiciel) en vue de valider sa conformité par rapport aux attentes.

Par ailleurs, comme le montrent bien les définitions ci-dessus, chacun de ces types de simulation est utilisé en fonction du stade que l'on a atteint lors du cycle de développement d'un système. En effet, au cours de la phase d'ingénierie, le MIL et le SIL sont utilisés, tandis que pendant l'intégration et la validation, le HIL, le VIL et les tests sur route sont utilisés. Ainsi, il convient à ce stade de rappeler la différence entre la vérification et la validation :

- « verification: determination of completeness and correct specification or implementation of requirements from a phase (1.89) or subphase (1.128) » (ISO 26262-1, 2011)
- « validation: set of activities gaining confidence that an item is able to accomplish its expected functionalities and missions » (ISO/PAS 21448, 2019)

Le choix de recourir à la simulation pour effectuer les différents tests et valider le système s'explique particulièrement par les avantages qu'elle offre. La section suivante fait état de ces avantages.

#### *1.4.2.2 Intérêt de la validation par simulation de la sécurité du VA*

Comparée aux tests physiques (en conditions réelles du véhicule ou des composants) notamment les roulages, qui nécessitent de longues heures dans le contexte de la validation de la sécurité du VA, la simulation apparaît comme l'alternative la plus prometteuse. En effet, elle offre les avantages suivants (Staplin et al., 2018) : la contrôlabilité des tests, la prévision de l'exécution des tests, la reproductibilité des tests et l'efficacité en terme de durée de test.

A ce titre, certains projets ont déjà testé l'utilisation de la simulation pour la validation du VA. En effet, l'une des premières solutions pour répondre à l'impossibilité de valider les ADAS par roulage a été proposée avec le projet de recherche et développement COVADEC (Conception et Validation des Systèmes Embarqués d'Aide à la Conduite) ou encore « Design and Validation of ADAS ». Il a été lancé en 2013 (Raffaëlli et al., 2016) et s'intéressait principalement à la validation des systèmes utilisant des capteurs vidéo. Ce projet a permis la mise en place d'une chaîne de simulation grâce à l'utilisation d'une stratégie reposant notamment sur l'application d'une approche statistique pour l'identification des cas de test et sur l'exécution de ces cas de tests dans un environnement ad hoc. Les premiers essais avec une telle stratégie de validation ont montré de bons résultats, dont la réduction de l'effort de test (au regard des « safety goals ») d'environ 90% par rapport à d'autres méthodes de validation (preuve formelle, roulage en conditions réelles...). Cependant, sa mise en application sur un nombre faible d'échantillons de cas de test ne garantit pas son utilisation systématique dans le cas du VA. En effet, la méthode n'assure pas l'exhaustivité des cas de test compte tenu de la difficulté qu'il y a à identifier tous les paramètres influents. Elle reste également dépendante de l'outil MaTeLo (Markov Test Logic) utilisé pour la génération des cas de test.

Un second projet, le projet SVA<sup>3</sup> ("SVA - Simulation pour la sécurité du Véhicule Autonome," 2015) a débuté en 2015 pour une durée de 4 ans avec pour objectif de fournir des méthodes et outils d'aide à la conception et à la validation de la sécurité du VA via l'usage de la simulation numérique. Le projet comptait 9 partenaires industriels et 4 partenaires académiques. Les deux principaux attendus du projet étaient, d'une part, la mise en place d'une plateforme et des outils de simulation pour permettre de concevoir des VA sûrs et les valider, et d'autre part, la spécification et le développement des modèles du VA et de son contexte. Ainsi, parmi les résultats obtenus à l'issue du projet, figurent la mise en place d'une spécification de

---

<sup>3</sup> <https://www.irt-systemx.fr/projets/sva/>

l'environnement du VA et la modélisation numérique de cet environnement, ou encore la mise en place d'une méthodologie pour l'évaluation d'un module de décision.

Cependant, la complexité du problème de validation de la sécurité du VA révèle une insuffisance de ces résultats. Pour combler ce manque, un nouveau projet a vu le jour. En effet, dans la continuité du projet SVA, le projet 3SA<sup>4</sup> (Simulation pour la Sécurité des systèmes du véhicule Autonome) a été lancé en 2019. Les activités qui sont menées dans ce projet sont notamment : la modélisation de capteurs, l'étude des méthodes et outils de simulation des systèmes de conduite autonome et la construction de la bibliothèque de scénarios dont ceux qui sont sécuritaires. Ce projet a une durée de 4 ans et est donc toujours en cours de déroulement.

Toutefois, comme nous pouvons le constater l'aspect pratique de l'utilisation de la simulation pour la validation de la sécurité du VA cache d'autres exigences qu'il convient d'analyser attentivement. En effet, l'environnement de simulation pour le test et la validation, ainsi que son architecture doivent répondre à des spécifications bien définies.

#### *1.4.2.3 Exemples d'environnement de test et de chaînes de simulation pour la validation de la sécurité du VA*

Le système requis pour tester et valider la sécurité du VA doit être capable de traiter plusieurs aspects spécifiques. En effet, pour la validation d'un véhicule terrestre automatisé, Sun et al. (Sun, Yang, & Meng, 2018) proposent un système qui comprend la modélisation des éléments du test, qui est modulaire et conçu étape par étape avec un niveau de complexité qui est progressif. L'environnement du système de test est hiérarchique et développé selon les niveaux de modélisation du contenu du test. Il contient également les méthodes de test et la méthode d'évaluation de ces tests.

Un autre environnement de test a été proposé par Staplin et al. (Staplin et al., 2018). Le cadre de test proposé vise à la fois les tests boîte noire (analyse des fonctionnalités) et les tests boîte blanche (analyse de la structure et du fonctionnement interne). Il inclut les principaux éléments de fonctionnement des ADS (manœuvre tactique, ODD [Operational Design Domain] et les capacités OEDR [Object and Event Detection and Response]) qui ont un impact direct sur leur sécurité globale. La figure 5 donne un aperçu de la composition de l'architecture de simulation proposée par ces auteurs. Nous pouvons y voir apparaître les éléments d'entrée qui peuvent être simulés (en jaune) tels que l'ODD et les données des capteurs, les éléments pouvant être contrôlés ou mesurés (orange), les éléments de sortie à mesurer (bleu) et les éléments liés au système ADS (gris).

---

<sup>4</sup> <https://www.irt-systemx.fr/avec-le-projet-3sa-systemx-poursuit-ses-travaux-dans-le-domaine-de-la-simulation-numerique-appliquee-a-la-securite-du-vehicule-autonome/>

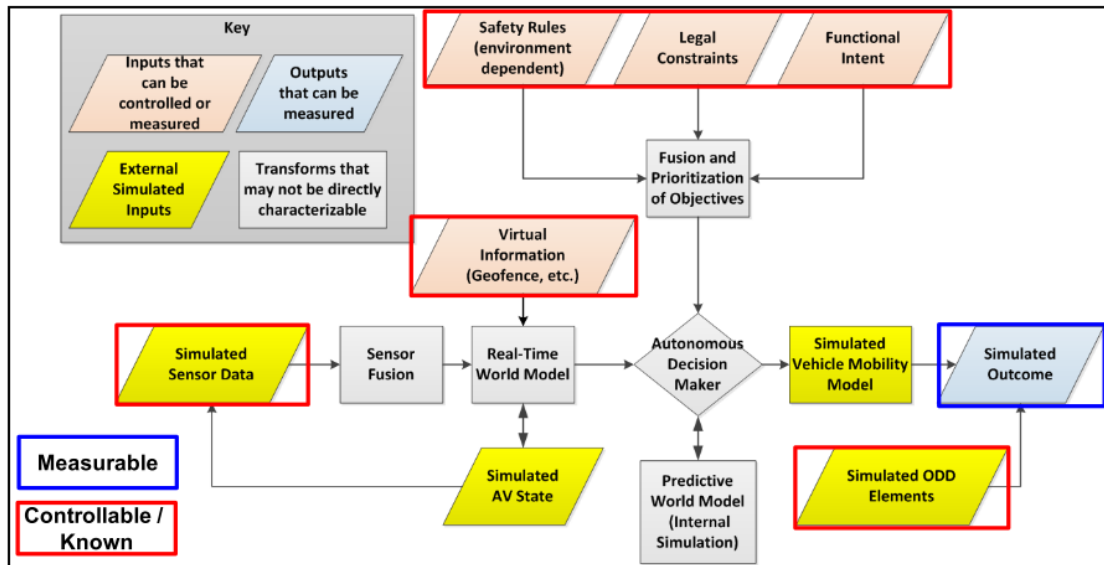


Figure 5 : Architecture théorique de simulation des ADS (Staplin et al., 2018)

Une autre chaîne de simulation que nous avons analysée est celle de Hallerbach et al (Hallerbach, Xia, Eberle, & Koester, 2018). Ils proposent une chaîne de simulation de type MIL (Model-In-the Loop) pour l'identification des scénarios pouvant conduire à un risque pour le VA. L'environnement de simulation comprend une simulation de la dynamique du véhicule, une simulation du trafic et une simulation de la coopération. La chaîne de simulation proposée (Figure 6) vise à répondre aux questions suivantes concernant la mise en circulation de ces véhicules automatisés :

- Quels scénarios doivent être testés par rapport au processus de développement du véhicule ?
- Quelles sont les exigences fonctionnelles et non fonctionnelles spécifiques de l'évaluation ?
- Quel test doit être effectué dans quel environnement de test ?
- Quels sont les avantages et les contraintes d'un environnement de test spécifique ?

Contrairement à la chaîne de simulation générique de Staplin et al. présentée précédemment, celle proposée par Hallerbach et al. est exclusivement basée sur du MIL. Toutefois, une telle chaîne de simulation axée sur la recherche des scénarios critiques pour le VA, a l'avantage de contribuer à résoudre le problème d'explosion combinatoire des scénarios. Elle offre, en effet, la possibilité de connaître et de prioriser les scénarios susceptibles de mettre en défaut le VA lors de sa validation finale.



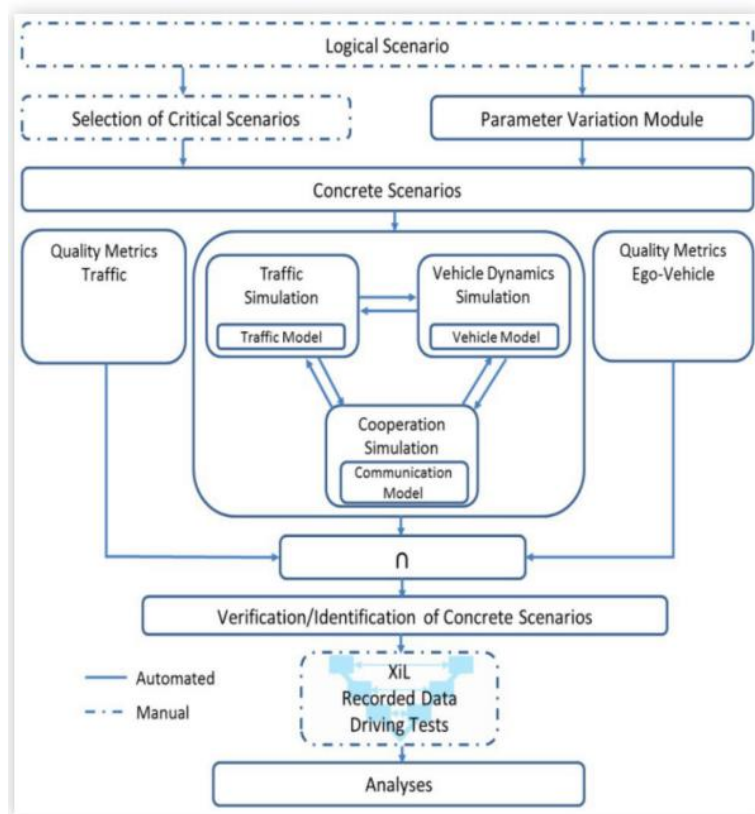


Figure 6 : Chaîne de simulation pour la vérification et l'identification de scénarios critiques pour les véhicules coopératifs et automatisés (Hallerbach et al., 2018).

Enfin, dans la chaîne de validation par simulation (figure 7) proposée par Jesenski et al (Jesenski et al., 2019), on voit apparaître clairement trois principaux modules : le module de génération des cas de test, celui de l'exécution de la simulation et enfin le module d'évaluation. Un critère d'arrêt de simulation est défini, puis, les simulations sont effectuées jusqu'à ce que ce critère d'arrêt soit rempli. Ce critère d'arrêt peut être soit un critère de couverture, soit une statistique qui doit être atteinte avec une certaine précision.

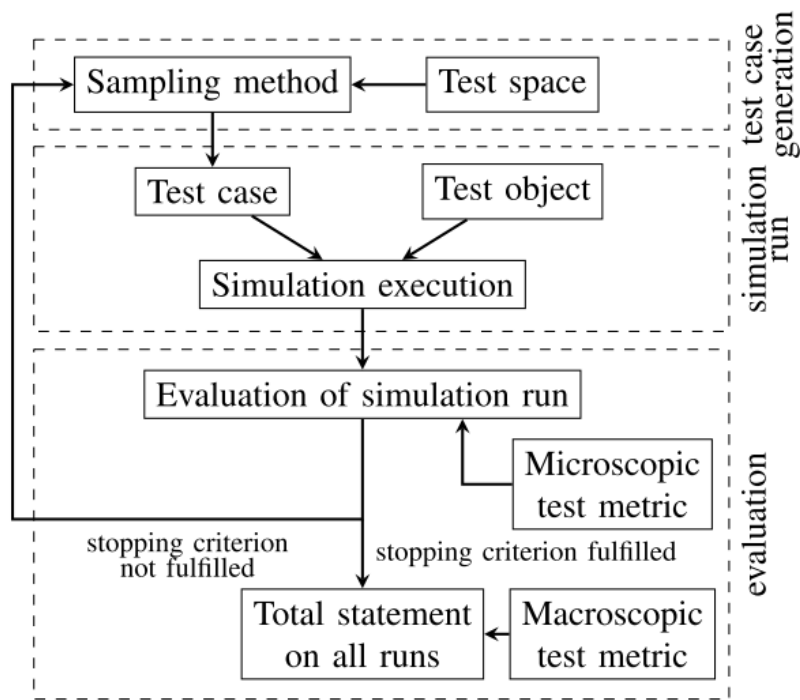


Figure 7 : Procédure de validation par simulation (Jesenski et al., 2019).

Chacune des chaînes de simulations mentionnées met en avant des caractéristiques importantes, qui peuvent être regroupées dans un même environnement de simulation afin d’augmenter son efficacité pour la validation :

- la modélisation des éléments du test, la définition de méthodes de test et la caractérisation de la manière d’évaluer ces tests (Sun et al., 2018)
- la recherche des scénarios critiques (Hallerbach et al., 2018).
- la modularité des blocs (le module de génération des cas de test, celui de l’exécution de la simulation et le module d’évaluation (Jesenski et al., 2019))
- la définition d’un critère d’arrêt de simulation (Jesenski et al., 2019))
- l’évolutivité selon le niveau de test (Staplin et al., 2018)

Ainsi, la structure du système pour la génération des scénarios et la validation par simulation de la sécurité du VA, qui sera proposé dans le chapitre 3 tient compte de ces caractéristiques.

L’approche de validation par simulation de la sécurité du VA offre bien des avantages (la contrôlabilité des tests, la prévision de l’exécution des tests, la reproductibilité des tests et l’efficacité en termes de durée de test, ...) et nécessite de mettre en place un environnement dédié. Toutefois, il convient de s’interroger sur comment mettre en place cette validation par simulation, de sorte à répondre à l’exigence de « kilométrage à parcourir » qui, bien que trop élevé et difficilement faisable en roulage, est importante pour justifier d’une couverture suffisante de l’environnement opérationnel du VA.

Pour répondre à ce besoin, l’approche basée sur les scénarios (scenario-based approach) s’avère être une alternative intéressante (Menzel, Bagschik, Isensee, Schomburg, & Maurer, 2019). En effet, lors de la validation par simulation, à défaut de déployer le VA dans l’environnement de simulation et d’observer son comportement, il devient nécessaire d’identifier au préalable l’ensemble des scénarios de test qu’il devra subir. D’une part, une telle approche permet d’avoir

une connaissance et un suivi de l'ensemble de ces scénarios de test tout en gérant la complexité liée à leur description. D'autre part, on a la possibilité de sélectionner les scénarios auxquels on veut que le VA soit confronté (en particulier ceux considérés comme redoutables) et qui permettraient d'atteindre rapidement la couverture souhaitée (notamment le kilométrage à parcourir). Cependant, comment procéder à l'identification de ces scénarios ?

L'état de l'art relatif à cette question est présenté dans la section suivante.

## 1.5 IDENTIFICATION DES SCENARIOS POUR LA VALIDATION PAR SIMULATION DU VA

Des approches sont utilisées au niveau industriel pour identifier les scénarios pertinents nécessaires à la validation du VA. L'une des premières approches concerne l'utilisation du retour d'expérience. L'objectif de cette approche est d'utiliser les expériences antérieures basées sur des fonctions de conduite antérieures comme les systèmes ADAS ou les systèmes de conduite manuelle pour identifier une première liste de scénarios que les constructeurs jugent pertinents pour tester le VA. Les retours des clients (ou utilisateurs des véhicules) sont également utilisés pour compléter cette liste. Ils sont en effet aptes à informer les constructeurs des événements ou des problèmes qu'ils ont observés au cours de l'utilisation de leur véhicule. De même, les bases de données d'accidentologie peuvent être utilisées pour identifier les situations critiques qui peuvent constituer un défi pour le VA. Comme tous les scénarios ne peuvent pas être dérivés d'expériences antérieures en raison de la complexité de l'environnement opérationnel du VA et du manque de retour d'expérience de leur utilisation, d'autres stratégies doivent être utilisées. Une stratégie consiste à utiliser les roulages pour recueillir des informations et cibler des scénarios spécifiques tout en ouvrant la possibilité de créer de nouveaux scénarios par simulation sur la base de ceux observés. A titre d'exemple, nous pouvons citer le projet MOOVE mené par l'institut VEDECOM (VEDECOM, 2019). Ce projet compte 5 partenaires qui sont principalement des constructeurs et fournisseurs. Il consiste à faire rouler des véhicules fortement équipés de capteurs d'environnement (radar, lidar, caméras, gps) pour collecter le plus d'informations possibles sur les situations de conduite qui peuvent être ensuite utilisées pour créer des scénarios pour la validation du VA.

Un autre moyen d'identifier des scénarios est d'utiliser les connaissances des experts sur les technologies qui sont implémentées sur le VA. A titre d'exemple, « les experts capteurs » de par leur expertise de ces composants, en connaissent leurs faiblesses ou limites de fonctionnement, les « experts des fonctions ADAS », savent, quant à eux, définir les exigences qui y sont associées et leurs limites de performance. Ainsi, ces experts peuvent se réunir, dans des groupes de travail ou lors de séances de brainstorming, afin de déterminer les exigences auxquelles le VA doit répondre et des scénarios génériques qui peuvent être utilisés pour le tester. Les nombreux projets et consortiums (MOOVE, SVA, PEGASUS...) qui ont vu le jour, ont pour but d'encourager et d'accélérer ce processus.

Il convient également de noter que les gouvernements sont en train de réviser la réglementation et de définir les procédures à suivre par les constructeurs pour valider et déployer leurs véhicules automatisés. Dans ce sens, ils ont identifié, en collaboration avec les constructeurs et les équipementiers, certains scénarios qui doivent impérativement être testés de sorte que le VA soit conforme aux réglementations.

Par ailleurs, toutes ces approches d'identification de scénarios pour la validation basée sur des scénarios peuvent être classées en deux approches courantes (Menzel et al., 2019) : « data-driven approach » qui consiste à générer les scénarios à partir des données collectées par roulage, et « knowledge-driven approach » qui vise à générer les scénarios à partir des connaissances existantes, notamment les recommandations fournies par les instances de régulation, puis à terme, à les améliorer avec les informations issues des données collectées. Selon Menzel et al., les approches basées sur les données font face à certaines limitations telles que la non-description de tous les aspects d'un scénario, la non-prise en compte de connaissances supplémentaires comme les dépendances de paramètres qui peuvent être effectuées lors de la description de scénarios et enfin, elles ne relient pas les classes de scénarios groupés dans un domaine de conception opérationnelle (ODD).

Malgré les efforts déployés par les industriels, il est difficile de prévoir l'ensemble des situations réelles auxquelles seront confrontés les VA, en raison des multiples variations des conditions environnementales (conditions de circulation, conditions météorologiques, infrastructures, comportements des autres usagers de la route et leurs évolutions dans le temps, etc).

De ce fait, d'autres approches pour maîtriser le processus de génération de scénarios ont été proposées. La première recommandation consiste à aborder le déploiement du VA par niveau d'automatisation (niveaux définis dans le tableau 2). De cette façon, le véhicule se limite à un certain nombre de manœuvres tactiques et peut s'acquitter de sa mission dans un environnement dédié et maîtrisé appelé ODD (Operational Design Domain). L'ODD décrit le domaine d'exploitation spécifique dans lequel le système est conçu pour fonctionner correctement. Dans son ODD, le système est capable de gérer les cas d'utilisation prévus par le constructeur. Ce dernier dispose ainsi d'une flexibilité dans les offres qu'il pourra proposer à sa clientèle. Par conséquent, les scénarios à générer sont limités à cet ODD et ces cas d'utilisation et de ce fait, l'espace de génération de scénario devient plus maîtrisable.

Une autre recommandation pour maîtriser la génération des scénarios est leur hiérarchisation. La hiérarchisation permet d'avoir une déclinaison progressive des scénarios. Menzel et al. (Menzel, Bagschik, & Maurer, 2018) ont proposé une classification pour les scénarios en trois niveaux d'abstraction : fonctionnel, logique et concret. Le scénario fonctionnel décrit toutes les entités et leurs relations sous forme linguistique compréhensible par l'homme. Le second, le scénario logique, utilise le scénario fonctionnel pour décrire l'espace d'état à l'aide de plages de paramètres. Enfin, le scénario concret permet d'attribuer des valeurs concrètes aux paramètres précédemment définis. C'est le modèle de scénario le plus proche de la réalité que rencontre le VA et tel que pourrait le décrire le conducteur. Un scénario concret s'obtient ainsi en choisissant une valeur pour chaque paramètre dans la plage de valeurs définie au niveau du scénario logique correspondant. **Les scénarios concrets permettent de définir les cas de test à exécuter lors de la validation.** Les définitions proposées pour ces trois niveaux d'abstraction se présentent comme suit (Menzel et al., 2018) :

- Functional scenario: *”Functional scenarios include operating scenarios on a semantic level. The entities of the domain and the relations of those entities are described via a linguistic scenario notation. The scenarios are consistent. The vocabulary used for the description of functional scenarios is specific for the use case and the domain and can feature different levels of detail.”*

- Logical scenario: *”Logical scenarios include operating scenarios on a state space level. Logical scenarios represent the entities and the relations of those entities with the help of parameter ranges in the state space. The parameter ranges can optionally be specified with probability distributions. Additionally, the relations of the parameter ranges can optionally be specified with the help of correlations or numeric conditions. A logical scenario includes a formal notation of the scenario.”*
- Concrete scenario: *”Concrete scenarios distinctly depict operating scenarios on a state space level. Concrete scenarios represent entities and the relations of those entities with the help of concrete values for each parameter in the state space.”*

L’intérêt de cette structuration en trois niveaux d’abstraction, est qu’elle permet une approche basée sur les scénarios pour le développement du VA, tout en étant conforme au processus de développement du standard ISO 26262 (Menzel et al., 2018). En effet, les scénarios peuvent être utilisés à différentes étapes du processus et notamment lors de la validation de la safety et des tests (« 4-9 Safety validation », « 4-8 Item integration and testing »). Par ailleurs, le processus de développement des activités du SOTIF est étroitement lié à celui de l’ISO 26262 et la validation de la sécurité nécessite des interactions entre ces deux standards. Ainsi, bien qu’ayant défini ces niveaux d’abstraction en prenant pour référence l’ISO 26262, ceux-ci pourraient être adoptés dans le cadre de la validation relevant du SOTIF (Safety Of The Intended Functionality), qui comme nous l’avons souligné, préconise entre autres, l’usage de la simulation des scénarios.

Nous avons vu que plusieurs solutions sont envisagées et proposées pour aider à l’identification de l’ensemble des scénarios pour la validation du VA. Toutefois, la présence d’incertitude liée d’une part, aux connaissances dont nous disposons, et d’autre part, aux résultats des évaluations, peut également rendre la tâche de validation laborieuse, comme nous pouvons le voir dans la section suivante.

## 1.6 PRISE EN COMPTE DE L’INCERTITUDE

Les systèmes autonomes sont confrontés à plusieurs types d’incertitudes (L. Zhao et al., 2018) notamment (1) l’incertitude épistémique sur l’environnement (manque de connaissances de l’environnement), (2) l’incertitude des mesures des capteurs, (3) les incertitudes d’interprétation générées par les algorithmes de fusion des capteurs, (4) les incertitudes de prise de décision concernant les différents arbitrages (qui pourraient être contradictoires) entre lesquels le système doit décider et (5) les incertitudes liées à la dynamique de l’évolution du système et de l’environnement. Ces incertitudes empêchent également les concepteurs de définir des cas de tests avec précision et exhaustivité. Il semble donc important d’en tenir compte lors de la démonstration de la sécurité du VA.

Pour ce faire, les méthodes existantes pour la modélisation et le traitement des incertitudes peuvent être utilisées : la théorie des probabilités, la théorie des possibilités et la théorie de l’évidence de Dempster-Shafer (Lopez & Sarigul-Klijn, 2010).

A ce titre, certaines de ces théories ont été appliquées à la conception du VA dans le but d’améliorer ses capacités. En effet, D. Althoff et al. (D. Althoff, Weber, Wollherr, & Buss,

2016) ont présenté une méthode d'évaluation de la sécurité des trajectoires, qui utilise la théorie des probabilités pour déterminer la probabilité de collision du véhicule avec un obstacle sur chaque trajectoire et cela, dans un contexte où l'environnement est dynamique et incertain. Dans leur travail, Laugier et al. (Laugier et al., 2011), proposent d'évaluer le risque de collision pour l'ego-véhicule. De même, ils ont utilisé une approche probabiliste pour l'analyse des scènes dynamiques et l'évaluation des risques de collision. L'approche tient compte des incertitudes dans la modélisation de l'environnement, la détection et le suivi des objets dynamiques. Un autre exemple (Xie et al., 2017) traite d'une méthode d'évaluation de situation visant à améliorer la prise de décision des véhicules intelligents de type IAVs (Intelligent alternative-energy vehicles). L'approche utilisée tient compte des risques liés à l'incertitude dans un environnement de trafic dynamique et se base sur un modèle stochastique de l'environnement. Le risque est évalué en tenant compte du temps de collision, de la masse des véhicules ainsi que de la vitesse relative.

Les théories pour le traitement et la modélisation de l'incertitude ont été également appliquées pendant la vérification globale de la sécurité du système. En effet, M. Althoff (M. Althoff, 2010) propose d'utiliser la technique de recherche d'atteignable « reachability analysis technique » pour la vérification de la sécurité des systèmes dynamiques. La méthode consiste, pour un ensemble d'états et de paramètres initiaux, à calculer l'ensemble exact ou approximatif d'états qui peuvent être atteints par le système. Si l'ensemble atteignable n'interfère pas avec un ensemble d'états dangereux, la sécurité du système est garantie. Pour l'appliquer à la sécurité du VA, il étend le concept à l'analyse stochastique « stochastic reachability analysis » qui mesure la probabilité d'atteindre un ensemble d'états dangereux et permet ainsi, de prédire la probabilité d'accident du VA pour une trajectoire donnée. Pour ce faire, il utilise certaines méthodes, dont les chaînes de Markov, qui calculent l'ensemble des états accessibles.

Toutes ces méthodes, en tenant compte de l'incertitude, contribuent à l'amélioration de la sécurité des capacités ou des performances du système lors de sa conception. Cependant, peu de méthodes abordent la manière de quantifier les incertitudes liées à l'exécution et à l'analyse des scénarios lors de la validation de la sécurité du VA. En effet, les incertitudes auxquelles sont sujets le VA et son environnement opérationnel influencent les évaluations de sécurité et donc la confiance que l'on aura dans la stratégie de validation.

## 1.7 SYNTHÈSE DES CHALLENGES OBSERVÉS

Parmi les challenges et les problématiques observés dans les sections précédentes, on note une augmentation de la complexité de l'architecture du VA et la variabilité des performances des technologies qui le composent notamment les capteurs qui peuvent être limités dans certaines conditions environnementales. Cela s'explique en autres, par le fait que l'environnement opérationnel est lui-même évolutif et très dynamique.

Ainsi, la difficulté liée à l'identification exhaustive des scénarios subsiste. Par conséquent, les constructeurs sont toujours à la recherche d'une stratégie de génération complète, qui offre la possibilité d'extrapoler la génération des scénarios que l'on n'aurait pas imaginés. Cela implique toutefois, de définir des concepts et des terminologies pour structurer cette identification des scénarios.

Aussi, bien qu'ayant le choix entre les différentes architectures de validation par simulation proposées dans la littérature, on note l'absence de proposition d'une stratégie autour d'un système global de validation qui intègre à la fois la manière de générer les scénarios et leurs simulations. Une telle stratégie doit tenir compte du caractère évolutif et variable de l'architecture du VA (des technologies qu'il intègre) selon les niveaux d'automatisation et doit donc être adaptable selon le système que l'on veut tester. Aussi, elle doit permettre, d'explorer l'espace des scénarios de manière itérative, de sorte à tenir compte de la présence d'incertitude dans l'environnement opérationnel du VA, ou encore de confronter les résultats obtenus en amont de la simulation (lors de la génération) avec celles obtenues après la simulation.

Pour obtenir cette stratégie, il faudra avant tout répondre aux questions suivantes :

- Quel cadre conceptuel est pertinent pour la validation de la sécurité du VA ?
- Quels indicateurs et quelle structure d'un système de validation par simulation de la sécurité du VA, adopter ?

La suite du mémoire vise à apporter des éléments de réponse pour répondre à ces questions et obtenir la stratégie souhaitée.

## 1.8 CONCLUSION

Ce premier chapitre a permis de faire un état de l'art des approches pour la démonstration de la sécurité du VA ainsi que des problématiques et des challenges associés. Il a permis d'abord, de définir le concept de sécurité utilisé dans ce mémoire. Ensuite, nous avons présenté l'architecture fonctionnelle du VA tout en relevant les problématiques technologiques auxquelles ce dernier est confronté. En outre, l'analyse et la mise en avant des périmètres adressés par chacun des deux principaux référentiels ISO 26262 et ISO PAS 21448 ont été faites. Par ailleurs, les méthodes de validation de la sécurité du VA ont été présentées avec une analyse plus étendue en ce qui concerne les méthodes de validation par simulation. Cela a permis d'aborder l'architecture de simulation et de donner quelques exemples de chaînes de simulation. La validation par simulation nécessitant de définir au préalable les scénarios de test, nous avons également présenté différentes stratégies d'identification des scénarios qui sont actuellement employées. Enfin, il est apparu important de souligner les incertitudes liées au VA et à son environnement opérationnel car cela impacte le processus de validation ainsi que les résultats qui seront obtenus.

Ce bilan est l'occasion pour nous de résumer le champ adressé dans ce travail de thèse. En effet, comme nous l'avons expliqué, nous traitons dans ce mémoire, l'aspect sécurité au sens « Safety » du VA. Ensuite, les activités de spécification d'une stratégie de génération de scénarios pour la validation par simulation du VA que nous souhaitons mener, s'inscrivent bien dans le cadre du référentiel ISO 21448 SOTIF. L'objectif pour nous est ainsi de contribuer à la démonstration de la « Safety Of The Intended Functionality » pour le VA équipé d'une fonction d'automatisation donnée. Toutefois, cette génération et les résultats qui en découlent doivent, en plus de couvrir des indicateurs de sécurité à définir, tenir compte des incertitudes soulignées précédemment.

Nous estimons que la mise en place d'une telle stratégie prenant en compte ces nombreux aspects, se fera d'abord par l'utilisation du « knowledge-driven approach (générer les scénarios à partir des connaissances existantes), la spécification de l'ODD et l'utilisation de niveaux d'abstraction des scénarios (fonctionnel, logique et concret). Puis, la stratégie sera élaborée en ayant recours à d'autres outils tels que les analyses de risques et des données statistiques et les méthodes d'échantillonnage. La première étape pour la construction de cette stratégie de génération est la définition des concepts clés associés et ce sera l'objet du chapitre suivant.



---

## CHAPITRE 2. CONCEPTS CLÉS DE LA GÉNÉRATION DE SCÉNARIOS

---

Dans le contexte de l'identification et la génération des scénarios pour la validation de la sécurité du VA, le besoin de définir certains concepts comme celui de « scénario », de scène, de situation ou encore d'événement, s'est fait sentir. Ce besoin se justifie par la volonté d'avoir un cadre conceptuel précis facilitant la génération des tests afin de permettre une exploration des scénarios et finalement assurer une validation pertinente.

Des propositions de définitions ont été faites pour tous ces concepts mais elles restent généralement fonction des approches de générations adoptées par les auteurs. Ainsi, pour s'assurer que les définitions sont communes à tous, des travaux ont été menés afin d'établir un consensus. Certains auteurs (Dickmanns, 2007) (Ulbrich et al., 2015) (Geyer et al., 2013) ont passé en revue les définitions des termes "scène, situation et scénario" et ont proposé des adaptations dans le contexte d'un VA. Les définitions proposées par Ulbrich et al. (Ulbrich et al., 2015) ont été considérées comme des références dans la version actuelle (ISO/PAS 21448, 2019) du PAS SOTIF. Cependant, ces dernières ne font toujours pas l'unanimité.

Le but de ce chapitre est d'établir le cadre conceptuel sur lequel va s'appuyer la stratégie de génération qui sera proposée en répondant à la question ci-dessous :

### **Comment spécifier les concepts clés de la génération des scénarios ?**

Pour ce faire, nous proposons de revoir d'abord les propositions existantes pour ces concepts. Puis, nous nous positionnerons sur certains choix pour ce qui est de la définition des concepts liés au VA et à ses fonctions d'automatisation de la conduite. Nous proposerons nos propres définitions permettant de décrire un scénario. Enfin, un modèle de connaissance synthétisera l'ensemble des concepts. Une analyse sera faite pour illustrer ce modèle de connaissance avec une fonction d'automatisation de niveau 3.

### 2.1 ETAT DE L'ART

Des études existantes ont déjà proposé des définitions pour le concept de scénario. Allenby et Kelly (Allenby & Kelly, 2001) définissent le scénario comme une séquence d'actions qui illustrent le comportement du système ou encore comme les instances opérationnelles de l'utilisation du système : « *Scenarios are sequences of actions used to illustrate system behaviour. While a use case is intended to represent system functions for the general case, scenarios represent operational instances of system use.* »

Plus tard, Xiong (Xiong, 2013) propose une autre définition dans le contexte d'utilisation d'un simulateur de conduite en ces termes : « *A scenario is a pre-defined environment that experimenters need a participant to experience in a driving simulator. It includes the physical scene, pre-defined traffic flow, simulated vehicles' interactions with the participant's vehicle and measurements that need to be collected.* »

De plus, Geyer et al. (Geyer et al., 2013) introduisent le terme de situation dans le scénario : « *The term 'situation' describes the current state. Hence, a scenario includes at least one situation within a scene including the scenery and dynamic elements.* »

Enfin, Ulbrich et al. (Ulbrich et al., 2015) proposent une formulation du scénario qui est proche de celle de Allenby et Kelly, à la différence qu'ils insistent sur le terme de « scene » et soulignent la nature temporelle du scénario : « *A scenario describes the temporal development between several scenes in a sequence of scenes. Every scenario starts with an initial scene. Actions & events as well as goals & values may be specified to characterize this temporal development in a scenario. Other than a scene, a scenario spans a certain amount of time.* »

En analysant toutes ces définitions, nous pouvons constater qu'il existe quelques différences entre elles. Ainsi, une volonté d'établir un consensus s'est fait sentir et a donné lieu à des réflexions notamment dans le cadre du PAS SOTIF 21448. Alors que les définitions proposées par Ulbrich et al. (Ulbrich et al., 2015) ont été considérées comme des références dans les versions déjà élaborées de l'ISO-PAS 21448, nous nous sommes aperçus que certains termes faisaient encore l'objet de discussions. C'est notamment le cas des termes « scenery » et « self-representations » qui peuvent porter à confusion. En outre, la définition que proposent Ulbrich et al. (Ulbrich et al., 2015) pour le concept de scène utilisé pour définir un scénario, demeure difficile à cerner : « *A scene describes a snapshot of the environment including the scenery and dynamic elements, as well as all actors' and observers' self-representations, and the relationships among those entities. Only a scene representation in a simulated world can be all-encompassing (objective scene, ground truth). In the real world it is incomplete, incorrect, uncertain, and from one or several observers' points of view (subjective scene)* »

A travers cette définition, on comprend que la scène peut contenir beaucoup d'informations et sa mise en œuvre peut être très subjective et varier d'une personne à l'autre. De plus, le terme "snapshot" fait perdre aux éléments de l'environnement le caractère stable (sans perte de mouvement ou de durée de vie) qu'ils peuvent avoir.

De plus, comme nous pouvons le noter dans les définitions précédentes, d'autres concepts présents dans ces définitions de scénario, sont ceux de « scène », « événement » et « situation ». Avant d'exposer la définition que nous avons retenue pour un scénario, nous examinons le concept de situation.

Dans sa thèse de doctorat (Xiong, 2013), Xiong considère la situation comme l'une des interactions auxquelles un sujet serait exposé. Geyer et al. (Geyer et al., 2013) proposent une ontologie de la génération de cas d'utilisation et des catalogues de tests pour le VA dans laquelle la situation est définie comme suit : « *[...] the situation itself is defined by the set of criteria that need to be true to conduct the associated action* ». Ulbrich et al. (Ulbrich et al., 2015) ont également proposé une définition de ce concept : « *A situation is the entirety of circumstances, which are to be considered for the selection of an appropriate behavior pattern at a particular point of time. It entails all relevant conditions, options and determinants for behavior.* »

Un autre exemple de la définition de ce concept est le suivant (Rocklage, 2018) : « *A situation is defined as the current state of all traffic participants together with the ego vehicle state (cf. Def. 1)* ». Cette définition rappelle celle de Mauborgne et al. dans laquelle le concept d'« état » apparaît dans la situation : « An operational situation is defined as a stationary state composed of a state of the system and conditions of the environment (Mauborgne et al., 2016) ».

En effet, nous recherchons la situation centrée sur le VA et donc avoir connaissance de l'état du VA et des éléments de la situation (Rocklage, 2018) et d'autre part, savoir quelles conditions doivent être vraies pour solliciter une réaction du VA (Ulbrich et al., 2015). Par cette approche, nous mettons en avant les facteurs d'influence et les interactions entre les éléments de la situation et le VA. Par ailleurs, la situation indique également un caractère restrictif aux éléments pertinents de la scène et s'avère donc d'un niveau d'abstraction plus intéressant par rapport à la scène. En outre, la « situation opérationnelle » est souvent prise en compte dans les scénarios de description des accidents (Jang, Kwon, & Lee, 2015) ou dans les méthodes de détermination des « événements dangereux / hazardous events » (ISO/PAS 21448, 2019)(ISO 26262-3, 2011) (ISO/PAS 21448 2019) (ISO 26262 2011). De plus, le VA devra interagir avec tous les éléments présents autour de lui lors de son utilisation car ils ont potentiellement une influence sur son comportement. De ce fait, le concept de situation est pertinent pour décrire les conditions d'utilisation du VA et représente une base intéressante pour définir le scénario.

Comme mentionné dans le chapitre 1, des recommandations ont été faites pour maîtriser la génération des scénarios de validation de la sécurité du VA parmi lesquelles la spécification de l'environnement dans lequel le système est conçu pour fonctionner. Pour que cet environnement appelé « Operational Design Domain (ODD) » soit spécifié, la fonction d'automatisation concernée doit être définie ainsi que les manœuvres qu'elle est censée réaliser. A ce titre, les performances fonctionnelles attendues de cette fonction doivent être décrites. Ainsi, on voit apparaître d'autres concepts importants (ODD, Manœuvres, Performances fonctionnelles) qui nécessitent une attention particulière.

Cet état de l'art, même s'il est non exhaustif, montre bien la diversité des concepts manipulés dans le domaine de la sécurité du VA et l'absence de consensus encore aujourd'hui sur la définition de concepts clés, comme situation ou scénario. De plus, l'utilité de certains concepts tels que « scene ou scenery » n'est pas évidente.

Il est donc nécessaire de proposer un cadre conceptuel pour la génération de scénarios. Ce cadre conceptuel devra permettre de limiter le nombre de concepts manipulés tout en permettant de supporter le processus de génération de scénarios.

Dans les sections suivantes, nous proposons un cadre conceptuel constitué des concepts liés d'une part, au contexte d'utilisation (§2.2), et d'autre part, à un scénario (§2.3). Ce cadre conceptuel est enfin synthétisé dans un modèle de connaissance, pertinent pour la génération de situations et de scénarios de validation du VA (§2.4).

## 2.2 DEFINITION DES CONCEPTS LIES AU VA ET A SON USAGE DANS L'ENVIRONNEMENT

Pour répondre à la mission qui lui est assignée, le VA doit répondre à de nombreuses exigences fonctionnelles (Matthaei & Maurer, 2015) dont la perception de son environnement ou la coopération avec les autres usagers de la circulation. Le terme « mission » renvoie ici, à la définition proposée par Mauborgne « the specific task, duty or function defined to be accomplished by a system » (MAUBORGNE, 2016).

En effet, la complexité de l'environnement fait que nous ne disposons pas de garantie concernant sa capacité à répondre à toutes les exigences que les concepteurs vont définir. De même, cette complexité influence la capacité à spécifier les scénarios de tests requis en vue d'éprouver et de vérifier ses performances. Ce constat nous a donc conduit à retenir un premier concept clé que nous allons analyser : l'« *ODD, Operational Design Domain* ».

### 2.2.1 Définition du concept « ODD »

L'« *ODD* » (Operational Design Domain) désigne le domaine opérationnel dans lequel le système de conduite automatisée doit opérer. Plusieurs propositions ont été faites pour définir l'ODD et qualifier ses éléments de description. D'abord, dans le rapport fourni par la US DOT et la NHTSA (U.S. DOT- Department of Transportation - NHTSA, 2016), l'ODD est défini de la façon suivante :

*The ODD should describe the specific operating domain(s) in which the HAV<sup>5</sup> system is designed to properly operate. The defined ODD should include the following information to define HAV systems' capabilities:*

- *Roadway types on which the HAV system is intended to operate safely;*
- *Geographic area;*
- *Speed range;*
- *Environmental conditions in which the HAV will operate (weather, daytime/nighttime, etc.); and*
- *Other domain constraints.*

Ensuite, nous retrouvons cette autre définition de la NHTSA (NHTSA - National Highway Traffic Safety Administration, 2017) qui reste similaire à la précédente avec quelques petites différences de formulation :

*The ODD is the definition of where (such as what roadway types and speeds) and when (under what conditions, such as day/night, weather limits, etc.) an ADS<sup>6</sup> is designed to operate. The ODD would include the following information at a minimum to define each ADS's capability limits/boundaries:*

- *Roadway types (interstate, local, etc.) on which the ADS is intended to operate safely;*
- *Geographic area (city, mountain, desert, etc.);*

---

<sup>5</sup> HAV: Highly Automated Vehicle

<sup>6</sup> Automated Driving System

- *Speed range;*
- *Environmental conditions in which the ADS will operate (weather, daytime/nighttime, etc.); and*
- *Other domain constraints.*

Nous pouvons constater l'apparition des mêmes éléments clés (*roadway, geographic, ...*) que précédemment dans cette version de définition fournie par la SAE (SAE international J3016, 2016) :

*The specific conditions under which a given driving automation system or feature thereof is designed to function, including, but not limited to, driving modes.*

- *An ODD may include geographic, roadway, environmental, traffic, speed, and/or temporal limitations. A given ADS may be designed to operate, for example, only within a geographically-defined military base, only under 25 mph, and/or only in daylight.*
- *An ODD may include one or more driving modes. For example, a given ADS may be designed to operate a vehicle only on fully access-controlled freeways and in low-speed traffic, high-speed traffic, or in both of these driving modes.*
- *In the previous version of this document, the term driving mode was used more extensively. In this updated version, ODD is the preferred term for many of these uses.*

Par ailleurs, il apparaît clairement que le caractère restrictif de l'ODD à certaines conditions dépend du niveau d'automatisation considéré. Le tableau 2 présenté dans le chapitre 1 illustre ce propos. En effet, du niveau 1 au niveau 4, l'ODD est limité car tout système doté d'une fonction appartenant à l'un de ces niveaux, ne peut fonctionner que dans des conditions spécifiques. A l'opposé, seul le niveau 5, qui renvoie à une automatisation complète du système, présente un ODD illimité. Ainsi, dans ce niveau, il n'y a aucune condition qui restreint le fonctionnement du système automatisé.

Enfin, sans donner une définition à l'allure descriptive des éléments de composition de l'ODD comme ce fut le cas avec les définitions précédentes, il est prescrit dans le document Safety First (Aptiv et al., 2019), que la détermination de l'ODD consiste à reconnaître clairement les limites du système qui permettent de le restreindre à une fonctionnalité sûre :

*As soon as system limits that restrict the safe functionality of the automated system are recognized, the system shall react to compensate or shall issue a driver takeover request with a sufficient time frame for the takeover.*

En synthèse de toutes ces propositions, nous retenons que la spécification de l'ODD a pour but de garantir la sécurité en ne déployant les fonctions d'automatisation de la conduite que dans des environnements maîtrisables par ces dernières. Ce qui est exactement l'objectif de l'ISO 21448 à savoir limiter le fonctionnel à un cadre d'utilisation sûre.

Pour la suite de notre analyse, nous proposons de définir l'ODD en prenant pour référence la définition fournie par la NHTSA (NHTSA - National Highway Traffic Safety Administration, 2017) :

*The ODD is the definition of where (such as what roadway types and speeds) and when (under what conditions, such as day/night, weather limits, etc.) an ADS is designed to operate. The ODD would include the following information at a minimum to define each ADS's capability limits/boundaries:*

- *Roadway types (interstate, local, etc.) on which the ADS is intended to operate safely;*
- *Geographic area (city, mountain, desert, etc.);*
- *Speed range;*
- *Environmental conditions in which the ADS will operate (weather, daytime/nighttime, etc.); and*
- *Other domain constraints.*

L'ODD fournit une représentation de l'environnement opérationnel du VA avec ces éléments saillant qui seront en interaction avec le VA et qui solliciteront des actions de sa part. L'ODD sera donc utile dans la modélisation de la situation du VA.

Par ailleurs, en référence à la définition de l'ODD retenue, nous considérerons l'infrastructure physique comme étant composée de zones géographiques qui ont chacune différents types de chaussée et de symboles de signalisation routière. Ainsi, pour identifier les types d'infrastructures, nous proposons de prendre en compte la configuration spatiale, la dynamique du véhicule et le type d'usagers la fréquentant. Le tableau 3 donne la liste des types d'infrastructure que nous avons identifiés.

<b>Types infrastructures</b>	
	Voies à chaussées séparées (Autoroute, Voie rapide)
	Souterrain-Tunnel
	Pont-Autopont
	Bretelle
	Voie ferrée
	Zone piétonne/Passage piéton
	Zone de péage
	Zone de travaux
	Zone école
	Intersection en X
	Zone Intersection en T
	Zone Intersection en Y
	Zone Intersection à plus de 4 branches
	Zone de passage à niveau (Voie de tram, Passage à niveau protégé)
	Giratoire
	Rond-point
	Aires de repos
	Parking
	Impasse

*Tableau 3 : Types d'infrastructures*

## 2.2.2 Définitions : Cas d'utilisation (Use case), Cas de test (Test case), Performance fonctionnelle et Limitation de performance

- **Cas d'utilisation (Use case) et cas de test (test case)**

Les **cas d'utilisation** d'un système sont définis lors des phases de spécification de ce dernier. Un cas d'utilisation se définit au sens de l'ingénierie système comme étant une « Description de l'usage attendu d'un système, vu sous l'angle de l'un de ses utilisateurs » (MAUBORGNE, 2016). Le cas d'utilisation est un service que le système rend à ses utilisateurs (certains auteurs parlent aussi des fonctionnalités du système), tandis que le scénario correspond à une séquence d'interactions entre le système et son environnement, pour pouvoir obtenir ce service.

Ainsi, un cas d'utilisation peut donner lieu à plusieurs scénarios. Cela apparaît dans la définition proposée par le SOTIF (ISO/PAS 21448, 2019): « *specification of a generalized field of application, possibly entailing the following information about the system: one or several scenarios, the functional range, the desired behaviour and the system boundaries.* »

Le cas d'utilisation est donc intimement lié à la fonctionnalité et à la performance fonctionnelle attendue du système. Sa définition permet de caractériser le système à un niveau fonctionnel. De ce fait, une fonction d'automatisation donnée peut avoir plusieurs cas d'utilisation. C'est le cas de la fonction d'automatisation Traffic Jam Chauffer (TJC) qui dispose entre autres des cas d'utilisations suivants : « Ensure the driver takeover request, Ensure the longitudinal and the lateral control » (Smaoui & Liu, 2018).

Par ailleurs, le **cas de test** quant à lui, se définit en ces termes : “A test case is a set of preconditions, inputs (including actions, where applicable), and expected results, developed to determine whether or not the covered part of the test item has been implemented correctly.” (ISO 29119 - 4). Ainsi, le cas de test correspond à une exécution d'un scénario concret (dernier niveau d'abstraction du scénario). Il associe les aspects que l'on souhaite vérifier pour le système (notamment ses performances fonctionnelles) ainsi que les conditions ou critères permettant d'évaluer ces aspects.

Le tableau 4 synthétise les définitions retenues pour le cas d'utilisation et le cas de test.

Concepts	Définitions
Cas d'utilisation (Use case)	“Specification of a generalized field of application, possibly entailing the following information about the system : one or several scenarios, the functional range, the desired behaviour and the system boundaries.” (ISO/PAS 21448, 2019)
Cas de test (test case)	“A test case is a set of preconditions, inputs (including actions, where applicable), and expected results, developed to determine whether or not the covered part of the test item has been implemented correctly.” (ISO 29119 - 4)

Tableau 4 : Synthèse des définitions retenues pour le « cas d'utilisation » et le « cas de test ».

Comme l'identification d'un cas d'utilisation ou la réalisation d'un cas de test pour le VA impliquent également la définition des performances fonctionnelles attendues, il convient de définir également ce terme.

- « **Performance fonctionnelle** » et « **Limitation de performance** »

Pour comprendre ce que l'on entend par « performance fonctionnelle » et « Limitation de performance » du VA, nous nous sommes référés d'abord au PAS SOTIF (ISO/PAS 21448, 2019). Nous y retrouvons les définitions suivantes :

**Performance limitation:** *insufficiencies in the implementation of the intended functionality*  
**EXAMPLE:** *Incomplete perception of the scene, insufficiency of the decision algorithm, insufficient performance of actuation.*

**Intended functionality:** *behaviour specified for a system*

(Note 1 de la définition "3.10 Safety Of The Intended Functionality") **Nominal performance** *includes intended functionality and the implementation of intended functionality that can be affected by performance limitations or by foreseeable misuse by persons.*

De ces définitions, nous pouvons comprendre qu'une performance fonctionnelle désigne une capacité attendue du VA. A l'opposé, la limitation de performance désigne l'incapacité du VA à réaliser ce que l'on attend de lui. Ainsi, est généralement associé à chaque technologie (notamment celles que l'on retrouve dans le VA), « une plage de fonctionnement » ou « limite de validité de fonctionnement » pour définir les plages de valeurs qu'elle est capable de traiter (par exemple, une plage de détection pour une caméra).

De ce fait, on parle de performance ou de limitation de performance en lien avec les capteurs, la reconnaissance ou la prise de décision. Par ailleurs, le terme « skill » tel qu'introduit et utilisé par Reschka et al. (Reschka, Bagschik, Ulbrich, Nolte, & Maurer, 2015), puis par Bagschik et al. (Bagschik, Reschka, Stolte, & Maurer, 2016) fait référence à ce que l'on entend par performance fonctionnelle pour le système automatisé. En effet, Reschka et al, définissent le terme Skill en ces termes : *A skill is the description of an activity related to a certain task including a performance level (skill level).* Pour Bagschik et al, *a skill is an abstract description of an activity which the system has to provide to fulfill the intended task [16].* Ainsi, définir un « skill » relatif au système VA revient à identifier la capacité et donc la performance fonctionnelle que l'on attend de lui. Ses performances fonctionnelles vont donc concerner principalement les modules qui le composent, à savoir, la perception de son environnement, la prise de décision pour réagir aux situations ainsi que l'actionnement : *« Abilities and skills cover all aspects of the driving task including environment and self perception, data processing, decision making, and behavior execution (Reschka et al., 2015)».*

Enfin, dans leur rapport, Staplin et al. (Staplin et al., 2018) emploient plutôt le terme « capabilities » pour ce qui est de l'identification des capacités attendues du VA. L'identification des « capabilities » s'appuie sur l'analyse des scénarios de conduite. Il s'agit d'identifier les dangers possibles dans les scénarios ainsi que les événements connus ou non, pour ensuite déduire les attendus souhaités vis-à-vis du VA. A titre d'exemple, nous pouvons noter les « capabilities » suivantes : Detect & Respond to Speed Limit Changes (Including



Advisory Speed Zones), Detect Passing and No Passing Zones, Detect & Respond to Stopped Vehicles, Detect & Respond to Intended Lane Changes/Cut-Ins, ...

Les performances fonctionnelles ainsi que les limitations associées évoluent selon la fonction d'automatisation considérée. Le tableau 5 synthétise les définitions retenues pour ces deux termes. Nous verrons plus loin leur identification dans le cas d'une fonction d'automatisation de type TJC (traffic Jam Chauffeur) qui sera également décrite.

Concepts	Définitions
<b>Performance fonctionnelle</b>	<ul style="list-style-type: none"> <li>• Une performance fonctionnelle désigne une capacité attendue du VA.</li> <li>• “A skill is an abstract description of an activity which the system has to provide to fulfill the intended task”(Bagschik et al., 2016)</li> </ul>
<b>Limitation de performance</b>	“insufficiencies in the implementation of the intended functionality” (ISO/PAS 21448, 2019)

Tableau 5 : Synthèse des définitions retenues pour la « performance fonctionnelle » et la « limitation de performance fonctionnelle ».

### 2.2.3 Définitions : Mode de fonctionnement et manœuvre opérationnelle du VA

La définition fournie par l'ISO 26262 permet de comprendre ce qu'est **un mode de fonctionnement** : « *operating mode: perceivable functional state of an item or element* ». L'exemple fourni par le standard pour soutenir cette définition permet de mieux comprendre les types de mode de fonctionnement que l'on peut avoir pour un système de type véhicule : « *EXAMPLE : System off; system active; system passive; degraded operation; emergency operation* ».

Dans le contexte du VA, le véhicule doit être totalement maître de la conduite notamment pour les niveaux d'automatisation élevés. Dans de telles situations, il faut que les modes de fonctionnement soient suffisamment complets pour couvrir tous les besoins de maîtrise de risque. Ainsi, comparé aux modes de fonctionnement classiques, de nouveaux modes ont été pensés selon le principe d'automatisation de la conduite et pour assurer une bonne sécurité du VA. La figure 8 est une machine à états correspondant à un exemple de modes de fonctionnement du VA. Sur cette figure, deux niveaux de définition des modes de fonctionnement ont été représentés. Au niveau 1, apparaissent, les modes suivants : Mode off ; Mode utilisation ; Mode maintenance\_Configuration.

- **Mode Off** : le système est hors service.
- **Mode utilisation** : le système est en cours d'utilisation.
- **Mode maintenance\_Configuration** : le système est en cours de maintenance.

Le niveau 2 correspond à des sous modes du mode utilisation. En effet, pendant son utilisation, la fonction d'automatisation possède d'autres modes à savoir : Mode Init, Mode Available, Mode Active, Mode GiveBack, Mode SafeState\_MRM.

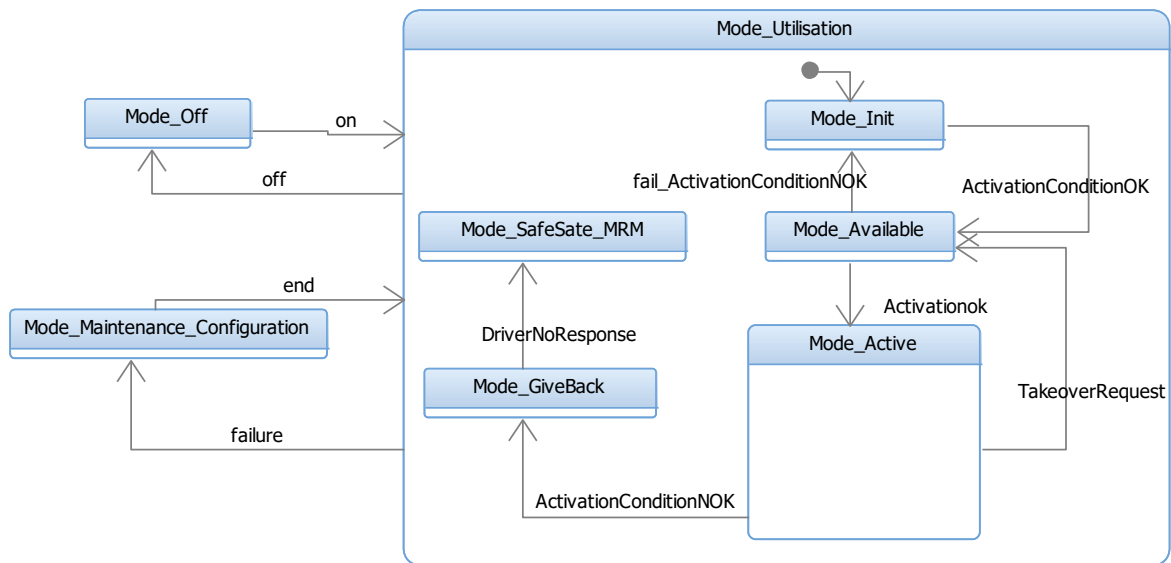


Figure 8 : Exemple de machine à états illustrant les différents modes de fonctionnement du VA

- **Mode Init** : le système est en cours d'initialisation, il attend que les conditions d'activation de la fonction d'automatisation soient disponibles.
- **Mode Available** : le système est dans ce mode lorsque les conditions d'activation sont disponibles (Enclenchement de la transition **ActivationConditionOK**).
- **Mode Active** : c'est le mode dans lequel le système se trouve lorsque la fonction d'automatisation est activée (après enclenchement de la transition **ActivationOK**). La transition **TakeoverRequest** correspond à une demande de reprise en main du VA par le conducteur, ce qui fait revenir le VA dans le mode précédent (Mode Available).
- **Mode Give back** : le système rentre dans cet état lorsque la fonction ne peut plus garantir son fonctionnement nominal, soit les conditions de disponibilité ne sont plus remplies, soit une défaillance est détectée (après enclenchement de la transition **ActivationConditionNOK**).
- **Mode SafeState\_MRM (Minimum Risk Manoeuvre)** : Ce mode correspond à une réduction du risque dans le cas où le conducteur ne répond pas à une demande de reprise en main. Il peut s'agir d'une phase de décélération du véhicule.

Cette description nous a permis d'identifier quelques modes de fonctionnement du VA. Cependant, une fois que le système est activé (mode actif), il faut que le véhicule soit capable d'effectuer la dynamique requise (déplacement) pour se déplacer dans son environnement. Cela nous conduit à analyser le deuxième concept qui est la manœuvre opérationnelle.

Une **manœuvre opérationnelle** peut se définir comme étant le comportement ou le déplacement observable du véhicule après l'exécution d'une ou de plusieurs actions. Nous retenons, ainsi, la vision de la manœuvre telle que mentionnée par Bach et al. (Bach, Otten, & Sax, 2016) : « *The presented approach defines maneuvers as an abstract definition of actions*

». Dans la littérature, des listes de manœuvres ont été identifiées. D’abord, Nagel et al. (Nagel, Enkelmann, & Struck, 1995) ont proposé une liste de 17 manœuvres. Cette liste a longtemps servi de point de départ pour de nombreuses autres analyses autour des manœuvres. En effet, dans le cadre d’une expérience pour la reconnaissance automatique de manœuvres, Gerdes (Gerdes, 2006) a sélectionné à partir de la liste de Nagel et al., 10 manœuvres (cf. tableau 6) qu’il considère comme étant mutuellement exclusives. Certaines de ces manœuvres se retrouvent également dans les propositions plus récentes faites dans le cadre du VA. En effet, Hungar et al. (Hungar, Köster, & Mazzega, 2017) proposent une liste de manœuvres qui est explicitement assimilée à une liste de scénarios fonctionnels. Cette liste est supposée regrouper l’ensemble des scénarios de haut niveau auxquels le véhicule peut être confronté. Enfin, la dernière liste que nous mentionnerons est celle donnée par Staplin et al. (Staplin et al., 2018). Ils ont proposé une liste de manœuvres tactiques et opérationnelles pour les ADS (Automated Driving Systems). Cette liste (Cf. tableau 7) est censée être générique de sorte à couvrir également les manœuvres associées à des systèmes de niveaux d’automatisation élevés (4 ou 5).

Les manœuvres décrites dans les propositions précédentes sont intéressantes et peuvent être utilisées pour décrire le comportement du VA. Cependant, dans la liste de Staplin et al., certaines manœuvres (Navigate Roundabouts, Navigate On/Off-Ramps, ...) sont trop attachées à l’ODD ou à des situations génériques, et non pas à la réaction du VA. Quant à la liste de Gerdes, les 7 premières manœuvres sont intéressantes car traduisent le comportement du VA tandis que les deux dernières sont dépendantes de l’ODD. Or, pour un souci de maîtrise de la complexité, nous souhaitons, avoir des manœuvres élémentaires qui traduisent exclusivement la manière dont se comporte un véhicule. Ces manœuvres doivent être, à l’instar de la proposition de Gerdes (Gerdes, 2006), mutuellement exclusives. Ainsi, bien que les listes précédentes s’appliquent au contexte du VA, certaines manœuvres restent assez génériques et ne respectent pas le principe d’exclusion souhaité.

1. Stopped
2. Follow road
3. Follow car
4. Turn left
5. Turn right
6. Merge left
7. Merge right
8. Overtake
9. Enter freeway
10. Exit freeway

Tableau 6 : Liste des manœuvres proposée par Gerdes et al. (Gerdes, 2006)

1. Parking
2. Maintain Speed
3. Car Following
4. Lane Centering –
5. Lane Switching/Overtaking
6. Enhancing Conspicuity
7. Obstacle Avoidance
8. Low-Speed Merge
9. High-Speed Merge
10. Navigate On/Off-Ramps
11. Right-of-Way Decisions
12. Follow Driving Laws
13. Navigate Roundabouts
14. Navigate Intersection
15. Navigate Crosswalk
16. Navigate Work Zone
17. N-Point Turn
18. U-Turn
19. Route Planning

Tableau 7 : Liste des manœuvres tactiques et opérationnelles des ADS proposée par Staplin et al. (Staplin et al., 2018).

De ce fait, nous avons défini deux critères pour nous aider à identifier et à faire le choix des manœuvres opérationnelles qui seront exploitées dans le cadre de la génération des scénarios. Ce sont les critères d'unicité et de complétude.

- **Critère 1** : Règle d'unicité => une manœuvre n'est pas incluse dans une autre.
  - Les conditions de validité des manœuvres sont différentes.
  - Le VA fait toujours un contrôle latéral et un contrôle longitudinal pour accomplir chaque manœuvre.
  - Nous considérons que par défaut avant et après l'intention d'exécution d'une manœuvre quelconque, le VA est dans sa voie et maintient sa vitesse : Keep lane/Lane centering and Regulate speed/Maintain speed
- **Critère 2** : Règle de complétude => Tout scénario de déplacement du VA est une combinaison de ces manœuvres.

A l'aide de ces deux critères, nous avons analysé les listes de manœuvres précédemment mentionnées et avons défini une nouvelle liste qui sera exploitée par la suite pour la génération des scénarios. Cette liste est présentée dans le tableau 8. A noter que ces manœuvres opérationnelles ne peuvent être observées que lorsque nous sommes dans l'un des modes suivants : Mode Active, Mode Give back, Mode SafeState\_MRM.

Modes dans lesquels l'observation des manœuvres est possible	Liste des manœuvres opérationnelles
Mode Active, Mode Give back, Mode SafeState_MRM	1. Follow road
	2. Follow a target/ Car Following
	3. Stopping
	4. Braking (manœuvre d'urgence)
	5. Lane Changing Left (LCL)
	6. Lane Changing Right (LCR)
	7. Lane Biasing
	8. Turning Left (TL)
	9. Turning Right(TR)
	10. Overtaking
	11. In Reverse movement
	12. Merging-to-left-lane
	13. Merging-to-right-lane
	14. U-turn-to-the-left
	15. U-turn-to-the-right
	16. N-Point Turn

Tableau 8 : Liste des manœuvres opérationnelles

Comme nous pouvons le constater ces manœuvres opérationnelles s'appliquent aussi bien au VA qu'aux autres véhicules.

Toutefois pendant notre analyse, nous avons constaté que certains des véhicules présents dans l'environnement opérationnel, ont des manœuvres ne résultant pas d'un comportement normal attendu. Ce constat a été également observé par Deo et al. lors de la classification des manœuvres et la prédiction des mouvements des véhicules autour du VA sur autoroute (Deo, Rangesh, & Trivedi, 2018). En effet, parmi les 10 manœuvres retenues, figurent les manœuvres « Cut-ins » et « Drift into ego lane » :

- « *Cut-Ins: Cut-ins involve a surround vehicle passing the ego vehicle and entering the ego lane in front of the ego- vehicle.* »
- « *Drift Into Ego Lane: Another important maneuver class is when a surround vehicle drifts into the ego vehicle lane in front or behind the ego vehicle.* »

Non seulement ces manœuvres n'apparaissent pas dans les listes précédentes, mais en plus, elles sont éprouvantes pour le VA car il doit s'adapter pour garantir la sécurité et éviter tout risque de collision.

Nous proposons de systématiser l'identification de telles manœuvres car elles sont des exemples de déviations et doivent être considérées afin de tester la réaction du VA face à de telles situations. Le tableau 9 illustre ces manœuvres déviantes.

Manœuvres opérationnelles déviantes
1. Cut-in left
2. Cut-in right
3. Cut through
4. Drift into Ego lane in front
5. Drift into Ego lane to rear of the Ego

Tableau 9 : Manœuvres opérationnelles déviantes d'autres usagers

Cette section a permis de définir les concepts en lien avec une fonction d'automatisation donnée à savoir : ODD, Use case, Test case, Performance fonctionnelle, limitation de performance, mode de fonctionnement et manœuvre opérationnelle.

La spécification de l'ensemble de ces éléments permet de caractériser la fonction d'automatisation concernée. Leur identification repose non seulement sur les travaux existants mais aussi sur les résultats de roulage, du profil de mission et de l'analyse d'experts. Toutefois, cela n'est pas suffisant pour pouvoir spécifier les scénarios auxquels sera soumis un VA. En effet, il faut également fixer les concepts liés à la définition d'un scénario.

### 2.3 DEFINITION DES CONCEPTS LIES AU SCENARIO

Comme indiqué précédemment dans la section 1 de ce chapitre, il est difficile de se positionner sur l'une des définitions proposées pour le concept de scénario. Nous proposons donc comme alternatives quelques définitions qui permettent de remédier aux points de blocage évoqués. En effet, la définition que nous proposons pour le scénario est basée sur celle de la situation opérationnelle ; et implique donc le caractère stable que peuvent avoir les éléments de l'environnement tel que cela transparait dans la réalité. Il met également en évidence un niveau d'abstraction qui permet de s'assurer que nous agrégeons les événements importants qui pourraient se produire pendant la phase d'exploitation du VA.

Avant de définir le scénario, nous allons d'abord définir le concept de « situation opérationnelle ». La situation opérationnelle dépend des entités avec lesquelles le VA est en interaction. Une entité correspond à une catégorie d'éléments existant dans l'ODD du VA (éléments environnementaux (luminosité, pluie, ...), éléments de l'infrastructure (Chaussée, panneaux, ...), Objets-Acteurs (dynamique ou statique)).

Dans la suite des travaux, nous appellerons « *entité* » l'une des catégories suivantes : Infrastructure, Autres usagers, Conducteurs/Passagers, Conditions atmosphériques (ou climatiques), VA.

- Nous considérons qu'« *une entité* » est caractérisée par des paramètres qui peuvent prendre leurs valeurs dans différentes plages de valeurs.

A noter que dans la littérature, pour désigner le VA d'intérêt, le terme Ego\_Véhicule est habituellement utilisé.

Ainsi, nous définissons la situation opérationnelle comme suit :

- **Situation opérationnelle** : Ensemble des états du VA et des autres entités d'un environnement opérationnel présentes pendant un laps de temps, défini par la stabilité de ces états.
  - Un état correspond à un ensemble de valeurs prises par les paramètres caractérisant l'entité considérée.
  - Un état est dit stable (stationnaire) si les paramètres le décrivant restent dans une plage de valeur limitée, permettant de maintenir le même comportement.
  - Dans un état donné, le VA a un certain comportement correspondant aux actions réalisées.
  - « L'environnement est défini comme tout ce qui est susceptible d'influencer ou d'être influencé par le système. » (AFIS, 2009)

Ensuite, un événement peut se produire dans une situation et exiger ou non une réaction du VA. L'association d'un événement à une situation initiale et la nécessité pour le VA de réagir ou non, décrivent un scénario, que nous définissons comme suit :

- **Scénario** : Description, dans un intervalle de temps donné, de l'enchaînement temporel de situations opérationnelles. Le passage d'une situation (initiale) à une autre (intermédiaire, puis finale) est causé par un ou plusieurs évènements.
  - **Évènement** : Modification de l'état d'une ou plusieurs entités de l'environnement (VA et autres) qui induit, peut induire ou doit induire une nouvelle action de la part du VA (nouveau comportement). Un paramètre a pris une valeur différente de sa valeur initiale.
  - **Action** : Réaction du VA à la suite d'un évènement (définition proposée selon la perspective du VA)

La figure 9 est une illustration de la description d'un scénario, se déroulant en ville ('Infrastructure'), par temps ensoleillé ('Conditions atmosphériques').

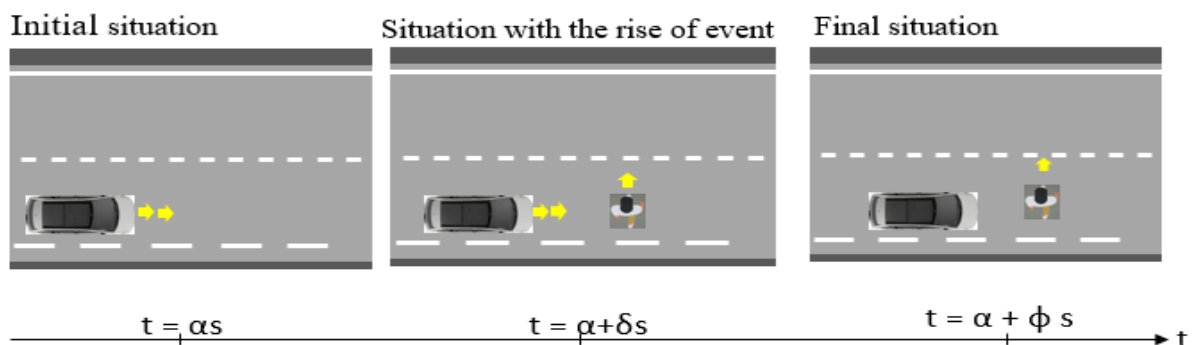


Figure 9 : Un exemple de scénario

Le scénario décrit l'évolution de la situation opérationnelle pendant la durée  $\Phi$  (en seconde, s) dans l'intervalle  $[t_1 = \alpha s, t_2 = (\alpha + \Phi) s]$ .

- A  $t = \alpha s$ , le VA est en roulage (voir Figure 9). A noter que cette situation initiale est caractérisée par différents paramètres, par exemple : ‘Nombre d’usagers’ (de l’entité ‘Autres usagers’) = 0 ; ‘Manoeuvre\_Ego’ = Follow Road, ‘Vitesse\_Ego’ = 40km/h, ‘Position\_Ego sur la chaussée’ = voie de droite.
- A  $t = \alpha + \delta s$ , un piéton traverse la voie du VA à une distance  $d = \beta$  (en mètre, m) de ce dernier, ce qui correspond à un évènement puisqu’il y a une modification de l’état ‘Autres usagers’ (Entité ‘Autres usagers’ = piéton, paramètres : ‘Nombre d’usagers’ = 1, ‘Position’ = voie VA, ‘Distance’ =  $\beta m$ , ‘Vitesse’ = 4km/h, ‘Direction’ = perpendiculaire à celle du VA, ...).
- A  $t = (\alpha + \Phi) s$ , le VA freine jusqu’à l’arrêt (Action) et se retrouve à une distance  $d = \theta m$  du piéton. => Evolution de la situation opérationnelle via une modification de l’état ‘Comportement du VA’. (Entité VA, paramètres : ‘Manoeuvre’ = Stopping, ‘Vitesse\_Ego’ = 0, ‘Position sur la chaussée = voie de droite ...)

Si la distance  $d$  est inférieure à une distance de sécurité, il y a risque de collision. Dans cette situation, on attend que le VA réagisse en conséquence, en particulier, avec un freinage d’urgence (manœuvre Braking). Evidemment, d’autres paramètres doivent être précisés pour caractériser la situation.

Par ailleurs, bien que nous ayons mentionné la présence de paramètres dans l’ODD et leur utilisation pour la description des scénarios, il faut procéder à leur identification de façon pertinente en vue de savoir comment cette utilisation se fera (quels paramètres il va falloir faire évoluer ou non). La section suivante fait état de cet aspect.

## 2.4 DETERMINATION DES PARAMETRES DE LA GENERATION

Tout d’abord, le VA (selon la fonction d’automatisation dont il est équipé) est supposé évoluer dans un environnement cible qui est son ODD. Cet ODD est caractérisé par des paramètres qui permettent de l’identifier et d’utiliser le véhicule uniquement dans ce dernier. Ensuite, tout au long de son utilisation dans son ODD, le VA sera amené à exécuter des manœuvres opérationnelles ou à être confronté aux manœuvres opérationnelles d’autres usagers. Comme déjà souligné, chaque manœuvre caractérise un scénario fonctionnel et des critères de validité permettent de la spécifier et de la distinguer d’une autre. Ces critères représentent en quelque sorte des contraintes à respecter pour que le scénario fonctionnel (ainsi que les scénarios concrets qui en découlent) soient valides.

Prenons l’exemple d’un scénario de Car Following. Il met en situation deux véhicules Ego et Lead, positionnés dans la même voie, et le Lead se trouve devant l’Ego. L’Ego roule à une vitesse  $V_{Ego}$  tandis que le Lead roule à une vitesse  $V_{Lead}$ . Les paramètres caractérisant ce scénario de car Following sont les suivants :

- *Présence Lead*
- *Interdistance (Ego-Lead) > D safe exprimé en seconde (2 s)*



En outre, alors que la situation fonctionnelle reste une spécification de haut niveau, la situation logique, elle, est une déclinaison possible de la situation fonctionnelle. Cette déclinaison se traduit à la fois en espace et en temps grâce à certains paramètres. Si l'on se réfère à la description des connaissances en cinq couches, proposée par Bagschik et al. (Bagschik et al., 2018), les éléments variables appartiennent à la quatrième couche. Il s'agit des interactions entre les objets dynamiques (à savoir les participants du trafic). Comme mentionné par ces derniers, d'autres interactions existent avec les autres couches notamment avec l'Infrastructure mais aussi avec la météo. Etant donné que nous voulons évaluer les performances fonctionnelles du VA d'un point de vue SOTIF et ce, dans différentes configurations de situations, tout élément pouvant influencer de telles performances doit être pris en compte. Ainsi, les influences de l'infrastructure, de la météo et du conducteur doivent être prises en compte.

Ainsi, les *paramètres de variabilité du scénario* sont des paramètres dynamiques des usagers présents, tels que la position, la vitesse, l'accélération, le temps, ... ou encore ceux liés à la météo ou au trafic qui eux aussi subissent des évolutions en espace et en temps dans le scénario. De ce fait, les *invariants du scénario* sont des paramètres qui n'évoluent pas tout au long de la durée du scénario. Ils se composent des *invariants de l'ODD*.

Par exemple, dans l'ODD du TJC (Traffic Jam Chauffeur), il est spécifié que l'infrastructure est de type « Voies à chaussée séparée ». Le paramètre indiquant le type d'infrastructure est un invariant pour cet ODD. Enfin, il est à noter que les éléments de l'ODD (notamment le type d'infrastructure) font partie des premiers éléments qui permettent de caractériser un scénario.

D'autre part, nous avons fait une proposition particulière pour ce qui est de la position des autres usagers autour du VA « Position\_AutreVehicule.i ». En effet, comme le VA est le système sous test, il représente l'élément de référence en fonction duquel les autres éléments seront décrits. Aussi, la portée des capteurs du VA et le besoin de le stimuler par le biais d'éléments pouvant influencer son comportement, nous pousse à ne considérer dans chaque situation opérationnelle que son environnement immédiat. De ce fait, nous décomposons cet environnement immédiat sous forme de zones géographiques, définissant chacune une position pouvant être occupée par un autre usager autour du VA. La figure 10 présente les 8 positions identifiées : Left (1), Front Left (2), Front (3), Front Right (4), Right (5), Rear Right (6), Rear (7), Rear Left (8). Chaque position peut avoir deux valeurs : soit elle est occupée par un usager et prend la valeur « Vrai », soit elle n'est pas occupée et prend la valeur « Faux ». Ainsi, « Position\_AutreVehicule.i » signifie que l'autre véhicule occupe la position N°i (i varie de 1 à 8) et « Position\_AutreVehicule.i » prend donc la valeur vraie.

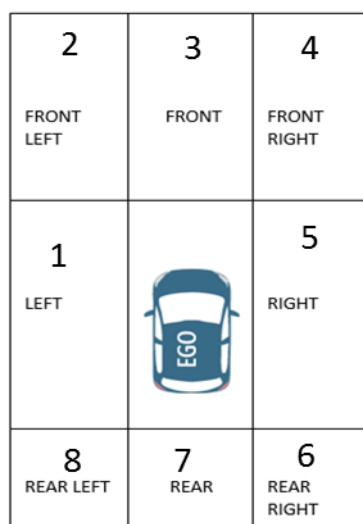


Figure 10 : Cartographie de l'environnement immédiat autour du VA

Plusieurs concepts ont été introduits dans ce chapitre : ODD, Cas d'utilisation, Performance fonctionnelle et Limitation de performance), Manœuvre opérationnelle (et mode de fonctionnement), Scénario, Situation, Evènement, Action. La section suivante propose un modèle de connaissance pour regrouper l'ensemble de ces concepts.

## 2.5 MODELE DE CONNAISSANCE POUR LA GENERATION DE SITUATIONS ET DE SCENARIOS

En vue d'avoir une vue opérationnelle de l'utilisation des concepts introduits et de vérifier l'existence d'une cohérence entre ces derniers, nous proposons également d'établir un modèle de connaissance (Figure 11) qui s'appuie sur l'ensemble de ces concepts. Ce modèle de connaissance (ou modèle conceptuel) utilise le langage de modélisation UML (Unified Modelling Language) et plus particulièrement, le diagramme de classes. Parmi les classes représentées, une partie représente les entités de l'environnement opérationnel du VA tandis qu'une autre, permet au travers d'une abstraction de représenter les concepts opérationnels de la génération à savoir : Scénario, Situation, Evènement. L'ensemble du modèle représente les concepts clés pour modéliser un scénario.

La classe `op_scenario` représente le scénario opérationnel qui est la résultante de la situation opérationnelle et de l'évènement. Un évènement (classe `Event`) peut provenir d'une ou de plusieurs sources (classe `Event_source`). Les sources d'évènements ne sont autres que les différentes entités présentes dans la situation.

On retrouve également dans ce modèle, les éléments caractérisant l'ODD (`Physical_infrastructure`, `Other_Road_User`, `Weather_Condition`) du VA pour la fonction d'automatisation considérée. Quant à la situation opérationnelle, elle dispose au minimum d'une infrastructure physique, peut contenir zéro ou plusieurs usagers et a au moins une condition climatique spécifiée tandis qu'une infrastructure physique, un usager ou une

condition climatique donnée n'appartiennent qu'à une situation opérationnelle. La classe Ego\_V représente le VA et intègre les manœuvres et modes opérationnels autorisés pour ce dernier. L'Ego\_V dispose au maximum d'un conducteur et peut ne pas avoir de passagers.



## 2.6 DISCUSSION

De nombreux concepts en lien avec le VA et son usage dans l'environnement existent dans la littérature. Cela crée une confusion dans les échanges. Se positionner sur certains choix ou définir clairement les concepts que nous emploierons dans le cadre de ce mémoire, vise à supprimer toute ambiguïté et à en faciliter la compréhension.

Dans les travaux recensés ou analysés, la description du scénario utilise parfois le concept de scène. Ce concept de par sa définition, intègre de nombreux éléments de l'environnement et les décrit comme étant figés. Contrairement à cela, la définition du scénario (élémentaire) que nous proposons permet d'une part d'intégrer l'état du VA dans la description du scénario, et d'autre part, de limiter cette description aux éléments clés (une situation initiale et un évènement voire plusieurs évènements se déroulant dans le même intervalle de temps) pouvant susciter une réaction du VA.

En outre, nous avons choisi de formuler les entités en cinq (5) catégories distinctes d'éléments. Cette catégorisation a été motivée par un souci de définir clairement des catégories de sources distinctes à partir desquelles l'on pourrait générer les évènements nécessaires pour tester le VA. D'autres catégorisations peuvent être adoptées notamment la structuration en cinq couches définies par (Bagschik et al., 2018) ou encore celle en trois entités : « The driver, the vehicle with the automated driving system and the traffic environment » proposée par (Aptiv et al., 2019).

Par ailleurs, l'analyse faite sur les paramètres indique qu'il existe certains d'entre eux qui sont invariants dans la génération des scénarios et d'autres qui ne le sont pas. De plus, il faut souligner la présence d'incertitude liée à ces paramètres. D'abord, il y a la présence de l'incertitude épistémique parce que l'on peut oublier des entités clés de l'environnement ou des paramètres les décrivant. Puis, il faut tenir compte de l'incertitude aléatoire car on se rend compte qu'on ne connaît pas à l'avance les situations réelles qui seront rencontrées.

Enfin, bien que certains auteurs aient noté l'existence de manœuvres relevant d'un mauvais comportement des autres usagers présents dans l'environnement, leur identification n'est pas systématique. La nécessité de garantir un niveau de sécurité élevé pour le VA, exige de le tester en présence d'usagers ayant de telles manœuvres et implique donc de systématiser leur identification.

## 2.7 CONCLUSION

Le présent chapitre nous a permis de définir les concepts qui seront utiles par la suite pour définir la méthodologie de génération des scénarios de validation du VA en répondant à la question :

### **Comment spécifier les concepts clés de la génération des scénarios ?**

Ces concepts sont nombreux et au vu des nombreuses définitions, il a fallu soit se positionner sur certains choix, soit proposer de nouvelles définitions. Ainsi, deux catégories de concepts ont été abordées : celle liée à l'usage du VA et à son environnement opérationnel et celle liée

au concept de scénario lui-même. En outre, nous avons synthétisé l'ensemble de ces concepts et leurs relations dans un modèle de connaissance.

Cependant, la définition des concepts n'est pas suffisante pour définir la stratégie de génération des scénarios et de validation par simulation du VA. En effet, il faut disposer des indicateurs qui vont permettre de guider et de juger de la pertinence, voire de la performance, de cette stratégie. Le chapitre suivant propose une synthèse sur les indicateurs manipulés dans la littérature, ainsi que ceux, que nous retiendrons pour la stratégie de génération qui sera proposé.

---

## CHAPITRE 3. STRUCTURE ET INDICATEURS DE PERFORMANCE D'UN SYSTEME DE GENERATION DE SCENARIOS ET DE VALIDATION PAR SIMULATION DE LA SECURITE DU VA

---

Kalra et paddock (Kalra & Paddock, 2016) ont démontré l'impossibilité de se limiter uniquement aux tests de roulage pour la validation du VA en terme de fiabilité et de sécurité. L'indicateur à la clé de cette démonstration est le nombre de kilomètres à parcourir pour obtenir cette validation du VA, à savoir des milliards de kilomètres. Cela apparaît donc comme une justification supplémentaire pour recourir à la fois à une approche basée sur les scénarios et plus spécifiquement à une approche basée sur la simulation pour la validation du VA. Par ailleurs, comme l'ont si bien soulignée Lakomicki et al. (Paula Lakomicki, Tourbier, Castanier, & Grall, 2019), la raison pour laquelle la méthode de validation par roulage n'est pas pratique d'un point de vue « Safety » est qu'elle privilégie les conditions de roulage les plus fréquentes ne présentant pas de risques. De ce fait, il est attendu de la validation par simulation basée sur des scénarios, de pouvoir remédier à cet inconvénient, en générant aussi bien des scénarios de roulage fréquents que des scénarios rares mais potentiellement critiques. L'objectif étant ainsi, de contribuer à la démonstration de la « Safety Of The Intended Functionality (SOTIF) » pour un VA d'un niveau d'automatisation donné.

De ce fait, il importe de se demander quels indicateurs permettront de mesurer la performance de la génération des scénarios et de la validation par simulation de la sécurité du VA. En effet, bien que certains indicateurs existent dans la littérature, pris individuellement, ils demeurent insuffisants pour garantir le niveau de performance recherché dans le contexte du VA.

Ce chapitre 3 vise à répondre à ce besoin en répondant à la question suivante :

**Quelle structure de système et quels indicateurs vont permettre de guider et de juger de la pertinence, voire de la performance, de la stratégie de génération et de validation par simulation de la sécurité du VA ?**

Nous ferons en premier lieu, un état de l'art pour analyser les indicateurs utilisés jusqu'ici dans le contexte de la génération de scénarios et de validation pour le VA. Puis, nous proposerons et définirons les indicateurs sur lesquels nous souhaitons nous appuyer dans ce travail de thèse. Pour ce faire, nous mettrons en place plus globalement, la structure du système de génération des scénarios et de validation par simulation de la sécurité du VA, ainsi que la manière dont les indicateurs seront exploités dans cette structure.

Ces indicateurs serviront par la suite (dans le chapitre suivant) à définir et orienter la stratégie de génération et de simulation que nous jugerons pertinente pour la validation de la sécurité (safety) du VA.

### 3.1 ETAT DE L'ART SUR LES INDICATEURS DE PERFORMANCE DE LA GENERATION DE SCENARIOS ET LA VALIDATION PAR SIMULATION DE LA SAFETY DU VA

Différents indicateurs de performance (ou critères, métriques) ont déjà été proposés dans la littérature pour mesurer la performance des tests réalisés. Dans cette section, nous allons introduire les concepts clés, comme la couverture de test, l'indicateur de distance, la probabilité d'accident ou plus généralement, le risque associé à un scénario.

Dans le contexte de l'ingénierie du logiciel, *la couverture de test* (Test coverage) est l'indicateur couramment utilisé pour mesurer la performance des tests réalisés. La couverture de test se définit comme suit : “ degree, expressed as a percentage, to which specified test coverage items have been exercised by a test case or test cases”(ISO/IEC/IEEE 29119-1: *Software and systems engineering--Software testing--Part 1: Concepts and definitions.*, 2013). Cette notion de couverture est également présente dans le cas de l'utilisation de scénarios pour la validation par simulation du VA. En effet, il faut justifier que les scénarios utilisés pour la validation par simulation du VA, couvrent bien l'ensemble de son environnement opérationnel. Une telle justification peut s'appuyer sur le fait que le roulage (en conditions réelles) contient des « temps morts » non utiles à la validation alors que l'utilisation des scénarios permet de se concentrer uniquement sur ce qui est pertinent d'un point de vue validation. Aussi, l'utilisation de scénarios permet la création de nouveaux scénarios par combinaison et en faisant varier les paramètres les décrivant. Cependant le nombre important de paramètres d'influence crée une explosion combinatoire qui rend impossible le test de tous les scénarios possibles (Amersbach & Winner, 2019a). Il est donc nécessaire de définir des scénarios pertinents pour la validation du VA.

Pour ce faire, Amersbach et Winner (Amersbach & Winner, 2019a) ont proposé une équivalence à *l'indicateur de distance* proposé par Kalra et Paddock. Il s'agit, pour une cible de distance à parcourir pour la validation du VA (selon la fonction d'automatisation qu'il intègre), de déterminer le nombre de scénarios à tester correspondant. Une fois ce nombre obtenu, à l'aide d'hypothèses (définissant notamment le facteur temps réel et le facteur de parallélisation pour la simulation), le nombre de scénarios qui peuvent être simulés est estimé. D'autres auteurs comme Zhou et Re (Zhou & Re, 2017) préfèrent directement recourir à l'indicateur de couverture du nombre de scénarios critiques en utilisant pour référence des bases de données dans lesquelles des milliers de scénarios sont enregistrés. Ici la base de données de référence qu'ils utilisent est la SHRP 2 NDS (The Second Strategic Highway Research Program (SHRP 2) Naturalistic Driving Study (NDS)) qui comprend 775 événements critiques sur les autoroutes. L'idée est de vérifier quel *pourcentage de scénarios critiques de la base de référence* a été couvert par les scénarios générés par Zhou et Re.

En outre, nous avons évoqué la présence d'un nombre important de paramètres concernés pour l'identification des scénarios. Ces paramètres ont des plages de valeurs continues ou discrets. Ce qui fait appel à un autre besoin qui est de procéder à un échantillonnage lors de la création des scénarios. Selon Jesenski et al. (Jesenski et al., 2019), il existe dans la littérature deux approches pour échantillonner : « Coverage-based sampling » et « Statistical sampling ». La première méthode vise à échantillonner autant de paramètres différents que possible et a pour indicateur *la couverture de tous les paramètres*. La seconde méthode cherche à montrer une évidence statistique (exemple la *probabilité d'accident*) concernant l'objet testé et a pour indicateur la variance des résultats statistiques de la simulation.



Pour répondre à leur objectif de générer avec une grande résolution un ensemble d'échantillons qui définissent les régions où les limites de performance du système se produisent, Mullins et al. (Mullins, Stankiewicz, Hawthorne, & Gupta, 2017) ont défini trois critères : « *Efficiency, Diversity, Scalling* ». Le premier critère « *Efficiency* » vise, comme son nom l'indique l'efficacité. Son but est d'identifier les limites de performances avec le plus petit nombre d'échantillons possible. Il est mesuré grâce aux trois métriques suivantes formalisées selon le contexte de leur travail : la précision, la convergence et la résolution. Ensuite, le critère de diversité « *Diversity* » vise à obtenir des scénarios représentatifs de toutes les limites de performance du système. Il se mesure également avec la couverture mais aussi avec les distributions des modes et des limites de performance. Enfin, le dernier critère « *Scalling* » aborde la question de l'extension de la proposition à une plus grande dimension en termes d'état de l'espace (dimension des données d'entrée) et de taille de l'ensemble des échantillons.

Pour rappel, la validation de la sécurité du VA est requise pour s'assurer de sa capacité à répondre, de façon sûre, à tous les scénarios auxquels il sera confronté, en particulier ceux identifiés comme potentiellement dangereux, et de vérifier si son propre comportement ne conduit à aucun événement redouté. De ce fait, il importe également de se demander comment mesurer et évaluer le caractère dangereux d'un scénario lors de la validation.

L'ISO 26262 évalue le *risque associé à un scénario* via la combinaison de la sévérité, de l'exposition et de la contrôlabilité : « combination of the probability of occurrence of harm (§1.56) and the severity (§1.120) of that harm ». Les termes sévérité, exposition et contrôlabilité se définissent quant à eux comme suit :

- « Severity: estimate of the extent of harm (§1.56) to one or more individuals that can occur in a potentially hazardous (§1.57) situation »
- « Controllability: ability to avoid a specified harm (§1.56) or damage through the timely reactions of the persons involved, possibly with support from external measures (§1.38) »
- « Exposure: state of being in an operational situation (§1.83) that can be hazardous (§1.57) if coincident with the failure mode (§1.40) under analysis »

Pour exprimer le risque dans le cas d'un scénario, Feng et al. et Hallerbach et al., nous proposent des définitions de la criticité d'un scénario :

- « Critical scenarios are defined as scenarios that need to be tested, regardless, whether the requirements are functional or non-functional » (Hallerbach et al., 2018).

Deux catégories de métriques sont utilisées pour l'évaluation des scénarios critiques : les métriques standards (time-to-collision, time-to-brake, required-deceleration) et de nouvelles métriques de qualité de trafic proposées par les auteurs.

- « The criticality of a scenario measures the importance in evaluating a performance metric » (Feng et al., 2020a). « Safety, Functionality, Mobility, Rider's comfort » sont les indicateurs de performance manipulés par les auteurs.

Par ailleurs, comme nous pouvons le constater dans le tableau 10, différentes métriques de « *Safety* » peuvent être utilisées lors des évaluations. Elles sont classées sur deux niveaux. Ainsi, les métriques au niveau microscopique seront privilégiées pour évaluer chaque scénario individuellement, tandis que lors de l'agrégation des résultats, une évaluation au niveau macroscopique devra être conduite.

	Metrics for accident severity	Metrics for criticality
microscopic	<ul style="list-style-type: none"> <li>• physical metrics (collision speed, ...)</li> <li>• physiological metrics (injury severity [5], ...)</li> <li>• economic metrics</li> </ul>	<ul style="list-style-type: none"> <li>• physical metrics (PET [57], WTTC [58], TTX (TTC [59], TTB [60], ...), headway, DCE [61], ...)</li> </ul>
	Metrics on accident cases	Metrics on all cases
macroscopic	<ul style="list-style-type: none"> <li>• injury rate [5]</li> <li>• fatality rate</li> <li>• ...</li> </ul>	<ul style="list-style-type: none"> <li>• accident rate [54]</li> <li>• prevention rate</li> <li>• conflict rate [5]</li> <li>• ...</li> </ul>

Tableau 10 : Différentes métriques de "Safety" (Jesenski et al., 2019)

En synthèse, les indicateurs de performance identifiés précédemment, résument l'idée qu'un scénario est critique s'il nécessite d'être testé pour mesurer la sécurité du VA. Toutefois, cette criticité ne peut se mesurer de façon effective qu'une fois la simulation effectuée et la réaction du VA observée. Par ailleurs, on sait que le nombre de scénarios à tester est très élevé et que l'identification de tous les scénarios critiques peut être lente. Pourtant, nous n'avons pas trouvé dans la littérature une métrique permettant d'orienter la génération de scénarios a priori, en identifiant au préalable les scénarios potentiellement critiques en vue de les tester en priorité. Aussi, ces indicateurs de performance identifiés ont le même objectif, à savoir, montrer que l'on arrive à un certain niveau de performance avec les éléments de test requis pour la validation du VA. Cependant, l'utilisation individuelle de chaque indicateur n'est pas pertinente pour atteindre l'objectif de démonstration de la sécurité du VA. En effet, nous estimons qu'une utilisation conjointe de plusieurs indicateurs peut avoir un impact significatif dans la performance de la génération de scénarios et la validation par simulation de la sécurité du VA. Ainsi, n'ayant pas trouvé de cadre d'évaluation de la safety reposant sur un ensemble cohérent d'indicateurs de performance, nous proposons dans la section suivante un ensemble d'indicateurs qui peuvent être utilisés conjointement, a priori et a posteriori, et qui permettront de juger de la performance de la stratégie de génération et de validation par simulation du VA.

### 3.2 STRUCTURE DU SYSTEME DE GENERATION DES SCENARIOS ET DE VALIDATION PAR SIMULATION DE LA SAFETY DU VA

La structure du système de génération de scénarios ainsi que les indicateurs de performance que nous proposerons visent à guider la manière d'identifier les scénarios pour évaluer la sécurité du VA dans le cadre du SOTIF.

Pour répondre à l'objectif de contribuer à la démonstration de la « Safety Of The Intended Functionality (SOTIF) » pour le VA, ce futur standard recommande l'utilisation systématique de la simulation (massive). Comme déjà évoqué, l'objectif visé par un tel processus de validation par la simulation massive est de réduire *le risque des scénarios dangereux connus* et de démontrer que le risque résiduel lié à des scénarios potentiellement dangereux inconnus est minime et acceptable. De ce fait, le besoin est de définir une stratégie qui génère un ensemble de scénarios critiques pour le VA, satisfaisant cet objectif.

La figure 12 synthétise la structure du système de génération des scénarios et de validation par simulation de la Safety du VA que nous retenons dans ce travail de thèse. Elle donne une vue globale de la chaîne de validation par simulation.

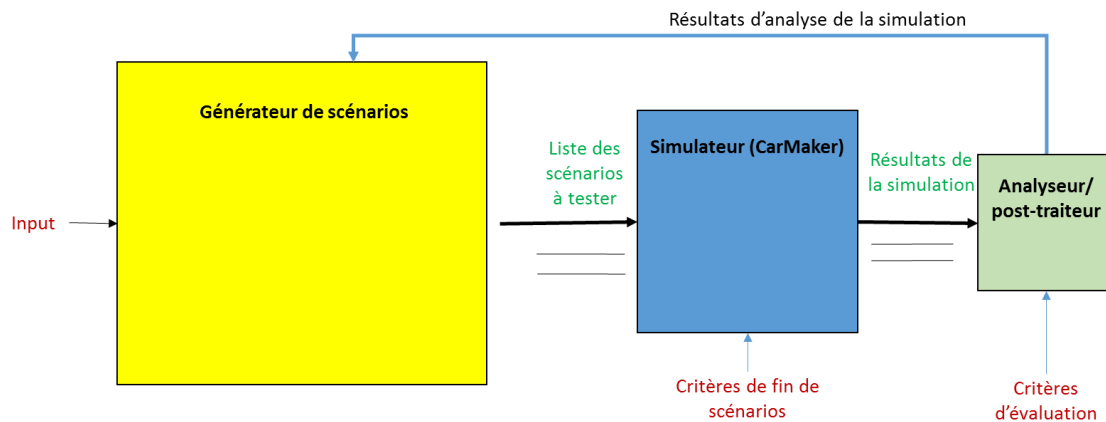


Figure 12 : Structure du système de validation par simulation massive

Cette chaîne se compose comme suit :

- **Le simulateur (en bleu)**

Le simulateur est utilisé pour simuler l'environnement opérationnel et le comportement du VA en vue de sa validation. De ce fait, il intègre l'ensemble des modèles des entités que l'on peut retrouver dans cet environnement :

- Modèle de comportement du VA (dynamique du véhicule, modèles des capteurs)
- Modèle de comportement des autres usagers (générateur de trafic)
- Modèles de l'infrastructure
- Modèle des conditions météorologiques
- Modèle du conducteur

Pour effectuer les simulations, le simulateur prend en entrée un ou plusieurs scénarios de tests, qu'il exécute ensuite. Des critères de fin de scénarios lui sont associés afin de déterminer quand arrêter la simulation d'un scénario. Le simulateur fournit en sortie des résultats de simulation qui seront analysés par un post-traitteur.

- **L'évaluation des scénarios à travers l'analyseur ou le post-traitteur (vert)**

L'analyseur peut être dans certains cas (et c'est ce qui se rencontre le plus souvent) directement intégré au simulateur. Il analyse les résultats des simulations en se basant sur des critères d'évaluation. Un critère d'évaluation représente ou découle d'une exigence que la fonction d'automatisation doit respecter. Un tel critère permet d'obtenir des indicateurs de performance de la fonction d'automatisation. Dans le cas de la validation de la sécurité du VA, il importe

d'être capable d'évaluer quand un scénario est critique ou pas. Pour ce faire, nous introduirons *un indicateur de criticité*. En outre, pour anticiper le besoin d'une classification plus fine des scénarios simulés, nous introduirons d'autres critères d'évaluation en lien avec les performances fonctionnelles de la fonction d'automatisation. Enfin, cette phase d'évaluation doit permettre, à l'issue de la validation, de mesurer le risque global associé à la fonction d'automatisation considérée. Nous proposons d'effectuer cette mesure via *l'indicateur de risque final*.

Par ailleurs, le niveau de confiance que l'on pourra accorder en la sécurité du VA sur la base des simulations est dépendant des incertitudes dont sont entachées l'ensemble des évaluations ou encore les ressources utilisées. Nous proposons donc d'en tenir compte lors de l'estimation du risque final associé au VA en introduisant un *indicateur de confiance*.

- **La boucle de retour entre l'analyseur et le générateur**

Cette boucle matérialise l'utilisation des résultats en cours obtenus par l'analyseur, pour améliorer la génération des scénarios de validation. En effet, devant le caractère ouvert et vaste de l'espace des scénarios, nous estimons que l'obtention d'une identification systématique de tous les scénarios critiques n'est pas évidente. Nous faisons l'hypothèse de la nécessité de recourir à un processus itératif basé sur les résultats de simulation pour l'amélioration de la recherche des scénarios pertinents mis en évidence par la simulation (lors du non-respect d'un critère d'évaluation).

- **Le générateur automatique de scénarios (en jaune)**

C'est le cœur du périmètre de cette thèse. Le générateur fournit l'ensemble des scénarios qui seront utilisés pour tester le comportement du VA. Pour permettre de structurer l'identification des scénarios de validation, et guider la stratégie de génération, la méthodologie proposée va s'appuyer sur plusieurs principes :

- La prise en compte des connaissances disponibles sur la fonction d'automatisation considérée, sur le véhicule équipé de la fonction et sur l'environnement opérationnel dans lequel elle sera déployée. Comme déjà mentionné, une telle approche de génération des scénarios à partir des connaissances disponibles est connue sous le nom de « knowledge-driven approach ». Cette connaissance fait ici référence au profil de mission, auquel s'ajoutent d'autres connaissances, notamment celles portant sur la sensibilité des organes de perception, décision et actions du VA. En effet, rappelons que le déploiement d'un VA se fera selon le profil de mission auquel son constructeur le prédestine : définition d'un domaine de fonctionnement opérationnel (ODD), spécification des fonctions, identification des aptitudes du conducteur... Bien que le profil de mission résulte en général d'un choix stratégique, les constructeurs expérimentés doivent s'appuyer sur leurs expériences passées, capitalisées et répertoriées sous formes de données lors des campagnes d'investigation. Toutes ces données permettent de mener ensuite d'une part, des analyses de risques, et d'autre part, des analyses statistiques qui fournissent des informations que nous jugeons exploitables dans le cadre de la stratégie de

génération qui sera proposée. De ce fait, le profil de mission représente l'information connue sur la réalité et sert à ce titre, de référence pour mesurer d'autres indicateurs : *la couverture et la représentativité statistiques*. En effet, un aspect important est de s'assurer que les scénarios générés pour la simulation sont crédibles et couvrent l'ensemble des paramètres de l'environnement opérationnel du VA qui ont été identifiés par le profil de mission : c'est bien l'intérêt de la mesure de l'indicateur de couverture. De plus, il faut que les répartitions statistiques associées au profil de mission se reflètent dans les tirages obtenus à la fin de la validation : c'est l'intérêt de la mesure de l'indicateur de représentativité.

- Le sur-échantillonnage des scénarios critiques. Rappelons que les scénarios les plus fréquents seront rencontrés et testés lors des phases de validation par roulage sur route. L'intérêt pour les constructeurs de la validation par simulation est avant tout de traiter l'ensemble des scénarios critiques possibles, même rares. Il apparaît évident que la méthodologie de génération des scénarios devra permettre de tester prioritairement des scénarios potentiellement critiques, sans pour autant négliger les autres pour s'assurer de la couverture et pour pouvoir calculer des indicateurs rapportés à une distance (ou un temps) de roulage, respectant le profil de mission.
- La structuration de la génération des scénarios en trois niveaux d'abstraction (fonctionnel, logique et concret) tels que proposés par Menzel et al. (Menzel et al., 2018). Une telle structuration permet de décliner les scénarios de façon progressive, en offrant une approche hiérarchique d'obtention des scénarios. De plus, même si on dispose de ce cadre structurel pour la génération, son opérationnalisation n'est pas immédiate. Il reste encore des questions auxquelles il faut apporter des réponses : comment définir les plages de valeurs des scénarios logiques, comment définir des indicateurs pour orienter la génération en fonction de la criticité potentielle des situations fonctionnelles ou logiques, ...

En résumé, le système de validation par simulation doit permettre de démontrer que le VA atteint les objectifs attendus de performances fonctionnelles, en particulier pour la sécurité. Pour mener à bien cet objectif, nous estimons que l'ensemble du processus à savoir la génération des scénarios requis, leur simulation ainsi que leur évaluation, doit s'appuyer sur un ensemble d'indicateurs : *un indicateur de criticité, un indicateur de risque final, un intervalle de confiance (prise en compte de l'incertitude), un indicateur de couverture statistique, un indicateur de représentativité statistique*.

Par ailleurs, de cette analyse, on voit ressortir deux aspects clés que nous abordons dans notre travail :

- la définition d'une heuristique de recherche et de génération des scénarios
- l'estimation de l'indicateur final de risque (**probabilité d'occurrence d'une situation critique pour le VA**)

Nous proposons dans la section suivante de procéder à l'analyse détaillée de l'ensemble des indicateurs.

### 3.3 DEFINITIONS ET MESURES DES INDICATEURS POUR LA GENERATION DES SCENARIOS ET LA VALIDATION PAR SIMULATION DU VA

Cette partie vise à montrer comment nous souhaitons mesurer chacun des indicateurs identifiés précédemment.

#### 3.3.1 Indicateur de couverture

Le profil de mission (PM) auquel est prédestinée chaque fonction d'automatisation est connu d'avance grâce aux expériences passées. Cela permet de disposer d'une référence pour ce qui est de la réalité (ou de la connaissance réelle) de l'environnement opérationnel considéré. Toutefois, bien que cela ne fasse pas partie du cadre de la thèse, il faut noter que l'obtention de ce profil de mission de référence n'est pas facile. Par exemple, il faut veiller à couvrir l'ODD de la fonction et à agréger suffisamment d'information.

L'indicateur de couverture se mesure ici en référence au profil de mission. La couverture vise à s'assurer que l'ensemble des scénarios générés pour la simulation couvre bien l'ensemble des paramètres de l'environnement opérationnel du VA qui ont été identifiés grâce au profil de mission. En d'autres termes, l'indicateur de couverture aide à répondre à la question « tous les paramètres du PM sont-ils pris en compte dans la génération ? » Couvrir l'ensemble des paramètres permet de couvrir une variété de scénarios. Par ailleurs, nous avons évoqué le fait que la stratégie de génération que nous souhaitons élaborer s'alignera sur la structuration en trois niveaux d'abstraction : scénarios fonctionnels, logiques puis concrets. Dans cette structuration, alors que les scénarios fonctionnels sont décrits à un niveau linguistique, les scénarios logiques eux, sont déduits en paramétrisant les scénarios fonctionnels et en spécifiant leurs plages de valeurs et cela, grâce au profil de mission. De ce fait, mesurer l'indicateur de couverture revient à déterminer le pourcentage de scénarios logiques explorés lors de la phase d'obtention des scénarios concrets à simuler, par rapport au nombre total de scénarios logiques. Ainsi, en générant au minimum un scénario concret à partir de chaque scénario logique, le PM sera couvert à 100%. Toutefois, rappelons que le nombre important de paramètres et l'étendue de leurs plages de valeurs créent une explosion combinatoire qui impose de bien choisir le pas de discrétisation ou encore la loi d'échantillonnage lors de la génération des scénarios concrets. Cet aspect sera étudié dans le chapitre 4 lors de la spécification de la stratégie de génération.

#### 3.3.2 Indicateur de représentativité des scénarios concrets générés

Le profil de mission nous permet de disposer de connaissances sur les répartitions statistiques des valeurs des paramètres décrivant l'environnement opérationnel. L'indicateur de représentativité vise à vérifier si une telle répartition des valeurs pour un paramètre donné, se reflète dans les tirages effectués lors de la génération en répondant à la question suivante : « les scénarios concrets générés et simulés sont-ils représentatifs du profil de mission ? ». Une telle évaluation peut être faite à l'aide d'un test du khi deux d'adéquation en vérifiant si l'échantillon de valeurs tirées pour chaque variable aléatoire contenue dans la génération, donne des

observations comparables à celles de sa distribution de probabilité définie a priori (dans le profil de mission). (Laurencelle, 2012).

Cependant, si une plage de valeur est continue, et que pour un scénario concret, on tire une valeur aléatoire sans préciser de pas de discrétisation, alors il y aura une infinité de scénarios concrets possibles. Cette infinité de scénarios concrets crée une explosion combinatoire qui empêche de tester tous les scénarios concrets compte tenu du temps élevé de simulation que cela prendrait. De plus, même si l'on venait à le faire, cela consommerait un temps important de la validation sans nécessairement apporter d'information supplémentaire à l'estimation du niveau de risque associé au VA. Toutefois, le souci de garantir une représentativité de la génération vis-à-vis de la clientèle cible, est une raison nécessaire et suffisante de garantir l'atteinte de cet indicateur. Ainsi, nous proposons de vérifier l'atteinte de cet indicateur en dernier lieu, c'est-à-dire, à l'issue de l'estimation du risque final associé au VA et au besoin, d'effectuer des tirages supplémentaires pour atteindre un objectif de représentativité fixé.

### 3.3.3 Indicateurs de criticité et de sensibilité

Les stratégies de génération de scénarios dans le cadre du processus de validation par simulation du VA sont principalement basées sur une analyse a posteriori de la criticité. En effet, c'est au cours de la simulation, et après analyse des résultats que les scénarios critiques sont identifiés. Pourtant, l'analyse des scénarios ne vise pas uniquement à vérifier si le comportement du VA ne mène à aucune situation critique. Elle est également nécessaire pour identifier les scénarios pertinents en vue d'optimiser le processus de validation et de s'assurer que les scénarios potentiellement critiques ont été pris en compte.

Ainsi, de notre point de vue, une analyse a priori et une analyse a posteriori doivent être effectuées et incluses dans la stratégie de génération de scénarios et d'évaluation de la Safety du VA. Cet objectif nous amène à considérer l'analyse de la criticité à deux niveaux : une phase d'estimation de la criticité et une phase d'évaluation de la criticité. L'estimation de la criticité est faite en amont de la simulation. Son but est d'identifier parmi les scénarios qui seront soumis au VA pour simulation, ceux qu'il aura potentiellement de la difficulté à appréhender et qui l'amèneraient à avoir une réaction critique. Ainsi, elle aide à prioriser les scénarios potentiellement critiques lors de la génération et la simulation de scénarios. Contrairement à l'estimation, l'évaluation de la criticité se fait en aval et, par conséquent, une fois que la simulation du scénario a été effectuée. Elle sert à vérifier si la réaction du VA s'est avérée être effectivement critique ou non, et à identifier des scénarios à réintroduire dans la simulation.

#### 3.3.3.1 Estimation de la criticité (a priori) et sensibilité

Les points discutés dans cette section visent à établir une analyse a priori des éléments qui permettent une identification initiale des scénarios potentiellement critiques pour le VA. Dans un premier temps, nous procéderons à une analyse préliminaire de risques (APR) et une identification des facteurs de criticité et des types d'événements, puis dans un second temps, nous proposerons une analyse de sensibilité du VA à chacune des plages de valeurs des paramètres modélisant la situation opérationnelle.

### 3.3.3.1.1 APR, facteurs de criticité et types d'évènements

La première étape de l'estimation de la criticité est la mise en place d'une APR, suivie d'une analyse des facteurs de criticité et des types d'évènements que le VA peut rencontrer.

- APR en vue de l'identification des conséquences (Hazardous behaviors) des insuffisances fonctionnelles du VA

Nous avons évoqué, dans les chapitres précédents, l'existence de limitations de performance pour une fonction d'automatisation donnée. Elles sont en lien avec les capteurs, la reconnaissance ou la prise de décision. Leur identification se base sur la connaissance des performances fonctionnelles attendues de la fonction d'automatisation, mais aussi sur les problématiques technologiques qui lui sont associées. Nous pouvons noter à titre d'exemple, le cas des capteurs dont les performances sont principalement altérées par la météo ou encore la qualité de l'infrastructure routière. L'objectif de cette étape dans l'estimation de la criticité est d'identifier de manière détaillée les comportements potentiellement dangereux (Hazardous behaviors) que le VA pourrait avoir. Cela permettra, d'une part, de prendre conscience des dangers potentiels en cas de mauvaise réaction du VA, et d'autre part, de tenir compte des facteurs pouvant être à l'origine de telles réactions lors de la création des scénarios.

Pour ce faire, nous proposons de procéder à une APR dans laquelle nous nous focaliserons sur les risques dont l'origine pourraient être des limitations de performances fonctionnelles. Toutefois, n'oublions pas que le VA est caractérisé par un niveau d'automatisation auquel est associé un ODD. Par conséquent, avant d'effectuer l'APR, nous devons préciser le niveau d'automatisation considéré, l'ODD et donc la fonction d'automatisation concernée ; ce qui équivaut à la phase de définition du système tel que spécifié dans la norme ISO 26262. En outre, dans une analyse de risques, les niveaux de sévérité sont indépendants de la nature des causes et, par conséquent, les classes de sévérité données par la norme ISO 26262 peuvent être utilisées (voir tableau 11).

Nous avons illustré le principe de l'analyse à travers le tableau 12 en utilisant la fonction d'automatisation TJC (Traffic Jam Chauffeur). Il s'agit d'une fonction d'automatisation de niveau 3, conçue pour prendre en charge la conduite autonome sur voies à chaussées séparées (autoroute et voies rapides) en conditions d'embouteillage où la vitesse est limitée à une vitesse maximale  $V_{max}$  (autour de 60 à 70 km/h). Le véhicule Ego (le véhicule équipé de la fonction d'automatisation) suit le véhicule qui précède, maintient sa position dans sa voie et gère l'accélération et le freinage dans la limite spécifiée. Le conducteur peut effectuer d'autres activités mais doit rester vigilant et être capable de reprendre le contrôle du véhicule sur sollicitation du système. Le système doit permettre à ce dernier d'activer la fonction ou d'intervenir à tout moment pour reprendre le contrôle du véhicule et doit lui laisser le temps pour le faire.

Le tableau 12 montre que l'analyse APR pour le TJC, consiste à définir pour une limitation de performance donnée, son scénario d'occurrence, puis son effet (conséquence) à la fois sur le VA et sur les usagers présents, et enfin, à déterminer la sévérité associée à l'effet observé.



A la fin de l'analyse, plusieurs comportements dangereux potentiels sont identifiés parmi lesquels on peut citer : « No activation, Erroneous activation, Insufficient longitudinal acceleration, Excessive longitudinal acceleration, excessive lateral deceleration ».

Comme nous pouvons le noter dans le tableau 12, une bonne connaissance de la fonction d'automatisation permet dans un second temps, de pouvoir identifier, en plus des comportements dangereux du VA, les causes ou évènements à l'origine des limitations de performance qui ont contribué à l'apparition de ces comportements dangereux.

Severity		
	Class	Description
1	S0	No injuries
2	S1	Light and moderate injuries
3	S2	Severe and life-threatening injuries (survival probable)
4	S3	Life-threatening injuries (survival uncertain), fatal injuries

Tableau 11 : Classes de sévérité (ISO 26262-3, 2011)

<i>An example of PHA for TJC potential hazardous behaviors identification.</i>	
• <b>Potential performance limitation:</b>	<ul style="list-style-type: none"> <li>○ Incomplete perception of the target due to dark environment</li> </ul>
• <b>Scenario of occurrence:</b>	<ul style="list-style-type: none"> <li>○ Initial situation: “Target following” as operational maneuver, Moment of the day = Night, Level of brightness = high (road lighting)</li> <li>○ Sources of Event: Weather conditions</li> <li>○ Events: Level of brightness = Low (Dark road, dark road with incoming head lamps)</li> </ul>
• <b>Effect:</b>	<ul style="list-style-type: none"> <li>○ On AV (Hazardous Behavior): Excessive longitudinal acceleration due to a wrong perception of the target resulting in a wrong estimation of its speed.</li> <li>○ On users (On the situation): Potential Harmful situation due to a collision (at least moderate harmful situation)</li> </ul>
• <b>Severity:</b>	>= S1 (depends on dynamics conditions)

Tableau 12 : Illustration de l'APR basée sur les limitations de performance dans le cas du TJC

- Facteurs de criticité et leur classification par types d'évènements

Nous avons défini le concept de « scénario » comme l'occurrence à la fois d'une situation et d'un évènement en lien avec la situation (Cf. §2.3 du chapitre 2).

Ainsi, le risque engendré par l'occurrence d'un scénario est lié aux états des paramètres décrivant la situation et à leurs éventuelles évolutions (c'est-à-dire l'évènement).

Cela pose la question suivante : quels sont les états des paramètres qui, s'ils sont présents dans la situation, peuvent induire le risque d'un comportement (ou d'une réaction) inadapté (e) du VA ?

Ces états de paramètres sont des facteurs de criticité qui peuvent être identifiés grâce au retour d'expérience (bases de données de roulage, retour des concepteurs des fonctions du VA) et à l'expertise. Leur identification se fait principalement à l'intérieur de l'ODD de la fonction

d'automatisation considérée. Cependant, bien qu'une fonction d'automatisation ne doive pas être utilisée en dehors du nominal prévu par le constructeur, il pourrait être intéressant de la tester avec des événements (évolutions d'états de paramètres) survenant en dehors de l'ODD pour évaluer son niveau de robustesse. De tels événements peuvent augmenter la criticité d'un scénario et sont donc qualifiés d'événements critiques.

A titre d'exemple, prenons le cas du TJC. La fonction ne peut être utilisée que sur voie à chaussées séparées. Son utilisation sur d'autres types d'infrastructures (intersection, roundabout, pedestrian crossing, stop lights, giving way, priority entry, u-turn, working zone, tunnel) peut être dangereuse parce que la fonction n'est pas faite pour être utilisée dans de telles conditions. Il est donc intéressant d'effectuer quelques tests sur ces infrastructures pour vérifier si la réaction du VA est adaptée.

Ainsi, les facteurs de criticité peuvent être organisés en types d'événements appartenant à deux catégories : les événements survenant à l'intérieur de l'ODD (Tableau 13) et ceux apparaissant en dehors de l'ODD (Tableau 14). Dans la première catégorie, on rencontre les événements relevant des limitations de performance de la fonction d'automatisation, des déviations dans les comportements des autres usagers ainsi que des transitions dans les manœuvres opérationnelles des usagers. Dans la seconde, on a principalement les événements relevant des contraintes d'utilisation de la fonction et des transitions entre les modes de fonctionnement du VA. Par ailleurs, il est important de noter que la notion d'évènement telle que considérée ici englobe celle de « triggering condition » définie dans le PAS 21448 SOTIF comme suit :

- *Triggering conditions: specific conditions of a scenario (3.23) that serve as an initiator for a subsequent system reaction, possibly leading to a hazardous behavior*

Parmi les événements « Triggering conditions », certains sont connus et d'autres inconnus. L'ISO / PAS SOTIF stipule qu'une identification des « triggering conditions » peut être soutenue par une description détaillée du modèle de l'environnement. Ainsi, les événements recherchés proviennent bien des entités de l'environnement opérationnel du VA tel que nous pouvons l'illustrer avec les exemples mentionnés dans les tableaux 13 et 14.

Exemples d'évènements survenant à l'intérieur de l'ODD		
Types	Evènements	
Limitations de performances connues (à l'intérieur de son ODD) : E1	E11	L'entité "infrastructure" est la source de la limitation
	E12	L'entité "météo" (condition atmosphérique) est la source de la limitation
Déviations et violations des consignes de sécurité et du code de la route : Ed	Ed1	Déviations dans le comportement des autres usagers par rapport à la voie de circulation (et aux emplacements dédiés)
	Ed2	Déviations dans le comportement des autres usagers par rapport à l'exécution des manœuvres (dépassement, sortie, Insertion,...) en toute sécurité (au respect des distances de sécurité)
	Ed3	Déviations dans le comportement des autres usagers par rapport au respect des limitations de vitesse
	Ed4	L'entité " Driver_passenger" est la source de la limitation à savoir les mésusages (Ex : Augmentation_vitesse)
Evènements du type transitions entre manœuvres : ET	ET	Correspond aux conditions de validité de la manœuvre

Tableau 13 : Typologies d'évènements survenant à l'intérieur de l'ODD

Exemples d'évènements en dehors de l'ODD		
Types	Evènements	
Contraintes liées à l'utilisation de la fonction (Limites) : Ec (en dehors du nominal prévu par le constructeur)	Ec1	Contraintes sur l'infrastructure (route, chaussée, vitesse)
	Ec2	Contraintes sur la météo
	Ec3	Contraintes sur le Driver_passenger (Interactions avec le véhicule)
	Ec4	Contraintes sur les autres usagers
Evènements du type transitions entre modes de fonctionnement (Cf. figure 8 chapitre 1) : EM	EM	Correspond aux conditions de validité du mode

Tableau 14 : Typologies d'évènements survenant en dehors de l'ODD

La recherche des facteurs de criticité et l'identification des types d'évènements source, visent à cibler les scénarios potentiellement à risque qu'il faudra nécessairement tester. Toutefois, pour mieux prendre en compte la contribution de chaque facteur dans l'estimation du risque, une analyse de la sensibilité a priori a été introduite.

#### 3.3.3.1.2 Détermination de la sensibilité du VA à chaque plage de valeurs

Lors de l'obtention des scénarios logiques (chapitre 4), le domaine de définition de chaque paramètre sera décomposé en plages de valeurs. Cette décomposition en plages de valeurs, offre l'avantage contrairement à l'espace de variation entier du paramètre, de pouvoir analyser au plus près, la plage de valeurs qui peut être en cause dans l'obtention d'un scénario critique. Etant donné que nous sommes sur une analyse en amont de la simulation, ce niveau d'impact sera appelé « sensibilité a priori ». **La sensibilité mesure le degré avec lequel la plage de valeur peut leurrer la fonction d'automatisation.** Ainsi, l'analyse de la sensibilité a priori vise à identifier le niveau de sensibilité du VA à chaque plage de valeurs de chaque paramètre (y compris ceux pouvant faire l'objet d'évènements) apparaissant dans la génération. Elle est obtenue grâce à l'expertise et en considérant les éléments composant l'architecture du VA. Ces éléments sont la perception (et ses cinq (5) technologies de capteurs présentées sur la figure 13), la décision (fusion et règle), et l'actionnement.

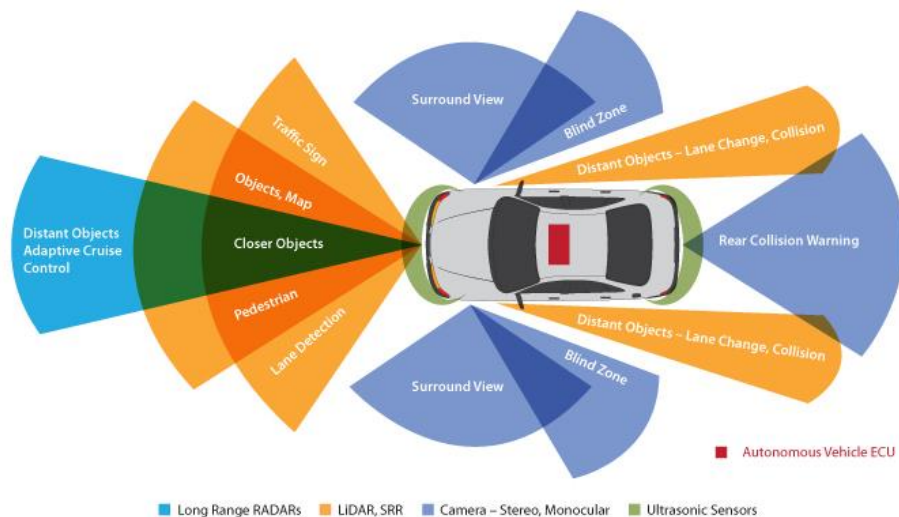


Figure 13 : Technologies de capteurs sur le VA

Les cinq technologies sont regroupées de la sorte : les radars (longue et courte portée), les ultrasons, les lidars, les caméras stéréoscopiques (vision 3D) et les caméras monoculaires.

Le processus proposé pour la détermination de la sensibilité n'est pas lié à des composants en particulier. Il offre la possibilité d'être adaptable selon les particularités des composants que l'on aura sur un véhicule donné. Le principe repose sur de l'expertise et reste paramétrable. Cela ne remet donc pas en cause la démarche globale, d'autant plus que le résultat de l'analyse est inhérent aux technologies intégrées dans le Véhicule. Par ailleurs, la connaissance des composants peut permettre d'affiner les plages de valeurs des paramètres et éventuellement les paramètres eux-mêmes (toujours grâce à l'expertise incluant les connaissances des fournisseurs).

La détermination du niveau de sensibilité du VA à une plage de valeurs s'obtient en deux étapes.

- a) D'abord, pour chacune des composantes de l'architecture du VA citées ci-dessus, on interroge l'expert sur la possibilité qu'elle puisse être leurrée par la plage de valeurs via la question suivante : *La technologie de capteur (ou la décision ou l'actionnement) est-elle sensible ou non performante dans cette plage ?*

La réponse attendue de l'expert est soit oui, soit non. Ensuite, l'échelle décrite par le tableau 15, permet de déterminer le niveau de sensibilité du VA à la plage suivant la (les) composante(s) du VA impactée(s).

Proposition de contribution d'une technologie de capteur ou d'un module du VA au calcul de la sensibilité a priori du VA à une plage de valeurs		
Classe	Description	Valeur de sensibilité correspondante
1	La plage de valeurs leurre une seule technologie de capteurs sur cinq	0,2
2	La plage de valeurs leurre deux technologies de capteurs sur cinq	0,4
3	La plage de valeurs leurre trois technologies de capteurs sur cinq	0,6
4	La plage de valeurs leurre quatre technologies de capteurs sur cinq	0,8
5	La plage de valeurs leurre les cinq technologies de capteurs	1
	La plage de valeurs leurre la décision prise par le VA (en l'absence d'un quelconque leurre vis-à-vis des capteurs)	
	La plage de valeurs leurre l'actionnement	

Tableau 15 : Proposition d'une échelle de mesure de sensibilité a priori du VA à une plage de valeurs

Pour illustrer ce principe, prenons le cas du paramètre « Visibilité ». Le fait de décomposer le domaine de définition en trois plages de valeurs : Faible, Moyen, Elevée, permet de pouvoir définir le niveau d'impact de chaque plage dans la création d'un scénario potentiellement critique pour le VA. Le tableau 16 illustre la détermination du niveau de sensibilité a priori du VA à chacune des plages de visibilité.

La première étape est de répondre à la question suivante pour chaque plage et chaque composante du VA : « la techno 1 / la techno 2 / la techno 3 / la techno 4 / la techno 5 / la décision / l'actionnement » est-elle non performante dans les plages de variation du paramètre visibilité « Faible / Moyen / Elevée » ?

Les réponses obtenues de l'expert « OUI / NON » sont indiquées alors dans le tableau 16.

- b) La deuxième étape est d'identifier pour chaque plage, les types de composantes leurrées ainsi que la valeur de sensibilité correspondante. Si l'on considère la plage visibilité « Faible », on note qu'elle peut leurrer trois composantes du VA qui sont toutes des technologies de capteur. D'après l'échelle (tableau 15) cela correspond à un niveau de sensibilité égale à 0.6. En suivant le même principe pour les autres plages, la sensibilité du VA à chacune des plages peut être obtenue.

Paramètre	Plage de valeurs	Techno 1 : Radar	Techno 2 : Lidar	Techno 3 : Ultrason	Techno 4 : Caméra stéréo	Techno 5 : Caméra mono	Décision	Action -nement	Sensibilité du VA à la plage
Visibilité	Faible (< Time To Collision (TTC))	NON	OUI	NON	OUI	OUI	NON	NON	0.6
	Moyen [TTC, TTC]	NON	NON	NON	OUI	OUI	NON	NON	0.4
	Elevée (> 2TTC)	NON	NON	NON	NON	NON	NON	NON	0

Tableau 16 : Illustration de la détermination du niveau de sensibilité a priori du VA à une plage de valeurs

En outre, il est à noter lors de cette analyse de sensibilité que, pour certains paramètres, les plages de valeurs représentant des facteurs de criticité, auront des niveaux de sensibilité élevés. C'est notamment le cas pour les paramètres suivants :

- Au niveau de la perception : le nombre de voies, l'état de la surface (chaussée), l'état du marquage, la position des usagers autour du VA, la proximité par rapport à l'Ego (TIV), type de visibilité, niveau de luminosité, type de précipitation.
- Au niveau de la décision : la complexité de la situation, qui dépend du nombre d'éléments présents (nombre d'interactions) et de la dynamique des usagers présents (manœuvres opérationnelles)
- Au niveau de l'actionnement : la courbure de la route, l'état de la chaussée...

La sensibilité a priori du VA à une plage de valeurs permet d'anticiper la détermination du niveau potentiel d'impact que la plage peut avoir sur ce dernier lors du déroulement d'un scénario. Ainsi, cette étape servira également par la suite, à alimenter l'analyse des niveaux de sensibilité des situations logiques auxquelles le VA pourra être confronté, de sorte à guider la recherche et l'échantillonnage des scénarios.

Les étapes proposées dans cette section « estimation de criticité (a priori) et sensibilité » sont les suivantes : une APR en vue de l'identification des conséquences des insuffisances fonctionnelles du VA, la recherche des facteurs de criticité et leur classification par types d'évènements et enfin, la détermination de la sensibilité a priori du VA à chacune des plages de valeurs. Ces étapes représentent une première phase dans la spécification des indicateurs qui vont permettre de juger de la performance et de la robustesse de la stratégie de génération.

La section suivante aborde l'évaluation de la criticité a posteriori, après obtention de résultats de simulation de scénarios.

### 3.3.3.2 *Evaluation de la criticité a posteriori*

Nous souhaitons non seulement vérifier si le comportement du VA n'est pas dangereux, mais aussi vérifier si la situation finale résultant de sa réaction n'est pas critique pour lui et pour les autres usagers. Par conséquent, à la fin du processus de simulation, nous aurons besoin de certains critères, qui seront utilisés pour vérifier ces aspects et établir une classification des scénarios simulés afin d'identifier ceux qui nécessiteront plus d'intérêt. Cet intérêt peut être traduit par le sur-échantillonnage d'un scénario ou la répétition de la simulation de ce scénario pour mener des analyses de sensibilité plus poussées sur certains paramètres.

- Indicateurs d'évaluation d'un scénario (après simulation)

Dans le cadre de l'analyse de risques sur les scénarios, la classification des scénarios se limite à déterminer si le scénario est critique. Le choix est fait d'évaluer le caractère « critique » au regard de la survenue d'un accident. Une telle classification est également valable dans notre contexte car nous voulons évaluer le VA en termes de sécurité. Par ailleurs, classifier les scénarios peut présenter un intérêt pour le constructeur avec une analyse portant au-delà de la sécurité. En effet, l'analyse des résultats de la simulation est l'occasion de vérifier si le comportement attendu en termes de réalisation des manœuvres a été effectué ou non. Par conséquent, nous proposons trois indicateurs pour évaluer les scénarios après la simulation et établir leur classification : l'accomplissement de la manœuvre (AM), la présence d'un « hazardous behaviour » (HB) et la sévérité (S). AM vérifie si le VA a effectué la manœuvre attendue, HB doit vérifier si son comportement a été dangereux ou non et S évalue l'étendue des dommages en cas de présence d'un HB. Précisons maintenant comment chacun de ces indicateurs (ou critères) sera mesuré.

- Mesure du critère « Accomplissement de la manœuvre opérationnelle (AM) »

La mesure du critère AM se fait en vérifiant si les conditions de validité de chaque manœuvre sont respectées ou non. Une telle vérification permet également de s'assurer de la conformité à la spécification fonctionnelle du VA.

Par exemple, supposons que dans le scénario simulé, le VA est supposé effectuer une manœuvre de maintien de la voie (a lane-keeping maneuver). La validité de cette manœuvre repose sur l'élément suivant : Distance séparant le VA de la ligne de marquage (ligne latérale de séparation et de démarcation des voies) > seuil (exemple 1 m). Ainsi, à la fin du scénario, pour vérifier si le véhicule a bien exécuté la manœuvre, nous vérifierons si sa position dans la voie respecte cette condition.

- Mesure du critère « hazardous behavior (HB) »

Comme nous l'avons présenté initialement, les potentiels HB du VA peuvent s'identifier grâce à l'APR. La mesure du critère HB se fait en vérifiant si le VA passe d'un comportement inadapté à un comportement dangereux. Il peut s'agir d'un différentiel anormal de vitesse par rapport aux autres usagers et/ou de positionnement.

À titre d'exemple, à l'approche d'une zone de travaux, limitée à 50 km/h, le VA ne détecte pas le panneau de limitation de vitesse. Il ne décélère pas jusqu'à la nouvelle vitesse et garde sa

vitesse à 80 km/h. La différence de vitesse est anormale et peut être dangereuse. Ici, le HB est "Pas de décélération" à l'approche d'une zone de travaux.

- Mesure du critère « Sévérité »

Les classes de sévérité ont été identifiées plus haut dans le tableau 11. La sévérité dépend des conditions dynamiques (telles que la vitesse ou l'accélération) et plus généralement de leurs conséquences. Toutefois, lors de la simulation, elle peut être mesurée dans un premier temps, en vérifiant l'existence d'un contact physique entre le VA et un autre usager de la route présent dans la situation finale (distance nulle). Cela signifie qu'une collision s'est produite et qu'il y a une distance nulle entre l'usager concerné et le VA (l'Ego\_véhicule).

Pour affiner et améliorer cette mesure, nous proposons deux alternatives.

a) La première est de considérer la vitesse relative avant le contact physique, qui peut être utilisée pour estimer l'étendue des dommages et ainsi, définir la sévérité de la collision. Ceci étant, pour faciliter l'analyse, il faut connaître au préalable les seuils de vitesse relative menant aux différentes sévérités en fonction des usagers en collision. L'information sur les différents seuils (suivant chaque type d'utilisateur) peut être obtenue à l'aide de données sur l'accidentologie ou les profils de mission. Pour obtenir la sévérité de la collision, on tiendra compte de la nature de l'obstacle, de la vitesse au moment du choc et du type de collision (frontale, latérale ou arrière). Ainsi, les usagers avec lesquels le VA pourrait entrer en collision et leurs paramètres peuvent être définis comme suit :

- les usagers en présence :
  - piéton, vélo, trottinette, (usagers vulnérables)
  - objet fixe, rigide (arbres, murs, panneaux de signalisation, ...)
  - objet mobile (animaux, ...)
  - un autre véhicule de même gabarit
  - un véhicule poids lourd
- Et leurs paramètres ou attributs :
  - Vitesse relative de l'entité par rapport au VA (direction, sens et intensité)
  - Masse ou rigidité de chaque usager

Par ailleurs, dans le cas d'objets comme le sac plastique, un ballon ou un cône de sécurité, ... ce n'est pas le choc qui pose souci. C'est la réaction du VA qui peut créer une situation dangereuse s'il effectue un freinage d'urgence inapproprié ou un évitement inapproprié.

Nous donnons dans le tableau 17, des exemples de sévérité (d'une collision) sur la base de différence de vitesse entre le véhicule porteur de la fonction d'automatisation (le VA) et deux types d'usagers, dans le cas d'un choc frontal.



<b>Exemple 1</b>	Vitesse $v$ du véhicule porteur (km/h)	$v < 5$	$5 < v < 20$	$20 < v < 40$	$40 < v$
	Choc frontal avec un piéton	S0	S1	S2	S3
<b>Exemple 2</b>	Différence de vitesse $Dv$ (km/h)	$Dv < 15$	$15 < Dv < 30$	$30 < Dv < 50$	$50 < Dv$
	Choc frontal avec un véhicule	S0	S1	S2	S3

Tableau 17 : Exemples de sévérité sur la base de différence de vitesse entre le VA et d'autres types d'usagers, pour un choc frontal

b) La deuxième alternative pour affiner l'analyse de la sévérité d'un scénario est de recourir aux métriques de criticité standards : time-to-collision (TTC), time-to-brake (TTB), required-deceleration, headway... (Hallerbach et al., 2018) (Feng et al., 2020a) (D. Zhao et al., 2017) (Mullins et al., 2017) (Jesenski et al., 2019). Dans ce cas, il serait intéressant de disposer d'une fonction permettant de mesurer directement cette criticité, et éventuellement, la présence ou non de collision au cours de la simulation. De ce fait, il faut spécifier le seuil  $\gamma_s$  en dessous duquel un scénario concret  $x_i$  est identifié comme étant critique par la fonction  $f$  choisie (il y a collision ou risque de collision) de tel sorte que  $f(x_i) \leq \gamma_s$ .

Dans le cadre de ce travail, la criticité sera assimilée à la présence de collision et c'est la première alternative pour affiner l'analyse de sévérité qui sera considérée.

- Classification des scénarios (après simulation)

Maintenant que les indicateurs d'évaluation des scénarios sont identifiés et mesurés, nous allons les utiliser pour établir les classes des scénarios simulés. Nous avons déterminé cinq issues possibles caractérisant la situation finale résultant de la réponse du VA. Dans cette classification, la sévérité est spécifiée suivant la présence ou non de collision (pour l'affiner, il faudra tenir compte des conditions dynamiques, telles que mentionnées précédemment). A noter qu'en absence de collision, il n'y a pas de dommage, et donc la classe de sévérité est 1 (sévérité S0). Cependant, dès que l'on observe une collision (classe 5), il est probable qu'il y ait des dommages, et dans ce cas, toutes les classes de sévérité peuvent être en jeu (S0, S1, S2 et S3). La figure 14 résume les différentes classes obtenues.

- Classe 1 : Situation sûre avec AM et pas de HB. La situation finale montre que la réaction du VA ne met en danger aucun des usagers présents. La manœuvre attendue a été effectuée et son action ne représente pas un HB ( $AM = 1, S0, HB = 0$ ).
- Classe 2 : Situation sûre sans AM et sans HB. La situation finale montre que la réaction du VA ne met en danger aucun des usagers présents. Cependant, la manœuvre attendue n'a pas été effectuée, mais l'action du VA ne représente pas un HB ( $AM = 0, S0, HB = 0$ ).
- Classe 3 : Situation inévitable, indépendante de la réaction du VA, causée par d'autres véhicules. La manœuvre du VA reste conforme au comportement attendu, mais le scénario d'accident est inévitable<sup>7</sup>. ( $AM = 1, S \geq S0, HB = 0$ )

<sup>7</sup> Par exemple, un autre usager se rabat devant le VA sans respecter la distance de sécurité et freine brutalement.

- Classe 4 : Situation dangereuse avec HB mais sans aucun impact sur la sécurité (avec ou sans AM). La situation finale montre que la réaction du VA est de type HB et met donc en danger les utilisateurs présents dans la situation, et cela indépendamment du fait que la manœuvre attendue ait été effectuée ou pas. Cependant, aucun incident ou dommage n'est observé (AM = 0 ou AM=1, S0, HB = 1).
- Classe 5 : Situation avec HB et avec préjudices, ce qui a un impact sur la sécurité (avec ou sans AM). La situation finale montre la présence d'un incident (collision) pour les usagers, et cela indépendamment du fait que la manœuvre attendue ait été effectuée ou pas (AM = 0 ou AM=1, S >=S0, HB = 1).

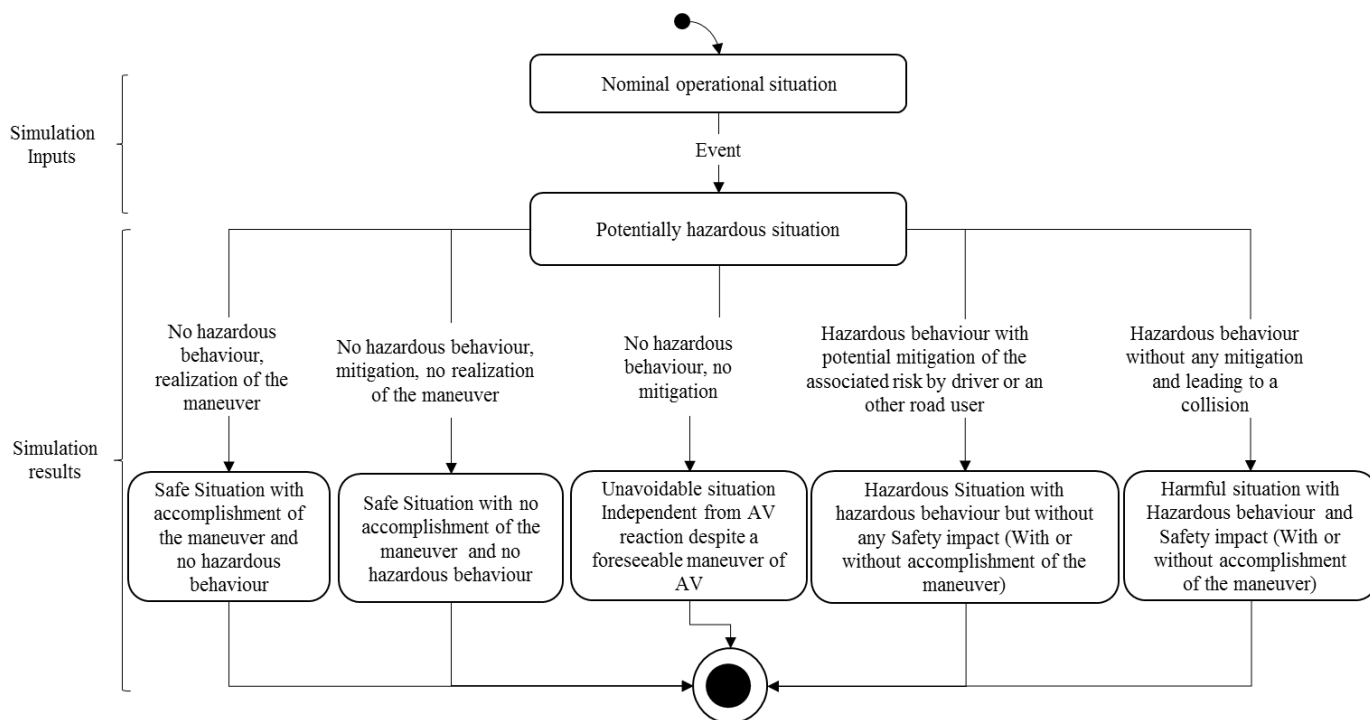


Figure 14 : Classification des scénarios après simulation

La classe 5 est celle mettant en jeu un impact de sécurité (du fait de la présence d'une collision) pouvant être causé par le VA. C'est la classe qui nous intéressera dans le cadre de l'estimation du niveau de risque associé au VA. Elle regroupe tous les scénarios résultant d'une collision indépendamment de leurs niveaux de sévérité (S0, S1, S2 et S3). Pour une analyse plus fine de l'impact Safety, il faut réaliser une analyse en affinant la classe 5 grâce aux paramètres dynamiques du scénario tels qu'illustré notamment avec le tableau 17.

Une telle qualification de la situation finale en vue de savoir si le scénario s'est déroulé comme espéré, a l'avantage de permettre au constructeur d'utiliser les résultats d'analyse pour améliorer le développement de la fonction d'automatisation en termes de performances fonctionnelle et de sécurité.

Maintenant que nous disposons d'indicateurs pour classer les résultats des simulations, nous proposons dans les deux prochaines sections d'aborder comment estimer le risque final associé au VA tout en tenant compte des incertitudes liées aux évaluations.

### 3.3.4 Incertitude et indicateur de confiance

« Dans un contexte d'évaluation des risques, une analyse d'incertitude est un processus ayant pour objectif d'identifier, décrire, quantifier et communiquer les incertitudes associées aux résultats» (Makowski et al., 2016). Dans le cadre de la validation par simulation du VA basée sur les scénarios, il y a deux grands systèmes sur lesquels nous avons de l'incertitude. D'un côté, nous avons de l'incertitude sur l'environnement de simulation (écart de représentativité entre le simulateur et la réalité) et sur l'analyseur. En effet, la modélisation du comportement du VA et de ses interactions avec l'environnement peut être sujette à de l'incertitude, notamment en ce qui concerne la caractérisation des capteurs. Aussi, le niveau de modélisation de l'environnement de test, la mesure des indicateurs de sécurité (TTC, vitesse relative en cas de choc, ...) ou encore la classification des résultats de simulation (les faux négatifs et faux positifs), peuvent être entachés d'incertitudes. De telles incertitudes provoquent un doute sur les résultats obtenus à l'issue de la validation par simulation, impactant ainsi la confiance globale que l'on pourra accorder à la sécurité du VA. De ce fait, le constructeur devra démontrer que le niveau de confiance à accorder au système de simulation et d'analyse est acceptable. Cet aspect n'entre pas dans le périmètre de notre thèse.

De l'autre côté, le deuxième système sur lequel figure de l'incertitude est l'environnement opérationnel du VA (niveau de modélisation du profil de mission). Cette incertitude doit être prise en compte dans la génération des scénarios et les évaluations. Deux catégories d'incertitudes sont à évaluer : l'une épistémique et l'autre aléatoire. L'incertitude épistémique porte sur :

- les entités (elles ne sont pas toutes connues),
- les paramètres (tous les paramètres pertinents ne sont pas connus) ou leurs plages de valeurs (elles ne sont pas bien délimitées),
- les combinaisons entre entités et paramètres (les compatibilités ne sont pas bien modélisées. Par exemple la neige et le soleil éblouissant surviennent en même temps)
- l'identification des événements (le VA n'identifie pas correctement un événement. Par exemple, une personne portant un costume d'éléphant sur une trottinette traverse une route, un autre usager a un comportement imprévu, ne respectant pas le code de la route, d'autres usagers qui disparaissent dans le pont devant le VA (écroulement du pont), ...)

Quant à l'incertitude aléatoire, elle s'applique sur :

- les valeurs des paramètres (incluant les événements) (les valeurs des paramètres ne sont pas connues de façon déterministe),
- les combinaisons entre les valeurs (les combinaisons entre les valeurs ne sont pas connues de façon déterministe).

L'incertitude épistémique est difficilement quantifiable. Elle peut être toutefois réduite, au fur et à mesure que l'on obtient des connaissances sur l'environnement opérationnel considéré. Ainsi, pour en tenir compte, nous proposons que les bases de connaissances (les paramètres et leurs plages de valeurs) utilisées pour les analyses soient basées sur une dynamique

enrichissante, c'est-à-dire qu'elles soient mises à jour en cas de découverte de nouveaux paramètres. Un tel travail est à faire par le constructeur.

Comme évoqué dans l'état de l'art présenté au chapitre 1, l'incertitude aléatoire peut être caractérisée à l'aide de la théorie des probabilités. Une recommandation à ce sujet apparaît dans la définition du scénario logique dans laquelle il est précisé que les plages de valeurs des paramètres peuvent être optionnellement spécifiées avec les distributions de probabilité. En effet, ces distributions permettent une génération stochastique des scénarios à l'aide notamment de procédés d'échantillonnage. Elles sont obtenues à l'aide des analyses statistiques sur les profils de missions. **Par hypothèse, nous considérerons dans nos travaux que ces distributions ont été déterminées et nous sont fournies.**

La prise en compte de l'incertitude aléatoire se fera donc en deux étapes :

1) En effectuant les tirages des scénarios de manière aléatoire, c'est-à-dire en suivant des distributions de probabilités

2) En calculant, un intervalle de confiance sur l'indicateur de risque associé au VA. Le caractère aléatoire des scénarios obtenus génère une incertitude sur les résultats des évaluations notamment sur la criticité (dangerosité) de chacun d'eux ou sur l'indicateur de risque final associé au VA. D'une part, nous proposons de réduire l'incertitude sur ces évaluations grâce à un processus itératif permettant de réévaluer la criticité des scénarios après chaque simulation. D'autre part, étant donné que le calcul de l'incertitude sur une estimation revient au calcul de l'écart type associé à sa distribution, nous procéderons dans cette deuxième étape au calcul de l'écart type associé à l'estimation qui sera fournie, à savoir l'indicateur de risque final. Cela revient donc à fournir un intervalle de confiance dans lequel se situe la « vraie valeur » de l'indicateur de risque associé au VA.

### 3.3.5 Indicateur final de risque

Cet indicateur permet d'obtenir la probabilité d'occurrence de l'évènement d'intérêt (« Harmful situation » / Accident) lors de l'utilisation du VA. Son estimation constitue l'un des objectifs, voire le principal objectif à l'issue de la validation par simulation, et se fait à l'aide des résultats de la simulation.

Posons :

$\theta$  est l'évènement d'intérêt,

$P_k(\theta)$  est la probabilité d'occurrence de cet évènement d'intérêt,

$\tilde{P}_k(\theta)$  est l'estimateur de  $P_k(\theta)$ ,

100 (1- $\alpha$ ) % le niveau de confiance.

La validation du VA dans le contexte du SOTIF est faite en référence à une cible. Cette cible de validation est définie à partir des données statistiques sur le trafic. Pour que le système en cours de test (le VA) soit reconnu comme valide, il faut que la valeur de l'indicateur final de risque soit inférieure ou égale à la cible qui a été définie.

Pour ce faire, il faut estimer  $P_k(\theta)$  à l'aide de  $\tilde{P}_k(\theta)$  pour une précision  $\varepsilon$  et un niveau de confiance 100 (1- $\alpha$ )%. En plus de la cible de validation, la précision  $\varepsilon$  et le niveau de confiance 100 (1- $\alpha$ ) % sont des critères supplémentaires pour définir la condition d'arrêt de la génération.

Ils servent à la mise en place d'un intervalle de confiance et permettent ainsi de tenir compte de l'incertitude présente dans les évaluations telle qu'évoquée dans la section précédente. Nous avons formalisé cette condition d'arrêt de la génération et de la simulation selon deux cas de figures :

Cas 1) L'estimateur dépasse la cible de validation. Au bout de la  $k^{\text{ième}}$  simulation, on peut montrer que même si toutes les autres simulations étaient bonnes, notre estimateur dépasserait la cible.

Cas 2) Nous voulons procéder à une estimation par intervalle de confiance (IC), c'est-à-dire fournir un IC susceptible de contenir le risque associé au VA avec un niveau de confiance  $1-\alpha$  (Exemple  $1-\alpha = 0,95$ ). Ici l'intervalle souhaité est unilatéral ; ce qui veut dire que le risque est réparti sur une seule extrémité de l'intervalle (soit la borne supérieure de l'intervalle). En d'autres termes, il faut montrer que  $\tilde{P}_k(\theta) \leq \tilde{P}_{max}(\theta)$  avec une probabilité de  $1-\alpha$ . Sous-jacent à cela deux autres conditions seront ainsi à vérifier. En effet :

- le critère d'arrêt dépend de la couverture et de la précision de l'estimation : la génération et la simulation s'arrêtent quand le nombre d'échantillons générés permet de fournir un IC au niveau de confiance souhaité ( $1-\alpha$ ) avec une précision inférieure à un seuil  $\beta$ .

$$z_\alpha \frac{\sqrt{Var(\tilde{P}_k(\theta))}}{\tilde{P}_k(\theta)} < \beta, \text{ avec } Var(\tilde{P}_k(\theta)) \text{ la variance de l'estimation, } z_\alpha \text{ une constante (quantile) associée au niveau de confiance } 1-\alpha$$

- la cible de validation est alors un critère de comparaison et d'acceptation qui permet de juger si l'objectif de validation est atteint ou si la fonction est assez mature et robuste pour être acceptée. La cible est comparée à l'estimateur précédent : si  $\tilde{P}_{max}(\theta) \leq cible$  ou autrement dit si  $\tilde{P}_k(\theta) + \Delta\tilde{P}_k(\theta) < cible$  alors le critère d'acceptation du VA est atteint.

Nous illustrerons dans le chapitre 4 comment nous proposons de formaliser notre estimateur dans le cadre de la méthodologie de génération développée. La section suivante présente un indicateur complémentaire que nous avons introduit pour vérifier l'efficacité de la validation en termes de durée.

### 3.3.6 Indicateur de gain de durée de validation

C'est un indicateur qui peut s'avérer utile dans l'argumentation sur la démonstration de la sécurité du VA. Cependant, il ne se suffit pas à lui seul et doit être présenté comme un argument complémentaire, une fois la cible de validation atteinte. Son objectif est de vérifier si les scénarios identifiés et sélectionnés ont permis d'atteindre la cible de validation en un temps réduit. En d'autres termes, il s'agit de vérifier si la stratégie retenue de génération et de validation a permis de réduire le temps de validation initialement requis d'un facteur  $r$ .

Soit  $N$  le nombre de scénarios simulés par la stratégie proposée (et ce, peu importe la puissance des calculateurs).

Soit  $p = 10^{-x}/h$ , la cible de validation initialement requise en situation de conduite réelle et soit  $T_i$  son équivalent en durée de validation. Soit  $\tau_m$  la durée moyenne d'un scénario telle que

$\tau_m \in [\tau_{min}, \tau_{max}]$ . De façon générale, il est supposé qu'un scénario dure entre 10s et 30s en moyenne<sup>8</sup> ( $\tau_m \in [10, 30s]$ ) dans la vie réelle.

La durée totale de validation par la simulation pour les N scénarios simulés serait :

$$Tf = \tau_m * N.$$

Le gain obtenu par rapport à la cible de validation initiale est donné par le facteur  $r$  tel que :

$$r = Tf/ Ti.$$

Ce calcul simplifié est fait sous les hypothèses suivantes :

- les roulages couvrent toutes les situations de conduite qu'il est possible de rencontrer,
- il faut que le roulage de comparaison ait été fait dans l'ODD associé au système d'automatisation considéré.

### 3.4 DISCUSSION

Nous avons vu dans la littérature que plusieurs indicateurs (critères et métriques) de performance étaient proposés pour la validation du VA (Jesenski et al., 2019) (Amersbach & Winner, 2019a). Ces indicateurs s'utilisent, pour la plupart, pendant et après la simulation ou le roulage pour évaluer le VA. Ainsi, aucune proposition de métrique permettant d'identifier au préalable (avant la simulation) les scénarios potentiellement critiques, en vue d'orienter la génération, n'a été faite. De plus, l'utilisation individuelle des indicateurs fait perdre en efficacité dans la démonstration de la sécurité du VA.

De ce fait, nous avons proposé dans ce chapitre un ensemble d'indicateurs à utiliser conjointement qui permet d'avoir un cadre global d'évaluation de la sécurité du VA. Aussi, dans nos propositions, nous intégrons une analyse de la criticité des scénarios en amont de la simulation via un indicateur de sensibilité a priori. Cela permet d'orienter la génération des scénarios à simuler en vue de prioriser ceux qui sont à même d'être critiques.

Par ailleurs, pour combler le besoin de connaissances en vue de l'« **applicabilité** » des propositions que nous avons effectuées, certaines tâches doivent être réalisées par le constructeur. Elles sont à faire soit au préalable à la spécification de la génération des scénarios (avec la détermination du profil de mission), soit pendant cette spécification (mise à jour des paramètres de la génération afin de réduire l'incertitude épistémique).

### 3.5 CONCLUSION

Dans ce chapitre, nous avons répondu à la question : **Quelle structure de système et quels indicateurs vont permettre de guider et de juger de la pertinence, voire de la performance, de la stratégie de génération et de validation par simulation de la sécurité du VA ?**

D'une part, nous avons vu au travers de ce chapitre, la structure du système de génération des scénarios et de validation par simulation de la sécurité du VA. D'autre part, nous avons défini

---

<sup>8</sup> Source interne Stellantis

l'ensemble des indicateurs (critères) que nous prendrons en compte dans la mise en place de la stratégie qui servira à cette génération et validation. En effet, comme déjà souligné, l'utilisation de plusieurs indicateurs permettra une meilleure argumentation du processus de démonstration de la sécurité du VA.

La figure 15 résume l'utilisation des indicateurs dans le système de validation du VA, notamment lors de l'exploration et de l'obtention des scénarios à simuler (via le générateur en jaune) et lors de l'évaluation des résultats (via le post-traiteur)

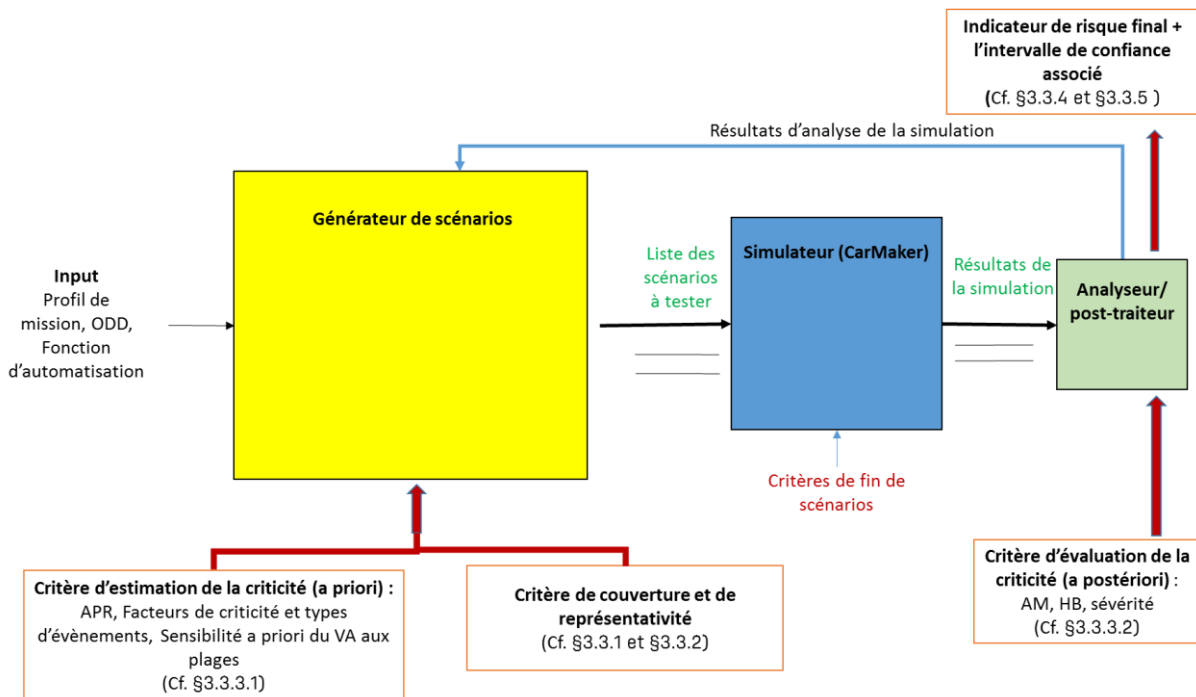


Figure 15 : Positionnement des indicateurs dans le système de génération et validation du VA

Les indicateurs d'estimation de la criticité, de couverture ou de représentativité servent à définir la performance de la génération, tandis que l'indicateur de risque final et l'intervalle de confiance associé, permettent d'estimer le résultat final du processus de validation par simulation tout en tenant compte des incertitudes dont sont entachées les évaluations. Tous réunis, ces indicateurs vont permettre d'avoir une stratégie globale qui répond aux deux dimensions de ce travail de thèse à savoir :

- la définition et l'amélioration de la performance de l'heuristique de recherche et de génération des scénarios (connaissance de la cartographie de l'espace des scénarios)
- l'estimation de l'indicateur final de risque associé au VA

Le chapitre suivant consiste en la mise en place de la stratégie de génération. Elle tient compte des indicateurs qui ont été définis.

---

## CHAPITRE 4. METHODOLOGIE DE GENERATION DE SCENARIOS

---

Rappelons que notre objectif général est de contribuer à répondre à la question : **Comment assurer la validation par simulation de la sécurité du VA au regard de ses limitations de performance (SOTIF) ?**

Nous avons proposé dans les chapitres 2 et 3, un cadre conceptuel (concepts clés, indicateurs de performance) que nous jugeons pertinent pour construire une méthodologie permettant de répondre à cet objectif.

Dans ce chapitre, nous proposons une méthodologie (et une stratégie) permettant d'apporter des éléments de réponse à la question de recherche générale, que nous reformulons plus précisément ainsi :

**Quelle stratégie utiliser pour la génération des scénarios nécessaires à la validation par simulation de la sécurité du VA ?**

Pour y répondre, nous allons apporter deux nouvelles contributions. D'une part, nous allons définir une méthodologie pour générer les scénarios nécessaires pour tester, via la simulation, le VA au regard de ses limitations de performance. D'autre part, nous allons proposer un cadre d'évaluation de la sécurité du VA avec une évaluation de la qualité de la génération et une estimation de la performance globale de sécurité du VA sur la base des scénarios testés.

Nous présentons d'abord un état de l'art des moyens et stratégies de générations déjà existants. Ensuite, en nous appuyant sur le cadre conceptuel proposé, nous montrons comment combiner les concepts retenus, en vue de procéder de manière effective à la mise en place d'une stratégie de génération de scénarios et d'estimation de la performance globale de sécurité du VA.

### 4.1 PARAMETRES, TECHNIQUES ET STRATEGIES UTILISES DANS LA GENERATION DE SCENARIOS

Plusieurs propositions existent dans la littérature en matière de représentation des connaissances ou de gestion des paramètres, ou encore en matière de techniques générales de génération automatique de scénarios de test ou de stratégies spécifiques au VA.



### 4.1.1 La modélisation et la gestion des paramètres dans la génération des scénarios

Plusieurs auteurs ont fait des propositions sur la manière de modéliser les paramètres de l'environnement en vue de leurs utilisations pour la description des scénarios.

Bagschik et al. (Bagschik et al., 2018) utilisent une représentation en 5 couches (Road-level (L1), Traffic infrastructure (L2), Temporary manipulation of L1 and L2 (L3), Objects (L4), Environment (L5)) pour mettre en place une ontologie de description des scènes de conduite en vue de la création des scénarios. Dans cette ontologie, les relations entre les paramètres sont modélisées (Exemple : « Yellow vehicle » is « located\_on » « Position #3 ») ainsi que les interactions entre les couches. En vue d'évaluer les concepts proposés, une ontologie comprenant 284 classes, 769 axiomes logiques et 75 règles du web sémantique, a été élaborée pour la génération des scènes des infrastructures autoroutières allemandes.

Ainsi, l'ontologie proposée est très utile et répond à un besoin existant aujourd'hui en ce qui concerne la modélisation de l'environnement opérationnel du VA. Cependant, la manière dont les scènes obtenues vont être utilisées pour construire les scénarios n'est pas traitée. De plus étant donné que les scènes sont obtenues sur la base d'un langage naturel, elles doivent être converties en des formats de données qui sont simulables.

Menzel et al. (Menzel et al., 2019) utilisent les scénarios fonctionnels proposés par Bagschik et al. comme point de départ pour ensuite les détailler et les transformer en des formats simulables comme OpenDRIVE et OpenScenario. Pour ce faire, les termes décrivant le scénario fonctionnel sont structurés suivant les 5 couches de Bagschik et al., et sont détaillés avec des paramètres. Les paramètres sont choisis selon les formats de données requis pour la simulation (ici OpenDRIVE et OpenSCENARIO). Par ailleurs, les dépendances entre les paramètres et les contraintes pour choisir leurs valeurs sont prises en compte via trois catégories de relations : « arrangement relations, object dependencies and parameter dependencies ».

Une telle proposition permet de fournir les éléments de base pour l'obtention des scénarios logiques notamment l'espace de variation des paramètres et les fichiers de données pour la simulation. Cependant, tous les éléments requis pour la simulation ne sont pas spécifiés, notamment les véhicules qui seraient équipés d'une fonction de conduite automatisée. Aussi, dans l'implémentation actuelle de la proposition, les connaissances détaillant l'espace de variation des paramètres et leurs contraintes de gestion sont directement modélisées dans le code source et ne sont donc pas fournis explicitement.

D'un autre côté, Chen et al. (Chen & Kloul, 2018) ont également utilisé des ontologies dans leur approche de génération des cas d'utilisation du VA sur autoroute. En effet, ils ont défini trois ontologies pour la caractérisation et la conceptualisation des éléments composant les cas d'utilisation : l'ontologie de l'autoroute, l'ontologie de la météo et l'ontologie du véhicule. Puis, la logique du premier ordre a été utilisée pour décrire les relations et les règles entre les éléments constitutifs de ces ontologies.

Néanmoins, la méthodologie proposée nécessite d'être améliorée pour anticiper tous les comportements du VA. Il faut modéliser dans un langage formel les cas d'utilisation générés, en vue de garantir leur robustesse et fiabilité.

Amersbach et al. (Amersbach & Winner, 2019b), abordent le problème de l'explosion de l'espace des paramètres qui est dû à la multitude de paramètres décrivant parfois un scénario et aux différentes valeurs que peut prendre chacun de ces paramètres. Selon les auteurs, cette

explosion résulte aussi du pas de discrétisation choisi pour discrétiser chaque espace (ou plage de valeurs) de chaque paramètre. Pour surmonter une telle explosion, ils développent l'idée d'effectuer les tests de validation en optant pour une décomposition fonctionnelle de la fonction de conduite automatisée en plusieurs couches : « Information access, Information reception, Information processing, situational understanding, Behavioral decision, Action ». Avec la solution proposée, la dimension du nombre de tests requis diminue considérablement. Cependant, nous pouvons noter que les auteurs n'ont pas démontré le fait que le test des couches fonctionnelles puisse remplacer le test du système complet.

Les travaux que nous venons d'analyser portent sur la question de la modélisation et du choix des paramètres des scénarios, de leur représentation et de l'explosion combinatoire qui peut en découler. Comme nous pouvons le constater, cette problématique est difficile, et n'a pas encore été résolue de façon satisfaisante.

#### 4.1.2 Les techniques utilisées dans la génération (automatique) de scénarios de test

Dans cette section, nous présentons quelques techniques qui ont été utilisées pour générer des scénarios à partir des représentations possibles des paramètres.

Prasanna et al. (Prasanna, Sivanandam, Venkatesan, & Sundarrajan, 2005) proposent un tour d'horizon sur les techniques (ou approches) de génération de cas de test. On retrouve les techniques suivantes : « random, path-oriented, goal-oriented and intelligent approaches ». Les « random techniques » sont des techniques aléatoires qui déterminent les cas de test sur la base d'hypothèses concernant les distributions des données d'entrée de l'élément testé. Elles peuvent permettre d'obtenir de nombreux cas de test, mais sont inefficaces dans la recherche de cas de test satisfaisant des exigences. Les « path-oriented techniques » utilisent généralement des informations sur le flux de contrôle en vue d'identifier un ensemble de chemins à couvrir pour générer les cas de test. Elles n'ont pas besoin de techniques optimisées pour la génération des cas de test. Cependant, le chemin à identifier, peut être infaisable car le générateur de cas de test peut échouer à trouver une entrée qui traverse ce chemin.

Les « goal-oriented techniques » identifient les cas de test couvrant un but sélectionné tel qu'une déclaration ou une branche, indépendamment du chemin emprunté. Enfin, les « intelligent techniques » sont des techniques intelligentes de génération automatique de cas de test. Elles sont pratiques et efficaces pour différents types de systèmes logiciels. Néanmoins, elles reposent parfois sur des calculs « complexes ».

En outre, d'autres approches sont identifiées avec l'arrivée des outils de modélisation. Les auteurs les ont classées en deux catégories : la génération de cas de test basée sur les spécifications et celle basée sur les modèles. Ces approches ont l'avantage d'être pratiques car dotées d'une flexibilité et d'une possibilité d'automatisation des tests. Toutefois, l'explosion combinatoire des paramètres à considérer dans la génération peut être un frein à leur usage.

Mahadik et al. (Mahadik, Bhattacharyya, & Kim, 2016) proposent également une revue de techniques de génération automatisée de cas de test. On y retrouve les techniques citées précédemment. Ils les classifient selon les catégories suivantes : « Random Test Data Generation Random, Symbolic Test Case Generation Technique, Static Test Generation,

Dynamic Test-data Generation (Execution of the program), Search-based Automatic Test Case Generation (application of optimization technique (OT)) ». Par ailleurs, on constate la présence de techniques basées sur l'optimisation : « Hill climbing (HC), Genetic Programming, the Memetic algorithms (MAs), Tabu Search (TS), Simulated Annealing ». Elles utilisent des méthodes basées sur la recherche (search based method) pour générer les cas de test. Le « Hill climbing (HC) » est un algorithme de recherche local qui se base sur un principe itératif pour tenter de trouver la meilleure solution à un problème. Le « Genetic Programming » s'inspire de l'évolution biologique pour trouver des programmes informatiques qui exécutent une tâche définie par l'utilisateur. Il s'agit d'une spécialisation des algorithmes génétiques. Quant aux algorithmes mémétiques « Memetic algorithms », elles sont des métaheuristiques qui utilisent à la fois la recherche globale et locale. En outre, le « Tabu Search » est une technique de recherche métaheuristique fondée sur le principe selon lequel, pour être qualifiée d'intelligente, la résolution de problèmes doit intégrer une mémoire adaptative et une exploration dynamique (évolutive). Enfin, le recuit simulé « Simulated Annealing » est un type de technique de recherche globale dont le principe est similaire à celui du Hill Climbing. Après avoir échantillonné la zone entière, il recombine le résultat en vue de l'améliorer.

L'ensemble de ces techniques basées sur l'optimisation considère le problème de génération de cas de test comme un problème d'optimisation. Elles peuvent permettre d'avoir de bons résultats. Cependant, elles produisent parfois un très grand espace de recherche.

Outre les papiers de type revue de la littérature, nous avons trouvé d'autres travaux qui exposent également des techniques pouvant être utilisés dans le cadre de la génération de tests. Sarmiento et al. (Sarmiento, Leite, Almentero, & Sotomayor Alzamora, 2016) proposent une méthode automatisée pour la génération de scénarios de test qui consiste à utiliser un langage spécifique « Restricted-form of Natural Language (RNL) » pour la description des scénarios. L'utilisation du RNL vise à limiter le vocabulaire utilisé dans la description et à définir des règles de syntaxe communes pour les phrases. En raison de l'ambiguïté des langages naturels, les scénarios obtenus nécessitent quelques améliorations avant de les utiliser pour le MBT (Model-based Testing) automatisé. Pour ce faire, les défauts sont identifiés et corrigés via un module de vérification de scénario. Ensuite, une méthode de transformation de modèle est implémentée pour traduire les scénarios du modèle informel au modèle formel en utilisant les réseaux de Petri. Enfin, les modèles de réseaux de Petri sont utilisés pour la génération automatisée des scénarios de test. L'utilisation du MBT est adaptée pour automatiser la génération des tests et l'intégration des critères de génération permet d'optimiser le processus de génération. Cependant, le MBT nécessite une construction appropriée du modèle et un choix adapté de notations formelles. De plus, le plein succès de la méthode proposée suppose que les ingénieurs utilisent la syntaxe et les règles sémantiques proposées par les auteurs.

Les techniques de génération de cas de test présentées dans cette section ont pour la plupart été implémentées dans le domaine du logiciel. Elles présentent certes des avantages, mais au vu de leurs inconvénients (inefficacité en cas d'explosion des paramètres, non identification de cas de test satisfaisant une exigence en particulier, complexité de la technique, large espace de recherche à explorer, utilisation de syntaxe ou de sémantique dédiée), nécessitent d'être approfondies davantage dans le cadre de leur utilisation pour la validation du VA. De ce fait, on pourrait se demander quelles sont les approches qui sont aujourd'hui utilisées dans le

contexte du VA. Ainsi, dans la partie suivante, nous présentons quelques stratégies de génération de scénarios, élaborées spécifiquement dans le contexte du VA.

#### 4.1.3 Les stratégies de génération de scénarios dans le contexte du VA

S. Prialé et al. (Prialé Olivares, Rebenik, Eichberger, & Stadlober, 2015) souhaitent générer des scénarios de conduite virtuelle via une approche stochastique pour le test des ADAS. Pour ce faire, ils proposent de générer les routes à l'aide des méthodes de Monte-Carlo par Chaînes de Markov (MCMC). Le MCMC aide à générer les éléments de construction géométrique de la route, dont les distributions de probabilité sont difficiles à calculer et simuler à cause du nombre de paramètres élevé. L'algorithme de MCMC utilisé est celui de Metropolis. Une telle approche stochastique peut donc être très appréciée dans le contexte du VA. Toutefois, l'approche employée ne met pas en avant les paramètres critiques qui sont présents dans les données du monde réel (l'analyse intégrant la fonction de densité de ces paramètres critiques n'est pas effectuée).

Chen et al. (Chen & Kloul, 2018) se sont basés sur les concepts statiques et mobiles décrits dans les trois ontologies (Autoroute, Météo et Véhicule) qu'ils ont proposées, pour mettre en place une hiérarchie à trois couches (couche de base, couche d'interaction et couche de génération) permettant de générer les cas d'utilisation du VA. Pour ce faire, la scène est obtenue au niveau de couche de génération en utilisant les concepts décrits dans la couche de base et les relations de la couche d'interaction. Cependant, l'aspect statique des scènes générées a conduit dans la suite de leurs travaux (Chen & KLOUL, 2019) à utiliser la technique de modélisation PEPA (Performance Evaluation Process Algebra) pour générer des scénarios. L'intérêt est porté alors sur la couche de génération en vue de modéliser les transitions dynamiques entre les différentes scènes pour l'obtention des scénarios.

Cette approche (utilisant la modélisation PEPA) est intéressante car elle fait partie des quelques approches qui présentent comment utiliser les scènes générées pour l'obtention des scénarios. Toutefois, son implémentation s'est faite sur un périmètre restreint. Il faut donc qu'elle soit étendue en intégrant dans la modélisation d'autres entités telles que l'impact de la météo.

La chaîne de simulation proposée par Hallerbach et al. (Hallerbach et al., 2018) vise à l'identification de scénarios critiques. Pour définir les scénarios critiques, les auteurs ont introduit de nouvelles métriques de qualité du trafic, en plus des métriques de mesure de risque standards, telles que le temps de collision (time-to-collision), le temps de freinage (time-to-brake), la décélération requise (required-deceleration). Pour définir les métriques de qualité du trafic, ils introduisent le concept de Domaine d'Intérêt (Domain of Interest - DOI) qui prend en compte l'évolution du Véhicule Ego et son environnement immédiat. Ce DOI est fonction de sous-métriques décrites à différentes échelles : macroscopique, microscopique, nanoscopique et la métrique individuelle (the macroscopic grade, the microscopic grade, the nanoscopic grade and the individual metric). Comme les sensibilités des métriques sont différentes, une optimisation est effectuée à l'aide des données d'entraînement afin d'améliorer leur poids et d'augmenter l'efficacité de la note globale.

L'idée de proposer de nouvelles métriques liées à la qualité du trafic est innovante et intéressante dans le contexte de l'identification des scénarios critiques pour le VA. Néanmoins,

l'approche globale proposée pour identifier les scénarios critiques a été implémentée dans le cas du MIL (Model-In-the-Loop). Son utilisation et sa conformité dans le cas d'autres types de test (« X-in-the-Loop methods, benches, and driving tests ») doivent être démontrées.

Feng et al. (Feng et al., 2020a) ont proposé une stratégie de génération qui se focalise sur la recherche de scénarios critiques pour construire une bibliothèque destinée à l'évaluation des métriques de performance du CAV (« Connected and Automated Vehicle »). Pour ce faire, les auteurs ont introduit la notion de « testing value » (valeur de test) qui fait référence à une fonction d'importance, selon laquelle les scénarios sont échantillonnés. La criticité d'un scénario est déterminée en associant ce scénario à la fonction d'importance. Cela signifie que plus la fonction d'importance d'un scénario est grande, plus sa probabilité d'échantillonnage est élevée, et donc les scénarios critiques seront identifiés et testés. Par conséquent, les scénarios qui composent la bibliothèque sont ceux avec une fonction d'importance supérieure à un seuil. Pour rechercher les scénarios critiques dans tout l'espace des scénarios, une fonction objectif auxiliaire donne des directions de recherche, une méthode d'optimisation à démarrage multiple (« a multi-start optimization ») est appliquée pour obtenir des scénarios critiques locaux et enfin, la méthode de remplissage par diffusion (« the seed-fill method ») est appliquée à la recherche des scénarios voisins des scénarios critiques locaux choisis comme points de départ. Comme le modèle de substitution (Surrogate model) utilisé pour identifier les scénarios critiques présente des disparités, une exploration est également effectuée en combinaison avec l'exploitation de la bibliothèque. Cette exploration permet d'identifier les scénarios critiques manqués. Par conséquent, les scénarios de la bibliothèque sont échantillonnés en fonction de leur valeur de criticité et pour faire face à l'exploration, les scénarios en dehors de la bibliothèque sont échantillonnés avec une faible probabilité. Enfin, les distributions de probabilité de test sont définies en fonction de l'exploitation et de l'exploration.

La stratégie proposée est très intéressante pour nous, car elle vise le même objectif à savoir identifier l'ensemble des scénarios nécessaires à la validation du VA. De plus, la notion de fonction d'importance développée permet de mettre en avant les scénarios critiques et donc de garantir une convergence rapide de la génération vers le seuil de précision voulu.

Toutefois, dans la méthode, les auteurs utilisent une fonction objectif dont la conception peut être difficile à élaborer. De plus, cette fonction est dépendante de la manœuvre du CAV considéré.

G. Mullins et al. (Mullins et al., 2017) ont développé une méthode pour générer des scénarios variés et difficiles pour les tests de véhicules autonomes. La méthode consiste à se concentrer sur les limites de performance du système en échantillonnant les régions limites. Pour ce faire, une méthode de recherche adaptative est utilisée pour générer notamment des échantillons dans ces régions limites. La technique d'échantillonnage adaptatif est un processus itératif consistant à soumettre des requêtes au SUT (System Under Test), à utiliser les scores renvoyés pour générer un méta-modèle, puis à appliquer une métrique d'information à ce méta-modèle pour générer un nouvel ensemble de requêtes. Les régions limites sont définies comme des régions de l'espace de test où de petits changements dans le scénario entraînent des transitions entre les modes de performance du système. Les modes de performance du système sont identifiés à l'aide de techniques de clustering non supervisées.

L'utilisation d'une approche d'échantillonnage adaptatif vise à identifier toutes les limites de performance possibles du système et n'est pas exclusivement dédiée aux plus extrêmes. Aussi,

cette approche, évite d'être confrontée à la difficulté de concevoir des fonctions objectif d'optimisation qui sont parfois dépendantes des systèmes. Cependant, la méthode proposée suppose des comportements d'autonomie déterministes du système, et ne peut donc pas être appliquée à des systèmes autonomes qui ont des moteurs de décision stochastiques.

Dans leur article, Zhao et al. proposent une approche accélérée de l'évaluation de la sécurité des VAs, en particulier en cas de cut-in<sup>9</sup> dangereux avec le choix de la collision frontale (ici l'avant du VA entre en collision avec le véhicule précédent) comme type d'accident cible à analyser (D. Zhao et al., 2017). Les auteurs avaient introduit dans leurs travaux précédents la méthode d'évaluation accélérée et les techniques d'échantillonnage de l'importance. Dans cet article, ils visent à fournir une évaluation accélérée avec une grande précision en utilisant la théorie de l'échantillonnage d'importance et la méthode de l'entropie croisée pour trouver la bonne distribution de l'IS (Importance Sampling). Pour ce faire, ils définissent une distribution théorique optimale de l'IS qui est conditionnée par l'occurrence de l'événement d'intérêt. Cette distribution ne peut être directement utilisée mais a l'avantage d'avoir une variance qui est de zéro. Ainsi, avec la « Cross entropy » (entropie croisée), la distribution de l'IS sera choisie parmi une famille de distribution en calculant la KL (Kullback–Leibler) divergence par rapport à la distribution théorique optimale. Le but est de retenir une distribution pour laquelle la KL par rapport à la distribution théorique optimale reste faible de telle sorte que les deux distributions soient proches et que la variance soit proche de zéro. Une telle méthode a l'avantage de permettre d'identifier les événements rares et d'améliorer le temps de validation. Cependant, et comme le souligne Lakomicki et al. (P Lakomicki, Castanier, & Grall, 2018), peu de paramètres sont utilisés pour caractériser la dangerosité du cas d'utilisation. Sachant que tous les paramètres existant dans l'environnement opérationnel peuvent affecter le comportement du véhicule, cette méthode ne peut pas être utilisée pour prétendre à l'exhaustivité de l'exploration de toutes les situations que le véhicule va rencontrer. De plus la méthode proposée n'a été appliquée que dans le cas d'une manœuvre opérationnelle (« Cut-in »).

Gietelink et al., (Gietelink, De Schutter, & Verhaegen, 2006) sont eux aussi confrontés à un problème similaire au nôtre dans le sens où leur travail s'inscrit dans le cadre de la validation probabiliste des systèmes avancés d'aide à la conduite. Ils proposent un algorithme aléatoire, basé sur l'échantillonnage d'importance adaptatif, pour générer les échantillons. L'efficacité de l'approche proposée a été prouvée suite à son implémentation sur un problème simple d'ACC (Adaptive Cruise Control). Toutefois, son application pour un système complexe et de niveau d'automatisation supérieure comme le VA (niveau 3 à 5) ne peut être systématique et nécessite une démonstration supplémentaire.

En synthèse, nous pouvons constater que les travaux présentés dans cette section poursuivent un même objectif, à savoir générer des scénarios pour la validation du VA. Les méthodes et stratégies employées diffèrent et présentent chacune des avantages. En effet, certaines stratégies s'appuient sur les ontologies et permettent d'aboutir à l'obtention des scénarios grâce à des

---

<sup>9</sup> Pour rappel, un « cut-in » est une manœuvre de dépassement et de rabattement rapide, c'est-à-dire le fait pour un véhicule de s'engager dans l'espace situé devant un autre véhicule et ce, de façon relativement dangereuse. Les cut-in sont potentiellement dangereux et peuvent entraîner des collisions.

techniques supplémentaires pour tenir compte de la dynamique des scénarios. D'autres propositions ont prouvé leur efficacité grâce à l'utilisation des méthodes d'apprentissage ou encore de méthodes d'échantillonnage telles que l'échantillonnage adaptatif et l'échantillonnage d'importance, en vue d'optimiser la génération.

Cependant, on observe des manques dans les stratégies proposées pour ce qui est des aspects suivants :

- la capacité de la stratégie à assurer une couverture des scénarios pertinents pour la validation du VA,
- la capacité à tenir compte de la criticité de certains paramètres,
- ou encore sur son évolutivité dans le cas d'un nombre de paramètres plus élevé ou d'un niveau d'automatisation plus élevé,
- ou enfin la réutilisation de la stratégie, notamment dans le cas où il est nécessaire de définir la fonction objectif (qui est difficile à élaborer).

Ces manques observés dans ces stratégies, doivent être comblés si nous voulons disposer de méthodes efficaces de génération et de validation par simulation de la sécurité du VA.

De ce fait, il y a un besoin à combler, notamment celui de mettre en place une stratégie complète de génération de scénarios et de validation, qui en tienne compte.

Ainsi, dans la section suivante, nous proposons une autre manière d'aborder la génération des scénarios, en adaptant la décomposition sur trois niveaux d'abstraction proposés par Menzel et al. (Menzel et al., 2018). La stratégie proposée s'appuie sur les concepts présentés dans le chapitre 2 et sur les indicateurs de performance définis dans le chapitre 3.

## 4.2 STRUCTURE DE LA METHODOLOGIE PROPOSEE POUR LA GENERATION DE SCENARIOS

Dans cette section, nous présentons la structure de la méthodologie de génération de scénarios, dont nous détaillerons les différentes étapes dans les sections suivantes.

Notre stratégie de génération s'inscrit dans un principe de structuration qui décline la génération en trois niveaux : génération de scénarios fonctionnels, logiques puis concrets. Le processus présenté dans la figure 16 illustre les étapes clés de la stratégie proposée. Il se subdivise en deux grandes phases : (I) le choix de la fonction d'automatisation et la définition de son contexte d'utilisation (AI, partie en gris) et (II) la génération des scénarios suivant les trois niveaux (AII, partie en bleu). Chaque phase comprend plusieurs étapes (ou activités) qui permettent de répondre à notre objectif.

La première phase vise à fixer le périmètre d'étude et à définir la fonction d'automatisation considérée. Elle consiste d'abord à définir l'ODD associé à la fonction d'automatisation (A1), puis les performances fonctionnelles attendues de la fonction (A2). Viennent ensuite les modes et manœuvres opérationnels associés (A3), enfin les critères de validité associés à chacun des modes et manœuvres opérationnels (A4).

La seconde phase vise à générer les trois catégories de scénarios.

Les scénarios fonctionnels sont obtenus en identifiant d'abord, les situations fonctionnelles (A5), puis les types d'évènements potentiellement associés (A6). Le principe d'identification

des situations puis des évènements fait référence à la manière dont nous avons défini un scénario (*description dans un intervalle de temps donné, de l'enchaînement temporel de situations opérationnelles. Le passage d'une situation (initiale) à une autre (intermédiaire) est causé par un ou plusieurs évènements*).

Les scénarios logiques s'obtiennent en définissant les paramètres de chaque scénario fonctionnel et en identifiant les plages de valeurs associées (A7). Ces plages sont, ensuite, combinées pour obtenir l'ensemble des scénarios logiques associés à chaque scénario fonctionnel (A8).

Les scénarios concrets associés à chaque scénario logique sont obtenus dans la dernière étape (A9). En vue de procéder à la simulation des scénarios concrets qui sont générés, les critères d'arrêt de leur simulation sont définis (A10). Par ailleurs, l'activité d'obtention des scénarios concrets est délicate, d'autant plus qu'elle va permettre de mesurer l'ensemble des indicateurs de performance que nous avons définis (Couverture, représentativité, criticité, indicateur final de risque et la prise en compte de l'incertitude).

Ainsi, pour accompagner la génération, une stratégie d'exploration des scénarios qui sert à estimer les indicateurs et valider la sécurité du VA, est proposée (AII.4). En effet, devant la multiplicité des scénarios concrets auxquels sera confronté le VA, il apparaît nécessaire de procéder à un échantillonnage en vue de prioriser les scénarios pertinents du point de vue des indicateurs de performance identifiés. De plus, en intégrant les indicateurs de criticité et de sensibilité tels que nous les avons spécifiés dans le chapitre 3, cela signifie que la stratégie proposée, et plus particulièrement celle de l'échantillonnage des scénarios concrets, combine à la fois une analyse a priori et une analyse a posteriori des scénarios générés et simulés, le tout dans un processus itératif.

L'information recueillie à chaque étape de l'itération permet d'alimenter le calcul de l'indicateur final de risque en vue de l'estimation des performances de sécurité du VA pour la fonction d'automatisation considérée.

La suite du chapitre explique comment chaque activité du processus est spécifiée, pour répondre à l'objectif global attendu de ce travail.



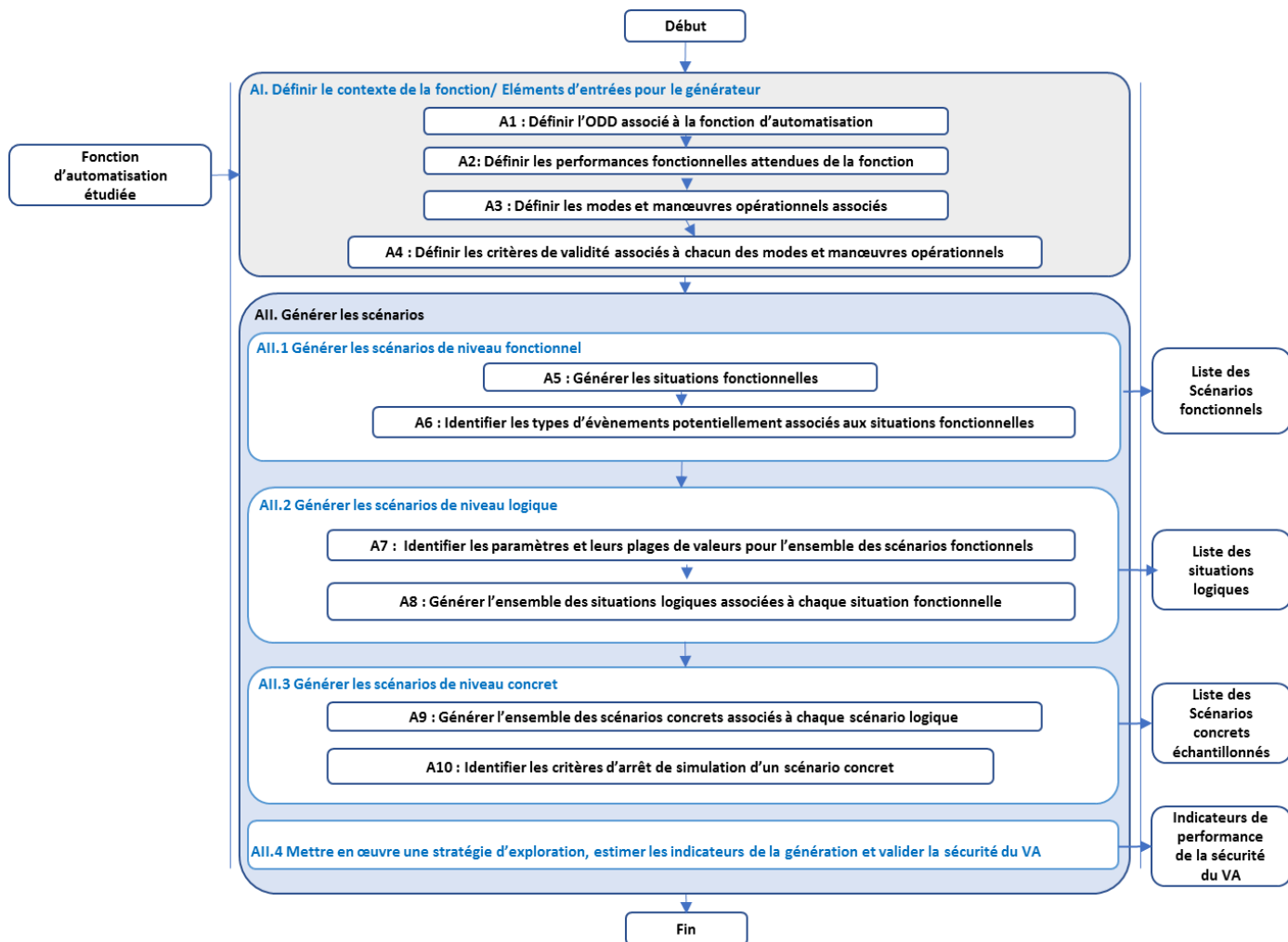


Figure 16 : Structure de la méthodologie proposée pour la génération de scénarios

#### 4.3 AI : DEFINIR LE CONTEXTE D'UTILISATION DE LA FONCTION D'AUTOMATISATION

C'est la première phase du processus de génération des scénarios. Comme évoqué, elle permet non seulement de fixer le périmètre de l'étude mais aussi d'identifier les éléments d'entrée pour la génération des scénarios. Elle se fait en quatre étapes :

- La première activité (A1) consiste à définir l'ODD associé à la fonction choisie

La description de l'ODD se fait en s'appuyant sur le modèle conceptuel (Figure 11) présenté dans le chapitre 2. En effet, nous avons organisé cette description de sorte à mettre en avant le concept de situation opérationnelle. Cela permet d'avoir une connaissance de l'état du VA (les informations sur les propriétés de l'Ego, à savoir, la fonction d'automatisation considérée, le niveau d'automatisation et la plage de vitesse correspondante) et des autres entités présentes

(l'infrastructure physique, les conditions de la météo et les autres usagers de la route). Cette activité se fait en support avec le concepteur de la fonction car il dispose d'une connaissance de sa spécification et des besoins client.

- La deuxième activité (A2) porte sur l'identification des performances fonctionnelles attendues de la fonction choisie

L'intérêt de cette activité est qu'elle permet d'approfondir la connaissance de la fonction d'automatisation en identifiant les performances attendues. Comme nous l'avons présenté dans le chapitre 2, c'est la base pour l'identification des limitations de performance fonctionnelle et des potentiels « hazardous behaviours » du VA qu'il faudra tester. Ainsi, la connaissance des comportements attendus du VA permet d'identifier ceux qui sont indésirables et par la même occasion d'obtenir les critères de fin de simulation de scénario que nous définirons dans l'activité 10. De même que l'activité précédente, cette activité nécessite un support car elle relève des spécifications du constructeur.

- La troisième activité (A3) concerne l'identification des modes et manœuvres opérationnels associés

Toujours dans le but d'améliorer notre connaissance de la fonction, nous proposons de spécifier également les modes et manœuvres opérationnels dans lesquels elle peut se retrouver ou qu'elle peut exécuter lors de son utilisation. Cette information est utile pour qualifier de façon précise le comportement du véhicule au moment de la survenue d'un quelconque événement. La manière dont ces modes et manœuvres peuvent être définis a été développé dans le chapitre 2.

- La dernière activité (A4) de cette phase de définition de contexte de la fonction est l'identification des critères de validité associés à chacun des modes et manœuvres opérationnels

Ces critères de validité caractérisent les modes et manœuvres opérationnels. D'abord, cela permet d'identifier leurs conditions d'enclenchement et de validité. Ensuite, cette information aide à qualifier les événements dont l'apparition engendre des changements ou des phases de transitions entre modes et manœuvres opérationnels.

En synthèse, cette phase AI permet de spécifier la fonction d'automatisation choisie, en définissant son ODD, ses performances fonctionnelles, puis les modes et manœuvres opérationnels associés ainsi que leurs critères de validité. Une fois cela fait, l'ensemble des informations récoltées va permettre de procéder à la phase de génération des scénarios (AII). Elle se fait en trois sous-phases dont la première est la génération des scénarios fonctionnels.

## 4.4 AII.1 GENERER LES SCENARIOS DE NIVEAU FONCTIONNEL

La complexité de l'environnement opérationnel du VA a conduit à différentes classifications des situations. Chacune d'elles répond à un contexte d'application particulier : sécurité routière/accidentologie, identification des zones de navigation possibles du VA, identification des acteurs et contraintes auxquels doit s'adapter le VA, définition du modèle comportemental du VA, besoin d'hierarchisation du processus de génération de test, ... Ces contextes donnent lieu chacun, à une configuration de situation possible dans laquelle le VA peut se retrouver.

Par ailleurs, nous avons défini les manœuvres opérationnelles comme permettant de décrire les différents comportements du véhicule et avons proposé des règles d'unicité et de complétude pour leur identification (chapitre 2). Etant donné que c'est le comportement du VA que nous voulons tester, la manœuvre opérationnelle semble être un point de départ pertinent pour aborder le problème de génération de scénarios. Ainsi, de même que la plupart des travaux dans le contexte du VA, nous proposons de caractériser les scénarios fonctionnels par des manœuvres opérationnelles. Comme exemples, on parlera donc de scénario fonctionnel de « car following » ou de « Lane changing ». Toutefois, la définition d'un scénario (= situation + évènement) exige que nous apportions encore plus de détails à cette caractérisation, notamment en définissant les situations fonctionnelles et les évènements que l'on peut retrouver dans un scénario fonctionnel.

- A5. Générer les situations fonctionnelles

Différentes classifications de situation existent selon différents contextes d'application. Bien qu'ayant défini la situation comme décrivant l'état du VA et des autres entités de son environnement opérationnel, nous devons lors de la génération des situations fonctionnelles, rester cohérent avec la définition du niveau fonctionnel donné par Menzel et al. A ce stade de l'identification, l'information détaillée sur les paramètres et leurs valeurs n'est pas à renseigner, le but étant simplement de connaître les configurations de situations qu'il faudra prendre en compte lors de la génération des scénarios de test. De ce fait, l'identification des situations fonctionnelles proposée ici, est basée principalement sur les informations recueillies lors de la définition de la fonction d'automatisation, de son contexte d'utilisation ou encore des manœuvres opérationnelles. La figure 17 montre le processus d'obtention des situations fonctionnelles. Elles sont obtenues par combinaison des renseignements fournis par l'ODD (type de densité de trafic, Type d'infrastructure), et des modes et manœuvres opérationnels. La densité du trafic peut être fluide, embouteillée ou en accordéon. Elle est liée au nombre d'utilisateurs présents dans le trafic (c'est-à-dire autour du VA).

Exemple : si  $\text{Nombre\_usagers} < 3$  alors le trafic est fluide, sinon le trafic est embouteillé ou en accordéon.

Quant à l'infrastructure, plusieurs types tels que ceux définis dans le chapitre 2 (Tableau 3) peuvent être rencontrés.

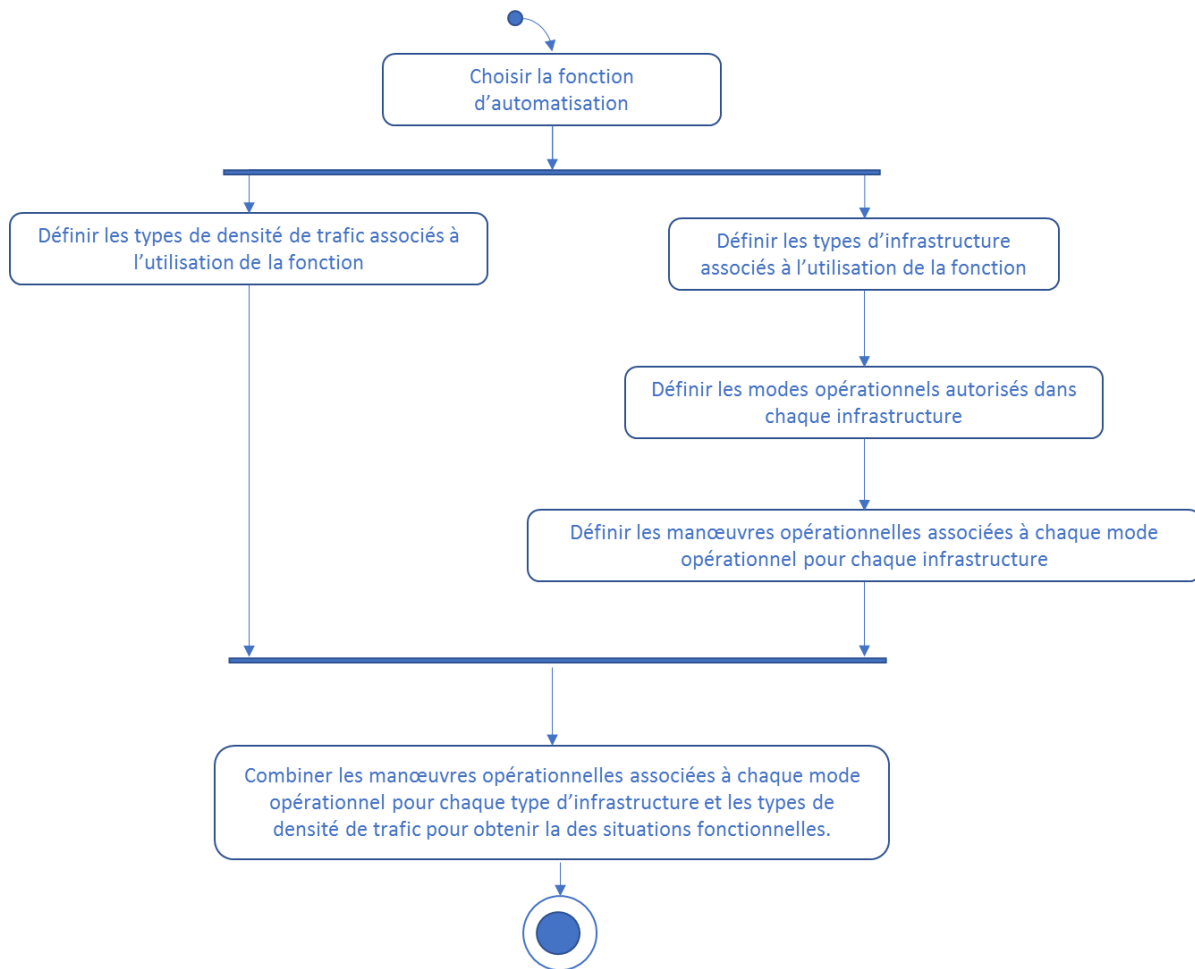


Figure 17 : Processus d'obtention des situation fonctionnelles

En outre, une fois les déclinaisons de situations fonctionnelles effectuées, une description linguistique est requise si l'on veut être conforme à la définition du scénario fonctionnel. Toutefois, nous ne développerons pas cet aspect dans ce travail de thèse. Le lecteur pourra se référer aux travaux de Bagschik et al. (Bagschik et al., 2018). En effet, les scènes initiales et les scénarios fonctionnels qu'ils génèrent sont obtenus à partir d'une approche basée sur les connaissances. Il s'agit plus particulièrement de l'utilisation d'ontologie qui permet d'obtenir la description linguistique souhaitée grâce à la structure des informations suivant un modèle de cinq couches. En ce qui nous concerne, nous procéderons à une description de plus en plus fine des scénarios lors de la spécification des niveaux d'abstraction logiques, puis concrets.

Le processus d'obtention des situations fonctionnelles étant décrit, il faut définir les types d'évènements qui leur seront associés pour construire un scénario.

- Identifier les types d'évènements potentiellement associés aux situations fonctionnelles (A6)

Nous avons défini un évènement comme étant la modification de l'état d'une ou plusieurs entités de l'environnement (VA et autres) qui induit, peut induire ou doit induire une nouvelle action de la part du VA (nouveau comportement). Cela se traduit en d'autres termes par le fait

qu'un paramètre prenne une valeur différente de sa valeur initiale. En conséquence, tous les paramètres de l'environnement opérationnel du VA peuvent être à l'origine d'évènements. Certains évènements sont critiques et d'autres ne le sont pas. Les évènements critiques sont ceux qui peuvent augmenter la criticité d'un scénario. Nous les avons identifiés lors de la définition de l'indicateur de criticité (dans le chapitre 3, section 3.3.3.1.1). Il s'agit ici de tous les facteurs qui peuvent être à l'origine des limitations de performance du VA. Ils ont été organisés dans le chapitre 3 en évènements survenant à l'intérieur de l'ODD (Tableau 13) et ceux apparaissant en dehors de l'ODD (Tableau 14).

L'objectif dans cette étape (Activité 6) est d'identifier les évènements pouvant avoir un fort impact sur le comportement du VA et dans la confiance que l'on peut lui accorder, car ce sont ces évènements qu'il va falloir prioriser dans la génération.

L'identification des situations fonctionnelles et des types d'évènements permet d'obtenir l'ensemble des scénarios fonctionnels recherchés.

L'activité suivante fait partie de la phase d'obtention des scénarios logiques. Il s'agit de s'intéresser aux différents paramètres de la génération en identifiant leurs plages de valeurs, en vue de leur utilisation pour la suite du processus de génération.

#### 4.5 AII.2 GENERER LES SCENARIOS DE NIVEAU LOGIQUE

C'est la phase intermédiaire pour que les scénarios soient simulables par la suite. Il s'agit de faire apparaître les espaces de variation (ou plages de valeurs) des paramètres de toutes les entités présentes (Infrastructure, Autres usagers, Conducteurs/Passagers, Conditions atmosphériques, VA) dans le scénario fonctionnel. Suivant la manière dont ces espaces de variation sont découpés, un scénario fonctionnel aura un nombre plus ou moins important de scénarios logiques qui lui seront associés. Ainsi, nous verrons d'abord, comment nous avons identifié les paramètres et découper leurs espaces de variation en plusieurs sous espaces de variation (ou plages de valeurs). Puis, nous analyserons comment générer les scénarios logiques en combinant les plages de valeurs obtenues et cela en prenant en compte les contraintes d'association et la cohérence des scénarios.

- A7 : Identifier les paramètres et leurs plages de valeurs pour l'ensemble des scénarios fonctionnels

Nous faisons l'hypothèse de modélisation suivante : **la connaissance de l'expert va nous permettre de découper les espaces de variation et définir un nombre minimal de plages pour chaque paramètre, en fonction de son impact sur le VA** : le VA sera plus ou moins sensible à chaque plage.

Mais avant, commençons par la détermination des paramètres. Nous avons mentionné dans le chapitre 2 (section 2.4) l'existence de différents paramètres (paramètres de variabilités et les paramètres invariants) à considérer dans la génération des scénarios et plus particulièrement pour la description des scénarios. Paramétriser consiste ici à définir l'ensemble des paramètres associés à chaque entité présente dans la génération.

On rencontre différents types de paramètres (variables) dans l'ODD du VA :

- les variables qualitatives (nominale, ordinale, binaire). Par exemple : variable nominale = « Type d'usagers [piéton, cycliste, véhicule] », variable ordinale = « niveau de luminosité [Faible, Moyen, Fort, Très fort], Niveau de précipitation [Faible, Moyen, Fort, Très fort], Position [Gauche, Droite, Devant, Derrière, ...] », et variable binaire = « Type de roulage [Gauche, Droite] ».
- les variables quantitatives (discrètes et continues). Par exemple : variable discrète = « Nombre de voie [1, 2, 3 et plus] », variable continue = « Vitesse\_véhicule [0 à 130 km/h], Pluviométrie [0 à 100 mm/h] ».

Comme ces paramètres sont nombreux et la plupart ont des plages de valeurs continues, nous avons jugé bon de distinguer leurs plages de valeurs qui ont une contribution significative dans l'estimation de l'atteinte des performances de sécurité du VA. **Cette distinction est réalisée par un expert en sûreté de fonctionnement du VA.**

En outre, la discrétisation de données en statistique répond en général à des contraintes logiques, techniques ou visuelles et imposent de connaître le type de distribution auquel l'on a affaire.

Discrétiser consiste à effectuer une transformation qui peut se traduire par un découpage en classes, des données dont l'on dispose. Il s'agit souvent de transposer un état continu en un équivalent discret. Plusieurs méthodes statistiques de discrétisations existent (Discrétisation selon l'écart à la moyenne, Discrétisation en classes d'égale amplitude, Discrétisation selon les seuils naturels, Discrétisation selon les quantiles, ...). Dans le cas d'un nombre de paramètres important ayant des plages de valeurs continues, le pas de discrétisation doit être choisie suivant une analyse pertinente pour éviter toute explosion combinatoire.

Toutefois, le découpage en classes que nous voulons effectuer vise à s'assurer que nous couvrons bien le maximum de situations critiques possibles que le véhicule rencontrera. Pour cela, nous avons introduit une contrainte logique qui est de **faire apparaître dans nos classes les sous espaces de variation qui pourraient provoquer des situations critiques pour le VA.** Ainsi, à défaut d'avoir un seul espace de variation pour chaque paramètre, celui-ci pourra se retrouver avec plusieurs sous espaces de variation (plages de valeurs). Cela signifie que les facteurs de criticité (provenant des types d'évènements) qui sont des causes de limitation de performances, pourront être mis en avant au travers d'espaces de variation.

Prenons l'exemple du paramètre « niveau de pluviométrie » dans le cas de la météo. A défaut de spécifier uniquement une plage de valeur de la pluviométrie variant de 1 à 100 mm/h, nous proposons deux classes de variation : Faible = 1 à 7 mm/h et Forte = 8 à 100 mm/h. Les technologies de capteurs étant pour certaines sensibles aux fortes précipitations, un tel découpage permet de mettre en avant la plage de pluie forte, qui lorsqu'elle est combinée à d'autres paramètres, augmente davantage la possibilité d'avoir des scénarios logiques qui ont un fort impact de criticité.

De ce fait, ce découpage en sous espaces de variation (ou plages de valeurs) que nous préconisons est principalement guidé par une volonté de ciblage des scénarios logiques qui permettront de cibler les scénarios concrets critiques. L'inconvénient est que le découpage peut aboutir à une explosion combinatoire surtout si en plus des nombreux paramètres, les sous espaces de variation sont également nombreux. Nous tenons compte de ce challenge, de par la manière dont les scénarios logiques seront sélectionnés et échantillonnés pour l'obtention des scénarios concrets.

La section suivante consiste à établir le principe suivant lequel les combinaisons des espaces de variation sont effectuées pour l'obtention des scénarios logiques.

- A8 : Générer l'ensemble des situations logiques associées à chaque situation fonctionnelle

Un aspect important doit être pris en compte tout au long de la génération, notamment lors de la combinaison des plages de valeurs pour l'obtention des scénarios logiques. Il s'agit de la cohérence des scénarios par rapport à la réalité. En effet, les scénarios décrits doivent être le reflet de ce qui est possible dans la réalité. Pour s'en assurer, des contraintes d'association et/ou des relations de dépendance doivent être établies pour éviter la génération de scénarios dépourvues de sens. Pour identifier ces contraintes, les informations fournies par le code de la route ou les codes de bonnes pratiques, le retour d'expériences (données météorologiques, les données sur l'infrastructure routière, les données du trafic disponibles, les données sur la sécurité routière, ...) ont été utilisées.

S'ajoute également une analyse d'expert que nous jugeons utile pour corroborer l'ensemble des contraintes collectées. Par ailleurs, l'analyse peut être affinée en exploitant le profil de mission avec des outils statistiques. En effet, une analyse de la corrélation ou de la régression (statistique) serait appréciée en vue d'établir la relation entre le VA et l'évolution dynamique des autres usagers présents dans le scénario.

Toutefois, le choix de recourir à une telle analyse statistique ou à une autre, sera fonction de la stratégie d'échantillonnage envisagée pour la génération des scénarios concrets. Pour notre part, nous considérons une modélisation des contraintes sous forme de conditions logiques et numériques comme il est préconisé dans la définition du scénario logique.

Une fois les contraintes identifiées, le but de la génération des scénarios logiques va être de combiner les sous espaces de variation des paramètres en tenant compte de ces contraintes. Les contraintes apparaissent alors comme des vérificateurs. Ainsi, la génération des scénarios logiques se transforme en la résolution d'un problème combinatoire. En outre, il est à noter que l'intégration des contraintes permet non seulement d'obtenir la cohérence recherchée lors de la combinaison des espaces de variation des paramètres mais aussi, de réduire le champ des possibles en éliminant les combinaisons non pertinentes.

Pour obtenir les scénarios logiques, nous avons choisi de procéder en deux phases pour rester cohérent avec notre définition du scénario (= situation + évènement) : (1) générer les situations logiques, puis (2) identifier les évènements associés.

Les situations logiques s'obtiennent par combinaison des plages de valeurs des paramètres décrivant chaque situation fonctionnelle. Nous avons choisi de procéder à une méthode de combinaison systématique : c'est-à-dire que chacun des sous espaces de variation de chaque paramètre apparait dans chaque combinaison obtenue.

**Par exemple**, supposons que nous ayons ces trois paramètres à utiliser pour la description des scénarios : Nombre\_voies, Vitesse\_AutreVehicule.1 (km/h) et Vitesse\_Ego (km/h). Les plages de valeurs de chacun de ces paramètres sont présentées dans le tableau 18 :

Paramètres	Plages de valeurs	Variables
Nombre_voies	2	A1_1
	3 et plus	A1_2
Vitesse_AutreVehicule.1 (km/h)	Faible [0, 60 km/h]	A2_1
	Elevée (> 60km/h)	A2_2
Vitesse_Ego (km/h)	Faible [0, 60 km/h]	A3_1

Tableau 18 : Exemple de paramètres et plages de valeurs pour l'obtention de situations logiques

En combinant ces plages de façon systématique (2 plages\*2 plages \*1 plage), on obtient les 4 situations logiques suivantes :

- Situation logique 1 : A1\_1, A2\_1, A3\_1 = 2 voies \* Vitesse\_AutreVehicule.1.Faible \* Vitesse\_Ego.Faible
- Situation logique 2 : A1\_1, A2\_2, A3\_1 = 2 voies \* Vitesse\_AutreVehicule.1.Elevée \* Vitesse\_Ego.Faible
- Situation logique 3 : A1\_2, A2\_1, A3\_1 = (3 et plus) voies \* Vitesse\_AutreVehicule.1.Faible \* Vitesse\_Ego.Faible
- Situation logique 4 : A1\_2, A2\_2, A3\_1 = (3 et plus) voies \* Vitesse\_AutreVehicule.1.Elevée \* Vitesse\_Ego.Faible

Par ailleurs, la manière de définir et d'obtenir les évènements sera développée lors de la mise en place d'une stratégie d'exploration (Section 4.7, AII.4).

La définition de l'ensemble des paramètres et leurs plages de valeurs, puis l'obtention des situations logiques après combinaison des plages de valeurs, permet de disposer de données exploitables numériquement. La section suivante décrit comment les utiliser pour procéder à la génération des scénarios concrets.

#### 4.6 AII.3 : GENERER LES SCENARIOS DE NIVEAU CONCRET

C'est la dernière phase pour obtenir des scénarios qui seront utilisés pour effectuer la validation par simulation.

- A9 : Générer des scénarios concrets associés à chaque scénario logique

Un scénario concret est un scénario instancié, pouvant être introduit dans un simulateur de VA, après avoir été converti dans un format compatible avec l'outil de simulation. Les scénarios concrets servent à la réalisation des simulations et à l'estimation du risque associé au VA. Ils sont générés à partir d'un scénario logique (situation logique + évènement), par le choix d'une valeur (concrète) dans l'espace de variation (ou plages de valeurs) de chaque paramètre de ce scénario logique. Le choix de la valeur concrète dans une plage de valeur, se fait à l'aide de méthodes d'échantillonnage. Il peut s'agir soit de fixer au préalable un pas de discrétisation, soit d'avoir recours à des méthodes d'échantillonnage plus élaborées reposant sur les fonctions de densités des plages de valeurs des paramètres. Avant d'effectuer cette génération de valeurs



concrètes, nous proposons dans la section 4.7 (via la phase AII.4), une stratégie d'analyse en amont qui va aider et guider le processus de génération.

Toutefois, étant donné que nous avons besoin de contrôler la simulation lors des tests, des critères d'arrêt de simulation d'un scénario concret ont été définis dans l'étape suivante.

- A10 : Identifier les critères d'arrêt de simulation d'un scénario concret

D'une part, nous souhaitons générer des scénarios à simuler (Scénario généré = Situation initiale + Evènement). Placé dans une situation initiale de roulage, le VA doit détecter un évènement potentiellement pertinent pour la modification de sa conduite. Il se trouve alors dans une situation intermédiaire. En fonction de sa réaction (ou non), la situation du VA va évoluer et se stabiliser dans une situation finale pour la simulation.

D'autre part, nous voulons analyser les résultats en fin de simulation d'un scénario (une fois la réaction du VA observée dans la situation finale). La difficulté est donc de définir les critères de fin de simulation d'un scénario. Pour cela, il va falloir déterminer quand la simulation d'un scénario est terminée, ou quand on peut l'arrêter (car la prolongation de la simulation ne fournira plus d'information pertinente).

Pour identifier ces critères, nous nous sommes basés sur : (1) les performances fonctionnelles attendues du VA (Activité A2), (2) les critères de validité des modes et manœuvres opérationnels et (3) sur une analyse des évènements redoutés. En effet, les performances fonctionnelles ont permis au travers d'une analyse de risque de connaître les évènements redoutés (hazardous behaviour » avec une sévérité de type collision) qui, dès lors qu'ils surviennent dans une situation intermédiaire, aboutissent à une situation finale avec préjudice (harmful situation) : la simulation peut être arrêtée, elle a fourni une information pertinente. Aussi, le scénario étant principalement caractérisé par la manœuvre, les critères de validité associés à cette dernière vont servir à savoir si la manœuvre est terminée ou non, et s'il y a violation de l'une de ses conditions de validité. Pour rappel, la figure 14 définie dans le chapitre 3 montre une classification des situations finales obtenues après simulation.

Ainsi, de l'ensemble de ces analyses, nous avons retenu 5 critères qui permettent de juger la pertinence de l'arrêt de la simulation d'un scénario :

1. Présence de collision
2. Demande de give back (il s'agit d'une demande de reprise en main faite par le VA au conducteur)
3. Fin de la manœuvre / changement de manœuvre (cela peut inclure un changement de mode comme le retour à un Etat safe)
  - Distance de sécurité rétablie (elle dépend de la vitesse)
  - Le VA n'est plus en situation dangereuse (par exemple, suite à un cut-in) si le Time To Collision est redevenu supérieur à un seuil
  - Critères de fin d'un scénario = Fin de la validité de la manœuvre opérationnelle du VA (elle a fini d'être exécutée) => Analyse du changement dans la manœuvre du VA (TIV (Temps Inter Véhicule) qui évolue brusquement, Demande de Give back, Collision, Etat safe).

4. Violation d'une condition de validité de la manœuvre ou présence de HB (Hazardous behaviour) : il s'agit d'analyser tout changement dans la manœuvre opérationnelle en cours du VA (Exemple : Evolution brusque du TIV)
5. En outre, nous proposons une « Durée maximale d'un scénario (en cas d'absence de changement de manœuvre) » qui permet d'éviter une boucle infinie (le scénario s'arrête au bout d'une durée maximale, à définir).

Par ailleurs, on pourrait se demander comment repérer systématiquement un comportement anormal du véhicule mettant un autre usager en danger. Nous verrons au travers des deux exemples ci-dessous que cela est pris en compte dans nos analyses.

- Exemple 1 : le VA ne s'arrête pas en présence d'un piéton arrêté au niveau du passage piéton

Nous avons structuré l'environnement physique du VA avec un paramètre « type d'infrastructure ». Le fait de tester le VA en infrastructure de type « zone piétonne ou passage piéton » signifie qu'il est possible de générer des événements de type « présence de piétons » et que le VA est supposé s'arrêter si le piéton est encore engagé sur le passage piéton à l'approche du VA. D'une part, dans un tel test, le non arrêt du VA peut mener à la collision avec le piéton (critère de fin du scénario). D'autre part, au bout de la durée maximale du scénario, on peut détecter grâce à ce test, un comportement anormal du VA (il n'a pas percuté le piéton mais ne s'est pas arrêté en présence d'un piéton engagé sur le passage piéton).

- Exemple 2 : Cas d'un scénario de « Turn Left »

Un véhicule voulant tourner à gauche se met sur la voie de gauche pour tourner à gauche. Donc si le VA ne se met pas sur la file de gauche suite à une demande de « turn left », c'est un comportement anormal. Il y a donc violation d'une condition de validité de la manœuvre « Turn Left », à savoir le positionnement sur la chaussée.

Devant le nombre élevé de scénarios logiques, et la multiplicité des scénarios concrets qu'il est possible d'obtenir (en théorie, une infinité à partir du moment où une plage de valeurs est continue), la mise en place d'une stratégie d'exploration et d'échantillonnage de l'espace des scénarios s'impose.

## 4.7 All.4 : Mettre en œuvre une stratégie d'exploration, estimer les indicateurs de la génération et valider la sécurité du VA

### 4.7.1 Proposition d'une stratégie d'exploration

La stratégie qui oriente la manière d'explorer l'espace des scénarios et leur échantillonnage doit être guidée par des indicateurs. Dans notre cas, les indicateurs qui seront utilisés sont ceux définis dans le chapitre 3 : *indicateur de criticité*, *indicateur de risque final*, *intervalle de confiance (prise en compte de l'incertitude)*, *indicateur de couverture statistique*, *indicateur de représentativité statistique*. Une fois mise en place, une telle stratégie doit permettre d'adresser deux dimensions à savoir la définition d'une heuristique de génération des scénarios concrets, puis l'estimation de l'indicateur final de risque associé au VA. Cet objectif global peut être

atteint en deux phases avec plusieurs sous-objectifs comme nous pouvons le voir dans le tableau 19.

Une première phase concerne l'obtention des scénarios avant la simulation. Elle vise à faire une première identification des scénarios concrets qu'il faudra générer pour la simulation.

La deuxième phase porte sur l'exploitation des résultats de la simulation des scénarios concrets au fur et à mesure de son déroulement. Lors de cette phase, le niveau de dangerosité des scénarios simulés, et donc la nécessité, ou non, de poursuivre leur génération, sera connue. Cette phase permettra d'alimenter la manière d'explorer l'espace des scénarios et permettra d'aboutir à une estimation finale des indicateurs retenus.

Phases	Sous-objectifs
Lors de la génération (obtention des scénarios concrets)	<ul style="list-style-type: none"> <li>• Identifier et obtenir les scénarios potentiellement critiques et non critiques</li> <li>• Faire le travail d'identification et d'obtention des scénarios en assurant la consistance (cohérence) et la couverture /représentativité par rapport à la réalité<sup>1</sup></li> </ul>
Pendant et après simulation (Exploitation des scénarios concrets)	<ul style="list-style-type: none"> <li>• Confirmer les scénarios critiques et non critiques</li> <li>• Utiliser cette confirmation pour renforcer la détection et l'obtention des scénarios critiques</li> <li>• Estimer l'atteinte de l'objectif de validation en termes de <math>10^{-x}/h</math></li> <li>• Montrer (qualitativement ou par calcul) que tout le processus (la manière dont les scénarios sont identifiés) permet d'optimiser le temps de validation initialement requis<sup>2</sup> d'un facteur<sup>3</sup> <math>r</math>.</li> </ul>

Tableau 19 : Sous-objectifs visés lors de la génération des scénarios concrets

1. La réalité est donnée par le profil de missions et les roulages.
2. Le temps de validation (en simulation ou en roulage) initialement requis  $T_i$  est une autre formulation de l'objectif de validation  $10^{-x}/h$  (Exemple : L'objectif de validation est  $10^{-6}/h$  pour la fonction d'automatisation considérée (TJC) et son équivalent en temps de validation est  $T_i = 1.2 * 10^6$ .) L'atteinte de l'objectif de validation avec optimisation de temps de validation revient à montrer, entre autres, que la performance de la méthode permet de réduire le temps  $T_i$  d'un facteur  $r$  (Voir l'indicateur de gain de durée de validation défini dans le chapitre 3, section 3.3.6).
3. Le facteur  $r$  représente alors la performance que notre méthode permet d'atteindre.

Nous avons envisagé différentes options d'exploration des scénarios logiques. Ces options d'exploration sont non exclusives et peuvent se présenter comme suit :

- 1) Exploration par le niveau de sensibilité : tirer les scénarios suivant le niveau de sensibilité a priori du VA au scénario logique.
- 2) Exploration par « le pire cas » : tirer les scénarios « les pires cas » et explorer leurs voisins, jusqu'à revenir à une zone non critique. Le « pire cas » est également qualifié au regard de la sensibilité qui suppose un ordre de sensibilité entre les plages de valeurs de chaque paramètre.

- 3) Exploration par la couverture : couvrir l'ensemble des scénarios logiques générés ; tirer au moins un scénario concret pour chaque scénario logique.
- 4) Exploration par la représentativité par rapport au profil de mission : tirer les scénarios de sorte que la répartition statistique que l'on obtient au fur et à mesure soit conforme au profil de mission
- 5) Coupler les étapes précédentes
  - Exemple : coupler l'option 1 et l'option 4, et mettre un filtre progressif selon le niveau de sensibilité du scénario logique.

L'exploration par « le pire cas » telle que décrite ne sera pas la stratégie d'exploration que nous retiendrons dans ce travail. Cependant, la formulation retenue pour l'exploration permettra tout de même de pouvoir cibler les situations les plus critiques pour le VA. Aussi, comme proposé dans le chapitre 3, l'indicateur de représentativité doit être adressé à l'issue de l'estimation de risque et une fois la cible de validation atteinte. Son utilité se révèle dans le besoin de rassurer davantage le client en assurant une représentativité statistique de la génération par rapport à l'utilisation habituelle qu'elle a de l'Ego véhicule. Ainsi, l'exploration par la représentativité ne sera pas privilégiée dans un premier temps car l'objectif de la génération et de la simulation est avant tout de cibler les scénarios permettant de garantir le niveau de sécurité cible pour le VA. Rappelons que l'espace des situations à explorer comporte certainement de nombreuses zones qui n'exposent pas (ou peu) le VA à des dangers. Les simulations portant sur ces zones doivent être limitées.

Les options d'exploration qui ont retenu notre attention sont celles par le niveau de sensibilité et la couverture. Le couplage de ces deux options donne une exploration par niveau de sensibilité et de couverture, permettant de tenir compte des indicateurs de criticité et de couverture que nous avons définis dans le chapitre 3. Ce choix d'exploration s'explique comme suit.

D'abord, l'intérêt de l'indicateur de sensibilité que nous avons proposé est qu'il permet d'une part, de se focaliser sur les scénarios potentiellement à risque pour le VA, et d'autre part, d'avoir une stratégie itérative de génération combinant à la fois une analyse a priori et une analyse a posteriori de la criticité des scénarios. En effet, la contribution des scénarios à risques dans la démonstration de l'atteinte de l'objectif de validation reste très significative comparée aux scénarios à faible sensibilité pour le VA, et permet d'avoir une estimation rapide de l'indicateur de risque final selon le niveau de précision voulu.

De plus, puisque les situations d'intérêt de type accident (« harmful situation ») sont rares (Feng et al., 2020a), (Kelly, Sinha, Namkoong, Duchi, & Tedrake, 2018), (D. Zhao et al., 2017), les scénarios à risques pouvant conduire à de telles situations sont eux-mêmes peu fréquents et peuvent être difficilement testables par roulage. D'où l'importance de la mise en place en amont de la simulation, d'une analyse élaborée qui guidera l'échantillonnage.

Aussi, avec la prise en compte des analyses a posteriori liées à l'indicateur de criticité (évaluation des scénarios après simulation), on aura une confirmation de criticité qui permettra de guider la manière d'explorer l'espace des scénarios.

Ensuite, l'intérêt de l'indicateur de couverture est qu'il vient en support à l'exploration par niveau de sensibilité. Il permettra tout au long de l'exploration par niveau de sensibilité, d'avoir

un regard sur le taux de scénarios logiques qui ont pu être tirés pour servir à échantillonner les scénarios concrets.

La figure 18 reprend de façon plus détaillée le principe que nous proposons pour la génération des scénarios concrets.

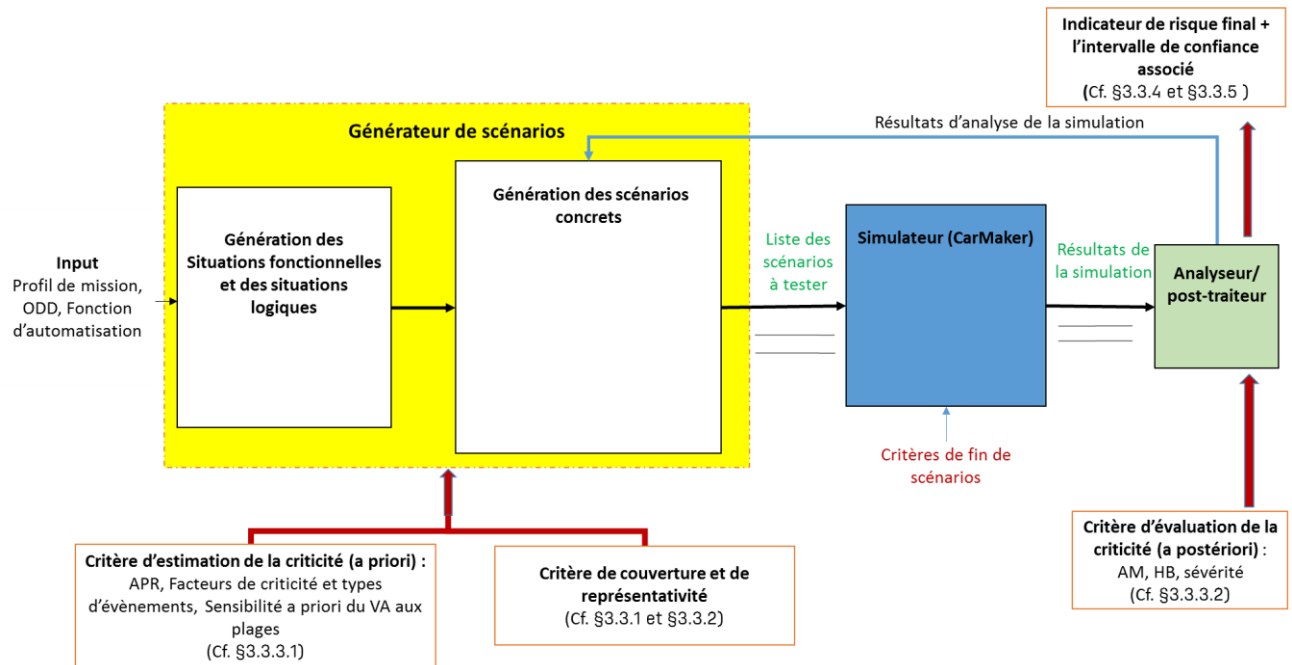


Figure 18 : Principe de génération et de validation par simulation des scénarios concrets

Le bloc en jaune représente le générateur. Il se subdivise en deux blocs : un bloc qui représente l'obtention des situations fonctionnelles et logiques, telle que spécifiées dans les paragraphes 4.4 et 4.5, puis un bloc pour l'obtention des scénarios concrets.

Afin de pouvoir définir la stratégie d'obtention des scénarios concrets via une exploration des scénarios par niveau de sensibilité et de couverture, il importe de revenir sur l'analyse de sensibilité. Nous avons analysé dans le chapitre 3, comment obtenir la sensibilité a priori du VA aux plages de variation. Pour que les scénarios puissent être échantillonnés selon des niveaux de sensibilité, il faut définir comment à partir de l'analyse de sensibilité a priori du VA à une plage, on obtient la sensibilité au niveau de la situation et de l'évènement. Etant donné que les scénarios concrets sont obtenus à partir des scénarios logiques, c'est au niveau logique que nous proposons de mener cette analyse de sensibilité. La section suivante explique comment calculer la sensibilité a priori du VA à une situation logique.

#### 4.7.2 Analyse de la sensibilité du VA aux situations logiques

En vue de répondre au premier sous-objectif visé dans la génération des scénarios concrets (Cf. Tableau 19) à savoir identifier les scénarios potentiellement critiques, nous allons procéder à une analyse de sensibilité du VA aux situations logiques.

Le calcul de la sensibilité a priori du VA aux situations logiques s'obtient en deux étapes. D'abord, nous considérons la sensibilité a priori du VA à chacun des sous espaces de variation

(ou plages de valeurs) caractérisant les paramètres de la génération suivant le principe décrit dans le paragraphe 3.3.3.1 du chapitre 3. Pour rappel, on considère la perception (avec cinq technologies de capteur), la décision et l'actionnement. Puis, pour chaque plage considérée, avec l'aide de l'expert, nous répondons à la question suivante :

***La technologie de capteur considérée (ou la décision ou l'actionnement) est-elle sensible ou non performante dans cette plage ?***

La réponse à cette question permet d'estimer la sensibilité a priori de chaque composante du VA (chaque technologie de capteur, décision, actionnement) à chacune des plages de valeurs d'un paramètre. Les réponses obtenues vont être utilisées pour déterminer la sensibilité a priori du VA à chaque situation logique. En effet, la situation logique est une combinaison de plages de valeurs. Nous proposons de calculer la sensibilité a priori du VA à une combinaison de plages (et donc à une situation logique) en agrégeant les sensibilités associées aux plages.

Pour permettre cela, nous avons fait le choix d'une échelle (tableau 15) décrivant la contribution d'une composante (Technologies de capteurs pour la perception, Décision, Action) du VA au calcul de la sensibilité a priori pour une plage.

Une nouvelle échelle (tableau 20) décrit la contribution de la sensibilité d'un organe du VA dans l'obtention de la sensibilité globale d'une situation logique. Cette nouvelle échelle présente une légère différence de formulation par rapport à la première (tableau 15). Le but est de faciliter le calcul de la sensibilité du VA à une situation logique, en déterminant directement la sensibilité de chaque organe (Perception, Décision, Action) à la situation logique. Chaque organe a une contribution maximale de 1 dans la sensibilité globale d'une situation logique. Nous faisons l'hypothèse que chaque technologie de capteur a une contribution de 1/5 (soit 0.2) dans la sensibilité à la situation logique si elle est impactée par au moins une plage de variation. Ainsi, la sensibilité d'une situation logique est comprise entre 0 et 3.

Reprenons les situations logiques 1 et 3 obtenues dans l'activité A8 (section 4.5) :

- Situation logique 1 :  $A1_1, A2_1, A3_1 = 2 \text{ voies} \times \text{Vitesse\_AutreVehicule.1.Faible} * \text{Vitesse\_Ego.Faible}$
- Situation logique 3 :  $A1_2, A2_1, A3_1 = (3 \text{ et plus}) \text{ voies} * \text{Vitesse\_AutreVehicule.1.Faible} * \text{Vitesse\_Ego.Faible}$

Les tableaux 21 et 22 présentent le calcul de la sensibilité pour chacune des deux situations logiques.

Contribution de la sensibilité d'une composante du VA (technologie de capteurs, décision, action) dans l'obtention de la sensibilité globale à une situation logique		
Classe	Description	Valeur correspondante
1	Une technologie de capteurs sur cinq est sensible à (ou leurrée par) une ou plusieurs des plages de valeurs composant la situation logique	0,2
2	Deux technologies de capteurs sur cinq sont leurrées par une ou plusieurs des plages de valeurs composant la situation logique	0,4
3	Trois technologies de capteurs sur cinq sont leurrées par une ou plusieurs des plages de valeurs composant la situation logique	0,6
4	Quatre technologies de capteurs sur cinq sont leurrées par une ou plusieurs des plages de valeurs composant la situation logique	0,8
5	Les cinq technologies de capteurs sont leurrées par une ou plusieurs des plages de valeurs composant la situation logique	1
	La décision prise par le VA (en l'absence d'un quelconque leurre vis-à-vis des capteurs) peut être leurrée par au moins une des plages de valeurs composant la situation logique	
	L'actionnement peut être leurré par au moins une des plages de valeurs composant la situation logique	

Tableau 20 : Proposition d'une échelle de contribution de la sensibilité d'une composante du VA dans l'obtention de la sensibilité d'une situation logique

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL1</b>							
A1_1							
A2_1							
A3_1							
Sensibilité de SL1 / composante							
Sensibilité de SL1	<b>0</b>						

Tableau 21 : Exemple de sensibilité d'une situation logique SL1

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL3</b>							
A1_2				1	1	1	
A2_1							
A3_1							
Sensibilité de SL3 /composante				0,2	0,2	1	
Sensibilité de SL3	<b>1,4</b>						

Tableau 22 : Exemple de sensibilité d'une situation logique SL3

Comme nous pouvons le voir, aucune composante n'a de sensibilité à une des plages présentes dans SL1. On obtient donc une sensibilité nulle. Dans le cas de SL3, seule la plage A1\_2 (nombre de voies = 3 et plus) peut leurrer à la fois deux capteurs ( $\Rightarrow$  contribution de 0.4 pour la sensibilité) et la décision ( $\Rightarrow$  contribution de 1 au calcul de sensibilité). On obtient une sensibilité de 1,4 pour SL3.

Par ailleurs, pour effectuer le tirage des scénarios, il faut tenir compte du caractère aléatoire de leurs occurrences comme mentionné dans le paragraphe 3.3.4 sur la prise en compte de l'incertitude dans le chapitre 3. Ainsi, la sensibilité du VA à une situation logique ne peut être utilisée telle qu'elle, pour effectuer la génération des scénarios concrets. De ce fait, nous proposons la mise en place d'une fonction de distribution de la sensibilité.

#### 4.7.3 Fonction de distribution de la sensibilité ou fonction d'importance des situations logiques

La fonction de distribution de la sensibilité  $q(Y_j)$  s'obtient en normalisant les sensibilités du VA aux situations logiques. Cette fonction de distribution permet de tirer l'une après l'autre, les situations logiques à partir desquelles seront générées par la suite les scénarios concrets à simuler. Comme nous pouvons le noter, dans une telle distribution, les situations logiques ayant des valeurs de sensibilité élevées auront également des valeurs de probabilité élevées et auront des occurrences plus fortes lors des tirages. Ainsi, sur la fonction de distribution de la sensibilité repose une fonction d'importance qui permet de privilégier le tirage de situations logiques  $Y_j$  pour lesquelles la sensibilité a priori du VA est élevée. La loi de probabilité de  $q(Y_j)$  se définit comme suit :

$$\begin{cases} q(Y_j) \in [0,1] \\ \sum_{Y_j} q(Y_j) = 1 \end{cases}$$

Soit  $S_j$  la sensibilité du VA à la situation logique  $Y_j$  et soit  $W = \sum_{Y_j} S_j$ , le facteur de normalisation. Ainsi la fonction de distribution de sensibilité ou d'importance peut être définie comme suit :

$$q(Y_j) = \frac{S_j}{W}$$

On peut vérifier que  $\sum_{Y_j} q(Y_j) = \sum_{Y_j} \frac{S_j}{W} = 1$ .



Par ailleurs, l'introduction de la fonction d'importance permet de mettre en place un échantillonnage d'importance dont l'utilisation a été préconisée dans des travaux précédents. En effet, la proportion des scénarios critiques étant très faible du fait de leur rareté (Kelly et al., 2018) (D. Zhao et al., 2017) (Feng et al., 2020a), leur identification ainsi que l'obtention d'un intervalle de confiance étroit (P Lakomicki et al., 2018) nécessiteraient un nombre de scénarios bien trop élevé (de l'ordre du million) pour que la simulation de Monte carlo soit utilisée (elle serait trop lente). Une alternative à ce problème est de recourir à d'autres méthodes d'échantillonnage dont l'échantillonnage d'importance (D. Zhao et al., 2017) (Feng et al., 2020a)(Gietelink et al., 2006). Ce type d'échantillonnage a fait ses preuves car il permet d'obtenir une vitesse de convergence rapide et une réduction du nombre de simulations.

Toutefois, avant de procéder à cet échantillonnage, il reste encore à considérer certains éléments. En effet, nous avons procédé à l'analyse de sensibilité sur les situations logiques. Cependant, pour générer des scénarios, il faut aussi créer des évènements. A ce titre, de même que pour la situation logique, une analyse de sensibilité sur les évènements sera introduite en vue de pouvoir également effectuer le tirage des évènements selon leur niveau d'impact potentiel sur le VA.

#### 4.7.4 Evènements et analyse de la sensibilité du VA, gradient de sensibilité et notion de voisinage

Rappelons qu'un évènement est la modification de l'état d'une ou de plusieurs entités de l'environnement (VA et autres) qui induit, peut induire ou doit induire une nouvelle action de la part du VA. Au niveau logique, les situations sont obtenues par combinaison de plage de variation. De ce fait, l'évènement se formule pour nous au niveau du changement de plage de valeurs pour un paramètre.

Le point d'entrée pour identifier les évènements est la situation logique initiale. L'évènement peut être soit une modification de la valeur d'un paramètre restant dans la même plage de valeurs ayant un certain niveau de sensibilité (le VA reste a priori dans la même situation logique), soit une modification d'une valeur d'un paramètre passant de la plage de valeurs initiale (de la situation logique initiale) vers une autre plage (d'une autre situation logique).

De ce fait, nous avons identifié trois niveaux d'impact possibles de l'évènement : fonctionnel, logique et concret.

La figure 19 illustre les trois niveaux d'impact. Considérons la situation logique SL1 appartenant à la situation fonctionnelle SF1.

- Impact fonctionnel : une fois généré, cet évènement fait passer d'une situation fonctionnelle à une autre. Par exemple, la modification d'une plage de valeurs de SL1 fait basculer vers une autre situation logique d'une situation fonctionnelle SF3.
- Impact logique : une fois généré, cet évènement fait passer d'une situation logique à une autre, à l'intérieur de la même situation fonctionnelle, fixée au départ. Par exemple, la

modification d'une plage de valeurs de SL1 fait basculer vers une situation logique SL3 appartenant également à SF1.

- Impact concret : une fois généré, cet évènement fait passer d'une situation concrète à une autre, à l'intérieur d'une même situation logique fixée au départ. Par exemple, aucune plage de SL1 n'est modifiée (les valeurs qui sont modifiées par l'évènement restent dans les mêmes plages de valeurs). Cependant, on considère une plage de valeurs de SL1 qui a un niveau de sensibilité non nulle. Le tirage d'une valeur concrète d'évènement à l'intérieur de cette plage, fait passer le VA d'une situation concrète SC1 à une autre SC2 à l'intérieur de SL1. Ainsi, par hypothèse, nous considérons que les autres évènements (issues des autres plages de sensibilités nulles) ne sont pas pertinents car non sensibles.

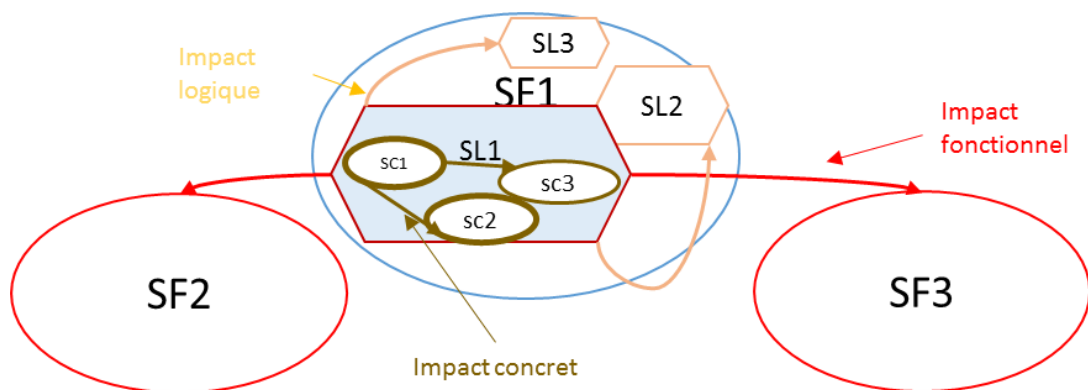


Figure 19 : Les trois niveaux d'impact d'un évènement

Les différents niveaux d'impact de l'évènement laissent entrevoir l'existence d'une variation du niveau de sensibilité pouvant lui être associée.

Ainsi, lorsque l'évènement concerne une modification de la valeur d'un paramètre dans une même plage de valeurs (impact au niveau concret), sa sensibilité s'obtient avec la sensibilité a priori du VA à la plage telle que définie dans le chapitre 3. Nous noterons par  $\Delta(Ax)$  un évènement concernant un changement de valeur à l'intérieur d'une même plage de valeurs Ax. Lorsque l'évènement est une modification avec changement de plage de valeurs (Impact logique ou fonctionnel) (nous noterons par  $\Delta(Ax, Ay)$  un évènement concernant un changement de plage de valeurs), la détermination de la sensibilité de cet évènement demande d'être élaborée davantage.

Nous proposons de la calculer au travers d'un concept que nous appelons « **gradient de sensibilité** ».

Nous définissons le gradient de sensibilité comme la valeur absolue de la différence de sensibilité entre deux situations logiques. Il est ainsi associé à l'évènement ayant provoqué le passage de la situation logique initiale vers une situation intermédiaire.

- Cas où l'évènement a un impact au niveau logique : bien qu'il soit possible de modifier simultanément plusieurs plages de valeurs (et donc de considérer l'occurrence simultanée de plusieurs évènements élémentaires), seule la modification d'une plage est

considérée dans le cadre de ce travail. En d'autres termes, nous ne considérerons que les événements élémentaires pour lesquels une seule plage de valeurs est modifiée.

Nous définissons aussi le concept de « *voisinage* ». En effet, lorsque nous sommes dans une situation fonctionnelle SF donnée, les situations logiques qui lui sont associées sont toutes connues. Ainsi, pour une situation logique  $SL_i$  de SF choisie, n'importe quel événement élémentaire impactant le niveau logique, permet d'aboutir à une autre situation logique (notée  $SL^*_i$ ) de SF, que nous appelons situation voisine de  $SL_i$  de niveau 1.

En considérant la possibilité de générer simultanément 2, 3 ou n événements élémentaires, on augmente considérablement l'explosion combinatoire de la génération des scénarios. De ce fait, dans ce travail de thèse, nous ne considérons que la génération d'événements élémentaires. Cela signifie que seul le *voisinage de niveau 1* des situations logiques sera considéré : partant d'une situation logique initiale  $SL_1$ , les situations logiques intermédiaires à considérer sont celles qui diffèrent d'une seule plage de valeurs. En outre, le gradient de sensibilité de l'événement impactant le niveau logique s'obtient par la valeur absolue de la différence de sensibilité entre la SL initiale et la SL intermédiaire (à l'intérieur d'une même SF). Etant donné que nous savons comment obtenir la sensibilité de chaque situation logique (paragraphe 4.7.2), le gradient s'obtient donc aisément.

**Par exemple**, on considère à nouveau les deux situations logiques 1 et 3 obtenues dans l'activité A8 (section 4.5) et le calcul de leurs sensibilités (Tableau 21 et 22) :

- Situation logique 1 :  $A1\_1, A2\_1, A3\_1 = 2 \text{ voies} * \text{Vitesse\_AutreVehicule.1.Faible} * \text{Vitesse\_Ego.Faible}$
- Situation logique 3 :  $A1\_2, A2\_1, A3\_1 = (3 \text{ et plus}) \text{ voies} * \text{Vitesse\_AutreVehicule.1.Faible} * \text{Vitesse\_Ego.Faible}$

Avec, sensibilité de  $SL_1 = 0$  et sensibilité de  $SL_3 = 1.4$

Si on considère  $SL_1$  comme la situation logique initiale, on voit que la modification de la plage  $A1\_1$  par  $A1\_2$  permet d'obtenir  $SL_3$  (situation logique intermédiaire). De plus cette modification ne concerne qu'une seule plage et donc,  $SL_3$  est une situation logique voisine de niveau 1 de  $SL_1$ .

Ainsi, vu que la « modification de  $A1\_1$  par  $A1\_2$  » conduit à l'obtention d'une autre situation logique ( $SL_3$ ), nous sommes bien en présence d'un événement impactant le niveau logique. La sensibilité de cet événement  $\Delta(A1\_1, A1\_2)$  s'obtient par le gradient (valeur absolue de la différence entre la sensibilité de  $SL_3$  et celle de  $SL_1$ ) et est égale à 1.4.

- Cas où l'événement a un impact au niveau fonctionnel : lorsqu'ils sont générés, les événements impactant le niveau fonctionnel font sortir le VA de la SF en cours d'analyse. Si tel est le cas, cela signifie que la nouvelle plage de valeurs est soit en dehors des conditions de validité de la manœuvre opérationnelle caractérisant la SF, soit en dehors de l'ODD.

Exemple : Alors que l'Ego est dans une situation fonctionnelle SF1 avec une manœuvre de « car following », l'occurrence de l'événement « passage de deux voies à une voie »

engendre un changement de voie et donc le passage à une autre manœuvre de type « Lane changing », dans une autre situation fonctionnelle SF2.

Pour obtenir le gradient de sensibilité de l'évènement impactant le niveau fonctionnel, on va s'intéresser à la nouvelle plage obtenue suite à la modification. Nous proposons de calculer sa sensibilité d'abord, en agrégeant les sensibilités de chaque technologie ou organe du VA (telle que définie dans le chapitre 3), puis en ajoutant un terme de 1 à cette valeur. En effet, nous considérons que, compte tenu du fait qu'un tel évènement induit un changement vers une autre SF, une difficulté supplémentaire s'ajoute à l'organe de décision du VA. Pour en tenir compte, nous avons décidé d'ajouter un terme de 1 à la sensibilité obtenue pour le changement de plage de valeurs.

Exemple : Le VA est dans une situation fonctionnelle de « car following ». Survient alors un évènement de perte du lead (on passe de Présence à Absence du front vehicle). La perte du lead n'impacte aucune technologie de capteur (contribution à la sensibilité = 0) mais fait basculer vers une autre SF, à savoir du Road Following (contribution à la sensibilité = 1). Le gradient associé à cet évènement est de 1. Le gradient de sensibilité pour l'évènement « perte du lead » est donc de 1.

Pour mieux structurer l'identification des évènements impactant le niveau logique ou fonctionnel et procéder au calcul des gradients de sensibilité une matrice ou un graphe peuvent être utilisés. Dans notre cas, nous avons choisi une représentation sous forme de matrice / tableau.

Pour ce qui est de l'impact au niveau logique, la matrice est construite en considérant le voisinage de niveau 1 de chacune des SL. En lignes, nous considérons l'ensemble des SL associées à une SF. En colonnes, nous plaçons pour chaque SL en ligne, ses SL voisines de niveau 1 vers lesquelles le VA arrive après survenue de l'évènement (changement d'une plage de valeur pour un paramètre dans la SL initiale). La case au croisement entre la SL en ligne et sa SL voisine en colonne contient l'évènement auquel on associe le gradient de sensibilité. Nous en verrons l'illustration dans le chapitre 5.

Concernant l'impact au niveau fonctionnel, la matrice est construite en considérant en lignes et en colonnes, l'ensemble des manœuvres associées à une fonction d'automatisation (chaque manœuvre opérationnelle caractérise une SF). Pour chaque ligne et chaque colonne, sont mentionnées dans la case au croisement, les évènements qui font passer le VA de la manœuvre en ligne vers celle en colonne. A chacun des évènements, on détermine le gradient de sensibilité correspondant. Une illustration sera également fournie dans le chapitre 5.

Enfin, nous souhaitons effectuer le tirage des évènements logiques selon leurs niveaux de sensibilité. Ainsi, de même que pour les situations logiques, une fonction de distribution de la sensibilité est requise.

#### 4.7.5 Fonction de distribution de la sensibilité des évènements

Le principe d'obtention de la fonction de distribution de sensibilité reste le même que dans le cas des situations logiques : elle s'obtient par normalisation des sensibilités ou gradient de sensibilité des évènements. Aussi, comme déjà noté, c'est la situation logique considérée qui

permet d'identifier les évènements qui peuvent lui être associés et que nous avons classé en trois types selon le niveau d'impact : impact fonctionnel, impact logique, impact concret. De ce fait, pour chaque situation logique  $Y_j$ , nous disposons d'une liste  $E_j$  d'évènements  $e_{ji}$ . Ce sont les évènements appartenant à cette liste qui seront normalisés pour obtenir la fonction de distribution de sensibilité  $q(e_{ji})$ .

La loi de probabilité de  $q(e_{ji})$  se définit comme suit :

$$\begin{cases} q(e_{ji}) \in [0,1] \\ \sum_{Y_j} q(e_{ji}) = 1 \end{cases}$$

Soit  $S(e_{ji})$  la sensibilité d'un évènement  $e_{ji}$  et soit  $W_{E_j} = \sum_{e_{ji}} S(e_{ji})$ , le facteur de normalisation pour la liste  $E_j$  d'évènements  $e_{ji}$ . Ainsi la fonction de distribution de sensibilité peut être définie comme suit :

$$q(e_{ji}) = \frac{S(e_{ji})}{W_{E_j}}$$

Nous vérifions que :  $\sum_{e_{ji}} q(e_{ji}) = \sum_{e_{ji}} \frac{S(e_{ji})}{W_{E_j}} = 1$

La mise en place de la fonction de distribution de sensibilité sur les évènements est l'avant dernière phase dans l'identification des éléments d'entrée requis pour définir notre heuristique de génération. En effet, l'un des sous objectifs visés pendant et après la simulation est de fournir à la fin de la génération, une estimation du risque en fonction de l'ensemble des scénarios concrets générés et simulés. Cela correspond à l'indicateur final de risque que nous avons défini dans le chapitre 3. Nous proposons de revenir sur cet indicateur afin de l'ajuster et l'adapter, suite aux propositions qui précèdent.

#### 4.7.6 Estimation de l'indicateur final de risque

Comme présenté dans le chapitre 3, l'estimation de l'indicateur final de risque  $P_k(\theta)$  sert à vérifier si la cible de validation de la fonction d'automatisation est atteinte ;  $\theta$  étant l'évènement d'intérêt (« Harmful situation » / Accident). La cible de validation est d'un ordre de  $10^{-x}/h$  pouvant aller jusqu'à  $10^{-9}/h$  selon la fonction considérée. Quant à l'estimation du risque, un niveau de confiance doit lui être associé pour tenir compte des incertitudes liées aux évaluations. Pour cela, nous avons besoin d'un critère de précision et d'un critère de couverture de la génération, qui fourniront aussi un critère d'arrêt de la génération et de la simulation. Ainsi, l'estimation globale s'articule en trois points : l'estimation de l'indicateur de risque  $P_k(\theta)$ , l'estimation de la précision et l'estimation de la couverture.

L'état de l'art sur les stratégies d'échantillonnage pour la validation par simulation du VA montre que la méthode d'estimation classique, à savoir la méthode de Monte Carlo, ne peut être utilisée dans ce contexte. Les travaux précédents (Kelly et al., 2018)(D. Zhao et al., 2017) (Feng et al., 2020b) (Feng et al., 2020a) montrent que cette méthode demande un nombre trop important d'échantillons et est trop lente pour obtenir une convergence rapide vers l'intervalle de confiance à la précision  $\beta$  visée. En effet, la probabilité  $P_f$  visée pour l'évènement d'intérêt

dans le contexte de cette validation est souvent très faible (ex :  $10^{-8}/h$ ). Atteindre un tel objectif, demande un nombre N de simulations proportionnel à l'inverse de  $P_f$  ; ce qui est bien trop élevé. Avant donc d'exposer la méthode d'échantillonnage des scénarios par le niveau de sensibilité que nous proposons, revenons sur la méthode de Monte Carlo pour en démontrer les limites face à notre problématique.

- **Estimation par la méthode de Monte Carlo**

Soient  $\theta$  l'évènement d'intérêt critique (collision, conduisant à une « harmful situation ») permettant de mesurer l'indicateur final de risque  $P_f$ , F l'espace des scénarios concrets critiques,  $\Omega$  l'espace des situations logiques  $Y_j$  associées à une situation fonctionnelle SF et  $SCji$  un i-ème scénario concret généré à partir de  $Y_j$ . La fonction indicatrice de F est telle que :

$$I_F = \begin{cases} 1, & \text{si } SCji \in F \\ 0, & \text{sinon} \end{cases}$$

La probabilité d'avoir un scénario concret qui appartient à l'espace F (c'est-à-dire qui engendrera un « harmful event ») est :

$$P_f = P(SCji \in F) = P(F) = E(I_F(SCji))$$

Soit l'échantillon ( $SC1_1, \dots, SCj_l, \dots, SCk_{NT}$ ) obtenu à l'issue de la k-ième itération avec NT le nombre total de scénarios concrets simulés jusqu'à cette itération.

Pour NT suffisamment grand, la loi des grands nombres stipule que :

$$Pr(\lim_{NT \rightarrow \infty} \tilde{P}_k = P_f) = 1$$

Ainsi, l'estimation  $\tilde{P}_k$  de  $P_f$  par le principe de Monte Carlo s'écrit à l'aide de la moyenne empirique :

$$\tilde{P}_k = \frac{1}{NT} \sum_{i=1}^{NT} I_F(SCji) = \frac{Nc}{NT}, \text{ avec } Nc \text{ le nombre total de scénarios concrets critiques.}$$

D'après le théorème central limite,  $\tilde{P}_k$  suit approximativement la loi normale  $N(E(\tilde{P}_k), \sigma^2(\tilde{P}_k))$ , avec :

$$E(\tilde{P}_k) = E\left(\frac{1}{NT} \sum_{i=1}^{NT} I_F(SCji)\right) = P_f$$

$$\begin{aligned} \text{et } \sigma^2(\tilde{P}_k) &= \text{var}\left\{\frac{1}{NT} \sum_{i=1}^{NT} I_F(SCji)\right\} = \frac{1}{NT} [E\{I_F(SCji)^2\} - E^2\{I_F(SCji)\}] \\ &= \frac{(P_f - P_f^2)}{NT} = \frac{P_f(1 - P_f)}{NT} \end{aligned}$$

L'estimateur  $\tilde{P}_k$  est sans biais et sa précision est donnée par le rapport de l'écart entre l'une des bornes de l'intervalle de confiance et la moyenne, et la probabilité à estimer.

$$\frac{u_{\frac{\alpha}{2}}}{P_f} \sqrt{\frac{P_f(1-P_f)}{NT}} = u_{\frac{\alpha}{2}} \sqrt{\frac{(1-P_f)}{P_f NT}}$$

Avec  $u_{\frac{\alpha}{2}}$  le quantile de la loi normale centrée réduite.

Pour s'assurer que cette précision soit inférieure ou égale à  $\beta$ , cela implique que

$$NT \geq u_{\frac{\alpha}{2}}^2 \frac{(1-P_f)}{P_f \beta^2}.$$

Ainsi, quand  $P_f$  tend vers 0 ( $\theta$  est rare), le nombre NT tend vers l'infini et donc le caractère très faible de  $P_f$  (ex :  $10^{-8}/h$ ) implique un nombre NT trop élevé. D'où la vitesse de convergence faible avec la méthode de Monte Carlo.

Il faut dans ce cas, recourir à des méthodes d'échantillonnage beaucoup plus efficaces pour accélérer la convergence vers la précision  $\beta$ .

- **Estimation par l'échantillonnage d'importance ou niveau de sensibilité des situations logiques**

La méthode d'échantillonnage que nous proposons est l'échantillonnage par le niveau de sensibilité d'une situation logique. Elle s'apparente à l'échantillonnage d'importance (Importance Sampling (IS)) dont nous avons constaté l'efficacité à travers les travaux précédents (Gietelink et al., 2006) (D. Zhao et al., 2017) (Feng et al., 2020b) (Feng et al., 2020a). L'IS permet d'échantillonner avec une importance plus grande les scénarios critiques pour le VA. Son principe est de remplacer la fonction de densité  $f$  d'un vecteur aléatoire par une densité  $f^*$  qui offre une vraisemblance plus grande pour l'évènement final d'intérêt, tout en compensant le biais introduit par ce changement de densité.

Dans les paragraphes précédents, nous avons spécifié un ensemble d'éléments qui vont nous servir à proposer une estimation de l'indicateur de risque : l'obtention des situations fonctionnelles, l'obtention des situations logiques, la sensibilité des situations logiques. L'estimation proposée se fait en référence aux situations logiques échantillonnées, puis aux scénarios concrets générés à partir de ces dernières.

Par ailleurs, l'estimation du risque proposée est faite situation fonctionnelle par situation fonctionnelle.

Soient  $SF$  une situation fonctionnelle parmi les situations fonctionnelles de la fonction d'automatisation considérée,  $Y_j$  une situation logique appartenant à  $SF$ ,  $\theta$  l'évènement d'intérêt critique (Harmful situation) permettant de mesurer l'indicateur final de risque  $P_k(\theta/SF)$  associé à  $SF$  au bout de la  $k$ -ième itération,

Soit  $Y_j$  un vecteur à  $L$  dimensions tel que :

$$Y_j = \begin{bmatrix} \text{plage } 1, k_1 \\ \text{plage } i, k_i \\ \dots \\ \text{plage } L, k_L \end{bmatrix} \begin{matrix} \text{Para } 1 \\ \text{Para } i \\ \dots \\ \text{Para } L \end{matrix}$$

Para  $i$  prend ses valeurs dans les plages Plage  $i,1$  ... Plage  $i,k_i$  ... Plage  $i,Nb_i$

$Y_j$  représente une situation logique appartenant à SF.  $Y_j$  est composé de L plages de valeurs correspondant aux L paramètres permettant de modéliser une situation logique.

plage  $i$ ,  $k_i$  est la  $k_j$  ème plage de valeurs du paramètre  $i$ .

Un paramètre  $i$  peut avoir jusqu'à  $Nb_i$  plages de valeurs.

Soit l'échantillon de situations logiques  $(Y_1, \dots, Y_K)$  tiré dans SF à l'issue de la K-ième itération.

La formule des probabilités totales permet d'écrire :

$$P(\theta | SF) = \sum_{Y_j} P(\theta | Y_j) P(Y_j),$$

avec  $P(\theta | Y_j)$  la probabilité d'occurrence de  $\theta$  sachant  $Y_j$  et  $P(Y_j)$  la probabilité d'occurrence de  $Y_j$ .

Soit SC $_{ji}$  le  $i$ -ème scénario concret généré à partir de  $Y_j$  et  $P(\theta | SC_{ji})$  la probabilité d'occurrence  $\theta$  sachant SC $_{ji}$ . Par hypothèse,  $P(\theta | SC_{ji})$  se comporte comme une fonction indicatrice :

$$P(\theta | SC_{ji}) = I(SC_{ji}) = \begin{cases} 1, & \text{si } SC_{ji} \text{ conduit à l'accident} \\ 0, & \text{sinon} \end{cases}$$

Ainsi, si  $N_{cj}$  est le nombre cumulé de scénarios concrets critiques obtenus avec  $Y_j$  et  $N_j$  le nombre cumulé de tirages de scénarios concrets effectués avec  $Y_j$ , alors l'on obtient une estimation de  $P(\theta | Y_j)$  telle que  $P(\theta | Y_j) \approx \frac{N_{cj}}{N_j}$ .

En remplaçant  $P(\theta | Y_j)$  par sa correspondance, et pour K le nombre de situations logiques tirées jusqu'à la k-ième itération, on a :

$$P_k(\theta | SF) \approx \sum_{j=1}^K \frac{N_{cj}}{N_j} P(Y_j)$$

Soit L le rapport de vraisemblance tel que  $L(Y_j) = \frac{p(Y_j)}{q(Y_j)}$ , avec  $q(Y_j)$  la distribution de sensibilité ou fonction d'importance de  $Y_j$  définie dans le paragraphe 4.7.3 ( $q(Y_j)$  donne la distribution de probabilité pour le tirage des  $Y_j$ ).

$$\begin{aligned} \text{On a alors } \tilde{P}_k(\theta | SF) &= \sum_{j=1}^K \frac{N_{cj}}{N_j} \frac{P(Y_j)}{q(Y_j)} * q(Y_j) \\ &= \sum_{j=1}^K \frac{N_{cj}}{N_j} L(Y_j) * q(Y_j) \end{aligned}$$

Ainsi, en échantillonnant  $Y_j$  par  $q(Y_j)$ , l'estimateur  $\tilde{P}_k(\theta | SF)$  de  $P(\theta | SF)$  par l'échantillonnage d'importance (IS) à l'issue de la k-ième itération (pour un nombre K de situations logiques tirées) est :

$$\tilde{P}_k(\theta | SF) = \frac{1}{K} \sum_{j=1}^K \frac{N_{cj}}{N_j} L(Y_j), Y_j \sim q(Y_j)$$



L'échantillon fourni par l'IS pour une situation logique est  $\frac{Ncj}{N_j} L(Y_j)$  où  $Y_j$  est généré par  $q(Y_j)$  et permet d'obtenir un estimateur de  $P(\theta | SF)$  non biaisé.

Comme  $\tilde{P}_k(\theta | SF)$  est sans biais, son espérance est  $P_f = P(\theta | SF)$ .

$$\begin{aligned} \text{var} \{ \tilde{P}_k(\theta | SF) \} &= \text{var} \left\{ \frac{1}{K} \sum_{i=1}^K \frac{Ncj}{N_j} L(Y_j) \right\} = \frac{1}{K^2} \sum_{i=1}^K \text{Var} \left\{ \frac{Ncj}{N_j} L(Y_j) \right\} \\ &= \frac{1}{K^2} \sum_{i=1}^K \left[ E \left\{ \left( \frac{Ncj^2}{N_j^2} L(Y_j)^2 \right) \right\} - E^2 \left\{ \frac{Ncj}{N_j} L(Y_j) \right\} \right] \\ &= \frac{1}{K} \left[ E \left\{ \left( \frac{Ncj^2}{N_j^2} L(Y_j)^2 \right) \right\} - P_f^2 \right] \end{aligned}$$

**La précision fournie par l'IS** peut s'obtenir par la racine carrée de l'erreur quadratique moyenne (the relative rms errors) :

$$\sqrt{\frac{\text{var} \{ \tilde{P}_k(\theta | SF) \}}{P_f^2}} = \sqrt{\frac{\frac{1}{K} \left[ E \left\{ \left( \frac{Ncj^2}{N_j^2} L(Y_j)^2 \right) \right\} - P_f^2 \right]}{P_f^2}} = \sqrt{\frac{E \left\{ \left( \frac{Ncj^2}{N_j^2} L(Y_j)^2 \right) \right\} - P_f^2}{KP_f^2}} = \frac{1}{\sqrt{K}} \sqrt{\frac{E \left\{ \left( \frac{Ncj^2}{N_j^2} L(Y_j)^2 \right) \right\}}{P_f^2}} - 1$$

Pour que  $\frac{1}{\sqrt{K}} \sqrt{\frac{E \left\{ \left( \frac{Ncj^2}{N_j^2} L(Y_j)^2 \right) \right\}}{P_f^2}} - 1 \leq \beta$ , le nombre minimum de situations logiques à explorer par l'IS est tel que :

$$K \geq \frac{1}{\beta^2} \left( \frac{E \left\{ \left( \frac{Ncj^2}{N_j^2} L(Y_j)^2 \right) \right\}}{P_f^2} - 1 \right)$$

Ainsi, en calculant convenablement  $q(Y_j)$  avec l'aide de l'expert sûreté de fonctionnement et en prenant  $N_j$  le nombre total de scénarios concrets à générer dans  $Y_j$ , on obtient  $E \left\{ \left( \frac{Ncj^2}{N_j^2} L(Y_j)^2 \right) \right\}$  proche de  $P_f^2$  de sorte que le nombre de tirage de situations logiques  $K$  soit limité.

Quant à la couverture de la génération, elle se mesure à partir du nombre de situations logiques de la situation fonctionnelle qui ont été explorées. Ainsi, le taux de couverture  $TC$  se calculera tout au long de la génération. Pour un seuil minimal de couverture souhaité, le  $TC$  apparaît comme un critère supplémentaire à prendre en compte lors de l'échantillonnage des situations logiques et des scénarios concrets tel que :  $TC \geq \text{seuil}$

L'analyse proposée pour l'estimation est faite pour une situation fonctionnelle donnée. Pour obtenir un résultat global pour la fonction d'automatisation considérée, l'analyse sera faite sur chacune des situations fonctionnelles qui la caractérise.

Nous disposons donc à présent de tous les éléments requis pour la formalisation de l'heuristique de génération.

#### 4.7.7 Heuristique de génération des scénarios concrets

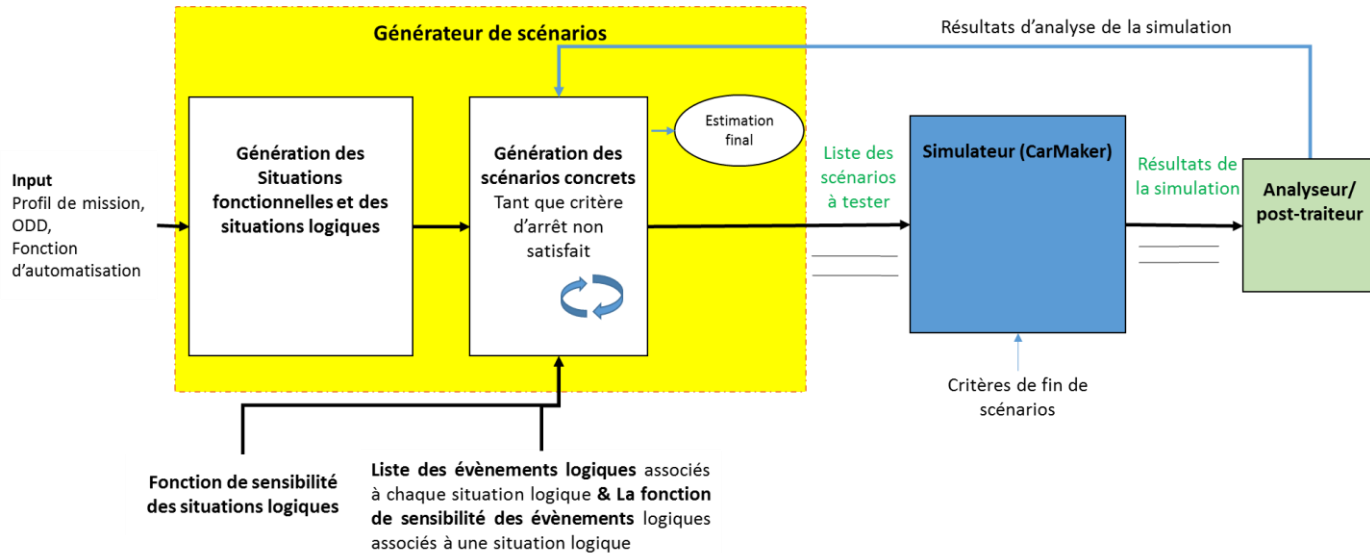


Figure 20 : Génération des scénarios concrets jusqu'à atteinte du critère d'arrêt

L'heuristique proposée pour l'obtention et la simulation des scénarios concrets vise d'une part, à identifier les scénarios critiques pour le VA tout en assurant une couverture par rapport à la réalité, et d'autre part, à estimer le risque final avec le niveau de précision souhaité.

Elle s'appuie sur une approche itérative qui permet d'identifier après simulation, les situations logiques qui produisent des scénarios concrets critiques en vue de les prioriser tout au long de la phase de test. Pour cela la génération combine à la fois une analyse de sensibilité a priori (avant simulation) et une confirmation de criticité (résultats d'analyse de la simulation) pour orienter l'exploration et l'échantillonnage comme le montre la figure 20.

En effet, sont fournis en entrée de la génération des scénarios concrets l'ensemble des situations logiques  $Y_j$  appartenant à une situation fonctionnelle  $SF$ , l'ensemble des événements  $e_{ji}$  associés à chaque situation logique  $Y_j$ , la fonction de distribution de sensibilité (ou fonction d'importance)  $q(Y_j)$  des situations logiques, la fonction de distribution de sensibilité  $q(e_{ji})$  sur chacun des événements associés à une situation logique  $Y_j$ . L'ensemble de ces éléments sont utilisés dans une heuristique qui invite à poursuivre la génération des scénarios concrets tant que le critère d'arrêt n'est pas satisfait et donc tant que l'estimation finale n'est pas obtenue :

$$\left\{ \begin{array}{l} \tilde{P}_k(\theta | SF) = \frac{1}{K} \sum_{j=1}^K \frac{N_{cj}}{N_j} L(Y_j) \\ Précision \leq \beta \\ TC \geq \text{seuil} \end{array} \right.$$

L'heuristique est décrite en trois étapes : la déclaration des variables, la description du principe de l'heuristique et sa formalisation.

### a. Déclaration des variables

Pour une situation fonctionnelle  $SF$  donnée, soient :

- $Y_j$  une situation logique appartenant à  $SF$ ,  $E_j$  la liste des évènements  $e_{ji}$  pouvant être associés à  $Y_j$  telle que  $e_{ji} \in E_j$ ,  $e_{ji}$  un évènement impactant soit le niveau fonctionnel, soit le niveau logique, soit le niveau concret
- $SC_{ji}$  un scénario concret généré à partir de  $Y_j$  et  $e_{ji}$
- $L1$  la liste des  $Y_j$  non classées,  $L0$  la liste des  $Y_j$  testées sans accident,  $L1$  la liste des  $Y_j$  testées avec accident,  $L2$  la liste des  $Y_j$  voisines de situations logiques testées sans accident et de plus faible sensibilité,  $L3$  la liste des  $Y_j$  voisines de situations logiques testées avec accident,  $LTest$  la liste des scénarios concrets à tester pendant une itération,  $Ltest = \emptyset$  (Initialisation)
- $N$  le nombre total de situations logiques dans  $SF$
- $N_j$  le nombre cumulé de tirages de situations concrètes, effectués dans la situation  $Y_j$ ,  $N_j=0$  (Initialisation)
- $n$  le nombre de tirages effectués dans chaque  $Y_j$  dans une itération
- $T_j=0$  si  $Y_j$  n'est pas encore tiré et  $T_j = 1$  sinon. Initialisation :  $T_j = 0$  pour  $j=1$  à  $N$
- $N_{cj}$  le nombre cumulé de scénarios concrets critiques obtenus avec  $Y_j$ ,  $N_{cj}=0$  (Initialisation) et  $nc$  le nombre de scénarios concrets critiques obtenus avec  $Y_j$  dans l'itération courante
- $K$  le nombre de SL tirées dans  $SF$
- $P$  le nombre de passe. Initialisation  $P = 0$ . Une passe est atteinte quand les  $Y_j$  présentes dans  $L1$  sont toutes classées, puis, que les  $Y_j$  présentes dans  $L3$  ont toutes été testées.

### b. Principe de l'heuristique d'exploration proposée

Nous allons explorer toutes les situations logiques  $Y_j$  (qui sont initialement dans  $L1$ ), soit par génération et simulation, soit par hypothèse de moindre risque pour une situation logique voisine moins sensible d'une situation logique testée sans accident.

Si pour une situation logique  $Y_j$  le nombre de scénarios concrets critiques est nul alors on retire  $Y_j$  à la liste de départ et on met  $Y_j$  dans  $L0$  car on sait qu'elle n'a pas produit d'accident. Pour chaque situation logique voisine de moindre sensibilité, si elle n'a pas été classée dans  $L0$  ou  $L1$  préalablement, alors on la met dans  $L2$ . Cela signifie que l'on peut raisonnablement penser que cette situation logique est sûre.

Si pour  $Y_j$  le nombre de scénarios concrets critiques est non nul, on la met dans L1. Pour chaque situation logique  $Y_l$  voisine, si elle n'a pas été classée dans L0 ou L1 préalablement (elle est donc dans LI ou L2), alors on la met dans L3. On peut avoir un doute sur le fait que  $Y_l$  soit sans accident car elle est voisine d'une situation logique avec accident.

Quand toutes les situations logiques sont classées, on teste les situations logiques de L3. Si les scénarios concrets générés à partir d'une situation logique  $Y_j$  de L3 produisent un (ou plusieurs) accident(s), les voisins de  $Y_j$  qui seraient dans L2 seront remis dans L3 (doute).

Quand on a terminé ces tests (fin d'une première passe), on vérifie si on a obtenu la précision souhaitée.

Sinon on va boucler pour faire d'autres tirages jusqu'à avoir une précision souhaitée, puis la couverture souhaitée.

on calcule alors  $\tilde{P}_k(\theta | SF)$ .

### c. Formalisation de l'heuristique

Choix d'une situation fonctionnelle

Choix de n

Tant que Précision  $> \beta$ , faire test

P=P+1

Tant que LI  $\neq \emptyset$

Choix d'une situation logique Yj dans LI selon la distribution de sensibilité q(Yj)

k := k+1

Pour i := 1 à n

Choix de 1 évènement eji à associer à Yj parmi l'ensemble Ej grâce à la distribution de sensibilité q(eji)

Si Tj=0, Tj := Tj+1 ( Yj est tirée)

Echantillonnage d'un scénario concret SCji à partir de Yj et de eji

Ltest := Ltest +Scji

Fin de Pour

Nj := Nj+n

Simulation de Ltest et résultats

Ncj :=Ncj+ncj

Si Ncj=0 alors LI:= LI-Yj, L0:= L0+Yj,

et pour chaque Y1  $\in V(Yj)_{1 \neq j}$ , tel que  $q(Y1) \leq q(Yj)$ , si Y1  $\notin$  L0 ou

L1 alors L2:= L2+Y1 et LI:= LI-Y1

Sinon (Ncj>0) LI:= LI-Yj, L1:= L1+Yj

et pour chaque Y1  $\in V(Yj)_{1 \neq j}$ , si Y1  $\notin$  L0 ou L1 alors L3:= L3+Y1 et

LI:= LI-Y1

Si P> 1 estimer P( $\theta$ /SF), la couverture et la précision

Si Précision  $< \beta$  et TC  $\geq$  seuil, stopper la génération et la simulation.

Fin de tan que

Tant que L3  $\neq \emptyset$  (Test de toutes les Yj dans L3)

Choix d'une situation logique Yj dans L3

k := k+1

Pour i := 1 à n

Choix de 1 évènement eji à associer à Yj parmi l'ensemble Ej grâce à la distribution de sensibilité q(eji)

Echantillonnage d'un scénario concret SCji à partir de Yj et de eji

Ltest := Ltest +Scji

Fin de Pour

$N_j := N_j + n$

Simulation de  $L_{test}$  et résultats

$N_{c_j} := N_{c_j} + n_{c_j}$

Si  $N_{c_j} > 0$  alors pour chaque  $(Y_1 \in V(Y_j)_{1 \neq j} \text{ et } Y_1 \in L_2)$  alors  $L_2 := L_2 - Y_1$  et

$L_3 := L_3 + Y_1$

Fin de tant que

Estimer  $P(\theta/SF)$ , la précision et le taux de couverture  $TC = \sum_{j=1}^N T_j / N$

Si Précision  $> \beta$ , retourner à la ligne « Tant que Précision  $> \beta$ , faire test ».

Sinon aller à « Fin de Tant que »

Fin de Tant que ( $\Rightarrow$  Précision  $< \beta$ )

Si Précision  $< \beta$  et  $TC \geq \text{seuil}$ , stopper la génération et la simulation

Sinon (Précision  $< \beta$  et  $TC < \text{seuil}$ ) aller à « Tant que  $TC < \text{seuil}$  »

Tant que  $TC < \text{seuil}$  (Test des  $Y_j$  dans  $L_2$  pour atteindre la couverture)

Choix d'une situation logique  $Y_j$  dans  $L_2$

$k := k + 1$

Pour  $i := 1$  à  $n$

Choix de 1 événement  $e_{ji}$  à associer à  $Y_j$  parmi l'ensemble  $E_j$  grâce à la distribution de sensibilité  $q(e_{ji})$

Echantillonnage d'un scénario concret  $SC_{ji}$  à partir de  $Y_j$  et de  $e_{ji}$

$L_{test} := L_{test} + SC_{ji}$

Fin de Pour

$N_j := N_j + n$

Simulation de  $L_{test}$  et résultats

$N_{c_j} := N_{c_j} + n_{c_j}$

Si  $N_{c_j} > 0$  alors pour chaque  $Y_1 \in V(Y_j)_{1 \neq j}$ ,  $L_2 := L_2 - Y_1$  et  $L_3 := L_3 + Y_1$

Estimer le taux de couverture  $TC = \sum_{j=1}^N T_j / N$

Si  $TC \geq \text{seuil}$ , aller à « Fin de tant que »

Sinon aller à « Tant que  $TC < \text{seuil}$  »

Fin de tant que

Aller à « Tant que  $L_3 \neq \emptyset$  »

## 4.8 DISCUSSION

La génération de scénario de tests pour la simulation est confrontée à un problème d'exploration d'un espace très grand, voire infini (nombreuses entités, nombreux paramètres pour les décrire, nombreuses plages de valeurs continues). Les approches que nous avons trouvées dans la littérature et les cas d'étude traités sont souvent limités à une manœuvre précise (par exemple, le cut-in ou le car following) et ne portent pas encore sur l'ensemble du profil de mission du VA. Elles manquent ainsi d'évolutivité lorsque nous sommes en présence d'un nombre de paramètres plus élevé ou d'un niveau d'automatisation plus élevé du VA. Aussi, on note dans certaines de ces approches, l'absence d'une analyse de criticité en amont de la simulation qui permettrait de sur-échantillonner les paramètres critiques, ou encore une difficulté à leur réutilisation comme avec le cas de la définition d'une fonction objectif.

Nous avons proposé dans ce travail de thèse, une stratégie de génération et de validation par simulation de la sécurité du VA qui tient compte de l'ensemble de ces aspects. Cette stratégie s'aligne sur une structuration en trois niveaux d'abstraction : fonctionnel, logique et concret. Elle tient compte du profil de mission du VA suivant son ODD (Operational Design Domain) et le niveau d'automatisation associé. Ainsi, elle ne se limite pas exclusivement à une seule manœuvre opérationnelle mais peut s'étendre à plusieurs selon les performances fonctionnelles attendues du VA. De plus, l'approche proposée intègre, en plus de l'évaluation de la criticité des scénarios concrets simulés, une phase d'estimation de la criticité et de la sensibilité a priori du VA, en amont de la génération et de la validation. Une telle considération permet de mettre l'accent sur les scénarios potentiellement critiques dès le début de la génération. La stratégie se termine par l'obtention d'une heuristique qui guide dans la manière d'explorer l'espace des scénarios et donne à la fin une estimation des indicateurs de performance de la génération et de validation de la sécurité du VA.

Cependant, on peut noter quelques limites dans la méthodologie proposée. D'abord, bien que nous ayons souligné la manière d'identifier les contraintes entre les paramètres et la nécessité de leur prise en compte, nous n'avons pas procédé à leur modélisation formelle. Le modèle conceptuel proposé au chapitre 2 peut servir de base pour définir une ontologie permettant de représenter les contraintes entre paramètres.

De plus, nous avons mentionné lors de la phase de l'obtention des scénarios logiques (phase AII.2 du processus), que leur génération peut faire l'objet de la résolution d'un problème combinatoire du fait de la combinaison entre les plages de valeurs des paramètres. Toutefois, comme on peut le constater, nous avons fait le choix de procéder autrement en optant pour une combinaison systématique des plages. La motivation derrière ce choix s'explique d'abord, par le fait que le découpage des plages suivant leur sensibilité, réalisé avec le support de l'expert, limite le nombre de plage au juste nécessaire. Puis, nous tenons compte dans la combinaison, des contraintes logiques d'association des paramètres. Cependant, pour favoriser « l'applicabilité » de la stratégie proposée, la pertinence du découpage en plages de valeurs pour chaque paramètre doit être vérifiée, d'autant plus qu'il guide l'ensemble de la stratégie de recherche des scénarios critiques. Une analyse de sensibilité peut aussi être réalisée en modifiant les frontières des plages et en vérifiant l'impact sur les résultats obtenus. En outre, une des limites observées pour l'application de la stratégie proposée est liée à l'environnement de simulation du VA. En effet, les environnements actuellement disponibles sur le marché, ne permettent pas de modéliser fidèlement certains paramètres, en particulier ceux liés aux

conditions climatiques (pluie, neige, brouillard). Une telle limite doit être comblée si l'on veut exploiter la stratégie pour la validation de la sécurité, en ce qui concerne le périmètre du SOTIF.

## 4.9 CONCLUSION

Dans ce chapitre, nous avons proposé une solution pour assurer la validation par simulation de la sécurité du VA au regard de ses limitations de performance (périmètre SOTIF) en répondant à la question de recherche suivante :

### **Quelle stratégie utiliser pour la génération des scénarios nécessaires à la validation par simulation de la sécurité du VA ?**

Cette solution se décline en deux objectifs à atteindre simultanément : fournir une heuristique performante de génération de scénarios à simuler et estimer l'indicateur de risque avec un niveau de précision et une couverture cible. Le tout, en vue d'atteindre la cible de validation d'un ordre de  $10^{-x}/h$  ( $x$  variant<sup>10</sup> suivant la fonction d'automatisation à valider). La performance de l'heuristique proposée s'évalue grâce à trois indicateurs : la criticité (analyse de sensibilité a priori du VA aux situations logiques et analyse des scénarios concrets critiques après simulation), la couverture et la représentativité de la génération. Aussi, elle a l'intérêt de pouvoir estimer au fur et à mesure que durent la génération et la simulation, l'indicateur final de risque qui servira à vérifier si la cible de validation est atteinte.

Par ailleurs, notre proposition répond bien aux attendus du SOTIF en ce qui concerne le traitement des « area 2 et 3 » à savoir : identifier les « Known unsafe scenarios (area 2) » et les « Unknown unsafe scenarios (area 3) ». En effet, l'« area 2 » est abordé en deux temps. D'abord, il est identifié grâce à la phase d'estimation de la criticité au cours de laquelle nous avons : une APR qui est réalisée en vue d'identifier les événements redoutés auxquels l'on l'expose avec la fonction d'automatisation choisie, les facteurs de criticité et les types d'événements qui sont présents dans l'ODD, une analyse de sensibilité a priori du VA aux plages de variation qui est faite puis utilisée pour établir l'analyse de sensibilité a priori aux situations logiques et l'analyse de sensibilité sur les événements. Ensuite, cet « area 2 » est réduit en générant systématiquement des scénarios concrets à partir de situations logiques et d'événements jugés sensibles. Quant à l'« area 3 », il est identifié et réduit grâce au caractère aléatoire de l'occurrence des scénarios, au processus itératif d'échantillonnage des scénarios concrets et à l'estimation de l'indicateur final de risque. Une telle procédure permet de tester aussi les scénarios non identifiés comme potentiellement critiques. Ainsi, à la fin de la validation, l'on montre que l'area 3 est traité si la cible quantitative de validation ( $10^{-x}/h$ ) est atteinte avec le niveau de confiance et la précision  $\beta$  souhaités.

Dans le dernier chapitre, nous illustrerons certains aspects de la stratégie globale de génération suivant ses trois principales phases de déclinaison : génération des scénarios fonctionnels, génération des scénarios logiques et enfin, la génération des scénarios concrets.

---

<sup>10</sup> Pour fixer un ordre de grandeur,  $x$  est habituellement pris entre 6 et 9.



---

## CHAPITRE 5. APPLICATION DE LA STRATEGIE DE GENERATION SUR UN CAS D'ETUDE

---

Le présent chapitre vise à illustrer l'ensemble des concepts introduits dans ce mémoire et ainsi que la stratégie proposée pour la génération des scénarios. Pour ce faire, nous considérerons que le VA est équipé de la fonction d'automatisation « Traffic Jam Chauffeur (TJC) », de niveau d'automatisation 3. Nous commencerons par une description de la fonction TJC. Ensuite, nous établirons le cadre conceptuel et la spécification (fonctionnelle) associés (phase 1 du processus décrit sur la figure 16). Enfin, nous montrerons comment générer les scénarios suivant les trois niveaux d'abstraction : fonctionnel, logique et concret (phase 2 du processus).

### 5.1 DESCRIPTION DE LA FONCTION TJC

Le TJC est une fonction d'automatisation de niveau 3, conçue pour prendre en charge la conduite autonome sur voies à chaussées séparées (autoroute ou voie rapide), en conditions d'embouteillage, où la vitesse est limitée à une vitesse maximale  $V_{max}$  (de l'ordre de 60 à 70 km/h). Le véhicule Ego (le véhicule équipé de la fonction d'automatisation, correspondant ici au VA) suit le véhicule qui précède, se maintient sur sa voie et gère l'accélération et le freinage dans la limite de vitesse autorisée. Le conducteur peut effectuer d'autres activités mais doit rester vigilant et reprendre le contrôle du véhicule dans un temps de l'ordre de 10 secondes sur sollicitation du système. Le système doit permettre au conducteur d'activer la fonction ou d'intervenir à tout moment pour reprendre le contrôle du véhicule et doit lui laisser le temps pour le faire.

### 5.2 CADRE CONCEPTUEL ET SPECIFICATION DE LA FONCTION TJC

Dans cette partie, nous donnons des éléments sur les concepts suivants dans le cas de la fonction TJC : ODD, cas d'utilisation, performance fonctionnelle (et limitation de performance), mode de fonctionnement et manœuvre opérationnelle. Ces concepts ont été introduits dans le chapitre 2.

- Description de l'ODD de la fonction TJC

Les entités de l'ODD sont définies dans le tableau 23 : le type d'infrastructure dans lequel doit être utilisée la fonction (autoroute, voies rapides), les autres usagers (pas de piéton, pas d'obstacle) et les conditions climatiques (pour la fonction TJC, il n'y a pas de contrainte particulière liée aux conditions climatiques). Des contraintes fonctionnelles, correspondant à la fonction TJC, sont définies dans la colonne « Ego véhicule ». Elles concernent la vitesse limite d'utilisation de la fonction (dans notre illustration, nous faisons le choix de limiter la vitesse à 60km/h : Plage de vitesse  $\leq 60\text{km/h}$ ), la nécessité de présence d'un conducteur et des exemples de manœuvres opérationnelles non autorisées. Par ailleurs, d'autres contraintes telles que les infrastructures non autorisées, ainsi que la condition d'embouteillage sont également spécifiées.

Description de l'ODD d'un TJC			
Infrastructure physique	Autres usagers	Conditions climatiques	Ego véhicule
<ul style="list-style-type: none"> <li>• Autoroute, voie rapide</li> <li>• Chaussée séparée</li> <li>• Pas d'intersection, pas de rond-point, pas de passage piéton, pas de feux stop, pas de céder le passage, pas d'entrée prioritaire, pas de demi-tour, pas de zone de travaux, pas de tunnel</li> </ul>	<ul style="list-style-type: none"> <li>• Pas de piéton, pas d'obstacle,</li> <li>• Pas de conducteur à contresens</li> </ul>	<ul style="list-style-type: none"> <li>• Type de précipitation : non spécifié</li> <li>• Luminosité : non spécifié</li> <li>• Température : non spécifié</li> </ul>	<ul style="list-style-type: none"> <li>• Equipé de la fonction TJC</li> <li>• Plage de vitesse : <math>\leq 60\text{km/h}</math></li> <li>• Présence d'un conducteur : oui</li> <li>• Pas de changement de voie (no lane changing)</li> <li>• Dynamique du véhicule : Pas de forte décélération, Pas de forte accélération, Pas de forte action sur le volant</li> <li>• Pas de remorque attachée</li> </ul>
<b>Autres contraintes</b> <ul style="list-style-type: none"> <li>• Concernant le type de voie : pas sur l'accotement, pas sur une voie d'entrecroisement, ni sur la voie d'insertion.</li> <li>• Pas d'obstacle</li> <li>• Condition d'embouteillage : 1 véhicule devant Ego, Vitesse <math>\leq 60\text{km/h}</math>, Différence de vitesse (entre usagers présents) <math>\leq 10\text{km/h}</math></li> </ul>			

Tableau 23 : Description de l'ODD d'un TJC

- Cas d'utilisation, performances fonctionnelles et limitation de performance pour la fonction TJC

La fonction TJC, comme toute autre fonction d'automatisation, est prévue pour répondre à des cas d'utilisation bien définis. Pour chacune de ces utilisations, des exemples de performances fonctionnelles correspondantes, ainsi que des exemples de limitations de performance ont été identifiées. Les limitations de performance sont définies en s'inspirant des modes de défaillance d'une fonction (« loss / lack / erroneous / unexpected »). Le tableau 24 regroupe l'ensemble de ces informations.

Cas d'utilisation	Performances fonctionnelles	Potentielles limitations de performance
Assurer les interactions avec les occupants du véhicule	Gérer l'activation	
	Répondre à la demande de reprise en main du conducteur	
	Alerter le conducteur	
	Redonner le volant au conducteur (Give Back)	
	Afficher les informations	
Percevoir la situation	Identifier le type d'infrastructure approprié	<ul style="list-style-type: none"> <li>- Perception incomplète/limitée (ex. le véhicule ne perçoit pas tous les éléments de la situation)</li> <li>- Perception erronée (par exemple, le vélo est vu comme une voiture)</li> <li>- Absence de perception (par exemple, la cible située devant le véhicule n'est pas vue).</li> <li>- Perte de perception (par exemple, le véhicule ne voit soudainement plus le véhicule cible)</li> <li>- Perception indésirable (par exemple, le véhicule voit des choses inexistantes)</li> </ul>
	Identifier la chaussée appropriée	
	Identifier les conditions météorologiques spécifiées	
	Identifier les autres objets pertinents	
Contrôler la trajectoire	Assurer le contrôle latéral	<ul style="list-style-type: none"> <li>- Performance insuffisante de l'actionnement (par exemple, l'angle du volant pour suivre la trajectoire n'est pas suffisant)</li> <li>- Performance excessive de l'actionnement (par exemple, accélération excessive due à une heuristique erronée)</li> <li>- Pas d'actionnement (par exemple, aucune décélération n'est déclenchée pour respecter la décision en raison d'une heuristique erronée)</li> <li>- Actionnement non souhaité (par exemple, le volant a déclenché un mouvement de lui-même en raison d'une décision erronée)</li> </ul>
	Assurer le contrôle longitudinal	
Prendre des décisions pour réagir à la situation	Sélectionner l'objet cible	<ul style="list-style-type: none"> <li>- Insuffisance de l'algorithme de décision (par ex. la décision n'est pas suffisante pour faire face à la situation en toute sécurité)</li> <li>- Décision incorrecte (par exemple, la décision est basée sur une mauvaise heuristique)</li> <li>- Pas de décision (par exemple, le scénario nécessite une décision, mais aucune n'est prise)</li> <li>- Décision non souhaitée (par exemple, le VA prend une décision alors que ce n'est pas nécessaire)</li> </ul>
	Éviter les obstacles	
	Respecter les règles de conduite	
	Éviter les collisions	

Tableau 24 : Exemple de cas d'utilisation, de performances fonctionnelles et de limitation de performances du TJC

- Mode de fonctionnement et manœuvre opérationnelle de la fonction TJC

Les modes de fonctionnement identifiés sur la figure 8 (Cf. §2.2.3 du chapitre 2) sont valables dans le cas de la fonction TJC : Mode Init, Mode Available, Mode Active, Mode Give back, Mode Safe state MRM (Minimum Risk Manoeuver). Quant aux manœuvres opérationnelles, toutes ne sont pas valables pour le TJC. En effet, compte tenu de la spécification de cette fonction, seule une des manœuvres listées dans le tableau 8 (Cf. §2.2.3 du chapitre 2), lui sera attribuée : Regulate distance /Car following. L'ensemble des manœuvres opérationnelles que peuvent avoir les autres usagers reste valable lors de l'utilisation de la fonction TJC.

- Les critères de validité associés à chaque mode ou manœuvre opérationnelle

Les critères de validité qui caractérisent les modes et manœuvres opérationnels dans le cas du TJC sont présentés dans les tableaux 25 et 26.

Modes opérationnels	Critères de validité/Enclenchement
Activation	Conditions d'activation OK Demande driver OK
GiveBack	Conditions de disponibilité NOK ou demande de « GiveBack » (Chaque fois qu'il y a risque de franchissement d'une limite de l'ODD)
MRM	Situation de « GiveBack » Driver NOK

Tableau 25 : Modes opérationnels et leurs critères de validité dans le cas du TJC

Manœuvres opérationnelles	Critères de validité / Enclenchement
Regulate distance / Car following	<ul style="list-style-type: none"> <li>• Activation OK</li> <li>• Présence du Lead (Véhicule devant Ego)</li> <li>• distance &gt; « D safe » exprimé en seconde (2 s)</li> <li>• TTC &gt; seuil (tmin)</li> </ul>

Tableau 26 : Manœuvres opérationnelles et leurs critères de validité dans le cas du TJC

## 5.3 ILLUSTRATION DE LA GENERATION DES SCENARIOS AVEC LE TJC

La génération des scénarios consiste en l'obtention des scénarios fonctionnels, logiques et concrets et est applicable au TJC.

### 5.3.1 La génération des scénarios fonctionnels

La génération des scénarios fonctionnels repose sur l'identification des situations fonctionnelles et des types d'évènements qui peuvent apparaître dans ces situations.

Pour rappel, l'identification des situations fonctionnelles repose sur la combinaison d'éléments suivants : les types de densité de trafic associés à l'utilisation de la fonction, les types

d'infrastructure, les modes opérationnels dans lesquels la fonction peut se retrouver et les manœuvres qu'elle peut exécuter. Le tableau 27 illustre la liste des six situations fonctionnelles que nous obtenons pour le TJC.

Fonction TJC	Type de densité de trafic associé à l'utilisation de la fonction : Embouteillé			Liste des situations fonctionnelles
	Les types d'infra associés à la fonction : Autoroute, Voie rapide	Les modes de fonctionnement dans l'infra « Autoroute » : Activation, GiveBack, MRM	La manœuvre opérationnelle associée au mode « Activation » pour l'infrastructure Autoroute : Car following	<ul style="list-style-type: none"> <li>Ego en situation de « Car following » dans le mode « Activation » sur Autoroute et en trafic embouteillé.</li> </ul>
			La manœuvre opérationnelle associée au mode « GiveBack » pour l'infrastructure Autoroute : Car following	<ul style="list-style-type: none"> <li>Ego en situation de « Car following » dans le mode « GiveBack » sur Autoroute et en trafic embouteillé.</li> </ul>
			La manœuvre opérationnelle associée au mode « MRM » pour l'infrastructure Autoroute : Car following	<ul style="list-style-type: none"> <li>Ego en situation de « Car following » dans le mode « MRM » sur voie rapide et en trafic embouteillé.</li> </ul>
	Les modes opérationnels dans l'infra « Voie rapide » : Activation, GiveBack , MRM		La manœuvre opérationnelle associée au mode « Activation » pour l'infrastructure voie rapide : Car following	<ul style="list-style-type: none"> <li>Ego en situation de « Car following » dans le mode « Activation » sur voie rapide et en trafic embouteillé.</li> </ul>
			La manœuvre opérationnelle associée au mode « GiveBack » pour l'infrastructure voie rapide : Car following	<ul style="list-style-type: none"> <li>Ego en situation de « Car following » dans le mode « GiveBack » sur voie rapide et en trafic embouteillé.</li> </ul>
			La manœuvre opérationnelle associée au mode « MRM » pour l'infrastructure voie rapide : Car following	<ul style="list-style-type: none"> <li>Ego en situation de « Car following » dans le mode « MRM » sur voie rapide et en trafic embouteillé.</li> </ul>

Tableau 27 : Liste des situations fonctionnelles dans le cas de la fonction TJC

Les types d'évènement dans le cas du TJC sont les mêmes que ceux définis lors de la spécification de la stratégie lors de la définition de l'indicateur criticité dans le chapitre 3. Ils sont repris dans les tableaux 28 et 29 ci-dessous. Bien que les typologies soient les mêmes, la déclinaison des évènements est différente selon les caractéristiques propres de l'ODD de la fonction d'automatisation concernée.

Evènements correspondant à l'ODD du TJC		
Types	Evènements	
Limitations de performances connues (à l'intérieur de son ODD) : EI	EI1	L'entité "infrastructure" est la source de la limitation
	EI2	L'entité "météo" (condition atmosphérique) est la source de la limitation
Déviations et violations des consignes de sécurité et du code de la route : Ed	Ed1	Déviations dans le comportement des autres usagers par rapport à la voie de circulation (et aux emplacements dédiés)
	Ed2	Déviations dans le comportement des autres usagers par rapport à l'exécution des manœuvres (dépassement, sortie, insertion,...) en toute sécurité (au respect des distances de sécurité)
	Ed3	Déviations dans le comportement des autres usagers par rapport au respect des limitations de vitesse
	Ed4	L'entité " Driver_passenger" est la source de la limitation, à savoir les mésusages (Ex : Augmentation_vitesse)
Evènements du type transitions entre manœuvres : ET	ET	Correspond aux conditions de validité de la manœuvre

Tableau 28 : Exemples de typologies d'évènements correspondant à l'ODD du TJC

Evènements en dehors de l'ODD du TJC		
Types	Evènements	
Contraintes liées à l'utilisation de la fonction (Limites) : Ec (en dehors du nominal prévu par le constructeur)	Ec1	Contraintes sur l'infrastructure (route, chaussée, vitesse)
	Ec2	Contraintes sur la météo
	Ec3	Contraintes sur le Driver_passenger (Interactions avec le véhicule)
	Ec4	Contraintes sur les autres usagers
Evènements du type transitions entre modes de fonctionnement : EM	EM	Correspond aux conditions de validité du mode

Tableau 29 : Exemples de typologies d'évènements survenant en dehors de l'ODD du TJC

Choix d'une situation fonctionnelle : pour la suite du raisonnement, nous nous focalisons sur une situation fonctionnelle spécifique : Ego en situation de « Car following » dans le mode « Activation » sur Autoroute et en trafic embouteillé.

Une fois le niveau fonctionnel de la génération traité, la phase suivante consiste en l'obtention des situations logiques.

### 5.3.2 La génération des situations logiques

Pour obtenir les situations logiques, il faut, pour les entités présentes (Infrastructure, Autres usagers, Conducteurs/Passagers, Conditions atmosphériques, VA) dans l'ODD, définir leurs paramètres et les plages de valeurs.

- Définition des paramètres et leurs plages de valeurs

Lors de la description du scénario, l'Ego véhicule est pris comme l'élément de référence en fonction duquel sont décrits les autres usagers. L'espace est configuré de sorte que le VA puisse être entouré de 8 positions pouvant être occupées (Cf. Figure 10 chapitre 2).

Variables / Identifiants des paramètres	Paramètres	Plages de valeurs	Identifiants de plages
A1	Position_AutreVehicule.1 (Left)	Vraie	A1_1
A2	Position_AutreVehicule.2 (Front left)	Vraie	A2_1
A3	Position_AutreVehicule.3 (Front)	Vraie	A3_1
A4	Vitesse_AutreVehicule.1 (km/h)	Faible [0,60]	A4_1
A5	Vitesse_AutreVehicule.2 (km/h)	Faible [0,60]	A5_1
A6	Vitesse_AutreVehicule.3 (km/h)	Faible [0,60]	A6_1
A7	Rayon de courbure	Faible	A7_1
		Elevé	A7_2
A8	Nombre_voies	2	A8_1
		3 et plus	A8_2
A10	Météo	Soleil normal	A10_1
		Soleil fort (éblouissement)	A10_2
		Pluie faible	A10_3
		Pluie forte	A10_4
		Brouillard léger	A10_5
		Brouillard dense	A10_6
A11	Présence objet latéral (barrière de sécurité, véhicule garé, mur en béton, pylône)	Absence	A11_1
		Présence	A11_2
A9	Vitesse_Ego	Faible [0, 60 km/h]	A9_1

Tableau 30 : Identification des paramètres de description des scénarios et de leurs plages de variation

Trois types de paramètres entrent en jeu dans la description : les *paramètres caractérisant le scénario*, les *paramètres de variabilité du scénario* et les *invariants du scénario*. Dans le cas du scénario fonctionnel de « car following », ils se présentent comme suit :

- les paramètres caractérisant ce scénario :
  - o Présence Lead
  - o Interdistance (Ego-Lead) > « D safe » exprimé en seconde (2 s)
- les paramètres de variabilité du scénario :
  - o Position\_AutreVehicule.i
  - o Vitesse\_AutreVehicule.i

- Rayon de courbure
- Nombre\_voies
- Météo
- Présence objet latéral (barrière de sécurité, véhicule garé, mur en béton, pylône)
- les invariants du scénario :
  - Type infrastructure
  - Nombre Usagers  $\geq 3$  (densité de trafic embouteillé)
  - Vitesse  $\leq V_{\max}(\text{TJC})$  (vitesse maximale autorisée pour la fonction TJC)

Le tableau 30 résume les paramètres du cas d'étude et les plages de valeurs.

Les espaces de variation des différents paramètres sont définis sous forme de plages de valeurs de sorte à différencier des classes de sensibilité du VA. Lorsque l'expert est questionné sur la sensibilité du VA à un paramètre, il lui est demandé de distinguer les plages de valeur de ce paramètre, qui peuvent avoir des impacts différents en termes de sensibilité du VA.

La vitesse dispose de trois plages de valeurs : Faible, Moyenne, Elevée.

Chaque position autour de l'Ego est soit occupée (Vrai), soit non occupée (Faux).

Les positions qui sont occupées sont fixées grâce à la spécification de la fonction TJC et à son ODD. En effet, pour que l'Ego équipé de la fonction TJC fasse du Car following, il faut qu'il y ait un véhicule devant lui (Présence Lead en position Front). De plus, pour respecter la condition d'embouteillage sur voie à chaussée séparée, il faut la présence de véhicules supplémentaires autour de l'Ego. Compte tenu du découpage proposé pour les zones autour du VA, les usagers considérés comme présents sont au minimum le véhicule devant l'Ego (Front), celui à gauche (Left) et celui en face du véhicule de gauche (Front Left). De ce fait, les positions renseignées et fixées à « vrai » sont les suivantes : Position\_AutreVehicule1 (Left), Position\_AutreVehicule2 (Front left) et Position\_AutreVehicule3 (Front).

Pour  $i = 1$  à  $3$ , la plage « Vraie » de « Position\_AutreVehicule.i » signifie implicitement, que pour les autres  $i > 3$ , « Position\_AutreVehicule.i » prend la plage de valeur « faux » (pas de présence dans cette zone).

La présence potentielle d'objet en position latérale est considérée via le paramètre « Présence objet latéral » qui peut prendre deux valeurs : Présence ou Absence.

Quant au paramètre « Vitesse\_AutreVehicule.i », il dépend du type d'infrastructure, mais aussi et surtout des contraintes liées à l'utilisation de la fonction TJC.

Ainsi, sans contrainte sur la vitesse, le découpage proposé sur une infrastructure de type Autoroute est le suivant : Faible [0,90 km/h], Moyenne [90,110 km/h], Elevée (>110 km/h). Par ailleurs, étant donné que pour la fonction TJC, il y a une vitesse maximale spécifiée (ici nous prendrons  $V_{\max}(\text{TJC}) = 60$  km/h), le découpage privilégié est celui qui prend en compte cette contrainte. Une seule plage de vitesse pour chaque usager « AutreVehicule.i » est alors retenue : Faible [0,  $V_{\max}(\text{TJC})$ ] soit [0, 60km/h].

L'information sur le type d'infrastructure est connue d'avance grâce à l'ODD. Il s'agit ici d'une infrastructure de type autoroute. Le nombre de voies est soit 2 voies, soit 3 voies et plus. Ce découpage s'explique par le fait que dans le cas de 2 voies, le danger ne peut provenir que d'un



côté tandis que dans le cas contraire (3 et plus), il peut provenir des deux côtés (il y a une complexité potentielle de la situation qui augmente avec le nombre de voies). Néanmoins, par défaut l'égo véhicule cherchera à rester le plus souvent sur la voie de droite sauf situation particulière : dépassement, voie dédiée à la sortie...

Le rayon de courbure est défini en deux plages : Faible et Elevé. En effet, selon la configuration de la route (et donc sa courbure), le champ de vision peut non seulement être impacté mais aussi, il peut y avoir un contrôle difficile du véhicule pouvant augmenter le risque associé à la situation.

Enfin, seuls trois types de conditions climatiques sont retenues pour décrire la météo : soleil, pluie, brouillard. Dans chaque cas, les plages de valeurs peuvent être soit faible ou légère, soit forte ou dense.

L'ensemble des paramètres et des plages définis vont servir à obtenir par la suite, les situations logiques et les événements.

- Combinaison des plages de valeurs pour obtenir l'ensemble des situations logiques associés à chaque situation fonctionnelle

Il importe lors de la combinaison des plages de valeurs, d'identifier et de tenir compte des contraintes et des dépendances nécessaires dans le but d'assurer la consistance des scénarios.

#### Prise en compte des contraintes d'association entre paramètres et plages

D'abord, nous avons les contraintes liées à la fonction TJC et à son ODD. En effet, le trafic embouteillé imposé par l'ODD de la fonction TJC pose les contraintes ci-dessous.

- Nombre\_Usagers  $\geq 3$ 
  - Position\_AutreVehicule.1 = Vraie, Position\_AutreVehicule.2 = Vraie, Position\_AutreVehicule.3 = vraie
- Vitesse\_AutreVehicule.i  $\leq 60$  km/h (pour tout i)
- Vitesse\_Ego  $\leq 60$  km/h

La manœuvre de Car following effectuée par la fonction TJC impose la contrainte suivante :

- « Position\_AutreVehicule.3 » doit être toujours vraie (Contrainte TJC)

Ensuite, il existe des contraintes liées aux scénarios puisqu'il faudra en tenir compte lors de la génération :

- « Position\_AutreVehicule.i » dépend de « Nombre\_Voies »
- $3 \leq$  « Nombre\_Usagers  $\leq 8$  » dans un scenario
- Vitesse\_AutreVehicule1.  $>$  Vitesse\_Ego (Contrainte Cut-in)

### Obtention des situations logiques après combinaison

En combinant les plages de valeurs des paramètres ci-dessus, nous obtenons quarante-huit combinaisons, soit quarante-huit situations logiques pour la situation fonctionnelle considérée. Le tableau 31 nous donne quelques exemples de situations logiques. L'ensemble des 48 situations logiques se trouve en annexe 1.

<b>Situation logique Y1 :</b> Position_AutreVehicule.1.Vraie * Position_AutreVehicule.2.Vraie * Position_AutreVehicule.3.Vraie * Vitesse_AutreVehicule.1.Faible * Vitesse_AutreVehicule.2.Faible * Vitesse_AutreVehicule.3.Faible * Rayon_courbure.Faible * Nombre_voies.2 * Soleil.Normal * Absence_Objet_latéral * Vitesse_Ego.Faible
<b>Situation logique Y14 :</b> Position_AutreVehicule.1.Vraie * Position_AutreVehicule.2.Vraie * Position_AutreVehicule.3.Vraie * Vitesse_AutreVehicule.1.Faible * Vitesse_AutreVehicule.2.Faible * Vitesse_AutreVehicule.3.Faible * Rayon_courbure.Faible * Nombre_voies.3 * Soleil.Fort * Présence_Objet_latéral * Vitesse_Ego.Faible
<b>Situation logique Y32 :</b> Position_AutreVehicule.1.Vraie * Position_AutreVehicule.2.Vraie * Position_AutreVehicule.3.Vraie * Vitesse_AutreVehicule.1.Faible * Vitesse_AutreVehicule.2.Faible * Vitesse_AutreVehicule.3.Faible * Rayon_courbure.Elevé * Nombre_voies.3 * Pluie.Forte * Présence_Objet_latéral * Vitesse_Ego.Faible
<b>Situation logique Y35 :</b> Position_AutreVehicule.1.Vraie * Position_AutreVehicule.2.Vraie * Position_AutreVehicule.3.Vraie * Vitesse_AutreVehicule.1.Faible * Vitesse_AutreVehicule.2.Faible * Vitesse_AutreVehicule.3.Faible * Rayon_courbure.Elevé * Nombre_voies.2 * Brouillard.Léger * Absence_Objet_latéral * Vitesse_Ego.Faible

Tableau 31 : Exemples de situations logiques obtenues par combinaison des plages de variation

Le nombre de situations logiques obtenues dépend du nombre de paramètres considérés et des plages de valeurs associées à chacun d'eux. Une explosion combinatoire peut être rapidement observée dès lors que les paramètres sont nombreux et que l'espace de variation de chacun est décomposé en deux ou trois plages.

Par exemple, si nous avons considéré les trois plages de valeurs Faible [0,90 km/h], Moyenne [90,110 km/h], Elevée (>110 km/h) pour la vitesse au lieu de l'unique plage Faible ([0, Vmax (TJC)] = [0, 60km/h]), nous aurions eu 144 situations logiques.

Cela signifie que la décision de découper ou non un espace de définition en plages de valeurs, et l'identification des contraintes héritées de l'ODD ou de la spécification de la fonction, doivent être faites avec attention, et ce en collaboration avec des experts. Une telle procédure permettra de limiter le nombre de combinaison au plus juste.

L'obtention des situations logiques est la phase intermédiaire pour procéder à la génération des scénarios concrets. Le nombre élevé de scénarios concrets qu'il est possible d'obtenir, nous a conduit à proposer une analyse en amont de la génération afin de favoriser l'obtention de ceux qui sont à risque pour le VA.

Une fois cette phase d'analyse terminée, on obtient les éléments nécessaires pour appliquer l'heuristique de génération des scénarios concrets proposée dans le chapitre 4, puis, estimer le risque final associé au VA.

### 5.3.3 Phase d'analyse en amont de la génération des scénarios concrets

Cette phase d'analyse consiste d'abord à étudier la sensibilité du VA aux situations logiques, puis à utiliser le résultat pour établir une fonction de distribution de la sensibilité sur les situations logiques. En outre, connaissant les types d'évènements auxquels est confronté le VA, les limites de l'ODD et à l'aide des plages de variations contenues dans les situations logiques, une identification des évènements selon les trois types d'impact (ceux impactant le niveau fonctionnel, ceux impactant le niveau logique et ceux impactant le niveau concret) est faite pour chacune des situations logiques. Enfin, une étude de sensibilité est mise en place sur les évènements de chaque situation logique afin d'avoir également une fonction de distribution de sensibilité par liste d'évènements associés à une situation logique.

Les paramètres et leurs plages de valeurs décrits dans le tableau 30 seront utilisés dans le cadre de cette analyse.

#### 5.3.3.1 *La sensibilité du VA aux situations logiques*

Pour obtenir la sensibilité du VA aux situations logiques, nous allons commencer par analyser la sensibilité du VA à chacune des plages de valeurs définies précédemment. Ces sensibilités serviront également lors de l'analyse de sensibilité des évènements. Pour les obtenir, les technologies de capteurs contenues dans l'architecture de la fonction TJC ainsi que les modules de décision et d'actionnement sont considérés. Ici, les composantes de l'architecture du TJC sont les mêmes que celles définies lors de la spécification de la méthode dans le chapitre 3. La réponse de l'expert à la question « la technologie (respectivement la décision ou l'actionnement) est-elle sensible ou non performante dans cette plage ? » permet de savoir si une des composantes de l'architecture peut être impactée ou non par une plage. Puis l'échelle du tableau 15 permet d'obtenir le niveau de sensibilité à attribuer à chaque plage. Le tableau 32 illustre les résultats obtenus.

Variables	Paramètres	Plages de valeurs	Identifiants des plages	Techno 1 (Radar)	Techno 2 (Lidar)	Techno 3 (Ultrason)	Techno 4 (Caméra stéréo)	Techno 5 (Caméra Mono)	Décision	Actionnement	Sensibilité pour la plage
A1	Position_AutreVehicule1 (Left)	Vrai	A1_1	NON	NON	OUI	NON	NON	NON	NON	0.2
A2	Position_AutreVehicule2 (Front left)	Vrai	A2_1	NON	NON	NON	NON	NON	NON	NON	0
A3	Position_AutreVehicule3 (Front)	Vrai	A3_1	NON	NON	NON	NON	NON	NON	NON	0
A4	Vitesse_AutreVehicule.1 (km/h)	Faible [0,60]	A4_1	NON	NON	NON	NON	NON	NON	NON	0
A5	Vitesse_AutreVehicule.2 (km/h)	Faible [0,60]	A5_1	NON	NON	NON	NON	NON	NON	NON	0
A6	Vitesse_AutreVehicule3 (km/h)	Faible [0,60]	A6_1	NON	NON	NON	NON	NON	NON	NON	0
A7	Rayon de courbure	Faible	A7_1	NON	NON	NON	NON	NON	NON	NON	0
		Elevé	A7_2	NON	NON	NON	OUI	OUI	NON	NON	0.4
A8	Nombre_voies	2	A8_1	NON	NON	NON	NON	NON	NON	NON	0
		3 et plus	A8_2	NON	NON	NON	OUI	OUI	OUI	NON	1.4
A10	Météo	Soleil normal	A10_1	NON	NON	NON	NON	NON	NON	NON	0
		Soleil fort (éblouissement)	A10_2	NON	NON	NON	OUI	OUI	NON	NON	0.4
		Pluie faible	A10_3	NON	NON	NON	NON	NON	NON	NON	0
		Pluie forte	A10_4	NON	OUI	NON	OUI	OUI	NON	OUI	1.6
		Brouillard léger	A10_5	NON	NON	NON	NON	NON	NON	NON	0
		Brouillard dense	A10_6	NON	OUI	NON	OUI	OUI	NON	NON	0.6
A11	Présence objet latéral (barrière de sécurité, véhicule garé, mur en béton, pylône)	Absence	A11_1	NON	NON	NON	NON	NON	NON	NON	0
		Présence	A11_2	OUI	NON	NON	NON	NON	NON	NON	0.2
A9	Vitesse_Ego	Faible [0, 60 km/h]	A9_1								

Tableau 32 : Analyse de sensibilité des plages de valeurs dans le cas du TJC

Ensuite, ces premiers résultats permettent de déterminer la sensibilité du VA aux 48 situations logiques obtenues. Ainsi, pour chaque combinaison de plages, nous avons proposé de calculer la sensibilité en agrégeant les résultats de chacune des plages qui la compose et en utilisant l'échelle définie par le tableau 20 (chapitre 4). Cette échelle donne la contribution de la sensibilité d'une composante du VA (technologie de capteurs, décision, action) dans l'obtention de la sensibilité globale d'une situation logique.

Des exemples de calcul sont présentés dans les tableaux 33 à 36 avec les quatre situations logiques mentionnées dans le tableau 31. Lorsque la technologie (ou la décision ou l'actionnement) est sensible à la plage de valeur AX\_X, cela est indiqué par le chiffre 1 (= Oui). Dans le cas contraire, cela signifie qu'il n'y a pas de sensibilité.

L'ensemble des résultats pour les 48 situations logiques se trouve en annexe 1.

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 1</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_1							
A10_1							
A11_1							
Sensibilité de SL1 /techno	0	0	0,2				
Sensibilité globale de SL1	<b>0,2</b>						

Tableau 33 : Sensibilité du VA à la situation logique Y1

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>Y14</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_2				1	1	1	
A10_2				1	1		
A11_2	1						
Sensibilité de Y14 /technologie	0,2		0,2	0,2	0,2	1	
Sensibilité de Y14	<b>1,8</b>						

Tableau 34 : Sensibilité du VA à la situation logique Y14

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>Y32</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_2				1	1	1	
A10_4		1		1	1		1
A11_2	1						
Sensibilité de Y32 /technologie	0,2	0,2	0,2	0,2	0,2	1	1
Sensibilité de Y32	<b>3</b>						

Tableau 35 : Sensibilité du VA à la situation logique Y32

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>Y35</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_1							
A10_5							
A11_1							
Sensibilité de Y35/ technologie			0,2	0,2	0,2		
Sensibilité de Y35	<b>0,6</b>						

Tableau 36 : Sensibilité du VA à la situation logique Y35

Comme le montrent les tableaux 33 à 36, les sensibilités obtenues pour les situations logiques sont différentes. Le VA est plus sensible à la situation logique Y32 tandis qu'il est moins sensible à la situation logique Y1.

Cependant, pour que les situations soient tirées suivant leur sensibilité, une fonction de distribution doit être mise en place.

### 5.3.3.2 Distribution de la sensibilité du VA aux situations logiques

Pour rappel, la distribution de la sensibilité du VA aux situations logiques telle que présentée dans le chapitre 4, s'obtient comme suit :

$q(Y_j) = \frac{S_j}{W}$  et  $\sum_{Y_j} q(Y_j) = \sum_{Y_j} \frac{S_j}{W} = 1$  où  $W = \sum_{Y_j} S_j$  est le facteur de normalisation,  $Y_j$  est la situation logique  $j$  et  $S_j$  sa sensibilité.

En considérant les 48 situations logiques et leur sensibilité, on obtient  $W = \sum_{j=1}^{48} S_j = 67.4$ . Ainsi, pour chacune des 4 situations logiques précédentes, la distribution de sensibilité est :

- Situation logique Y1 :  $q(Y1) = \frac{0.2}{67.4} = 2.97 * 10^{-3}$
- Situation logique Y14 :  $q(Y14) = \frac{1.8}{67.4} = 2.67 * 10^{-2}$
- Situation logique Y35 :  $q(Y35) = \frac{0.6}{67.4} = 8.9 * 10^{-3}$
- Situation logique Y32 :  $q(Y32) = \frac{3}{67.4} = 4.45 * 10^{-2}$

Bien évidemment la valeur obtenue pour  $q(Y32)$  est plus grande car la sensibilité du VA à Y32 est la plus forte. A noter aussi que la somme totale de probabilité pour les 48 situations est égale à 1, par définition.

Maintenant que nous avons les informations utiles pour les situations logiques, il faut traiter le cas des évènements.

### 5.3.3.3 Evènements et leur sensibilité

Les évènements associés à chaque situation logique sont de trois types : ceux impactant le niveau fonctionnel, ceux impactant le niveau logique et ceux impactant le niveau concret. Ils se présentent soit sous forme de plage de valeurs, soit sous forme de transition entre plage de valeurs. Pour chaque situation logique, une liste d'évènements lui est associée. Pour identifier cette liste, nous nous appuyerons sur les types d'évènements auxquels peut être confronté le VA en condition de TJC, les limites de l'ODD associé et les plages de valeurs des situations logiques. Pour illustrer cela, considérons la situation logique Y14 définie précédemment dans le tableau 34.

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>Y14</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_2				1	1	1	
A10_2				1	1		
A11_2	1						
Sensibilité de Y14 /technologie	0,2		0,2	0,2	0,2	1	
Sensibilité de Y14	<b>1,8</b>						

Les évènements pour cette situation sont tels que :

- Ceux impactant le niveau concret concernent les plages auxquelles au moins l'une des composantes de l'architecture du VA est sensible. Cela concerne les plages : A1\_1, A8\_2, A10\_2 et A11\_2. Leur sensibilité a été définie dans le tableau 37.

Pour rappel, on note par  $\Delta(Ax)$  un évènement concernant un changement de valeur à l'intérieur d'une même plage de valeurs  $Ax$ , puis par  $\Delta(Ax, Ay)$  un évènement concernant un changement de plage de valeurs.

On note  $e_{ji}$  un évènement  $i$  de la situation logique  $j$  et  $Se_{ji}$  sa sensibilité.

$e_{14.1} = \Delta(A1\_1)$	$e_{14.2} = \Delta(A8\_2)$	$e_{14.3} = \Delta(A10\_2)$	$e_{14.4} = \Delta(A11\_2)$
$Se_{14.1} = 0.2$	$Se_{14.2} = 1.4$	$Se_{14.3} = 0.4$	$Se_{14.4} = 0.2$

Tableau 37 : Sensibilité des évènements impactant le niveau concret pour Y14



- Ceux impactant le niveau logique consistent en un changement de plage de valeurs de la situation logique considérée et concernent ce que nous avons appelé le voisinage de niveau 1. En analysant les 48 situations logiques, celles qui diffèrent de Y14 d'une seule plage de valeurs sont : Y6, Y10, Y13, Y16, Y22, Y30, Y38, Y46 (elles représentent le voisinage de niveau 1 de Y14). Etant donné qu'un tel évènement fait passer d'une situation logique à une autre, le gradient (la valeur absolue de la différence de sensibilité entre la situation d'arrivée et celle de départ) est utilisé pour obtenir la sensibilité. Le tableau 38 donne les évènements et leur sensibilité dans le cas de la situation logique Y14.

		Y6	Y10	Y13	Y16	Y22	Y30	Y38	Y46
<b>Y14</b>	Evènement impactant le niveau logique	$e_{14.5} = \Delta(A10\_2, A10\_1)$	$e_{14.6} = \Delta(A11\_2, A11\_1)$	$e_{14.7} = \Delta(A8\_2, A8\_1)$	$e_{14.8} = \Delta(A7\_1, A7\_2)$	$e_{14.9} = \Delta(A10\_2, A10\_3)$	$e_{14.10} = \Delta(A10\_2, A10\_4)$	$e_{14.11} = \Delta(A10\_2, A10\_5)$	$e_{14.12} = \Delta(A10\_2, A10\_6)$
	Sensibilité de l'évènement	$Se_{14.5} = 0$	$Se_{14.6} = 0,2$	$Se_{14.7} = 1$	$Se_{14.8} = 0$	$Se_{14.9} = 0$	$Se_{14.10} = 1,2$	$Se_{14.11} = 0$	$Se_{14.12} = 0,2$

Tableau 38 : Sensibilités des évènements impactant le niveau logique pour Y14

- Ceux impactant le niveau fonctionnel font sortir le VA de la situation fonctionnelle de « Car following ». En considérant les conditions de validité du « Car following » et les contraintes de l'ODD mentionnées dans le paragraphe 5.3.2, les modifications de plages de valeurs (et donc les évènements) qui le font sortir de la situation de car following sont entre autres :
  - o  $e_{14.13} = \Delta(A3\_1, A3\_2)$  (passage de présence de lead à absence de lead vehicle),
  - o  $e_{14.14} = \Delta(A8\_1, A8\_0)$  (passage de 2 voies à 1 voie : fin de la voie de l'Ego)
  - o  $e_{14.15} = \Delta(A8\_2, A8\_0)$  (passage de 3voies et plus à 1 voie avec fin de la voie de l'Ego)

D'une part, la plage A3\_2 n'affecte aucune des composantes (technologies de capteur, décision, actionnement) de l'architecture du VA ; on obtient une première contribution de sensibilité égale à 0. D'autre part, A3\_2 fait changer de situation fonctionnelle (passage de car following à road following) ; on ajoute un facteur de 1 à la sensibilité.

De même, la plage A8\_0 n'affecte aucune technologie (contribution de sensibilité = 0) mais son occurrence implique un changement de voie de la part de l'Ego (ajout d'un facteur de 1 à la sensibilité) et donc fait changer de situation fonctionnelle ; on obtient donc une sensibilité de 1.

Le tableau 39 résume les évènements impactant le niveau fonctionnel.

Situation fonctionnelle de Car following		Road following	Lane changing left
	Evènement impactant le niveau fonctionnel	$e_{14.13} = \Delta(A3\_1, A3\_2)$	$e_{14.14} = \Delta(A8\_1, A8\_0)$ $e_{14.15} = \Delta(A8\_2, A8\_0)$
	Sensibilité de l'évènement	$Se_{14.13} = 1$	$Se_{14.14} = 1$ $Se_{14.15} = 1$

Tableau 39 : Sensibilités des évènements impactant le niveau fonctionnel pour Y14

Ainsi, la liste E14 des évènements associés à la situation logique Y14 regroupe les évènements identifiés dans les tableaux 37, 38 et 39 et contient au total 15 évènements allant de  $e_{14.1}$  à  $e_{14.15}$ . Le tableau 40 présente cette liste.

Comme pour les situations logiques, pour que les évènements soient tirés suivant leur sensibilité, une fonction de distribution est mise en place.

Par ailleurs, pour s'assurer de tirer également les évènements qui ont une sensibilité nulle (par exemple dans le cas de la liste E14 (Tableau 40), cela concerne  $e_{14.5}$ ,  $e_{14.8}$ ,  $e_{14.9}$  et  $e_{14.11}$ ), une valeur minimale non nulle de sensibilité doit leur être attribuée. Nous avons choisi cette valeur de sorte à ce qu'elle soit la plus faible de toutes les valeurs de sensibilité présentes dans la liste. Ainsi, nous attribuerons ici, une sensibilité de 0.1 aux évènements concernés (Cf. Tableau 40).

#### 5.3.3.4 Distribution de sensibilité sur les évènements

La fonction de distribution de sensibilité se définit comme suit :

$q(e_{ji}) = \frac{Se_{ji}}{W_{Ej}}$  et  $\sum_{e_{ji}} q(e_{ji}) = \sum_{e_{ji}} \frac{Se_{ji}}{W_{Ej}} = 1$ , où  $W_{Ej} = \sum_{e_{ji}} Se_{ji}$  est le facteur de normalisation pour la liste  $E_j$  d'évènements  $e_{ji}$  et  $Se_{ji}$  la sensibilité d'un évènement  $e_{ji}$ .

En considérant la liste E14 des 15 évènements associés à la situation logique Y14 et leurs sensibilités, on trouve :  $W_{E14} = \sum_{i=1}^{15} S_{14i} = 8.2$ .

La distribution de sensibilité des évènements de la liste E14 (associés à la situation logique Y14) est donnée dans le tableau 41. Par ailleurs, la somme de toutes les probabilités faisant 1, on vérifie que  $\sum_{i=1}^{15} q(e_{14i}) = 1$ .

Liste des évènements associés à la situation logique Y14														
Evènements impactant le niveau concret				Evènements impactant le niveau logique								Evènements impactant le niveau fonctionnel		
$e_{14.1} = \Delta(A1_1)$	$e_{14.2} = \Delta(A8_2)$	$e_{14.3} = \Delta(A10_2)$	$e_{14.4} = \Delta(A11_2)$	$e_{14.5} = \Delta(A10_2, A10_1)$	$e_{14.6} = \Delta(A11_2, A11_1)$	$e_{14.7} = \Delta(A8_2, A8_1)$	$e_{14.8} = \Delta(A7_1, A7_2)$	$e_{14.9} = \Delta(A10_2, A10_3)$	$e_{14.10} = \Delta(A10_2, A10_4)$	$e_{14.11} = \Delta(A10_2, A10_5)$	$e_{14.12} = \Delta(A10_2, A10_6)$	$e_{14.13} = \Delta(A3_1, A3_2)$	$e_{14.14} = \Delta(A8_1, A8_0)$	$e_{14.15} = \Delta(A8_2, A8_0)$
$Se_{14.1} = 0.2$	$Se_{14.2} = 1.4$	$Se_{14.3} = 0.4$	$Se_{14.4} = 0.2$	$Se_{14.5} = 0$ Soit $Se_{14.5} = 0.1$	$Se_{14.6} = 0.2$	$Se_{14.7} = 1$	$Se_{14.8} = 0$ Soit $Se_{14.8} = 0.1$	$Se_{14.9} = 0$ Soit $Se_{14.9} = 0.1$	$Se_{14.10} = 1,2$	$Se_{14.11} = 0$ Soit $Se_{14.11} = 0.1$	$Se_{14.12} = 0,2$	$Se_{14.13} = 1$	$Se_{14.14} = 1$	$Se_{14.15} = 1$

Tableau 40 : Liste E14 des évènements associés à la situation logique Y14

Evènements	$e_{14.1} = \Delta(A1_1)$	$e_{14.2} = \Delta(A8_2)$	$e_{14.3} = \Delta(A10_2)$	$e_{14.4} = \Delta(A11_2)$	$e_{14.5} = \Delta(A10_2, A10_1)$	$e_{14.6} = \Delta(A11_2, A11_1)$	$e_{14.7} = \Delta(A8_2, A8_1)$	$e_{14.8} = \Delta(A7_1, A7_2)$	$e_{14.9} = \Delta(A10_2, A10_3)$	$e_{14.10} = \Delta(A10_2, A10_4)$	$e_{14.11} = \Delta(A10_2, A10_5)$	$e_{14.12} = \Delta(A10_2, A10_6)$	$e_{14.13} = \Delta(A3_1, A3_2)$	$e_{14.14} = \Delta(A8_1, A8_0)$	$e_{14.15} = \Delta(A8_2, A8_0)$
Sensibilités	$Se_{14.1} = 0.2$	$Se_{14.2} = 1.4$	$Se_{14.3} = 0.4$	$Se_{14.4} = 0.2$	$Se_{14.5} = 0$ Soit $Se_{14.5} = 0.1$	$Se_{14.6} = 0.2$	$Se_{14.7} = 1$	$Se_{14.8} = 0$ Soit $Se_{14.8} = 0.1$	$Se_{14.9} = 0$ Soit $Se_{14.9} = 0.1$	$Se_{14.10} = 1,2$	$Se_{14.11} = 0$ Soit $Se_{14.11} = 0.1$	$Se_{14.12} = 0,2$	$Se_{14.13} = 1$	$Se_{14.14} = 1$	$Se_{14.15} = 1$
Probabilités associées	$q(e_{14.1}) = 0.024$	$q(e_{14.2}) = 0.17$	$q(e_{14.3}) = 0.049$	$q(e_{14.4}) = 0.024$	$q(e_{14.5}) = 0.01$	$q(e_{14.6}) = 0.024$	$q(e_{14.7}) = 0.122$	$q(e_{14.8}) = 0.01$	$q(e_{14.9}) = 0.01$	$q(e_{14.10}) = 0.146$	$q(e_{14.11}) = 0.01$	$q(e_{14.12}) = 0.024$	$q(e_{14.13}) = 0.122$	$q(e_{14.14}) = 0.122$	$q(e_{14.15}) = 0.122$

Tableau 41 : Distribution de sensibilités des évènements de la liste E14

Cette phase d'analyse en amont de la génération des scénarios concrets a permis d'illustrer comment déterminer les éléments requis (la sensibilité du VA aux situations logiques, la fonction de distribution de sensibilité des situations logiques, les événements associés à chaque situation logique et leur sensibilité et enfin, la fonction de distribution de sensibilité sur les événements d'une situation logique) pour l'application de l'heuristique proposée dans le chapitre 4 et l'estimation du risque associé au VA, équipé dans notre exemple, de la fonction d'automatisation TJC.

Ainsi, pour continuer l'illustration sur le cas d'étude, cette heuristique devrait être appliquée sur les 48 situations logiques associées à la situation fonctionnelle de « car following » que nous avons choisie. Cependant, nous proposons d'effectuer l'illustration sur quelques situations. Pour ce faire, nous verrons dans la section suivante, les résultats observés lors de l'échantillonnage et la simulation de scénarios concrets obtenus à partir de deux situations logiques simplifiées, que nous notons Y1 et Y2.

#### 5.3.4 Génération des scénarios concrets et expérimentation

La génération des scénarios concrets utilise l'analyse a priori sur les situations logiques et les plages de valeurs ainsi qu'une heuristique de génération pour prioriser l'obtention de scénarios concrets potentiellement critiques. Toutefois, **le but de cette expérimentation est de vérifier l'applicabilité de la modélisation d'un scénario concret à l'interface d'un outil de simulation.**

Par ailleurs, pour l'analyse a posteriori (après simulation), nous avons défini dans le chapitre 4, les critères de fin de scénarios suivant :

1. Présence de collision
2. Demande de give back
3. Fin de la manœuvre/ changement de manœuvre (inclus le retour à un Etat safe)
4. Violation d'une condition de validité de la manœuvre ou présence de HB
5. « Durée maximale d'un scénario (en cas d'absence de changement de manœuvre) »

En outre, la situation fonctionnelle considérée est toujours celle du car following : « Ego en situation de « Car following » dans le mode « Activation » sur Autoroute et en trafic embouteillé » (figure 21).

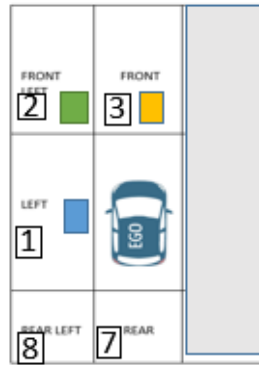


Figure 21 : Situation de car following sur deux voies

Les deux situations logiques simplifiées Y1 et Y2 sont les suivantes :

<p><b>Y1</b> = Position_AutreVehicule.1.Vraie * Position_AutreVehicule.2.Vraie *          Position_AutreVehicule.3.Vraie * Vitesse_AutreVehicule.1.Faible *          Vitesse_AutreVehicule.2.Faible * Vitesse_AutreVehicule.3.Faible * Nombre_voies.2</p>
<p><b>Y2</b> = Position_AutreVehicule.1.Vraie * Position_AutreVehicule.2.Vraie *          Position_AutreVehicule.3.Vraie * Vitesse_AutreVehicule.1.Faible *          Vitesse_AutreVehicule.2.Faible * Vitesse_AutreVehicule.3.Faible * Nombre_voies.3</p>

Tableau 42 : Situations logiques Y1 et Y2 considérées pour l'expérimentation

En analysant ces deux situations logiques, on remarque qu'elles diffèrent par le nombre de voies. Or pour rappel, la plage de valeurs « Nombre\_voies.3 » (sensibilité = 0) est plus sensible que la plage « Nombre\_voies.2 » (sensibilité = 1.4) (Cf. tableau 32). Ainsi, Y2 est plus sensible que Y1. En échantillonnant suivant la sensibilité, la probabilité de tirer la situation Y2 sera plus élevée que celle de tirer la situation Y1.

Par ailleurs, nous choisissons un évènement particulier qui est le cut-in provenant du type d'évènement Ed2 « Déviations dans le comportement des autres usagers par rapport à l'exécution des manœuvres », tel que mentionné dans le tableau 28. En effet, cet évènement de cut-in correspond au rabattement du véhicule de gauche (AutreVehicule.1 (Left)), devant l'Ego avec une distance inférieure à la distance de sécurité. Traduite en termes de plages de valeurs, cette distance décomposée en deux plages de valeurs, permet d'avoir un cut\_in.Faible (exemple : rabattement entre 0 et 5m) et un cut\_in.Autre (exemple : rabattement entre 5 et « D safe », avec « D safe » la distance de sécurité).

Ainsi, on a deux évènements **E1.1** = cut\_in.Faible et **E1.2** = cut\_in.Autre. L'analyse de sensibilité de ces deux évènements montre que E1.1 est un évènement impactant le niveau fonctionnel car provoquant la transition vers une situation fonctionnelle de « Braking (freinage d'urgence) » et a une sensibilité de 1, tandis que E1.2 est un évènement impactant le niveau logique avec une sensibilité minimale de 0.1. En échantillonnant suivant la sensibilité, la probabilité de tirer E1.1 sera plus élevée que celle de tirer E1.2.

Soit le tirage de Y1 avec l'évènement E1.1, qui permet d'obtenir le scénario logique 1. Et soit le tirage de Y2 avec l'évènement E1.2, permettant d'obtenir le scénario logique 2.

<b>Scénario logique 1 = Y1 + E1.1</b>		
Position_AutreVehicule.1.Vraie *	Position_AutreVehicule.2.Vraie *	Position_AutreVehicule.3.Vraie *
Vitesse_AutreVehicule.1.Faible *	Vitesse_AutreVehicule.2.Faible *	Vitesse_AutreVehicule.3.Faible *
Nombre_voies.2 * Distance de cut_in.Faible		
<b>Scénario logique 2 = Y2 + E1.2</b>		
Position_AutreVehicule.1.Vraie *	Position_AutreVehicule.2.Vraie *	Position_AutreVehicule.3.Vraie *
Vitesse_AutreVehicule.1.Faible *	Vitesse_AutreVehicule.2.Faible *	Vitesse_AutreVehicule.3.Faible *
Nombre_voies.3 * Distance de cut_in.Autre		

Tableau 43 : Scénarios logiques considérés pour l'expérimentation

#### 5.3.4.1 Environnement d'échantillonnage et de simulation

Les scénarios concrets sont générés via l'outil Matlab et la simulation se fait grâce à l'outil CarMaker (IPG Automotive)<sup>11</sup>. Pour ce faire, les scénarios concrets générés sous Matlab, sont d'abord convertis dans un format exécutable par le simulateur CarMaker (la formalisation se fait sous forme de fichier « test run »), avant d'être introduits dans ce dernier pour la simulation.

Ainsi, l'outil Matlab est un environnement de développement qui utilise un langage de script de même nom « Matlab ». CarMaker est un environnement de simulation composé d'un modèle de conducteur intelligent, d'un modèle de véhicule détaillé et de modèles flexibles pour la route et la circulation. La méthode de test dans CarMaker est basée sur les événements et les manœuvres. En effet, la modélisation d'actions spéciales, comme les activités du conducteur ou les interventions des systèmes, s'effectue intuitivement par le biais des manœuvres. Le simulateur contient un « Test Manager » qui assure l'automatisation du processus de test.

Le principe de fonctionnement de CarMaker peut être décrit comme suit :

- Il dispose d'un fichier de « Test run » qui correspond au scénario à tester. La simulation de plusieurs fichiers peut se faire rapidement, grâce à l'automatisation des tests.
- Des critères de succès ou d'échec (pass / fail), mais aussi de mesure de performances peuvent être mémorisés pour analyser a posteriori les résultats de simulation.
- En plus du temps alloué à la simulation d'un scénario, on peut définir des critères d'arrêt d'un scénario de test (par exemple : lorsque le temps inter véhicule avec le « lead vehicle » devient nominal, le scénario est terminé)

#### 5.3.4.2 Phase d'échantillonnage et de simulation (expérimentation)

Comme indiqué précédemment, le but de cette expérimentation est de vérifier l'applicabilité de la modélisation d'un scénario concret à l'interface d'un outil de simulation.

Nous faisons l'hypothèse que toutes les valeurs qui sont à l'intérieur d'une plage de valeurs ont la même probabilité d'être tirées. Et de ce fait, nous utilisons une loi uniforme pour le tirage des valeurs concrètes dans chaque plage. Pour chaque scénario logique, 100 scénarios concrets sont générés sous Matlab. Le scénario concret s'obtient en tirant une valeur concrète à l'intérieur de chacune des plages composant le scénario logique. Puisqu'un scénario représente

<sup>11</sup> <https://ipg-automotive.com/fr/produits-et-services/simulation-software/carmaker/>

pour nous, l'occurrence d'un évènement dans une situation, les tirages effectués dans les plages de valeurs vont servir en deux temps :

- les tirages dans certaines plages permettent d'avoir la situation de départ (situation initiale) à un instant t1
- les tirages dans les plages représentant des évènements, sont instanciés à des instants t2 et t3 suivant le moment où l'on veut enclencher l'évènement

Ainsi, dans le cas de notre illustration avec les scénarios logiques 1 et 2, la situation initiale est obtenue grâce à l'échantillonnage des paramètres de position et vitesse. Nous considérons que la « Vitesse\_AutreVehicule.1 » doit être supérieure à celle de l'Ego (d'une valeur max de 10 pour respecter la condition de dépassement et d'embouteillage). Les vitesses des autres véhicules sont prises comme étant les mêmes que celle de l'Ego. L'évènement de cut-in, matérialisé par le paramètre « Distance de cut\_in », est appliqué à l'instant t2.

Comme mentionné précédemment, pour rendre les scénarios concrets simulables (exécutables) dans le simulateur CarMaker, ceux-ci sont formalisés dans des fichiers appelés « Test run ». Ensuite, les 100 « Test run » correspondant aux 100 scénarios concrets pour chaque scénario logique, ont été regroupés dans un « Test manager » pour faciliter leur simulation de façon automatique.

La simulation prend fin si :

- une collision est observée
- L'Ego finit ses manœuvres avant la fin du trajet / la durée max de la simulation est atteinte.
- l'Ego finit le trajet avant la fin de ses manœuvres

La section suivante décrit les résultats de simulation obtenus.

#### *5.3.4.3 Analyse des résultats*

La phase de génération montre que les paramètres retenus et leurs plages de valeurs, permettent d'obtenir des scénarios concrets utilisables pour la simulation. Cependant, lors de la formalisation, une attention particulière doit être accordée aux dépendances entre paramètres pour éviter la génération de scénarios dépourvus de sens. C'est le cas des paramètres « vitesse » et « position » puisque la position d'un véhicule évolue avec sa vitesse.

Quant à la simulation, les résultats des 100 scénarios concrets associés au scénario logique 1, montrent que 33 d'entre eux sont critiques car ils conduisent à une collision entre l'Ego et l'autre véhicule<sup>1</sup>. Pour les 100 scénarios concrets associés au scénario logique 2, seule une collision est observée. Les annexes 2 et 3 donnent respectivement un aperçu des résultats avec identification des scénarios ayant conduit à la collision pour les scénarios logiques 1 et 2.

Bien que l'analyse de sensibilité ait montré que la situation logique Y2 est plus sensible que la situation logique Y1, le scénario logique 2 obtenu avec Y2, a produit moins de scénarios concrets critiques que celui obtenu avec Y1. En effet, cela se justifie par le fait que la sensibilité de l'évènement a joué un rôle dans les résultats obtenus. De ce fait, même si Y1 est moins sensible, son effet combiné à celui de l'évènement E1.1 qui est plus sensible que E1.2, a

augmenté le niveau de risque du scénario logique 1. Par ailleurs, on remarque que même si l'évènement E1.2 est moins sensible que E1.1, sa combinaison avec la situation Y2 de sensibilité élevée, a permis d'identifier un scénario concret critique dans le scénario logique 2.

De tels résultats confirment notre proposition initiale : une analyse de sensibilité a priori à la fois sur la situation et l'évènement est importante pour la recherche des scénarios critiques pour le VA. Aussi, on peut noter que le découpage des plages de valeurs selon la sensibilité est pertinent. En effet, comme on peut le voir avec les deux plages représentant les évènements E1.1 et E1.2, l'évènement E1.1 qui est beaucoup plus sensible a conduit à l'obtention de plus de scénarios critiques dans le scénario logique 1. Enfin, l'indicateur de criticité a posteriori a pu être utilisé à travers le critère de collision qui définit les scénarios concrets critiques à l'issue de la simulation.

## 5.4 DISCUSSION

Nous avons illustré dans ce chapitre les concepts introduits dans le mémoire ainsi que les éléments requis pour l'analyse de sensibilité a priori des scénarios et leur génération. La phase d'expérimentation a permis de vérifier que le modèle de scénario est utilisable dans un outil de simulation. Cette phase a également permis de constater qu'il est possible de produire des résultats en termes de collision, qui pourront être réutilisés dans une boucle itérative pour orienter la génération.

Ainsi, la sensibilité a priori est obtenue via les connaissances d'expertise (décomposition des plages de variation des paramètres en plages de valeurs de sensibilité différentes) et la sensibilité a posteriori, via les résultats courants des simulations pour orienter la génération dans une nouvelle boucle d'itération.

En termes de limites, nous considérons l'outil de simulation CarMaker comme une boîte noire dont l'étude est en dehors du périmètre de la thèse. En effet, nous n'avons pas étudié les limites fonctionnelles de la modélisation des capteurs dans cet outil. Aussi, il ne s'agissait pas dans l'expérimentation, d'analyser en détail la nature des accidents (par exemple : la différence de vitesse des usagers avant collision) mais, de vérifier qu'un outil de simulation comme CarMaker permet bien de simuler un scénario modélisé selon notre cadre conceptuel et d'obtenir l'information de l'occurrence d'une collision.

## 5.5 CONCLUSION

Ce chapitre 5 a permis d'appliquer les propositions faites dans ce travail de thèse dans le cas d'un VA équipé de la fonction TJC de niveau d'automatisation 3. D'une part, nous avons pu illustrer les concepts suivants : ODD, cas d'utilisation, performance fonctionnelle, limitation de performance, manœuvre opérationnelle, mode opérationnel, scénario, situation, évènement. D'autre part, nous avons montré comment générer les scénarios suivant les trois niveaux d'abstraction : fonctionnel, logique et concret. Au niveau fonctionnel, les situations fonctionnelles et les types d'évènements associés au VA pour la fonction TJC ont été identifiés.



Au niveau logique, nous avons vu comment obtenir les plages de valeurs des paramètres des entités décrivant les situations fonctionnelles et plus généralement l'ODD. La combinaison de ces plages permet d'obtenir les situations logiques associées à chacune des situations fonctionnelles. Au niveau concret, afin de guider l'échantillonnage et favoriser l'usage des indicateurs définis dans le chapitre 3 pour la génération et la validation, une phase d'analyse a été initiée en amont de l'obtention des scénarios concrets. L'illustration de l'indicateur de criticité a priori a été introduite lors de sa définition dans le chapitre 3. Elle a permis de définir via une APR, les événements redoutés possibles pour le TJC. Pour tenir compte de l'indicateur de sensibilité, les plages de valeurs précédemment identifiées pour la génération, ont été analysées suivant la sensibilité. Cette analyse de sensibilité a été utilisée pour construire ensuite, l'analyse de sensibilité des situations logiques associées à chaque situation fonctionnelle.

Aussi, pour les événements associés aux situations logiques, les distributions de probabilité sur les sensibilités ont été définies. Ces fonctions sont utiles pour effectuer le tirage des situations logiques et des événements suivant leur importance en termes de sensibilité. Enfin, comme l'objectif était avant tout de montrer la faisabilité et l'applicabilité de la méthode, et compte tenu des implications techniques complexes pour l'appliquer à toute l'heuristique, nous avons utilisé deux scénarios logiques simplifiés. D'abord, sur ces deux scénarios logiques, nous avons vu comment effectuer les tirages dans les plages de valeurs. Ensuite, les 100 scénarios concrets générés et simulés pour chacun, ont permis de confirmer la sensibilité estimée a priori pour chaque situation et événement logiques. De plus, l'indicateur de criticité a posteriori a pu être analysé au travers de critères ayant permis de juger de la présence ou non de collision et donc de criticité des scénarios concrets.

---

## CONCLUSION GENERALE ET PERSPECTIVES

---

Ce travail de thèse a permis de répondre à la question globale de recherche posée dans le chapitre introductif : **Comment assurer la validation par simulation de la sécurité du VA, au regard de ses limitations de performance ?**

La réponse apportée à cette question concerne la spécification d'une stratégie de génération de scénarios permettant d'identifier et générer des scénarios critiques, que les concepteurs de la fonction d'automatisation étudiée devront simuler pour vérifier le comportement du VA et estimer sa sécurité.

Cinq chapitres ont aidé à la mise en place de cette réponse. Nous avons commencé par un état de l'art des propositions existantes dans la littérature sur la validation de la sécurité du VA. Ensuite, après avoir relevé les aspects pertinents et les manquements observés dans ces propositions, nous avons proposé une solution qui entend combler les manques relevés.

L'objet de cette conclusion est de synthétiser les contributions apportées dans l'ensemble des chapitres, puis de présenter quelques perspectives envisageables, pour donner une suite à l'ensemble des travaux que nous avons adressés dans ce mémoire.

### SYNTHESE DES RESULTATS

Nous avons développé dans ce mémoire cinq contributions résumées comme suit.

D'abord, le chapitre 1 a permis de relever les challenges et les problématiques observés dans la démonstration de la sécurité du VA : aspects normatifs, chaînes de simulation, la présence d'incertitude dans l'environnement opérationnel du VA, complexité de l'architecture du VA, variabilité des performances et limites fonctionnelles des capteurs. Ce premier chapitre a donné l'occasion de résumer le champ adressé dans ce mémoire, à savoir que nous nous intéressons à la validation par simulation de la sécurité du VA (sécurité au sens « Safety »), et que ce travail s'inscrit dans le périmètre du SOTIF (Safety Of The Intended Functionality) (ISO PAS 21448).

Ensuite, le chapitre 2 a amorcé la phase de spécification de la solution, grâce à la mise en place du cadre conceptuel requis pour la génération des scénarios. En effet, nous avons relevé l'existence de nombreux concepts en lien avec le VA et son environnement opérationnel. Pour lever toute ambiguïté et faciliter la compréhension de nos propositions, nous avons pensé pertinent de fixer l'ensemble des concepts que nous jugeons utiles et nécessaires pour la mise en place de la stratégie de génération des scénarios. Par ailleurs, ce chapitre a également permis

de revenir sur les catégories d'entités présentes dans l'environnement du VA, ainsi que le besoin de définir les paramètres qui leur sont associés.

En outre, pour s'assurer d'obtenir une stratégie de génération de scénarios et de validation par simulation de la sécurité du VA qui soit pertinente, une structure de système et un ensemble d'indicateurs à utiliser conjointement ont été introduits dans le chapitre 3. Cette proposition a été motivée d'une part, par l'absence dans la littérature d'une métrique permettant d'identifier au préalable (avant la simulation) les scénarios potentiellement critiques, en vue d'orienter la génération et d'autre part, par l'intérêt de l'utilisation conjointe de plusieurs indicateurs, ce qui augmente l'efficacité de la démonstration de la sécurité du VA. Ainsi, nous avons proposé d'un côté, les indicateurs d'estimation de la criticité incluant l'indicateur de sensibilité, de couverture et de représentativité pour définir la performance de la génération, puis de l'autre côté, l'indicateur de risque final et l'intervalle de confiance associé, pour estimer le résultat final du processus de validation par simulation tout en tenant compte des incertitudes dont sont entachées les évaluations.

Le chapitre 4 propose une stratégie de génération et de validation par simulation de la sécurité du VA. Devant l'espace d'exploration des scénarios qui est très vaste, ou encore l'absence d'approche prenant en compte l'ensemble du profil de mission du VA, nous avons mis en place une stratégie qui se décline, pas à pas, et qui reste évolutive suivant les niveaux d'automatisation du VA. Ainsi, cette stratégie s'aligne sur une structuration en trois niveaux d'abstraction : fonctionnelle, logique et concret. Elle s'appuie sur le cadre conceptuel défini dans le chapitre 2 et sur l'ensemble des indicateurs proposés dans le chapitre 3. De ce fait, la stratégie proposée intègre une analyse a priori de la criticité des scénarios grâce notamment à la sensibilité, et permet de mettre l'accent sur les scénarios potentiellement critiques dès le début de la génération. Cette analyse est renforcée en cours de la simulation par la prise en compte des résultats obtenus pour classer les scénarios. Ce chapitre se termine par la mise en place d'une heuristique qui guide la manière d'explorer l'espace des scénarios et donne finalement une estimation des indicateurs de performance de la génération et de validation de la sécurité du VA.

Enfin, le 5 chapitre est le chapitre applicatif de nos propositions. Il s'appuie sur un cas d'étude pour illustrer à la fois les concepts de la génération ainsi que les indicateurs et les éléments de la stratégie de génération et de validation par simulation de la sécurité du VA. Pour ce faire, nous avons considéré le VA comme étant équipé de la fonction d'automatisation « Traffic Jam Chauffer (TJC) » de niveau d'automatisation 3.

## PERSPECTIVES

Nos travaux apportent une contribution à la démonstration de la sécurité du VA via la génération de scénarios et l'usage de la simulation. Pour que cette contribution aide de manière efficace au déploiement de VA sûrs, d'autres études doivent être menées.

D'abord, l'heuristique d'exploration et de génération des scénarios concrets nécessite d'être appliquée et testée en conditions réelles et à grande échelle. Cette heuristique s'appuie sur une approche itérative qui permet d'identifier après simulation, les situations logiques qui produisent des scénarios concrets critiques en vue de les prioriser tout au long de la phase de

test. Avant simulation, c'est la sensibilité qui permet de choisir les scénarios logiques qui sont à utiliser pour générer les scénarios concrets. Les éléments nécessaires à la mise en place de l'heuristique ont été illustrés. Cette illustration doit être poursuivie en mettant en place une implémentation globale de l'heuristique avec un moteur de génération et un environnement de simulation adapté. Cela nécessitera des travaux scientifiques et technologiques complémentaires au sein de l'entité en charge de la validation chez le constructeur en collaboration avec les fournisseurs de simulateur ou d'organes du VA.

A ce titre, une analyse de sensibilité de l'heuristique de génération peut être menée soit selon la méthode de calcul de sensibilité proposée, soit en introduisant des biais sur les valeurs de sensibilité estimées par l'expert ou encore en modifiant l'amplitude des plages de valeurs définies pour les paramètres.

Aussi, la notion de « voisinage » introduite peut être étendue à différents niveaux (voisinage de niveau X, avec  $X > 1$ ). De plus, le couplage des paramètres en tenant compte de leur dépendance peut être analysé et considéré de sorte à réduire davantage l'explosion combinatoire de la génération.

En outre, nous avons considéré l'incertitude au sens probabiliste. Une alternative serait d'utiliser la théorie de Dempster-Shafer pour combiner la croyance sur la sensibilité venant des experts et les résultats (des faits) provenant (en cours) de la simulation. Cela permettrait de tenir compte d'une masse de croyance sur les paramètres inconnus.

Un autre point mis en perspective concerne l'environnement de simulation lui-même. Les outils de simulation, actuellement utilisés dans le cadre de la validation par simulation du VA, présentent un écart de représentativité par rapport à la réalité. En effet, un effort supplémentaire doit être fourni dans la conception de ces outils notamment en ce qui concerne le niveau de modélisation de l'environnement de test (par exemple la modélisation des paramètres liés aux conditions climatiques « pluie, neige, brouillard ») ou encore la modélisation du comportement du VA et notamment de ses interactions avec l'environnement (par exemple : incertitude sur la caractérisation des capteurs ou de l'adhérence au sol). A défaut, cela risque de limiter la validation effective du VA par simulation, pour ce qui est du SOTIF et par conséquent, l'application effective de la stratégie proposée dans nos travaux.

Enfin, au-delà du périmètre SOTIF, d'autres challenges impactant la sécurité globale doivent être considérés pour aboutir à une couverture totale du volet sécuritaire lié au VA. Ils concernent la résistance des VA contre les attaques de cyber sécurité, la démonstration de sécurité des algorithmes d'IA (Intelligence Artificielle) et les aspects éthiques liés à la prise de décision du VA. De nombreux travaux y compris au niveau normatif sont actuellement en cours pour apporter des éléments de solutions à ces challenges.

---

## REFERENCES BIBLIOGRAPHIQUES

---

- AFIS. (2009). Découvrir et comprendre l'Ingénierie Système.
- Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, & Carl Landwehr. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, 01(1), 11–33. Retrieved from [https://www.nasa.gov/pdf/636745main\\_day\\_3-algirdas\\_avizienis.pdf](https://www.nasa.gov/pdf/636745main_day_3-algirdas_avizienis.pdf)
- Allenby, K., & Kelly, T. (2001). Deriving Safety Requirements Using Scenarios. *5th IEEE International Symposium on Requirements Engineering (ISRE'01)*.
- Althoff, D., Weber, B., Wollherr, D., & Buss, M. (2016). Closed-loop safety assessment of uncertain roadmaps. *Autonomous Robots*, 40(2), 267–289. <https://doi.org/10.1007/s10514-015-9452-1>
- Althoff, M. (2010). *Reachability Analysis and its Application to the Safety Assessment of Autonomous Cars*. PhD, Technische Universität München. <https://doi.org/10.1017/CBO9781107415324.004>
- Amersbach, C., & Winner, H. (2019a). Defining Required and Feasible Test Coverage for Scenario-Based Validation of Highly Automated Vehicles. *2019 IEEE Intelligent Transportation Systems Conference, ITSC 2019*, 425–430. <https://doi.org/10.1109/ITSC.2019.8917534>
- Amersbach, C., & Winner, H. (2019b). Functional decomposition—A contribution to overcome the parameter space explosion during validation of highly automated driving. *Traffic Injury Prevention*, 20(sup1), S52–S57. <https://doi.org/10.1080/15389588.2019.1624732>
- Aptiv, Audi, Baidu, BMW, Continental, Daimler, ... Volkswagen. (2019). *Safety first for automated driving*.
- Bach, J., Otten, S., & Sax, E. (2016). Model based scenario specification for development and test of automated driving functions. *IEEE Intelligent Vehicles Symposium, Proceedings, 2016-Augus(Iv)*, 1149–1155. <https://doi.org/10.1109/IVS.2016.7535534>
- Bagschik, G., Menzel, T., & Maurer, M. (2018). Ontology based Scene Creation for the Development of Automated Vehicles. In *2018 IEEE Intelligent Vehicles Symposium (IV)* (pp. 1–8). Changshu, China: IEEE. <https://doi.org/10.1109/IVS.2018.8500632>
- Bagschik, G., Reschka, A., Stolte, T., & Maurer, M. (2016). Identification of potential hazardous events for an Unmanned Protective Vehicle. In *2016 IEEE Intelligent Vehicles Symposium (IV)* (Vol. 2016-Augus, pp. 691–697). Gothenburg, Sweden: IEEE. <https://doi.org/10.1109/IVS.2016.7535462>
- Chen, W., & Kloul, L. (2018). An Ontology-based Approach to Generate the Advanced Driver Assistance Use Cases of Highway Traffic. In *10th International Joint Conference on*

*Knowledge Discovery, Knowledge Engineering and Knowledge Management* (pp. 1–11). Seville, Spain.

- Chen, W., & KLOUL, L. (2019). Stochastic modelling of Autonomous Vehicles Driving Scenarios using PEPA. In Springer (Ed.), *International Symposium on Model-Based Safety and Assessment* (pp. 1–15). [https://doi.org/10.1007/978-3-030-32872-6\\_21](https://doi.org/10.1007/978-3-030-32872-6_21)
- Deo, N., Rangesh, A., & Trivedi, M. M. (2018). How would surround vehicles move? A Unified Framework for Maneuver Classification and Motion Prediction, *3*(2), 129–140. <https://doi.org/10.1109/TIV.2018.2804159>
- Dickmanns, E. D. (2007). *Dynamic vision for perception and control of motion* (1st ed.). Springer-Verlag London. <https://doi.org/10.1007/978-1-84628-638-4>
- Feng, S., Feng, Y., Sun, H., Bao, S., Misra, A., Zhang, Y., & Liu, H. X. (2020a). Testing Scenario Library Generation for Connected and Automated Vehicles, Part I: Methodology. *IEEE Transactions on Intelligent Transportation Systems*, *22*(3), 1573–1582. <https://doi.org/10.1109/TITS.2020.2972211>
- Feng, S., Feng, Y., Sun, H., Bao, S., Misra, A., Zhang, Y., & Liu, H. X. (2020b). Testing Scenario Library Generation for Connected and Automated Vehicles, Part II: Case Studies. In *IEEE Transactions on Intelligent Transportation Systems*, 1–13. <https://doi.org/10.1109/TITS.2020.2988309>
- Gerdes, A. (2006). Automatic Maneuver Recognition in the Automobile: the Fusion of Uncertain Sensor Values using Bayesian Models. In *Proceedings of the 3rd International Workshop on Intelligent Transportation (WIT 2006)* (pp. 129–133). Hamburg, Deutschland.
- Geyer, S., Kienle, M., Franz, B., Winner, H., Bengler, K., Baltzer, M., ... Meier, S. (2013). Concept and development of a unified ontology for generating test and use-case catalogues for assisted and automated vehicle guidance. *IET Intelligent Transport Systems*, *8*(3), 183–189.
- Gietelink, O., De Schutter, B., & Verhaegen, M. (2006). Adaptive importance sampling for probabilistic validation of advanced driver assistance systems. *Proceedings of the American Control Conference, 2006*, 4002–4007. <https://doi.org/10.1109/acc.2006.1657344>
- Hallerbach, S., Xia, Y., Eberle, U., & Koester, F. (2018). Simulation-based Identification of Critical Scenarios for Cooperative and Automated Vehicles. *SAE Technical Paper 2018-01-1066*, 19. <https://doi.org/10.4271/2018-01-1066>
- Hellestrand, G. R. (2013). Engineering safe autonomous mobile systems of systems using specification (model) based systems architecture & engineering. In *SysCon 2013 - 7th Annual IEEE International Systems Conference, Proceedings*.
- Hungar, H., Köster, F., & Mazzega, J. (2017). Test Specifications for Highly Automated Driving Functions: Highway Pilot. In *Autonomous Vehicle Test & Development Symposium 2017* (pp. 1–27).
- ISO/IEC/IEEE 29119-1: *Software and systems engineering--Software testing--Part 1: Concepts and definitions*. (2013).
- ISO/PAS 21448. (2019). *ISO / PAS (Publicly Available Specification)*.

- ISO 26262-1. (2011). *Road vehicles - Functional safety - Part 1: Vocabulary* (Vol. 2011).
- ISO 26262-3. (2011). *Road vehicles - Functional safety - Part 3: Concept phase* (Vol. 2011).
- Jang, H. A., Kwon, H. M., & Lee, M. K. (2015). A Study on Situation Analysis for ASIL Determination. *Journal of Industrial and Intelligent Information*, 3(2), 152–157. <https://doi.org/10.12720/jiii.3.2.152-157>
- Jesenski, S., Stellet, J. E., Branz, W., & Zöllner, J. M. (2019). Simulation-Based Methods for Validation of Automated Driving: A Model-Based Analysis and an Overview about Methods for Implementation. *2019 IEEE Intelligent Transportation Systems Conference, ITSC 2019*, 1914–1921. <https://doi.org/10.1109/ITSC.2019.8917072>
- Kalra, N., & Paddock, S. M. (2016). *Driving to Safety*. RAND Corporation - [www.rand.org](http://www.rand.org). <https://doi.org/10.7249/RR1478>
- Kelly, M. O., Sinha, A., Namkoong, H., Duchi, J., & Tedrake, R. (2018). Scalable End-to-End Autonomous Vehicle Testing. In *32nd International Conference on Neural Information Processing Systems* (pp. 9849–9860).
- Kuhnt, F., Sahin, Ö., Kuhnt, F., Zöllner, J. M., & Stiller, C. (2016). Functional System Architectures towards Fully Automated Driving, (October 2017). <https://doi.org/10.1109/IVS.2016.7535402>
- Lakomicki, P., Castanier, B., & Grall, A. (2018). Incremental Reliability Modeling Framework to Optimize Vehicle's Validation Tests. In *Proceedings - Annual Reliability and Maintainability Symposium* (Vol. 2018-Janua). <https://doi.org/10.1109/RAM.2018.8463105>
- Lakomicki, Paula, Tourbier, Y., Castanier, B., & Grall, A. (2019). Encadrement de la fiabilité du véhicule autonome pour guider les tests de validation. In *Congrès Lambda Mu 21 "Maîtrise des risques et transformation numérique : opportunités et menaces ."* Reims, France.
- Laugier, C., Paromtchik, I., Perrollaz, M., Yong, M., Yoder, J. D., Tay, C., ... Negre, A. (2011). Probabilistic analysis of dynamic scenes and collision risks assessment to improve driving safety. *IEEE Intell Transportation Syst Mag*, 3. <https://doi.org/10.1109/MITS.2011.942779>
- Laurencelle, L. (2012). La représentativité d'un échantillon et son test par le Khi-deux Testing the representativeness of a sample. *Tutorials in Quantitative Methods for Psychology*, 8(3), 173–181. <https://doi.org/10.20982/tqmp.08.3.p173>
- Li, Q., Chen, L., Li, M., Shaw, S. L., & Nüchter, A. (2014). A sensor-fusion drivable-region and lane-detection system for autonomous vehicle navigation in challenging road scenarios. *IEEE Transactions on Vehicular Technology*, 63(2), 540–555. <https://doi.org/10.1109/TVT.2013.2281199>
- Liu, W., Weng, Z., Chong, Z., Shen, X., Pendleton, S., Qin, B., ... Ang, M. H. (2015). Autonomous vehicle planning system design under perception limitation in pedestrian environment. In *CIS-RAM* (pp. 159–166). <https://doi.org/10.1109/ICCIS.2015.7274566>
- Lopez, I., & Sarigul-Klijn, N. (2010). A review of uncertainty in flight vehicle structural damage monitoring, diagnosis and control: Challenges and opportunities. *Progress in Aerospace Sciences*, 46(7), 247–273. <https://doi.org/10.1016/j.paerosci.2010.03.003>

- Mahadik, P., Bhattacharyya, D., & Kim, H. jin. (2016). Techniques for automated test cases generation: A review. *International Journal of Software Engineering and Its Applications*, 10(12), 13–20. <https://doi.org/10.14257/ijseia.2016.10.12.02>
- Makowski, D., Albert, I., Bonvallot, N., Boudia, S., Bruyere, O., Glorennec, P., ... Saegerman, C. (2016). Prise en compte de l'incertitude en évaluation des risques : revue de la littérature et recommandations pour l'Anses. *Agence Nationale de Sécurité Sanitaire de l'Alimentation, de l'Environnement et Du Travail*, 1–90.
- Matthaei, R., & Maurer, M. (2015). Autonomous driving - A top-down-approach. *At-Automatisierungstechnik*, 63(3), 155–167. <https://doi.org/10.1515/auto-2014-1136>
- MAUBORGNE, P. (2016). *Vers une ingénierie de systèmes sûrs de fonctionnement basée sur les modèles en conception innovante*. Thèse de doctorat, Université de Lorraine.
- Mauborgne, P., Deniaud, S., Levrat, E., Bonjour, E., Micaëlli, J. P., & Loise, D. (2016). Operational and System Hazard Analysis in a Safe Systems Requirement Engineering Process - Application to automotive industry. *Safety Science*, 87(256–268). <https://doi.org/10.1016/j.ssci.2016.04.011>
- Menzel, T., Bagschik, G., Isensee, L., Schomburg, A., & Maurer, M. (2019). From Functional to Logical Scenarios : Detailing a Keyword-Based Scenario Description for Execution in a Simulation Environment. In *2019 IEEE Intelligent Vehicles Symposium (IV)* (pp. 2383–2390). <https://doi.org/10.1109/IVS.2019.8814099>
- Menzel, T., Bagschik, G., & Maurer, M. (2018). Scenarios for Development, Test and Validation of Automated Vehicles. In *2018 IEEE Intelligent Vehicles Symposium (IV)*. Chang Shu. <https://doi.org/10.1109/IVS.2018.8500406>
- Mullins, G. E., Stankiewicz, P. G., Hawthorne, R. C., & Gupta, S. K. (2017). Adaptive generation of challenging scenarios for testing and evaluation of autonomous vehicles. *Journal of Systems and Software*, 137, 197–215. <https://doi.org/10.1016/j.jss.2017.10.031>
- Nagel, H. H., Enkelmann, W., & Struck, G. (1995). FhG-Co-driver: From map-guided automatic driving by machine vision to a cooperative driver support. *Mathematical and Computer Modelling*, 22(4–7), 185–212. [https://doi.org/10.1016/0895-7177\(95\)00133-M](https://doi.org/10.1016/0895-7177(95)00133-M)
- NHTSA. (n.d.). NHTSA. Retrieved September 21, 2020, from <https://www.nhtsa.gov/technology-innovation/automated-vehicles-issue-road-self-driving>
- NHTSA - National Highway Traffic Safety Administration. (2017). *Automated driving systems - A Vision for Safety*.
- Petti, S., Bank, E. I., & Fraichard, T. (2015). Safe Motion Planning in Dynamic Environments. In *2005 IEEE/RSJ International Conference on Intelligent Robots and Systems* (pp. 2210–2215). <https://doi.org/10.1109/IROS.2005.1545549>
- Prasanna, M., Sivanandam, S. N., Venkatesan, R., & Sundarajan, R. (2005). A survey on automatic test case generation. *Academic Open Internet Journal*, 15, 1–7.
- Prialé Olivares, S., Rebenik, N., Eichberger, A., & Stadlober, E. (2015). Virtual Stochastic Testing of Advanced Driver Assistance Systems. In *Schulze T., Müller B., Meyer G. (eds) Advanced Microsystems for Automotive Applications 2015*. Springer, Cham. <https://doi.org/10.1007/978-3-319-20855-8>



- Raffaëlli, L., Vallée, F., Fayolle, G., De Souza, P., Rouah, X., Pfeiffer, M., ... Ahiad, S. (2016). Facing ADAS validation complexity with usage oriented testing. In *ERTS 2016* (pp. 1–13). Toulouse, France.
- Reschka, A., Bagschik, G., Ulbrich, S., Nolte, M., & Maurer, M. (2015). Ability and skill graphs for system modeling , online monitoring , and decision support for vehicle guidance systems. *2015 IEEE Intelligent Vehicles Symposium (IV)*, (Iv), 933–939. <https://doi.org/10.1109/IVS.2015.7225804>
- Rocklage, E. (2018). Teaching self-driving cars to dream: A deeply integrated, innovative approach for solving the autonomous vehicle validation problem. *IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC, 2018-March*, 1–7. <https://doi.org/10.1109/ITSC.2017.8317918>
- SAE international J3016. (2016). *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*.
- Sarmiento, E., Leite, J. C. S. P., Almentero, E., & Sotomayor Alzamora, G. (2016). Test Scenario Generation from Natural Language Requirements Descriptions based on Petri-Nets. *Electronic Notes in Theoretical Computer Science*, 329, 123–148. <https://doi.org/10.1016/j.entcs.2016.12.008>
- Smaoui, A. C., & Liu, F. (2018). A Model Based System Engineering Methodology for an Autonomous Driving System Design. In *25th ITS World Congress* (pp. 1–10). Copenhagen, Denmark.
- Staplin, L., Mastromatto, T., Lococo, K. H., Gish, K. W., W., K., & Brooks, J. O. (2018). *A Framework for Automated Driving System Testable Cases and Scenarios*. Washington.
- Sun, Y., Yang, H., & Meng, F. (2018). Research on an Intelligent Behavior Evaluation System for Unmanned Ground Vehicles. *Energies, MDPI, Open Access Journal*, 11(7), 1–23. <https://doi.org/10.3390/en11071764>
- SVA - Simulation pour la sécurité du Véhicule Autonome. (2015). Retrieved from <https://www.irt-systemx.fr/projets/sva/>
- U.S. DOT- Department of Transportation - NHTSA. (2016). *Federal Automated Vehicles Policy*.
- Ulbrich, S., Menzel, T., Reschka, A., Schuldt, F., & Maurer, M. (2015). Defining and Substantiating the Terms Scene, Situation, and Scenario for Automated Driving. In *IEEE Conference on Intelligent Transportation Systems*.
- Ulbrich, S., Reschka, A., Rieken, J., Ernst, S., Bagschik, G., Dierkes, F., ... Maurer, M. (2017). Towards a Functional System Architecture for Automated Vehicles. In *2016 IEEE Intelligent Vehicles Symposium (IV)* (pp. 1–21). <https://doi.org/10.1109/IVS.2016.7535402>
- VEDECOM. (2019). MOOVE. Retrieved from <http://www.vedecom.fr/presentation-du-projet-moove-a-lautonomous-vehicle-test-development-symposium-de-stuttgart/>
- Xie, G., Zhang, X., Gao, H., Qian, L., Wang, J., & Ozguner, U. (2017). Situational Assessments Based on Uncertainty-Risk Awareness in Complex Traffic Scenarios. *Sustainability*, 9(9), 1582. <https://doi.org/10.3390/su9091582>
- Xiong, Z. (2013). *Creating a Computing Environment in a Driving Vehicles*. PhD thesis, The

University of Leeds Institute for Transport Studies & School of Computing.

- Zhao, D., Lam, H., Peng, H., Bao, S., Leblanc, D. J., Pan, C. S., ... 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. <https://doi.org/10.1109/TITS.2016.2582208>
- Zhao, L., Arbaretier, E., Tlig, M., Zhao, L., Arbaretier, E., Tlig, M., ... Arbaretier, E. (2018). Validations par Virtualisation et Simulation : de nouveaux champs méthodologiques et techniques pour une ingénierie de conception sûre des systèmes autonomes. In *Congrès Lambda Mu 21 “ Maîtrise des risques et transformation numérique : opportunités et menaces ”* (pp. 1–9). Reims, France.
- Zhou, J., & Re, L. (2017). Reduced Complexity Safety Testing for ADAS & ADF. In *IFAC-PapersOnLine* (Vol. 50, pp. 5985–5990). Elsevier B.V. <https://doi.org/10.1016/j.ifacol.2017.08.1261>

---

## LISTE DES FIGURES ET DES TABLEAUX

---

### Liste de figures

Figure 1 : Un exemple de l'emplacement des technologies embarquées sur un VA.....	18
Figure 2 : Architecture simplifiée du VA (Source interne Stellantis).....	21
Figure 3 : Exemples de conditions difficiles de perception .....	22
Figure 4 : Illustration des "Area" à prendre en compte dans les activités du SOTIF.....	25
Figure 5 : Architecture théorique de simulation des ADS (Staplin et al., 2018).....	30
Figure 6 : Chaîne de simulation pour la vérification et l'identification de scénarios critiques pour les véhicules coopératifs et automatisés (Hallerbach et al., 2018). .....	31
Figure 7 : Procédure de validation par simulation (Jesenski et al., 2019).....	32
Figure 8 : Exemple de machine à états illustrant les différents modes de fonctionnement du VA .....	48
Figure 9 : Un exemple de scénario.....	53
Figure 10 : Cartographie de l'environnement immédiat autour du VA.....	56
Figure 11 : Modèle de connaissance des concepts de la génération de scénarios.....	58
Figure 12 : Structure du système de validation par simulation massive .....	65
Figure 13 : Technologies de capteurs sur le VA .....	74
Figure 14 : Classification des scénarios après simulation.....	80
Figure 15 : Positionnement des indicateurs dans le système de génération et validation du VA .....	85
Figure 16 : Structure de la méthodologie proposée pour la génération de scénarios.....	95
Figure 17 : Processus d'obtention des situation fonctionnelles .....	98
Figure 18 : Principe de génération et de validation par simulation des scénarios concrets ...	107
Figure 19 : Les trois niveaux d'impact d'un évènement.....	112
Figure 20 : Génération des scénarios concrets jusqu'à atteinte du critère d'arrêt.....	120
Figure 21 : Situation de car following sur deux voies.....	147

## Liste des tableaux

Tableau 1 : Récapitulatif des objectifs et des propositions de la thèse par chapitre .....	14
Tableau 2 : Niveaux d'automatisation d'un véhicule (SAE international J3016, 2016).....	16
Tableau 3 : Types d'infrastructures .....	44
Tableau 4 : Synthèse des définitions retenues pour le « cas d'utilisation » et le « cas de test ». .....	45
Tableau 5 : Synthèse des définitions retenues pour la « performance fonctionnelle » et la « limitation de performance fonctionnelle ». .....	47
Tableau 6 : Liste des manœuvres proposée par Gerdes et al. (Gerdes, 2006).....	49
Tableau 7 : Liste des manœuvres tactiques et opérationnelles des ADS proposée par Staplin et al. (Staplin et al., 2018). .....	50
Tableau 8 : Liste des manœuvres opérationnelles.....	51
Tableau 9 : Manœuvres opérationnelles déviantes d'autres usagers.....	52
Tableau 10 : Différentes métriques de "Safety" (Jesenski et al., 2019) .....	64
Tableau 11 : Classes de sévérité (ISO 26262-3, 2011) .....	71
Tableau 12 : Illustration de l'APR basée sur les limitations de performance dans le cas du TJC .....	71
Tableau 13 : Typologies d'évènements survenant à l'intérieur de l'ODD .....	72
Tableau 14 : Typologies d'évènements survenant en dehors de l'ODD .....	73
Tableau 15 : Proposition d'une échelle de mesure de sensibilité a priori du VA à une plage de valeurs .....	75
Tableau 16 : Illustration de la détermination du niveau de sensibilité a priori du VA à une plage de valeurs.....	76
Tableau 17 : Exemples de sévérité sur la base de différence de vitesse entre le VA et d'autres types d'usagers, pour un choc frontal.....	79
Tableau 18 : Exemple de paramètres et plages de valeurs pour l'obtention de situations logiques .....	102
Tableau 19 : Sous-objectifs visés lors de la génération des scénarios concrets.....	105
Tableau 20 : Proposition d'une échelle de contribution de la sensibilité d'une composante du VA dans l'obtention de la sensibilité d'une situation logique.....	109
Tableau 21 : Exemple de sensibilité d'une situation logique SL1 .....	109
Tableau 22 : Exemple de sensibilité d'une situation logique SL3.....	110
Tableau 23 : Description de l'ODD d'un TJC .....	128
Tableau 24 : Exemple de cas d'utilisation, de performances fonctionnelles et de limitation de performances du TJC .....	129
Tableau 25 : Modes opérationnels et leurs critères de validité dans le cas du TJC .....	130
Tableau 26 : Manœuvres opérationnelles et leurs critères de validité dans le cas du TJC ....	130
Tableau 27 : Liste des situations fonctionnelles dans le cas de la fonction TJC.....	131
Tableau 28 : Exemples de typologies d'évènements correspondant à l'ODD du TJC.....	132
Tableau 29 : Exemples de typologies d'évènements survenant en dehors de l'ODD du TJC	132
Tableau 30 : Identification des paramètres de description des scénarios et de leurs plages de variation.....	133
Tableau 31 : Exemples de situations logiques obtenues par combinaison des plages de variation .....	136
Tableau 32 : Analyse de sensibilité des plages de valeurs dans le cas du TJC .....	138

Tableau 33 : Sensibilité du VA à la situation logique Y1 .....	139
Tableau 34 : Sensibilité du VA à la situation logique Y14.....	140
Tableau 35 : Sensibilité du VA à la situation logique Y32.....	140
Tableau 36 : Sensibilité du VA à la situation logique Y35.....	141
Tableau 37 : Sensibilité des évènements impactant le niveau concret pour Y14 .....	142
Tableau 38 : Sensibilités des évènements impactant le niveau logique pour Y14.....	143
Tableau 39 : Sensibilités des évènements impactant le niveau fonctionnel pour Y14 .....	144
Tableau 40 : Liste E14 des évènements associés à la situation logique Y14.....	145
Tableau 41 : Distribution de sensibilités des évènements de la liste E14.....	145
Tableau 42 : Situations logiques Y1 et Y2 considérées pour l'expérimentation.....	147
Tableau 43 : Scénarios logiques considérés pour l'expérimentation.....	148

---

## ACRONYMES

---

<b>Sigles</b>	<b>Significations</b>
<b>ADAS</b>	Advanced Driver-Assistance System
<b>ADS</b>	Automated Driving System
<b>AMDEC</b>	Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
<b>APR</b>	Analyse Préliminaire de risques
<b>ASIL</b>	Automotive Safety Integrity Level
<b>HAZOP</b>	HAZard and OPerability study
<b>HB</b>	Hazardous Behaviour
<b>IS</b>	Importance Sampling
<b>MBSA</b>	Model-Based Safety Assessment
<b>MBSE</b>	Model-Based Systems Engineering
<b>MRM</b>	Minimum Risk Maneuver
<b>ODD</b>	Operational Design Domain
<b>PM</b>	Profil de Mission
<b>SC</b>	Scénario Concret
<b>SF</b>	Situation Fonctionnelle
<b>SL</b>	Situation Logique
<b>SOTIF</b>	Safety Of The Intended Functionality
<b>TIV</b>	Temps Inter Véhicule
<b>TJC</b>	Traffic Jam Chauffeur
<b>TTC</b>	Time To Collision
<b>VA</b>	Véhicule Autonome

---

ANNEXE 1 : LISTE DES 48 SITUATIONS LOGIQUES OBTENUES POUR LE CAS  
D'ETUDE ET LEURS SENSIBILITES

---

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
SL 1							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_1							
A10_1							
A11_1							
Sensibilité de SL1 /techno			0,2				
Sensibilité globale de SL1	<b>0,2</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
SL 2							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_2				1	1	1	
A10_1							
A11_1							
Sensibilité de SL2 /techno			0,2	0,2	0,2	1	
Sensibilité globale de SL2	<b>1,6</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
SL 3							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_1							
A10_1							
A11_1							
Sensibilité de SL3 /techno			0,2	0,2	0,2		
Sensibilité globale de SL3	<b>0,60</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
SL 4							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_2				1	1	1	
A10_1							
A11_1							
Sensibilité de SL4 /techno			0,2	0,2	0,2	1	
Sensibilité globale de SL4	<b>1,6</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
SL 5							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_1							
A10_1							
A11_2	1						
Sensibilité de SL5 /techno	0,2		0,2				
Sensibilité globale de SL5	<b>0,4</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
SL 6							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_2				1	1	1	
A10_1							
A11_2	1						
Sensibilité de SL6 /techno	0,2		0,2	0,2	0,2	1	
Sensibilité globale de SL6	<b>1,8</b>						



	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 7</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_1							
A10_1							
A11_2	1						
Sensibilité de SL7 /techno	0,2		0,2	0,2	0,2		
Sensibilité globale de SL7	<b>0,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 8</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_2				1	1	1	
A10_1							
A11_2	1						
Sensibilité de SL8/techno	0,2		0,2	0,2	0,2	1	
Sensibilité globale de SL8	<b>1,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 9</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_1							
A10_2				1	1		
A11_1							
Sensibilité de SL9 /techno			0,2	0,2	0,2		
Sensibilité globale de SL9	<b>0,6</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 10</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_2				1	1	1	
A10_2				1	1		
A11_1							
Sensibilité de SL10 /techno			0,2	0,2	0,2	1	
Sensibilité globale de SL10	<b>1,6</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 11</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_1							
A10_2				1	1		
A11_1							
Sensibilité de SL11 /techno			0,2	0,2	0,2		
Sensibilité globale de SL11	<b>0,6</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 12</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_2				1	1	1	
A10_2				1	1		
A11_1							
Sensibilité de SL12 /techno			0,2	0,2	0,2	1	
Sensibilité globale de SL12	<b>1,6</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 13</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_1							
A10_2				1	1		
A11_2	1						
	0,2		0,2	0,2	0,2		
	<b>0,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 14</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_2				1	1	1	
A10_2				1	1		
A11_2	1						
	0,2		0,2	0,2	0,2	1	
	<b>1,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 15</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_1							
A10_2				1	1		
A11_2	1						
	0,2		0,2	0,2	0,2		
	<b>0,80</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 16</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_2				1	1	1	
A10_2				1	1		
A11_2	1						
	0,2		0,2	0,2	0,2	1	
	<b>1,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 17</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_1							
A10_3							
A11_1							
			0,2				
	<b>0,2</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 18</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_2				1	1	1	
A10_3							
A11_1							
			0,2	0,2	0,2	1	
	<b>1,6</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 19</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_1							
A10_3							
A11_1							
			0,2	0,2	0,2		
	<b>0,6</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 20</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_2				1	1	1	
A10_3							
A11_1							
			0,2	0,2	0,2	1	
	<b>1,6</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 21</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_1							
A10_3							
A11_2	1						
	0,2		0,2				
	<b>0,4</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 22</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_2				1	1	1	
A10_3							
A11_2	1						
	0,2		0,2	0,2	0,2	1	
	<b>1,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 23</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_1							
A10_3							
A11_2	1						
	0,2		0,2	0,2	0,2		
	<b>0,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 24</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_2				1	1	1	
A10_3							
A11_2	1						
	0,2		0,2	0,2	0,2	1	
	<b>1,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 25</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_1							
A10_4		1		1	1		1
A11_1							
		0,2	0,2	0,2	0,2		1
	<b>1,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 26</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_2				1	1	1	
A10_4		1		1	1		1
A11_1							
		0,2	0,2	0,2	0,2	1	1
	<b>2,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
SL 27							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_1							
A10_4		1		1	1		1
A11_1							
		0,2	0,2	0,2	0,2		1
	<b>1,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
SL 28							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_2				1	1	1	
A10_4		1		1	1		1
A11_1							
		0,2	0,2	0,2	0,2	1	1
	<b>2,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
SL 29							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_1							
A10_4		1		1	1		1
A11_2	1						
	0,2	0,2	0,2	0,2	0,2		1
	<b>2</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 30</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_2				1	1	1	
A10_4		1		1	1		1
A11_2	1						
	0,2	0,2	0,2	0,2	0,2	1	1
	<b>3</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 31</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_1							
A10_4		1		1	1		1
A11_2	1						
	0,2	0,2	0,2	0,2	0,2		1
	<b>2</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 32</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_2				1	1	1	
A10_4		1		1	1		1
A11_2	1						
	0,2	0,2	0,2	0,2	0,2	1	1
	<b>3</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 33</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_1							
A10_5							
A11_1							
			0,2				
	<b>0,2</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 34</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_2				1	1	1	
A10_5							
A11_1							
			0,2	0,2	0,2	1	
	<b>1,6</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 35</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_1							
A10_5							
A11_1							
			0,2	0,2	0,2		
	<b>0,6</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 36</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_2				1	1	1	
A10_5							
A11_1							
			0,2	0,2	0,2	1	
	<b>1,6</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 37</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_1							
A10_5							
A11_2	1						
	0,2		0,2				
	<b>0,4</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 38</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_2				1	1	1	
A10_5							
A11_2	1						
	0,2		0,2	0,2	0,2	1	
	<b>1,8</b>						



	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 39</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_1							
A10_5							
A11_2	1						
	0,2		0,2	0,2	0,2		
	<b>0,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 40</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_2				1	1	1	
A10_5							
A11_2	1						
	0,2		0,2	0,2	0,2	1	
	<b>1,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 41</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_1							
A10_6		1		1	1		
A11_1							
		0,2	0,2	0,2	0,2		
	<b>0,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 42</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_2				1	1	1	
A10_6		1		1	1		
A11_1							
		0,2	0,2	0,2	0,2	1	
	<b>1,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 43</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_1							
A10_6		1		1	1		
A11_1							
		0,2	0,2	0,2	0,2	1	
	<b>1,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 44</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_2				1	1	1	
A10_6		1		1	1		
A11_1							
		0,2	0,2	0,2	0,2	1	
	<b>1,8</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 45</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_1							
A10_6		1		1	1		
A11_2	1						
	0,2	0,2	0,2	0,2	0,2		
	<b>1</b>						

	Techno 1	Techno 2	Techno 3	Techno 4	Techno 5	Décision	Actionnement
<b>SL 46</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_1							
A8_2				1	1	1	
A10_6		1		1	1		
A11_2	1						
	0,2	0,2	0,2	0,2	0,2	1	
	<b>2</b>						

	Techno		Techno	Techno	Techno	Décision	Actionnement
	1		2	3	4	5	
<b>SL 47</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_1							
A10_6		1		1	1		
A11_2	1						
	0,2	0,2	0,2	0,2	0,2		
	<b>1</b>						

	Techno	Techno	Techno	Techno	Techno	Décision	Actionnement
	1	2	3	4	5		
<b>SL 48</b>							
A9_1							
A1_1			1				
A2_1							
A3_1							
A4_1							
A5_1							
A6_1							
A7_2				1	1		
A8_2				1	1	1	
A10_6		1		1	1		
A11_2	1						
	0,2	0,2	0,2	0,2	0,2	1	
	<b>2</b>						

## ANNEXE 2 : RESULTATS DE SIMULATION POUR LE SCENARIO LOGIQUE 1

### Result Summary









#### Overall Results

<b>Number of Tests:</b>	<b>100</b>	<b>100.0 %</b>	
Tests passed:	67	67.0 %	✓
Tests skipped:	0	0.0 %	⏸
Tests with warning:	0	0.0 %	⚠
Tests failed:	0	0.0 %	✗
Tests with error:	33	33.0 %	⚡
Tests not executed:	0	0.0 %	⊘

#### Detailed Results

ID	Test	Result
1	SL1/SL1_TestRun1	✓
2	SL1/SL1_TestRun2	✓
3	SL1/SL1_TestRun3	⚡
4	SL1/SL1_TestRun4	✓
5	SL1/SL1_TestRun5	✓
6	SL1/SL1_TestRun6	⚡
7	SL1/SL1_TestRun7	✓
8	SL1/SL1_TestRun8	✓
9	SL1/SL1_TestRun9	✓
10	SL1/SL1_TestRun10	✓
11	SL1/SL1_TestRun11	✓
12	SL1/SL1_TestRun12	⚡
13	SL1/SL1_TestRun13	⚡
14	SL1/SL1_TestRun14	⚡
15	SL1/SL1_TestRun15	✓
16	SL1/SL1_TestRun16	✓
17	SL1/SL1_TestRun17	⚡
18	SL1/SL1_TestRun18	✓
19	SL1/SL1_TestRun19	✓
20	SL1/SL1_TestRun20	✓
21	SL1/SL1_TestRun21	✓
22	SL1/SL1_TestRun22	✓
23	SL1/SL1_TestRun23	⚡
24	SL1/SL1_TestRun24	⚡
25	SL1/SL1_TestRun25	✓
26	SL1/SL1_TestRun26	✓
27	SL1/SL1_TestRun27	✓
28	SL1/SL1_TestRun28	✓
29	SL1/SL1_TestRun29	✓
30	SL1/SL1_TestRun30	⚡
31	SL1/SL1_TestRun31	✓
32	SL1/SL1_TestRun32	✓
33	SL1/SL1_TestRun33	✓
34	SL1/SL1_TestRun34	✓
35	SL1/SL1_TestRun35	✓
36	SL1/SL1_TestRun36	⚡
37	SL1/SL1_TestRun37	✓
38	SL1/SL1_TestRun38	✓

ID	Test	Result
39	SL1/SL1_TestRun39	✓
40	SL1/SL1_TestRun40	✓
41	SL1/SL1_TestRun41	✗
42	SL1/SL1_TestRun42	✓
43	SL1/SL1_TestRun43	✗
44	SL1/SL1_TestRun44	✗
45	SL1/SL1_TestRun45	✗
46	SL1/SL1_TestRun46	✓
47	SL1/SL1_TestRun47	✓
48	SL1/SL1_TestRun48	✗
49	SL1/SL1_TestRun49	✗
50	SL1/SL1_TestRun50	✗
51	SL1/SL1_TestRun51	✓
52	SL1/SL1_TestRun52	✓
53	SL1/SL1_TestRun53	✓
54	SL1/SL1_TestRun54	✓
55	SL1/SL1_TestRun55	✓
56	SL1/SL1_TestRun56	✓
57	SL1/SL1_TestRun57	✓
58	SL1/SL1_TestRun58	✗
59	SL1/SL1_TestRun59	✓
60	SL1/SL1_TestRun60	✗
61	SL1/SL1_TestRun61	✓
62	SL1/SL1_TestRun62	✓
63	SL1/SL1_TestRun63	✗
64	SL1/SL1_TestRun64	✗
65	SL1/SL1_TestRun65	✓
66	SL1/SL1_TestRun66	✓
67	SL1/SL1_TestRun67	✓
68	SL1/SL1_TestRun68	✗
69	SL1/SL1_TestRun69	✗
70	SL1/SL1_TestRun70	✓
71	SL1/SL1_TestRun71	✗
72	SL1/SL1_TestRun72	✓
73	SL1/SL1_TestRun73	✓
74	SL1/SL1_TestRun74	✗
75	SL1/SL1_TestRun75	✗
76	SL1/SL1_TestRun76	✓
77	SL1/SL1_TestRun77	✓
78	SL1/SL1_TestRun78	✓
79	SL1/SL1_TestRun79	✗
80	SL1/SL1_TestRun80	✗
81	SL1/SL1_TestRun81	✗
82	SL1/SL1_TestRun82	✓
83	SL1/SL1_TestRun83	✓
84	SL1/SL1_TestRun84	✗
85	SL1/SL1_TestRun85	✓
86	SL1/SL1_TestRun86	✓
87	SL1/SL1_TestRun87	✓
88	SL1/SL1_TestRun88	✓
89	SL1/SL1_TestRun89	✓
90	SL1/SL1_TestRun90	✓
91	SL1/SL1_TestRun91	✓
92	SL1/SL1_TestRun92	✗

ID	Test	Result
93	SL1/SL1_TestRun93	
94	SL1/SL1_TestRun94	
95	SL1/SL1_TestRun95	
96	SL1/SL1_TestRun96	
97	SL1/SL1_TestRun97	
98	SL1/SL1_TestRun98	
99	SL1/SL1_TestRun99	
100	SL1/SL1_TestRun100	

## ANNEXE 3 : RESULTATS DE SIMULATION POUR LE SCENARIO LOGIQUE 2

### Result Summary

#### Overall Results

Number of Tests:	100	100.0 %	
Tests passed:	99	99.0 %	✓
Tests skipped:	0	0.0 %	ⓘ
Tests with warning:	0	0.0 %	⚠
Tests failed:	0	0.0 %	✗
Tests with error:	1	1.0 %	⚠
Tests not executed:	0	0.0 %	⊘

#### Detailed Results

ID	Test	Result
1	SL2/SL2_TestRun1	✓
2	SL2/SL2_TestRun2	✓
3	SL2/SL2_TestRun3	✓
4	SL2/SL2_TestRun4	✓
5	SL2/SL2_TestRun5	✓
6	SL2/SL2_TestRun6	✓
7	SL2/SL2_TestRun7	✓
8	SL2/SL2_TestRun8	✓
9	SL2/SL2_TestRun9	✓
10	SL2/SL2_TestRun10	✓
11	SL2/SL2_TestRun11	✓
12	SL2/SL2_TestRun12	✓
13	SL2/SL2_TestRun13	✓
14	SL2/SL2_TestRun14	✓
15	SL2/SL2_TestRun15	✓
16	SL2/SL2_TestRun16	✓
17	SL2/SL2_TestRun17	✓
18	SL2/SL2_TestRun18	✓
19	SL2/SL2_TestRun19	✓
20	SL2/SL2_TestRun20	✓
21	SL2/SL2_TestRun21	✓
22	SL2/SL2_TestRun22	✓
23	SL2/SL2_TestRun23	✓
24	SL2/SL2_TestRun24	✓
25	SL2/SL2_TestRun25	✓
26	SL2/SL2_TestRun26	✓
27	SL2/SL2_TestRun27	✓
28	SL2/SL2_TestRun28	✓
29	SL2/SL2_TestRun29	✓
30	SL2/SL2_TestRun30	✓
31	SL2/SL2_TestRun31	✓
32	SL2/SL2_TestRun32	✓
33	SL2/SL2_TestRun33	✓
34	SL2/SL2_TestRun34	✓
35	SL2/SL2_TestRun35	✓
36	SL2/SL2_TestRun36	✓
37	SL2/SL2_TestRun37	✓
38	SL2/SL2_TestRun38	✓

ID	Test	Result
39	SL2/SL2_TestRun39	✔
40	SL2/SL2_TestRun40	✔
41	SL2/SL2_TestRun41	✔
42	SL2/SL2_TestRun42	✔
43	SL2/SL2_TestRun43	✔
44	SL2/SL2_TestRun44	✔
45	SL2/SL2_TestRun45	✔
46	SL2/SL2_TestRun46	✔
47	SL2/SL2_TestRun47	⚠
48	SL2/SL2_TestRun48	✔
49	SL2/SL2_TestRun49	✔
50	SL2/SL2_TestRun50	✔
51	SL2/SL2_TestRun51	✔
52	SL2/SL2_TestRun52	✔
53	SL2/SL2_TestRun53	✔
54	SL2/SL2_TestRun54	✔
55	SL2/SL2_TestRun55	✔
56	SL2/SL2_TestRun56	✔
57	SL2/SL2_TestRun57	✔
58	SL2/SL2_TestRun58	✔
59	SL2/SL2_TestRun59	✔
60	SL2/SL2_TestRun60	✔
61	SL2/SL2_TestRun61	✔
62	SL2/SL2_TestRun62	✔
63	SL2/SL2_TestRun63	✔
64	SL2/SL2_TestRun64	✔
65	SL2/SL2_TestRun65	✔
66	SL2/SL2_TestRun66	✔
67	SL2/SL2_TestRun67	✔
68	SL2/SL2_TestRun68	✔
69	SL2/SL2_TestRun69	✔
70	SL2/SL2_TestRun70	✔
71	SL2/SL2_TestRun71	✔
72	SL2/SL2_TestRun72	✔
73	SL2/SL2_TestRun73	✔
74	SL2/SL2_TestRun74	✔
75	SL2/SL2_TestRun75	✔
76	SL2/SL2_TestRun76	✔
77	SL2/SL2_TestRun77	✔
78	SL2/SL2_TestRun78	✔
79	SL2/SL2_TestRun79	✔
80	SL2/SL2_TestRun80	✔
81	SL2/SL2_TestRun81	✔
82	SL2/SL2_TestRun82	✔
83	SL2/SL2_TestRun83	✔
84	SL2/SL2_TestRun84	✔
85	SL2/SL2_TestRun85	✔
86	SL2/SL2_TestRun86	✔
87	SL2/SL2_TestRun87	✔
88	SL2/SL2_TestRun88	✔
89	SL2/SL2_TestRun89	✔
90	SL2/SL2_TestRun90	✔
91	SL2/SL2_TestRun91	✔
92	SL2/SL2_TestRun92	✔



ID	Test	Result
93	SL2/SL2_TestRun93	✓
94	SL2/SL2_TestRun94	✓
95	SL2/SL2_TestRun95	✓
96	SL2/SL2_TestRun96	✓
97	SL2/SL2_TestRun97	✓
98	SL2/SL2_TestRun98	✓
99	SL2/SL2_TestRun99	✓
100	SL2/SL2_TestRun100	✓

---

## RESUME

---

Cette thèse CIFRE, réalisé au sein de Stellantis, fournit une stratégie de génération de scénarios, modélisée par niveaux d'abstraction et orientée par la sensibilité du VA, pour une validation par simulation. Ce travail s'inscrit dans le périmètre du standard ISO PAS 21448 /SOTIF (Safety Of The Intended Functionality).

Pour ce faire, la démarche suivie s'articule autour de cinq contributions :

- Une analyse de l'architecture fonctionnelle du VA et la mise en évidence des challenges liés à la validation de sa sécurité : aspects normatifs, chaînes de simulation, la présence d'incertitude dans l'environnement opérationnel du VA.
- La proposition d'un cadre conceptuel (modèle de connaissance) sur lequel s'appuiera la méthodologie de génération des scénarios qui sera proposée par la suite.
- Une synthèse sur les indicateurs manipulés dans la littérature, ainsi que ceux, que nous retiendrons dans notre stratégie de génération finale dont notamment l'indicateur de sensibilité. Elle donne également une structure du système de génération des scénarios et de validation par simulation de la sécurité du VA, ainsi que la manière dont les indicateurs seront exploités dans cette structure.
- La proposition d'une heuristique de génération des scénarios et l'estimation de l'indicateur de risque associé au VA. Cette quatrième contribution, s'appuie sur les éléments développés dans les contributions précédentes : le modèle conceptuel proposé (contribution 2), la structure du système de génération et de validation ainsi que les indicateurs associés (contribution 3).
- Enfin, la dernière contribution est une implémentation des propositions précédentes via un cas d'étude.

**Mots clés :** Véhicule Autonome (VA), SOTIF (Safety Of The Intended Functionality), Limitation de performances fonctionnelles, Insuffisances fonctionnelles, Scénarios critiques, Métrique de sensibilité, Stratégie de génération de scénarios, Validation par simulation

---

## ABSTRACT

---

This CIFRE thesis, carried out within Stellantis, provides a scenario generation strategy, modelled by levels of abstraction and oriented by the sensitivity of the AV, for a simulation-based validation process. This work is within the scope of the ISO PAS 21448 /SOTIF (Safety Of The Intended Functionality) standard.

To do this, the approach followed is based on five contributions:

- An analysis of the functional architecture of the AV and the highlighting of the challenges related to its safety validation: normative aspects, simulation chains, the presence of uncertainty in the operational environment of the AV.
- The proposal of a conceptual framework (knowledge model) on which the scenario generation methodology to be proposed later will be based.
- A summary of the indicators used in the literature, as well as those that we will use in our final generation strategy, including the sensitivity indicator. It also gives a structure of the system of scenario generation and simulation based validation of the safety of the AV, as well as the way in which the indicators will be exploited in this structure.
- The proposal of a scenario generation heuristic and the estimation of the risk indicator associated with the AV. This fourth contribution is based on the elements developed in the previous contributions: the proposed conceptual model (contribution 2), the structure of the generation and validation system and the associated indicators (contribution 3).
- Finally, the last contribution is an implementation of the previous proposals via a case study.

**Keywords:** Autonomous Vehicle (AV), Safety Of The Intended Functionality (SOTIF), Functional performance limitation, Functional insufficiencies, Critical scenarios, Sensitivity metric, Scenarios generation strategy, Simulation-based Validation process