Nouvelle méthodologie d'analyse de risque pour des Systèmes de Transport Routiers Automatisés (STRA)

Brini Manel, Martinez Alexandre, Arnoux Emmanuel

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Nouvelle méthodologie d'analyse de risque pour des Systèmes de Transport Routiers Automatisés (STRA)

New Safety methodologies for Automated Road Transport Systems (ARTS)

BRINI Manel
IRT SystemX
Pilote du groupe de travail Safety du projet SAM
manel.brini@irt-systemx.fr

MARTINEZ Alexandre
Renault
Expert Safety AD-ADAS
alexandre.martinez@renault.com

Arnoux Emmanuel
Renault
Leader du groupe de travail Safety & Validation de la PFA
emmanuel.arnoux@renault.com

Résumé — Le projet français SAM fédère des partenaires industriels de l'automobile et de la mobilité, des instituts de recherche et des autorités et services techniques français afin d'apporter des réponses aux questions soulevées par l'établissement de lois et règlements concernant la sécurité des Véhicules Particuliers Automatisés (VPA) et des Systèmes de Transport Routier Automatisés (STRA).
Dans le cadre de l'autorisation de mise en service des systèmes de transport routier automatisés, le groupe de travail « safety et validation » du projet SAM a défini en 2021 une approche sécuritaire fondée sur l'utilisation de trois méthodes d'analyse de risques complémentaires.
Ce document présente une nouvelle méthode d'analyse de risque basées sur des approches descendantes et ascendantes. L'objectif est de viser l'exhaustivité des études dans l'identification et l'évaluation des risques associés au STRA.
Pour répondre à cet objectif, ce document propose la combinaison de 3 types d'analyses de risques offrant un spectre plus large d'étude : une analyse de risques de type déductive, e.g. analyse préliminaire des dangers (APD), une analyse de risques de type inductive, e.g. analyse préliminaire des risques (APR), et une Analyse de Sécurité du Parcours (ASP).
Mots-clefs —Safety, STRA, APD, APR, ASP, GAME

Abstract — SAM research project is federating automotive and mobility partners, transport operators, research institutes and French authorities to bring answers to the questions risen by the establishment of French LOM law and international regulations concerning automated vehicles and Automated Road Transportation Systems (ARTS). The safety working group of SAM project developed in 2021 a safety approach based on the implementation of three complementary safety analyses compliant with GAME Safety Principle required by LOM law. The safety analyses will be described in this document in order to guarantee the utmost level of risk identification and treatment. They include a top-down approach (e.g. a Preliminary Hazard Analysis), a bottom-up approach (e.g. a Functional Hazard Analysis), and a Site Safety Analysis. In addition to these safety analyses, the document mainly describes the methodology for allocating quantitative safety targets as part of an explicit risk estimation.
Keywords: Safety, ARTS, FHA, PHA, SSA, GAME

I. INTRODUCTION

L'objectif de cette démarche est de viser par des études de sécurité complémentaires l'exhaustivité dans l'identification et l'évaluation des risques associés à un Système de Transport Routier Automatisé (STRA). L'Analyse Préliminaire des Dangers (APD) et l'Analyse Préliminaire des Risques (APR) peuvent avoir un caractère générique pour un système STRA et un périmètre plus large qu'une application donnée, et donc doivent être instanciées sur un parcours (ou une zone) donné.

À partir d'une liste standard des accidents (cf. table I) issue d'un consensus entre les industriels et les autorités françaises, l'APD identifie d'abord les situations dangereuses pouvant amener à ces accidents (contextualisées sous forme de scénarios, et eux-mêmes capitalisés dans une bibliothèque à titre de preuve), puis permet de choisir un type d'approche GAMÉ (Globalement Au Moins Équivalent) couvrant un ou un groupe d'accidents.

Pour rappel, selon le « guide d'application GAMÉ » [1] récemment publié par les autorités françaises pour l'autorisation de mise en service de STRA, dans le cas d'une démonstration GAMÉ, l'acceptabilité du risque du système étudié est évaluée en utilisant un ou plusieurs des principes

d'acceptation du risque suivants : l'application de codes de pratique, une comparaison avec des systèmes rendant des services comparables, et/ou une estimation explicite du risque. Lorsqu'aucun référentiel n'existe, par exemple pour la collision, l'APD permet d'identifier les scénarios d'accident en mettant en évidence les situations dangereuses. L'APD introduit une première analyse des contextes et des conditions conduisant à une situation dangereuse. Cette situation dangereuse pouvant entraîner ensuite un accident : par exemple, une survitesse peut être la cause d'un accident (e.g. collision) dans des conditions données.

TABLE I. LISTE STANDARD DES ACCIDENT DE NIVEAU STRA

Typologie	Accident potentiel
1. Collision	Collision avec usager de la voirie (cycliste, piéton, etc.)
	Collision (latérale/frontale) contre un obstacle massif (containers, animaux, etc.)
	Collision contre un autre véhicule
	Collision par un autre véhicule
2. Chute de personnes	Chute de personne à l'intérieur du véhicule
	Chute de personne à l'extérieur du véhicule pendant le mouvement du véhicule
	Chute de personne du quai pendant le transfert
3. Renverse-ment	Renversement véhicule
4. Electrisation /Électrocu-tion	Electrisation/Electrocution
5. Feu/ Explosion	Feu véhicule ou explosion
6. Autres accidents de passagers	Impossibilité de sortie du véhicule
	Passagers coincés/pincés par les ouvrants (fenêtres, portes, etc.)
	Entrainement de personne par le véhicule (en particulier entrainement de personnes lors de la sortie de la station ou suite à un coincement de vêtement)
	Blessure de personne par un véhicule (à l'arrêt ou en roulage : marche rétractable, proéminence du véhicule)
	Passagers heurtés par un pièce/objet projeté par le véhicule (perte d'une pièce/objet du véhicule, ..)
	Passagers heurtés par un objet transporté (ex. bagages, colis, etc.)
	Passagers en contact avec des objets agressifs du véhicule (coupants, etc.)
	Passagers en contact avec une source de chaleur importante
	Passagers en contact avec un liquide agressif
	Passagers/Opérateurs vont causer des accidents par ignorance d'un dysfonctionnement des fonctions liées à la sécurité (information IHM incorrecte pouvant conduire à une action non sûre)
	Passenger inhales exhaust/hazardous gas Les passagers inhalent les gaz d'échappement/gaz dangereux
	Les passagers ne peuvent pas alerter en cas de situation critique (pas de Ecall, pas d'accès avec le téléopérateur, perte de la gestion des passagers, etc.)
7. Perte des objets	Objet lourd tombe du véhicule et heurte le véhicule suivant
	Objet lourd tombe du véhicule et heurte un usager vulnérable
8. Autres accidents	Mauvaise interaction avec des véhicules d'intérêt général prioritaires (collision, blocages équipes de secours ou véhicules prioritaires, etc.)
	Possibilité d'évacuation insuffisante des passagers après une collision (ex. impossibilité de sortir, impossibilité de pénétrer dans le véhicule, perte, etc.)
	Arrêt du véhicule dans une zone à risque (passage à niveau, tunnel, viaduc,..)

L'APR identifie toutes les causes possibles d'une situation dangereuse, et permet par la prise en compte de l'architecture du système d'être plus spécifique et plus complète sur l'identification des risques qu'une APD. Une situation dangereuse reste généralement le résultat d'un événement déclencheur (par exemple, erreur de limitation de vitesse, pannes électriques/électroniques, insuffisances fonctionnelles, aléas de parcours, pannes mécaniques, etc.) et d'une incapacité du système à réaliser une mesure de réduction des risques (e.g. architecture de protection électrique/ électronique). Afin de compléter l'APD, l'APR s'appuie sur l'architecture fonctionnelle du système pour identifier les pannes et les insuffisances fonctionnelles pouvant conduire à des situations dangereuses.

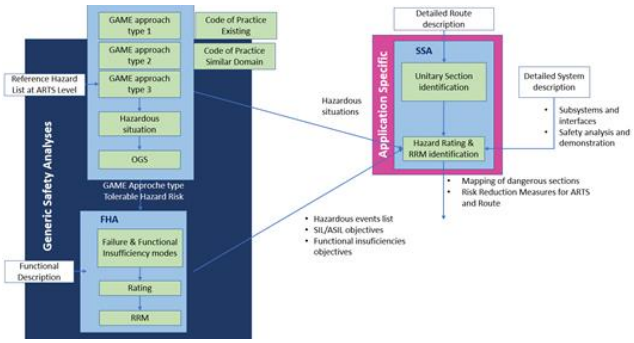

Figure 1: Allocation des objectifs quantitatifs des trois analyses (APD, APR, et ASP).

L'Analyse de Sécurité de Parcours (ASP) porte sur un parcours donné et vise à assurer la compatibilité du parcours avec le domaine d'emploi (dont l'ODD) d'un système technique générique, et à assurer la complétude et le caractère adapté des APD et APR génériques au moment de leur instanciation à un parcours donné.

L'analyse de sécurité de parcours se concentre sur un itinéraire, ou une zone, prédéfini et aboutit à ne couvrir qu'un sous-ensemble des situations possibles décrites dans les études APD et APR, comme décrit dans la figure 1. L'analyse de sécurité de parcours établit un ensemble de recommandations, d'exigences techniques, fonctionnelles et opérationnelles, sur sous-systèmes et composants (e.g. véhicules, infrastructures, connectivité, signalisation, …) du STRA. Toutes ces exigences contribuent à assurer la sécurité globale du système STRA.

Dans les chapitres suivants, les trois méthodes précédemment introduites seront présentées et analysées plus en détails.

II. L'ANALYSE PRELIMINAIRE DES DANGERS, COMME APPROCHE DESCENDANTE

La loi LOM [6] impose l'utilisation du principe de sécurité GAMÉ (Globalement Au moins Équivalent). Fin 2021, un guide d'application de ce principe [1] a été publié par le service technique français en charge des STRA. L'Analyse Préliminaire des Dangers (APD) permet, à partir de la liste standard des accidents, de définir le type d'approche GAMÉ à envisager. Lorsqu'il n'existe pas de cadre de référence existant, l'APD identifie les causes possibles par des analyses de risques détaillées et explicites.

A. *Description de la méthode*

Définition : Analyse déductive permettant, pour un accident potentiel donné (ex. : collision, incendie, de la table I), d'identifier les causes possibles sous forme de situations dangereuses contextualisées (ex. : survitesse, non-respect des feux de circulation, déviation latérale, etc.) et d'évaluer les risques associés.

L'APD permet de décrire des scénarios d'accidents en mettant en évidence pour chacun d'entre eux des situations dangereuses. Elle introduit également une première analyse et évaluation des contextes et des conditions faisant basculer une situation dangereuse vers un accident : par exemple, une survitesse peut être à l'origine d'un accident, dans des conditions données comme un virage et une route verglacée. Lorsqu'aucun code de bonnes pratiques n'existe pour le STRA ou pour d'autres systèmes comparables fournissant un service équivalent, l'analyse permet d'attribuer un Objectif Global de Sécurité (OGS) sur les causes possibles en tenant compte de la plausibilité des accidents. La valeur d'OGS est le seuil d'acceptabilité d'un risque établi sur la base d'un retour d'expérience significatif d'un service de transport comparable (par exemple, même domaine de conception fonctionnelle – ODD). Le THR (taux de risque tolérable) [3] peut être un exemple d'OGS. C'est la première étape pour aborder la liste des situations dangereuses. Ces situations dangereuses sont des éléments d'entrée pour l'analyse de sécurité de parcours et l'analyse préliminaire de risques.

B. *Etapes à suivre de la méthode*

La méthode de conduite de l'analyse préliminaire des dangers proposée suit les étapes suivantes :

1. Utilisation de la liste standard des accidents de niveau système STRA établie et reconnue par les experts en sécurité, des autorités françaises, d'instituts de recherche, et industriels [8],
2. Identification des situations dangereuses pouvant être à l'origine de l'accident,
3. Description des conditions conduisant à un accident en présence d'une situation dangereuse fondé sur des éléments de description du système (e.g. type d'infrastructure routière, dynamique du véhicule, conditions environnementales, objets et notamment autres usagers de la route, etc.).
4. Cotation du risque pour chaque couple (accident potentiel, situation dangereuse) en associant [3], [4], [5] : Une classe de sévérité (S) de l'accident, et une classe de fréquence d'occurrence de la situation dangereuse, qui prend en compte l'expression d'un Facteur de Réduction du Risque (FRR=E*C) comprenant une classe d'exposition (E) au contexte ayant conduit à l'accident, et une classe de contrôlabilité (C) pour tenir compte de la capacité à éviter l'accident des acteurs de la route impliqués dans la situation dangereuse étudiée (ex. : piéton, conducteurs d'autres véhicules, etc.).

Pour chaque situation dangereuse, i, TFR(i) est égal à OGS/FRR(i). Pour un accident donné, la somme de tous les produits, c'est-à-dire Σ TFR(i) x FRR(i), doit rester inférieure à la valeur l'OGS de cet accident.

Il est observé dans les études qu'une même situation dangereuse peut conduire à des accidents différents ou qu'un même accident peut résulter de situations dangereuses différentes. Les dangers peuvent résulter de défaillances ou d'insuffisances fonctionnelles (e.g. les conditions environnementales), de scénarios d'utilisation et de mauvaise utilisation, de tiers spécifiques, qui sont particulièrement étudiés en détail lors de l'étude APR.

C. *Conclusion*

Cette analyse doit se faire à haut niveau, et reste indépendante des solutions techniques. Les exigences de sécurité doivent guider la spécification du système tel qu'indiqué dans le modèle proposé dans la table II.

TABLE II. CANEVAS D'ANALYSE PRELIMINAIRE DE DANGER

Accident de niveau STRA	***Identification de la situation dangereuse***	***Cause racine possible***	***Evaluation des risqué***	***Exigence de sécurité au niveau STRA***

L'analyse reste dépendante des conditions d'utilisation du système (dont dépendent les FRR). Comme tout type d'analyse des risques, les critères d'évaluation des risques doivent être fortement validés afin d'assurer la compatibilité avec les conditions d'utilisation pendant la phase d'exploitation du cycle de vie du système.

III. L'ANALYSE PRELIMINAIRE DE RISQUES, COMME APPROCHE ASCENDANTE

L'APR permet d'identifier l'ensemble des causes, et notamment les défaillances fonctionnelles [5] et les insuffisances fonctionnelles [7], pouvant conduire à des situations dangereuses et d'évaluer les risques associés. Les causes des situations dangereuses sont appelées les événements redoutés [1] liés aux différents composants du système. Pour chaque événement redouté, l'analyse vise à clarifier l'impact sur la sécurité à travers l'évaluation des risques et assure une première définition des mesures techniques de réduction des risques afin d'atteindre un niveau acceptable de risques résiduels (ex. compatible avec un OGS).

A. *Description de la méthode*

L'analyse permet de définir des Mesures de Réduction des Risques (MRR) et/ou des Taux de défaillance ou d'insuffisance fonctionnelle acceptable (TFFR, TFIR) sur les macro-fonctions du système (cf. table III). C'est la première étape qui traite de la liste des événements redoutés. Ces événements redoutés peuvent constituer de nouveaux éléments d'entrée pour l'Analyse de Sécurité de Parcours, une fois l'option d'intégration des aléas de dysfonctionnement dans l'analyse de sécurité de parcours choisie, et pour les analyses plus détaillées réalisées par les constructeurs (AMDEC).

Les événements de type "situation de conduite en interaction avec un tiers" sont traités dans l'APR de manière générique (en réponse à un domaine d'utilisation générique donné).

TABLE III. DECOUPAGE FONCTIONNEL DU SYSTEME STRA

Fonctions (rang 1)	Fonctions (rang 2)
1-Assurer la définition, le suivi et le contrôle de la trajectoire du véhicule	1.1-Percevoir l'environnement (sense)
	1.2-Localiser le véhicule sur le parcours / zone
	1.3-Prendre la décision concernant la navigation/guidage (plan)
	1.4-Assurer le contrôle dynamique (act)
2- Se signaler vis-à-vis des autres usagers de la route (signalisation sonore, visuel, etc.)_	
3-Gérer les accès aux véhicules automatisés	3.1-Gérer le transfert des personnes aux points autorisés
	3.2-Maintenir le véhicule automatisé fermé hors transfert personnes/évacuation
	3.3-Permettre l'évacuation et l'accès des secours en cas d'urgence.
4-Assurer le confort des passagers et du personnel _	
5- Permettre aux usagers d'interagir avec des composants du système	5.1-Permettre la communication entre le personnel d'exploitation et les passagers (COM)
	5.2-Permettre la transmission de l'information voyageurs
	5.3-Permettre aux usagers l'accès à des services
6-Diagnostic de l'état des composants techniques du système	_
7-Gérer les composants d'infrastructure dynamiques (faisant partie du système	_
8-Assurer la communication et connectivité entre des composants techniques du système ou composants externes du système	Entre des composants techniques du système
	Entre des composants techniques du système et des composants externes du système
9-Assurer la supervision du parcours et des composants techniques du système Gestion de la flotte et des missions, du service dans son ensemble, surveillance de l'environnement des composants du système sur parcours/zone, changer/planifier la mission, enclencher un mode dégradé (refuge)…	9.1-Intervenir à distance sur des composants techniques du système
	9.2-Permettre la communication entre les personnels d'exploitation
	9.3-Permettre la communication entre le personnel d'exploitation et des intervenants extérieurs
	9.4-Enregistrer les données
	9.5-Afficher des états des composants du système

B. Etapes à suivre de la méthode

Les huit étapes de la méthode proposée sont :

1. Expression d'hypothèses sur une première architecture fonctionnelle du système.
2. Description fonction par fonction des modes de défaillances ou d'insuffisances fonctionnelles. Utilisation éventuelle de modes de défaillance génériques tels que "perte de", "non-stop de", "erroné", "intempestif", etc. Ce sont des dysfonctionnements, une attention particulière doit être portée à la qualité de l'expression (ex. détection d'obstacles, une fonction erronée doit être clairement et explicitement décrite).
3. Description des conséquences possibles de chaque dysfonctionnement en exprimant clairement un lien possible avec une situation dangereuse.
4. Lien avec l'ASP pour affiner le couple [situation dangereuse - contexte] et les conditions nécessaires à l'accident. Identifier le contexte de la situation, à partir de la description du type d'infrastructure, de la dynamique du véhicule, des personnes/objets exposés.
5. Évaluation de la sévérité, de l'exposition, de la contrôlabilité pour exprimer le niveau de risque résultant avant d'appliquer des mesures de prévention ou de protection).
6. Définition des mesures de réduction des risques (MRR) et rappel des niveaux d'intégrité sur les fonctions correspondantes, les protections ajoutées ou fonction déjà prévues.
7. Risque réévalué en supposant que les MRR sont appliquées correctement.
8. Expression d'exigences exportées si l'équipement concerné par la défaillance dangereuse ne permet pas de respecter pleinement l'exigence (mesures complémentaires exportées sur d'autres équipements ou sur d'autres éléments de l'environnement de l'équipement défaillant).

Note : Lorsqu'un véhicule ne garantit pas à lui-même la sécurité, des exigences supplémentaires, exportées sont à traiter ultérieurement sur d'autres systèmes ou sur un système de système (ex. connectivité, supervision, infrastructure, procédures, etc.).

C. Conclusion

L'APR couvre un système complet, ici le système technique de transport routier automatisé. Elle peut être établie à condition qu'il reste possible d'assurer une description fonctionnelle adaptée, c'est-à-dire qui ne fasse pas trop d'hypothèses sur l'architecture du système. L'analyse n'introduit pas les éléments de protection car un des objectifs reste de définir ces éléments et de les associer à des objectifs de sécurité (ex : consigne de direction erronée).

Comme pour toutes les méthodes proposées, les partenaires du projet SAM ont défini une template de la méthode présentée dans la table IV.

TABLE IV. CANEVAS D'ANALYSE PRELIMINAIRE DE RISQUES

Fonction	***Identification de la situation dangereuse***	***Accident potentiel de niveau STRA***	***Evaluation des risques***	***Exigence de sécurité au niveau STRA***

IV. ANALYSE DE SECURITE DE PARCOURS

L'Analyse de Sécurité de Parcours (ASP) est réalisée sur le parcours ou le site prédéfini sur lequel le STRA sera mis en service et débute par l'étape de description et de caractérisation du parcours. Il permet de cartographier les dangers spécifiques à chaque section ou regroupement de sections de l'itinéraire afin d'identifier les priorités d'action concernant la mise en œuvre des Mesures de Réduction des Risques (MRR), sur les sections de parcours. Cette analyse met en évidence les dangers d'une section mais aussi la dangerosité d'une situation ou d'une particularité du site.

A. Objectifs

L'objectif de l'ASP est d'identifier les risques et les situations particulières liées au parcours qui n'auraient pas été identifiées dans les deux premières analyses, et d'identifier des mesures de réduction des risques (MRR), si nécessaire, soit au niveau des infrastructures, soit au niveau du système STRA. L'étude permet :

- Soit pour tester le domaine d'opération (ODD, ou Operational Design Domain) du véhicule ou du système technique de transport routier, là où il y a des choix déjà faits (sur des véhicules par exemple) et ainsi préciser des mesures complémentaires de réduction des risques liés à des défaillances ou des insuffisances fonctionnelles,
- Soit de préciser l'ODD qui permettrait au système STRA de bien gérer toutes les situations ou scénarios pouvant survenir dans l'ODD, et ainsi d'orienter le choix des solutions.

B. Description de la méthode

Il est important d'utiliser les résultats des analyses APD et APR existantes pour assurer cette étude. L'ASP n'est pas destinée à remplacer les études APD et APR, mais à confirmer leur exhaustivité (en termes d'identification des risques) et leur exactitude (en termes d'évaluation des risques) en considérant toutes les caractéristiques du parcours, ou de la zone, étudié. Ainsi, il reste possible que certains scénarios spécifiques au parcours soient absents de l'APD au niveau du système STRA et l'ASP permet alors d'enrichir l'APD pour de futures réutilisations de l'APD sur d'autres voies d'application du système STRA. Les principes essentiels à prendre en compte sont les suivants :

- L'ASP reste focalisée sur les événements liés aux caractéristiques et éléments spécifiques d'une section du parcours ou de la zone étudiés,
- L'ASP traite également des événements, extérieurs aux véhicules et indépendants de l'emplacement sur le parcours ou de la zone (par exemple, les conditions météorologiques impactant la visibilité, les injonctions des forces de l'ordre, etc.)
- L'ASP ne considère pas a priori les événements liés à des défaillances ou des insuffisances fonctionnelles, mais il reste acceptable d'intégrer certains éléments prévisibles qui nécessitent des interventions extérieures aux véhicules (ex. demande d'intervention).

C. Etapes à suivre pour cette méthode

En tout premier lieu, le parcours doit être découpé en sections délimités par des critères. Par exemple : section avec les mêmes caractéristiques de route (e.g. limitation de vitesse, type de marquage au sol, bords de voie, etc.), sections avec des éléments particuliers (e.g. station, passage pour piétons, etc.).

Les étapes suivantes sont :

1. Observation des éléments nécessitant une réponse particulière (sollicitation, prise de décision) afin de gérer en toute sécurité le comportement routier des véhicules. Ces éléments constituent des particularités (situations dangereuses liées aux particularités du parcours). Par exemple, un passage piéton avec un masque de visibilité par un élément d'infrastructure sur le parcours, juste devant le véhicule, présence d'un collège à proximité du tronçon étudié, etc.
2. Regroupement possible des sections similaires qui se répètent sur le parcours (ex. regroupement de tous les passages pour piétons). La définition des MRR est ainsi unifiée et simplifiée. Ces MRR seront ensuite appliqués à chaque macro-section concernée.
3. Analyse de sécurité : Pour chaque section, les événements et les objets interagissant avec le système pouvant entraîner des situations dangereuses et des accidents (par exemple, une collision avec un utilisateur vulnérable) sont définis.
4. Évaluation initiale des risques : coter la sévérité de l'accident, la fréquence de l'événement déclencheur, l'exposition et la contrôlabilité. Ce travail permet de définir le niveau de dangerosité de la particularité ou de la section. Remarque : les classes d'exposition, de sévérité et de contrôlabilité doivent être homogènes parmi les 3 analyses de sécurité (APD, APR et ASP).
5. Définition du niveau d'acceptation du risque pour définir la MRR uniquement lorsque le niveau de risque est plus élevé.
6. Proposition des mesures de réduction des risques et établir une nouvelle cotation de la dangerosité de la particularité ou des tronçons (ex. pour la proximité du collège : barrière devant le collège, vitesse réduite, avertissement sonore, etc.).
7. Établissement un plan d'action (« Hazard Log ») pour gérer le suivi de toutes les mesures de réduction des risques proposées.
8. Mise à jour de la description de l'ODD, de l'OEDR, de la liste standard des accidents pour les STRA et d'autres documents pertinents.

Les particularités de l'itinéraire identifiées peuvent inclure tout équipement « support » (ex. feux communicants, barrières latérales) s'ils sont déjà prévus. L'analyse des dangers peut également conduire à compléter les besoins en équipements et à proposer des éléments d'installation complémentaires spécifiques aux particularités du parcours considéré lorsque le véhicule ne peut répondre correctement à tous les besoins.

D. Conclusion

Cette dernière analyse, dite « analyse de sécurité de parcours » précise les performances et les capacités fonctionnelles demandées. Elle pourrait également identifier de nouvelles frontières potentielles de l'ODD du système et ainsi proposer des MRR qui couvriront toutes les situations opérationnelles. Ces MRR peuvent inclure, une limitation initiale de l'ODD, une nouvelle réponse du STRA (y compris, manœuvre du véhicule, règle en service, etc.), ou modification

de l'infrastructure routière du parcours. Enfin, elle donne une carte des dangers et propose un premier ensemble d'exigences qui rendront l'opération du système sûre sur le parcours. Tous ces éléments sont synthétisés dans la table V proposé pour mener l'analyse.

TABLE V. CANEVAS D'ANALYSE PRELIMINAIRE DE RISQUES

Section du parcours	***Situation dangereuse***	***Accident potentiel de niveau STRA***	***Evaluation des risques***	***MRR***	***Evaluation du risque finale***

CONCLUSION

Cet article propose une méthodologie de sécurité pour l'autorisation de mise en service des Systèmes de Transport Routier Automatisés (STRA), conçu dans le cadre du projet SAM. Il comprend la description de trois analyses de sécurité complémentaires pour assurer l'identification des risques la plus exhaustive possible : une Analyse Préliminaire des Dangers (APD), une Analyse Préliminaire des Risques (APR) et une Analyse de Sécurité de Parcours (ASP). Chacune de ces trois méthodologies sera affinée et améliorée en continu au cours des années 2022 et 2023, en tirant parti des différentes expérimentations du projet SAM et sera présentée aux services techniques français chargés de définir le processus d'autorisation de mise en service de STRA. La prochaine étape, dans le projet SAM, sera la généralisation de cette méthodologie de sécurité aux systèmes de transport automatisés appliqués à la logistique et à la livraison de marchandises.

Les auteurs tiennent à remercier les autorités françaises très favorables à l'écosystème du STRA, et tous les membres du projet SAM (IRT SystemX, Alstom, Easymile, Keolis, PFA, RATP, Renault, SNCF, Stellantis, Transdev, Twinswheel, Vedecom, Valeo, Vinci) pour la fructueuse collaboration réalisée ces dernières années, et qui conduit à cette méthodologie et à cet article.

ACRONYMES

APD	Analyse Préliminaire des Dangers
APR	Analyse Préliminaire des Risques
ARTS	Automated Road Transportation Systems
ASIL	Niveau d'Integrité de Sécurité Automobile, de l'anglais *Automotive Safety Integrity Level*
ASP	Analyse de Sécurité de Parcours
C	Contrôlabilité
E	Exposition
FRR	Facteur de Réduction de Risque
GAME	Globallement Au Moins Equivalent(from French GAME)
OGS	Objectif Global de Sécurité
ODD	Domaine d'Opération, ou *Operational Design Domain*
OEDR	Réponse à la Détection d'Objets ou d'Evénements
MRR	Mesure de Réduction de Risque
S	Sévérité
SAM	Sécurité & Acceptabilité de la Mobilité Autonome
STRA	Système de Transport Routier Automatisé
TFFR	Tolerable Functional Failure Rate
TFIR	Tolerable Functional Insufficiency Rate
THR	Tolerable Hazard Rates Modes de Défaillances, de leur Effets, et de leur Criticité

REFERENCES

[1] STRMTG, « Guide d'application STRMTG GAME pour les STRA "Systèmes de Transport Routier Automatisés - Principe "GAME" Globalement Au Moins Equivalent », Ministère chargé des Transports – Service Technique des Remontées Mécaniques et des Transports Guidés, 2021.

[2] IEC 61508-1 (2011). International standard for electrical, electronic and programmable electronic safety related systems, Part 1 General requirements, International Electrotechnical Commission

[3] NF EN 50126-1 (2017). Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process, European Committee for Electrotechnical Standardization (CENELEC), Bruxelles.

[4] NF EN 50126-2 (2017). Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety. European Committee for Electrotechnical Standardization (CENELEC), Bruxelles.

[5] ISO 26262. Road vehicles – Functional safety. International Standardization Office, Genève.

[6] French decree (2021). Article R.3152-2 of Decree n° 2021-873 of 29th June 2021 related to LOM Law article 31, Journal Officiel, Paris.

[7] ISO PAS 21448 (2021). Road vehicles – Safety of the intended functionality. International Standardization Office, Genève.

[8] E.Arnoux (2020). RoundTable – Simulation data standardisation for Autonomous Vehicle: introduction. DSC 2020 Europe: Driving Simulation & Virtual Reality Conference & Exibition, Antibes.