

GUIDE TECHNIQUE



STRMTG

SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

SYSTÈMES DE TRANSPORT ROUTIER AUTOMATISÉS

Guide technique relatif à
la démonstration « GAME » pour les STRA

Version 1 du 31 août 2022



**MINISTÈRE
CHARGÉ
DES TRANSPORTS**

*Liberté
Égalité
Fraternité*

1. Objet – Domaine d'application – Destinataires

Ce guide technique est un premier complément au guide d'application GAME du STRMTG qui explicite une méthodologie de démonstration du principe « GAME » (Globalement au moins équivalent) prévue par le décret n°2021-873 du 29 juin 2021 portant application de l'ordonnance n° 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation (décret « STRA »). Le présent guide technique précise certains éléments permettant de guider la démarche GAME décrite dans le guide d'application GAME.

Comme ce dernier, il est applicable à un système de transport routier automatisé (STRA) défini par l'article R. 3151-1 du code des transports (ajouté par article 6 du décret STRA), comme étant un « *système technique de transport routier automatisé, déployé sur des parcours ou zones de circulation prédéfinis, et complété de règles d'exploitation, d'entretien et de maintenance, aux fins de fournir un service de transport routier public collectif ou particulier de personnes, ou de service privé de transport de personnes, à l'exclusion des transports soumis au décret n° 2017-440 du 30 mars 2017 relatif à la sécurité des transports publics guidés* ».

Il est destiné à l'ensemble des acteurs professionnels du secteur des transports routiers automatisés : organisateurs de service, maîtres d'ouvrage, exploitants, bureaux d'études, Organismes qualifiés agréés (OQA), concepteurs de systèmes techniques de transports routiers automatisés, constructeurs de matériels.

Les dispositions du présent guide visent à expliciter la réglementation de sécurité applicable sur certains aspects de la démonstration de sécurité. Elaborées en concertation avec la profession, elles offrent un cadre destiné à faciliter le travail des professionnels. Elles ne présentent pas un caractère réglementaire mais leur respect permet cependant de présumer de la conformité aux exigences réglementaires relatives au principe GAME et/ou de la pertinence de la démarche adoptée.

Les dispositions du présent guide sont limitées d'une part à la sécurité des personnes transportées et des tiers vis-à-vis du fonctionnement du système, et d'autre part limitées aux phases de fonctionnement pour lesquelles le contrôle dynamique du véhicule n'est pas assuré par un conducteur humain, sur la voirie ouverte à la circulation publique (c'est-à-dire sur la voirie dont rien ne s'oppose à l'usage par le public).

Il est précisé que dans ces conditions, la sécurité des personnels d'exploitation et de maintenance vis-à-vis du fonctionnement du système est traitée par le présent guide,

- au titre des personnes transportées, lorsqu'ils sont présents à bord des véhicules du système,
- et au titre de tiers, lorsqu'ils sont présents sur le parcours.

Par ailleurs, les dispositions du présent guide couvrent également la sécurité des tiers lorsqu'ils sont en interaction avec les équipements et aménagements spécifiquement mis en place pour le système, hors des phases de fonctionnement de ce système.

Les dispositions du présent guide ne traitent pas :

- des problématiques relatives aux risques cyber ;
- des problématiques relatives à la sûreté publique (colis suspect, acte de vandalisme...) ;
- des problématiques liées aux obligations réglementaires d'accessibilité du système de transport pour les personnes en situation de handicap ;
- des problématiques liées aux conditions d'hygiène et de sécurité des agents d'exploitation et de maintenance ;
- des procédures d'intervention et de sauvetage définies par les services de secours ;
- des problématiques liées aux Etablissements recevant du public (ERP) de type gare en tant que tel, hormis pour leurs interfaces avec le système de transport ;

- des problématiques liées à la Défense extérieure contre l'incendie (DECI) ;
- de la prise en compte des éventuels risques engendrés par les travaux de réalisation du projet lorsque ceux-ci n'ont pas d'impacts sur un système de transport routier automatisé existant ;
- des problématiques de performance du système.

Le présent guide ne saurait couvrir tous les volets de la démonstration GAME. Les éléments qu'il présente sont plus particulièrement destinés à être mis en œuvre dans le cadre de l'analyse détaillée des risques « Type 3 » présentée dans le guide d'application GAME.

Ce guide initial a vocation à être complété de manière incrémentale au fur et à mesure de l'enrichissement des travaux sur la démonstration de sécurité des STRA, notamment concernant les aspects liés aux objectifs de sécurité et à l'évaluation du risque, qui servira à décider de son acceptabilité.

Historique des mises à jour

N° version	Rédacteur	Date	Nature de la version
1	Pierre Jouve	31/08/2022	Création par le groupe de travail GAME (STRA)

RÉDACTEUR	VÉRIFICATEUR	APPROBATEUR
Pierre Jouve chef du département transports publics automatisés	Alexandre Dusserre chef du département métros et systèmes ferroviaires	Daniel Pfeiffer directeur



Service technique des remontées mécaniques et des transports guidés (STRMTG)
 1461 rue de la piscine
 38400 Saint Martin d'Hères
 tél. : 33 (0)4 76 63 78 78
 mèl. strmtg@developpement-durable.gouv.fr
www.strmtg.developpement-durable.gouv.fr

1	Préambule.....	5
2	Définitions	5
3	Liste des abréviations.....	9
4	Contexte réglementaire	10
5	Présentation de l'analyse détaillée des risques	11
5.1	Généralités.....	11
5.2	Champ de l'analyse détaillée.....	11
5.3	Canevas de l'analyse détaillée	12
5.4	Eléments pour le cas de l'analyse explicite (type 3b).....	14
6	Principes d'estimation du risque	16
6.1	Généralités.....	16
6.2	Estimation de la gravité	17
6.3	Estimation de la fréquence d'occurrence de l'accident	21
7	Exigences de haut niveau	24
8	Analyse déductive (analyse préliminaire des dangers)	44
8.1	Présentation	44
8.2	Trame.....	46
8.3	Eléments d'entrée de l'analyse déductive.....	48
9	Analyse inductive (analyse préliminaire des risques).....	59
9.1	Présentation	59
9.2	Trame.....	61
9.3	Eléments d'entrée de l'analyse déductive.....	63
10	Annexe.....	83

1 Préambule

Le décret n°2021-873 du 29 juin 2021 portant application de l'ordonnance n° 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation fixe les exigences de sécurité applicables aux Systèmes de transport routier automatisés (STRA) et notamment le principe « Globalement au moins équivalent » (GAME). Ce décret est appelé dans la suite de ce document « décret STRA ».

En complément du guide d'application GAME qui présente les différentes approches de la démonstration de sécurité dans le cadre du principe GAME, le présent guide vise à fournir des éléments d'entrée et des principes permettant de réaliser une analyse détaillée des risques dans le cadre d'un STRA.

Pour rappel, cette analyse détaillée des risques est l'une des approches de démonstration possibles au sein de l'approche GAME. Cette approche dite de « type 3 » vise notamment à couvrir les cas des systèmes intégrant des équipements ou des fonctions innovants et pour lesquels il n'existe ni référentiel réglementaire ou technique applicable au système complet, ni système de référence acceptable. Ainsi, cette approche repose sur la réalisation d'une analyse exhaustive des dangers et du traitement de chaque danger identifié, soit selon un référentiel hors-STRA démontré acceptable (type 3a), soit selon une analyse explicite découlant sur des mesures quantitatives et qualitatives (type 3b).

Le présent document décrit plus avant cette analyse détaillée et fournit les éléments d'entrée permettant d'initier la démarche d'analyse.

Les éléments détaillés ici sont le fruit des réflexions communes à l'ensemble des participants du groupe de travail GAME du STRMTG associant la profession. Néanmoins, le présent guide ne saurait prétendre à être exhaustif dans les éléments qu'il présente et a vocation à être enrichi au fur et à mesure des retours issus des différents cas d'application.

Ce document doit ainsi être considéré comme un premier guide permettant de :

- *Préciser le canevas de la démarche de type 3 « Analyse détaillée des risques » ;*
- *Lister les principaux éléments d'entrée à prendre en compte dans les différentes analyses.*

Il est rappelé qu'il appartient quoi qu'il en soit au porteur de l'analyse de compléter ou adapter ces différentes listes d'éléments d'entrée au vu des spécificités et du contexte du système analysé.

Par ailleurs, la non-prise en compte de certains éléments de ces listes reste possible, mais doit être justifiée par le porteur de l'analyse au vu des spécificités et du contexte du système analysé.

2 Définitions

Les définitions suivantes sont issues des articles R. 311-1, R. 311-1-1 et R. 3151-1 du code des transports :

« Contrôle dynamique » : exécution de toutes les fonctions opérationnelles et tactiques en temps réel nécessaires au déplacement du véhicule. Il s'agit notamment du contrôle du déplacement latéral et longitudinal du véhicule, de la surveillance de l'environnement routier, des réactions aux événements survenant dans la circulation routière et de la préparation et du signalement des manœuvres.

« Domaine d'emploi » : conditions d'emploi d'un système technique de transport routier automatisé associées à des parcours ou zones de circulation particulières et respectant son domaine de conception technique.

« Domaine de conception technique du système » : conditions d'opération dans lesquelles un système technique de transport routier automatisé est spécifiquement conçu pour fonctionner.

« Intervention à distance » : action exercée par la personne habilitée mentionnée à l'article L. 3151-3, située à l'extérieur du véhicule, dans le cadre d'un système de transport routier automatisé, aux fins :

- a) D'activer, de désactiver le système, de donner l'instruction d'effectuer, modifier, interrompre une manœuvre, ou d'acquiescer des manœuvres proposées par le système ;
- b) De donner instruction au système de navigation opérant sur le système de choisir ou de modifier la planification d'un itinéraire ou des points d'arrêt pour les usagers.

« Manœuvre à risque minimal » : manœuvre ayant pour finalité la mise à l'arrêt du véhicule en situation de risque minimal pour ses occupants et les autres usagers de la route, automatiquement effectuée par le système de conduite automatisé, suite à un aléa non prévu dans ses conditions d'utilisation, à une défaillance grave ou, dans le cas d'une intervention à distance, à un défaut d'acquiescement de manœuvre demandé par le système.

« Manœuvre d'urgence » : manœuvre automatiquement effectuée par le système de conduite automatisé en cas de risque imminent de collision, dans le but de l'éviter ou de l'atténuer.

« Modification substantielle » : toute modification d'un système de transport routier automatisé ou d'une partie de système existant, dès lors qu'elle modifie l'évaluation de la sécurité.

« Organisme qualifié » : organisme agréé pour procéder à l'évaluation de la sécurité de la conception, de la réalisation et de l'exploitation des systèmes de transport routiers automatisés.

« Parcours ou zone de circulation prédéfini » : ensemble des sections routières ou espace dont les limites géographiques sont définies, sur lesquelles est prévue la circulation ou l'arrêt d'un ou plusieurs véhicules d'un système de transport routier automatisé ;

Note : dans la suite du document, le terme "parcours" est communément utilisé en lieu et place de "parcours ou zone de circulation prédéfinie" ».

« Système de conduite automatisé » : système associant des éléments matériels et logiciels, permettant d'exercer le contrôle dynamique d'un véhicule de façon prolongée.

« Système technique de transport routier automatisé » : ensemble de véhicules hautement ou totalement automatisés, tels que définis aux 8.2 et 8.3 de l'article R. 311-1 du code de la route, et d'installations techniques permettant une intervention à distance ou participant à la sécurité ;

Note : dans la suite du document, la formulation « Système technique » est communément utilisée en lieu et place de « Système technique de transport routier automatisé ».

« Système de transport routier automatisé » : système technique de transport routier automatisé, déployé sur des parcours ou zones de circulation prédéfinis, et complété de règles d'exploitation, d'entretien et de maintenance, aux fins de fournir un service de transport routier public collectif ou particulier de personnes, ou de service privé de transport de personnes, à l'exclusion des transports soumis au décret no 2017-440 du 30 mars 2017 relatif à la sécurité des transports publics guidés.

« Véhicule hautement automatisé » : véhicule équipé d'un système de conduite automatisé exerçant le contrôle dynamique d'un véhicule dans un domaine de conception fonctionnelle particulier, pouvant répondre à tout aléa de circulation ou défaillance, sans exercer de demande de reprise en main pendant une manœuvre effectuée dans son domaine de conception fonctionnelle. Ce véhicule peut être intégré dans un système technique de transport routier automatisé tel que défini au 1o de l'article R. 3151-1 du code des transports.

« Véhicule totalement automatisé » : véhicule équipé d'un système de conduite automatisé exerçant le contrôle dynamique d'un véhicule pouvant répondre à tout aléa de circulation ou défaillance, sans exercer de demande de reprise en main pendant une manœuvre dans le domaine de conception technique du système technique de transport routier automatisé auquel ce véhicule est intégré, tels que définis aux 1° et 4° de l'article R. 3151-1 du code des transports.

En complément, il semble utile de préciser les termes suivant sur la base des définitions issues de publication existantes ou élaborées dans le cadre spécifique de ce guide, en concertation avec la profession (*lorsque la définition est issue d'un référentiel, la mention en italique renvoie à ce texte*) :

« Accident » : événement ou série d'événements inattendus conduisant à des dommages, qui peuvent engager la sécurité des personnes.

« Accident de la circulation » : collision entre un véhicule et un autre véhicule ou un obstacle mobile ou fixe.

« AMDEC (Analyse des modes de défaillances, de leurs effets et de leur criticité » : Méthode systématique d'évaluation d'une entité ou d'un processus afin d'identifier ses éventuels modes de défaillance hiérarchisés et leurs effets sur les performances de l'entité ou du processus, ainsi que sur l'environnement voisin et le personnel.

« Analyse des causes » : analyse des raisons à l'origine d'une situation dangereuse (*EN 50129:2018*).

« Analyse de risque » : utilisation systématique de toutes les informations disponibles pour identifier les dangers et estimer le risque (*Règlement UE 402/2013*).

« Concept de sécurité » : spécification des exigences de sécurité fonctionnelle, avec les informations associées, leur allocation aux différents éléments de l'architecture, et la description de leurs interactions nécessaires à l'atteinte des objectifs de sécurité.

« Criticité » : caractérisation du niveau de risque.

« Danger » : circonstance pouvant mener à un accident (*règlement UE 402/2013*).

« Défaillance » : cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou à fonctionner comme prévu (*CEI 61508-4:2010*).

« Dommage » : blessure physique, atteinte à la santé des personnes, ou atteinte aux biens matériels.

« Dysfonctionnement » : mauvaise réponse du système dans deux cas possibles :

- Lors d'une défaillance,
- Lors d'apparition de conditions de fonctionnement qui ne sont pas correctement gérées en raison de limitations fonctionnelles (insuffisances fonctionnelles).

« Equipement » : appareil unique ou ensemble de dispositifs ou appareils, ou ensemble des dispositifs principaux d'une installation, ou ensemble des dispositifs nécessaires à l'accomplissement d'une tâche particulière (*EN 50129:2018*).

« Estimation des risques » : processus utilisé pour aboutir à une mesure du niveau des risques analysés et qui comprend les étapes suivantes : analyse et estimation des conséquences, estimation de la fréquence.

« Evaluation des risques » : procédure fondée sur l'analyse de risque pour déterminer si le niveau de risque atteint est acceptable ou non (*règlement UE 402/2013*).

« Evènement » : modification de l'environnement extérieur ou dysfonctionnement du système considéré (e.g. ego véhicule), à un instant donné, que l'on peut caractériser, et devant être prise en compte en vue d'une décision.

« Evènement redouté » (ou « évènement dangereux ») : Évènement indésirable qui peut provoquer une situation dangereuse et dans certaines conditions un accident.

« Evitabilité » : capacité à éviter un accident grâce aux réactions opportunes des personnes impliquées, éventuellement avec l'aide de mesures externes au véhicule.

Note 1 : les personnes impliquées peuvent comprendre l'intervenant à distance, les éventuels conducteurs de véhicules tiers éventuels, les personnes situées au voisinage du véhicule, et dans certains cas les personnes transportées.

Note 2 : le paramètre « Ev » est une estimation de cette capacité d'évitement.

« Exigences de sécurité » : caractéristiques de sécurité (qualitatives ou quantitatives) d'un système y compris son exploitation (incluant les règles d'exploitation) et de son entretien qui sont nécessaires pour atteindre les objectifs de sécurité établis par la législation ou par l'entreprise ; (règlement UE 402/2013).

« Exposition » : état d'être dans une situation opérationnelle donnée qui peut être dangereuse si elle coïncide avec l'évènement redouté.

Note : le paramètre « E » représente la proportion de temps moyen d'exposition à une situation opérationnelle donnée par rapport au temps total d'exploitation.

« Gravité » (ou « Sévérité ») : estimation du niveau de dommage résultant d'un accident.

« Infrastructure » : L'infrastructure est l'ensemble des équipements constituant l'infrastructure routière et l'infrastructure numérique.

« Infrastructure routière » : ensemble constitué de :

- La chaussée ;
- Les équipements et aménagements de la route, comprenant notamment la signalisation horizontale (marquages, ...) et verticale (feux, panneaux classiques, panneaux à messages variables, ...), les éléments de sécurité (glissières, cônes, triangles, ...), les supports d'information (mobilier urbain, portiques, ...) et les stations voyageurs partagées ;
- Les équipements et aménagements spécifiques au système technique de transport routier automatisés comprenant notamment les capteurs débarqués, les marquages dédiés, les barrières fixes ou escamotables spécifiques et les stations voyageurs dédiées.

Note 1 : l'infrastructure routière peut être caractérisée par des descripteurs génériques, permettant ainsi de définir des catégories d'infrastructures (ex : nombre de voies, types de feux, densité de mobilier urbain, fonctionnalités des unités de bord de route) ; ces descripteurs peuvent ensuite être déclinés ou complétés de descripteurs spécifiques à l'infrastructure sur lequel le système est déployé (ex : localisation des feux, configuration géométrique précise de telle intersection).

Note 2 : la méthode de description de l'infrastructure routière (i.e. les listes de descripteurs pertinents) n'est pas développée dans cette première version du guide technique et le sera dans un complément ultérieur.

« Infrastructure numérique » : ensemble des équipements permettant la communication et la connectivité nécessaires au STRA, i.e. les unités de bords de route, les réseaux de communications 3G/4G/5G, C-ITS, reliant les différents composants connectés du système ou de l'écosystème et les équipements dédiés à la supervision.

« Mesure de réduction des risques » : série de mesures permettant de réduire la fréquence d'occurrence d'un danger ou d'en atténuer les conséquences afin d'atteindre et/ou de maintenir un niveau de risque acceptable ; (règlement UE 402/2013).

« Mode délégation de conduite » : mode dans lequel le système de conduite automatisé est en charge du contrôle dynamique du véhicule.

« Niveau de risque » : résultat d'une évaluation du risque qui quantifie la probabilité d'occurrence et la gravité de l'impact.

« Passager » : catégorie d'utilisateur situé à l'intérieur d'un véhicule du système qui ne peut prendre part à aucune action de contrôle dynamique de ce véhicule.

« Risque » : combinaison de la fréquence d'occurrence d'un dommage et de sa gravité.

« Risque résiduel » : risque subsistant après que des mesures de prévention ou de protection ont été prises.

« Sécurité de la fonction attendue » (SOTIF) : absence de risque inacceptable dû aux dangers résultant d'une insuffisance fonctionnelle de la fonction attendue ou d'un mauvais usage raisonnablement prévisible par les usagers.

« Système » : ensemble d'éléments (matériels, logiciels ou humains) reliés entre eux, considéré comme un tout dans un contexte défini et organisé de sorte à atteindre un objectif donné, dans certaines conditions.

« Sous-système » : partie d'un système, qui est elle-même un système (EN 50126-1:2017).

« Situation dangereuse » : situation dans laquelle des personnes sont (ou auraient pu être) exposées à un ou plusieurs dangers.

« Usager » (du système) : terme général faisant référence au rôle de l'humain par rapport à la délégation de conduite.

« Usager de la route » : toute personne faisant l'usage de la route (y compris les trottoirs et autres espaces adjacents) (EN ISO TR 4804 : 2020).

Note : les usagers du système sont une catégorie d'usagers de la route. Par opposition, les autres usagers de la route représentent les tiers.

3 Liste des abréviations

AMDEC : Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité

AOM : Autorité Organisatrice de la Mobilité

APD : Analyse Préliminaire des Dangers

APR : Analyse Préliminaire des Risques

ASIL : Niveau d'intégrité de sécurité automobile (« Automotive Safety Integrity Level ») (ISO 26262-1 : 2018)

DCST : Dossier de Conception du Système Technique

DPS : Dossier Préliminaire de Sécurité

DS : Dossier de Sécurité

E : classe d'Exposition

Ev : classe d'Évitabilité

ER : Évènement Redouté

ERP : Etablissement Recevant du Public

FRR : Facteur de Réduction du Risque

G : classe de Gravité

GAME : Globalement Au Moins Equivalent

IHM : Interface Homme Machine

MRM : Manœuvre à Risque Minimal

MRR : Mesure de Réduction du Risque

OGS : Objectif Global de Sécurité

OQA : Organisme Qualifié Agréé

OSS : Objectif Spécifique de Sécurité

PCC : Poste de Commande Centralisé

REX : Retour d'EXpérience

SD : Situation Dangereuse

SGS : Système de Gestion de la Sécurité en exploitation

SIL : niveau d'intégrité de sécurité (« Safety Integrity Level ») (EN 61508-4 : 2011)

SOTIF : sécurité de la fonctionnalité attendue (« Safety Of the Intended Functionality »)

STRA : Système de Transport Routier Automatisé

TFFR : taux de défaillance fonctionnelle acceptable (« Tolerable Functional Failure Rate »)

TFR : taux de dysfonctionnement acceptable (« Tolerable Fail Rate »)

TMD : Transport de Marchandises Dangereuses

4 Contexte réglementaire

Ce guide est applicable aux systèmes ou parties de systèmes de transport routier automatisés visés par l'article R. 3152-2. du code des transports créé par l'article 6 du décret STRA n° 2021-873 du 29 juin 2021.

Le décret STRA introduit l'obligation, pour les systèmes de transport routiers automatisés de respecter le principe « GAME » en ce qui concerne leur niveau de sécurité.

Cette exigence est formalisée par l'article R. 3152-2. du code des transports créé par l'article 6 du décret STRA :

« Art. R. 3152-2. – I. - Pour l'application de l'article L. 3151-1, tout système de transport routier automatisé ou toute partie d'un système de transport existant est conçu, mis en service et, le cas échéant, modifié de telle sorte que le niveau global de sécurité à l'égard des usagers, des personnels d'exploitation et des tiers soit au moins équivalent au niveau de sécurité existant ou à celui résultant de la mise en œuvre des systèmes ou sous-systèmes assurant des services ou fonctions comparables, compte tenu des règles de l'art, du retour d'expérience les concernant, et des conditions de circulation raisonnablement prévisibles sur le parcours ou la zone de circulation considéré. »

Le même article R. 3152-2 traite le cas où il est impossible de construire l'analyse par comparaison avec un système existant :

« Lorsqu'il est établi qu'il n'existe pas de système comparable pour évaluer la sécurité du système considéré ou de l'un de ses sous-systèmes, le niveau de sécurité peut être établi à partir d'une étude de sécurité spécifique pour le système ou le sous-système concerné menée conformément aux règles de l'art. »

D'une manière générale, le présent document est un complément au guide d'application GAME du STRMTG et en reprend le même périmètre d'application et les mêmes limites ; il est destiné à préciser la démarche d'analyse détaillée des risques (type 3).

Celle-ci correspond au cas où, dans le cas d'un STRA pour lequel il n'existe ni référentiel réglementaire ou technique applicable, ni système de référence, il est nécessaire d'analyser de manière détaillée les risques dans le contexte de ce système.

Il convient de noter que :

- Cette approche peut également être choisie volontairement à la place de l'approche par écarts (type 2) ;
- La démonstration de sécurité relative à un système peut s'appuyer sur une combinaison des différentes approches décrites dans le guide d'application GAME.

Ainsi, comme pour le guide d'application GAME :

- Au sens du présent document, la notion de système est employée de manière générique. Elle peut faire référence à un système complet de transport routier automatisé, à un système technique, à un sous-système ou à une composante ou à un équipement ;
- Les éléments de démonstration explicités dans le présent guide font uniquement référence à la sécurité des personnes transportées (y compris le personnel d'exploitation lorsqu'il est passager du système) et des tiers vis-à-vis du fonctionnement du système en exploitation.

5 Présentation de l'analyse détaillée des risques

5.1 Généralités

Le présent document vise à guider la réalisation de l'analyse détaillée des risques (type 3) au niveau d'un système technique ou d'un système STRA, dans le cadre de l'application du principe GAME.

Les objectifs visés sont multiples :

- Assurer une homogénéité des méthodes mises en œuvre en spécifiant notamment des points d'étape, de manière à favoriser les échanges entre les acteurs ;
- Initier la réflexion en mettant à disposition des éléments d'entrée pour les analyses ;
- Limiter les risques d'oubli ;
- Construire un cadre commun propice à la capitalisation des retours d'expérience des acteurs.

Le présent document ne saurait prétendre à être exhaustif :

- Certains domaines de la démonstration mériteront d'être détaillés dans les évolutions du présent document ou dans des documents complémentaires ;
- Les éléments fournis devront être enrichis au fur et à mesure des retours d'expérience des acteurs issus des différents cas d'application.

Il appartient toujours à l'entité responsable de l'analyse de compléter en tant que de besoin les différents éléments de ce guide, dans le but de réaliser une analyse couvrant les spécificités du système analysé.

Dans le même esprit, il est toujours possible de justifier de la non-prise en compte d'un élément du présent document qui serait non-applicable en raison des spécificités du système analysé.

5.2 Champ de l'analyse détaillée

Un STRA peut être constitué de différents éléments :

- Des véhicules hautement et/ou totalement automatisés ;
- Des installations techniques spécifiques au système permettant une intervention à distance ou participant à la sécurité, déployées sur le parcours ;
- Des installations techniques permettant une intervention à distance ou participant à la sécurité, dédiées à la supervision, déployées en dehors du parcours ;
- Des règles d'exploitation, et de maintenance (aspect organisationnel supporté par le SGS en exploitation) ;
- Un parcours et ses aménagements.

Il est également en interface avec différents éléments qui contribuent à son fonctionnement :

- Des équipements de communication et de localisation partagés extérieurs au système ;
- La chaussée routière sur laquelle peuvent circuler les véhicules du système ;
- Des installations techniques génériques préexistantes et partagées avec les usagers de la route ;
- Des services extérieurs (forces de l'ordre, services de secours, services de la voirie, services de prévision et d'information météo, services d'information trafic, etc.) ;
- Des règles de circulation applicables sur le parcours ;
- Etc.

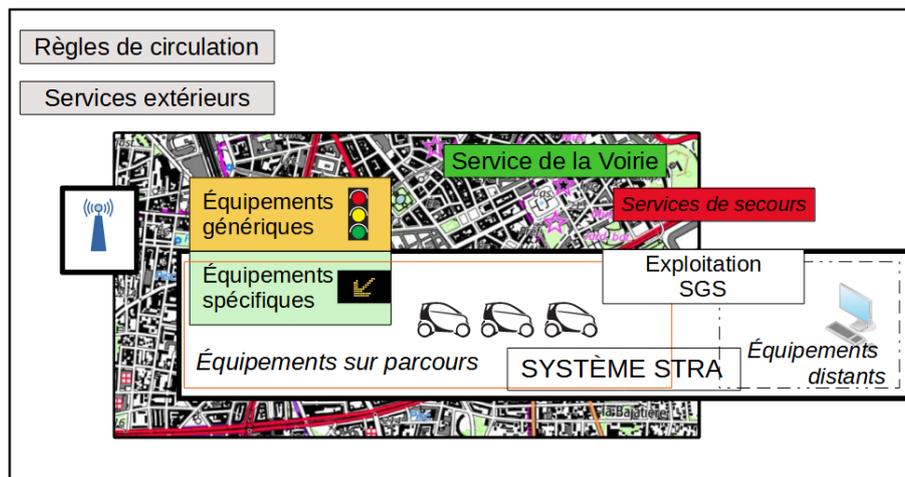


Figure 1 - Décomposition organique d'un STRA

Au sein de ces éléments constitutifs ou en interface, le champ de la démonstration de sécurité doit intégrer l'ensemble des éléments qui participent à la sécurité du système de transport STRA.

Parmi ces éléments, il convient de distinguer

- Les éléments qui font partie du système et sont directement intégrés dans la démonstration. Par exemple, les exigences relatives à un feu de circulation spécifique au système analysé sont directement spécifiées et résolues dans le cadre de la démonstration de sécurité ;
- Les éléments qui ne font pas partie du système mais qui participent à sa sécurité, pour lesquels la démonstration de sécurité pourra spécifier des exigences exportées, lesquelles devront être vérifiées par l'entité responsable. Par exemple, les exigences relatives à un feu de circulation préexistant et non spécifique au système analysé sont spécifiées sous forme d'exigences exportées et résolues dans un second temps sous la responsabilité de l'organisateur du service au stade du déploiement.

Comme précisé dans le guide d'application GAME, la démonstration de la sécurité doit être faite in fine au niveau du système de transport routier automatisé complet considéré, c'est à dire du système technique déployé sur un parcours donné et sujet à des règles d'exploitation, d'entretien et de maintenance. Ainsi, dans le cas où seul un sous-système ou un équipement ferait l'objet d'une analyse détaillée, la démonstration de sécurité finale devra porter in fine sur le système de transport routier automatisé complet.

5.3 Canevas de l'analyse détaillée

La démarche, couvrant les phases DCST et DPS / DS, vise à analyser les risques au niveau du système global, et à définir un ensemble d'exigences portant sur l'ensemble des éléments participants au système, i.e. le système technique, son architecture, le parcours et ses aménagements, les conditions d'exploitation, les conditions de circulation, les règles d'exploitation et de maintenance, etc.

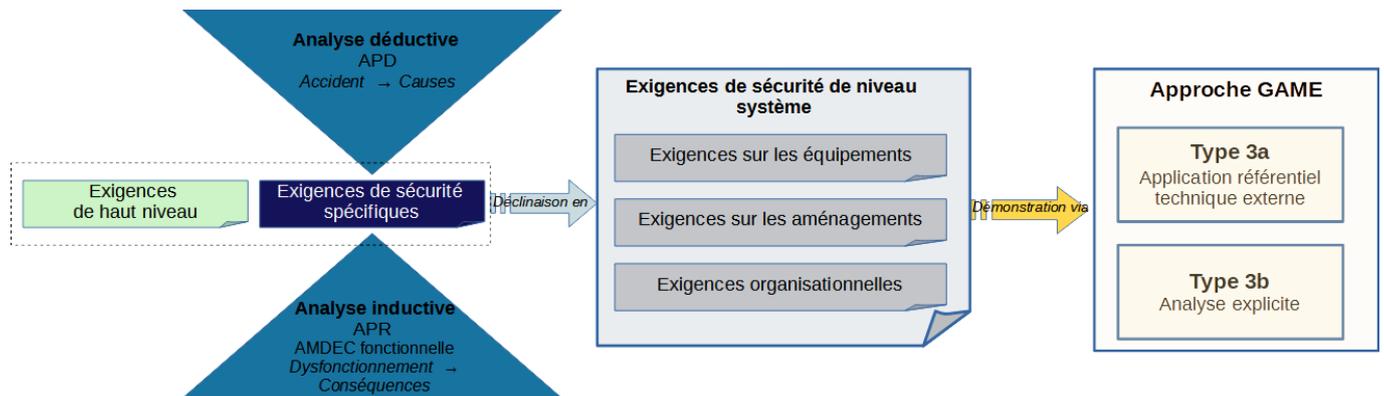


Figure 1 - Analyse détaillée type 3

On distingue 2 types d'exigences :

- Les exigences de haut niveau :

Les exigences de haut niveau présentées au chapitre 7 sont des exigences génériques essentielles applicables en dehors de tout contexte d'accident ou de toute situation dangereuse. Sauf justification, elles doivent être respectées par le système en toutes circonstances.

- Les exigences spécifiques :

Les exigences spécifiques sont définies pour le projet au moyen de 2 analyses complémentaires présentées aux chapitres 8 et 9 :

- Une analyse déductive qui a pour but d'identifier les combinaisons de causes possibles d'un accident. Cette analyse part des dangers pour en déterminer les causes possibles (type Analyse préliminaire des dangers (APD)) ;
- Une analyse inductive qui a pour but d'analyser de manière systématique les conséquences des dysfonctionnements potentiels du système. Cette analyse part des fonctions du système pour analyser l'ensemble des conséquences possibles de leur dysfonctionnement (type Analyse préliminaire des risques (APR) ou AMDEC fonctionnelle).

Ces deux analyses croisées sont complémentaires et doivent être conduites de manière à pouvoir s'alimenter l'une l'autre : tout risque identifié dans l'une des analyses doit être également analysé dans le cadre de l'autre. Ces analyses sont d'abord réalisées au stade du DCST, puis éventuellement complétées aux stades DPS et DS selon les résultats de l'analyse de sécurité du parcours.

La suite du document fournit des éléments destinés à servir ces différentes analyses.

Les exigences de sécurité de niveau système sont ensuite déclinées successivement aux sous-systèmes, équipements et composants du système, ou exportées vers les aménagements du parcours, ou les règles d'exploitation et de maintenance formalisées dans le système de gestion de la sécurité en exploitation (SGS).

Pour chaque risque identifié, les exigences issues de cette démarche peuvent se traduire par l'application d'un référentiel externe au domaine STRA pour lequel il a été démontré qu'il couvrait le risque considéré et son contexte (démonstration de type 3a du guide d'application GAME), ou par la mise en œuvre de mesures spécifiques après avoir démontré que leur combinaison permettait de ramener le risque résiduel à un niveau acceptable (démonstration de type 3b du guide d'application GAME).

Dans l'ensemble des travaux de la démonstration, chaque activité en lien avec la sécurité doit être tracée et documentée, (identification des risques, mesures de réduction des risques, résultats des estimations, ...). Cette exigence peut être par exemple satisfaite par la tenue d'un registre des situations dangereuses.

Analyse des scénarios incontournables

En complément, une analyse spécifique sera menée sur les scénarios incontournables pertinents pour le domaine d'emploi. Les prescriptions applicables à la définition des scénarios incontournables et à l'analyse de sécurité spécifique à y appliquer, feront l'objet de compléments au présent guide.

5.4 Eléments pour le cas de l'analyse explicite (type 3b)

Dans le cas où aucun référentiel technique externe au domaine STRA n'a été jugé acceptable (type 3a), il est nécessaire de conduire une analyse explicite afin de déterminer les mesures qualitatives et/ou quantitatives suffisantes applicables pour chaque risque identifié (type 3b).

Cette analyse peut être décomposée en 2 phases principales :

- Détermination d'un objectif global de sécurité (qualitatif et/ou quantitatif) ;
- Allocations successives de l'objectif de sécurité aux différents niveaux.

Objectifs de sécurité quantitatif

Un objectif global de sécurité (OGS) est défini lorsqu'il existe des données suffisantes, issues du retour d'expérience, cohérentes avec le domaine d'emploi du système ; cela peut être par exemple un objectif global de sécurité défini pour les accidents corporels de la circulation, par le « nombre d'évènements par km » ou le « nombre d'évènements par heure ».

Des objectifs spécifiques de sécurité (OSS) répartissant l'objectif global sur les différentes sous-catégories d'accidents sont définis si les données sont suffisamment précises et significatives ; cela peut être par exemple un objectif spécifique de sécurité défini pour les accidents corporels de la circulation de type « collision frontale avec un autre véhicule routier » par le « nombre d'évènements par km » ou le « nombre d'évènements par heure ».

Des éléments précisant ces objectifs seront apportés par les futures versions de ce guide au vu des différents travaux sur le sujet.

Allocation des objectifs de sécurité

Dans le cas d'une analyse explicite (type 3b), les objectifs qualitatifs ou quantitatifs doivent être alloués sur chaque fonction du système en lien avec les objectifs de sécurité issus de l'approche déductive et avec l'AMDEC fonctionnelle réalisée par l'approche inductive.

Cette allocation nécessite de déterminer l'indépendance des fonctions et d'analyser les combinaisons des dysfonctionnements pouvant mener à chaque accident de niveau système.

Cette allocation de niveau fonctionnel est le préalable à l'allocation d'objectifs de sécurité à chaque équipement et composant du système.

Ces différentes étapes d'allocation ne sont pas décrites à ce stade dans le présent guide technique. On pourra se référer aux publications pertinentes (comme par exemple la norme EN 50126-2)

Démarche d'analyse type 3b dans le cas où un objectif de sécurité quantitatif est défini

Le tableau suivant présente les étapes de la démarche d'analyse spécifique (type 3b) spécifiquement pour le cas où un objectif de sécurité quantitatif peut être défini.

	Activité	Observations et commentaires	Renvoi
1	<p>Convenir d'un Objectif global de sécurité (OGS) pour des catégories d'accidents (exemple : collision).</p> <p>Eventuellement, développer les OSS (Objectifs spécifiques de sécurité) pour chaque type d'accident dans la catégorie (exemple : collision avec différents tiers, ou collision sans tiers).</p>	<p>Le critère d'acceptation du risque peut être défini en termes de taux d'occurrence maximal acceptable d'accident (OGS).</p> <p>Associer pour chaque type d'accident l'OSS qui lui correspond.</p>	Ce point sera abordé dans une version ultérieure de ce guide
2	Rappeler les situations dangereuses via une APD (Analyse préliminaire des dangers).	<p>Identification des situations dangereuses (SD) pour un scénario d'accident donné.</p> <p>Identification des SD concernées par l'OSS.</p>	Cf. chapitre 8
	Calculer un objectif TFR relatif aux SD qui intègre l'expression de contexte propice à l'accident	<p>Considération de la plausibilité de réalisation d'un accident selon le contexte réel au moment de l'apparition de la situation dangereuse (conditions de réalisation).</p> <p>Le TFR représente le taux de dysfonctionnements, i.e. le taux des défaillances et des insuffisances fonctionnelles.</p>	Non traité dans le présent guide
3	APR (Analyse préliminaire de risques)	<p>Identification des causes des SD.</p> <p>L'APR permet de faciliter l'identification des dysfonctionnements du système STRA en les liant aux SD.</p>	Cf. chapitre 9
4	<p>Répartir les objectifs de TFR (relatif aux SD) sur les fonctions du système STRA.</p> <p>Le TFR est réparti sur les défaillances des fonctions techniques = TFFR. Ces défaillances constituent les ER (événements redoutés)</p>	<p>Cette répartition en TFFR peut-être une équipartition sur les fonctions du système STRA concernées par l'accident ou une répartition tenant compte de la complexité et/ou des REX des fonctions du système STRA concerné.</p> <p>L'objectif de cette étape permet de vérifier que $TFR < \sum_i TFFR(i)$.</p>	Non traité dans le présent guide
5	Traduire et convertir les fréquences TFFR en niveau SIL ou ASIL cohérents.	A partir des objectifs TFFR et selon le référentiel pertinent, associer à chaque fonction du système STRA son niveau de SIL et/ou d'ASIL cohérent au TFFR.	Non traité dans le présent guide
6	Traduire le TFR en objectifs concernant les insuffisances fonctionnelles	-	Non traité dans le présent guide

Tableau 1 – Etapes de la démarche d'analyse spécifique (type 3b) cas quantitatif

6 Principes d'estimation du risque

6.1 Généralités

L'analyse concerne l'ensemble des évènements pouvant conduire à des accidents de niveau système. Le périmètre à prendre en compte dans l'analyse recouvre l'ensemble des évènements pouvant se dérouler au cours du fonctionnement du système en exploitation, et pouvant entraîner des conséquences pour la sécurité des personnes transportées et des tiers.

Elle ne se limite donc pas aux accidents de la circulation mais intègre par exemple les évènements, les défaillances et les insuffisances fonctionnelles liés à l'incendie ou aux échanges voyageurs (Cf. tableau 8 du présent document).

La définition de l'accident recouvre les évènements conduisant à des dommages (matériels et/ou humains) qui peuvent engager la sécurité des personnes.

Un évènement ne pouvant en aucun cas engager la sécurité des personnes n'est pas considéré comme un accident dans le cadre de ce guide.

Un accident peut être vu comme la combinaison d'une situation dangereuse pré-accidentelle et d'une ou plusieurs conditions de réalisation, sans lesquelles l'accident ne peut avoir lieu.

Par exemple, une collision à une intersection peut être due à la situation dangereuse « non-respect de la signalisation » qui n'est pas suffisante en elle-même. La collision aura lieu si un véhicule tiers traverse l'intersection à ce moment.

La situation dangereuse elle-même peut être la conséquence d'un évènement redouté chapeau, lui-même généré par différents évènements ou combinaisons d'évènements.

Dans le même exemple, la situation dangereuse « non-respect de la signalisation » peut être due, par exemple, à une défaillance du système ou une mauvaise perception due à un masquage.

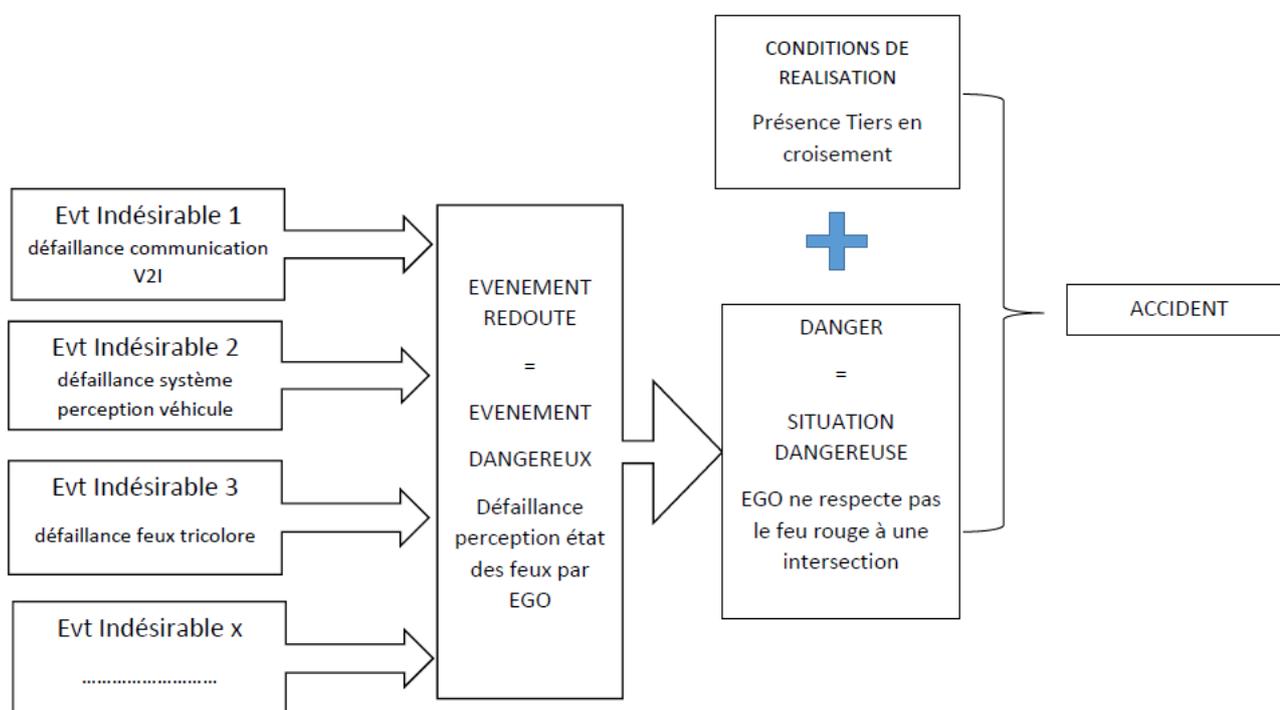


Figure 3 – Déroulement accident

Le risque est la combinaison de la fréquence d'occurrence d'un dommage et de sa gravité. Les métriques de gravité et de fréquence d'occurrence des accidents sont détaillées dans la suite du chapitre.

Un risque représenté par un évènement est estimé en tenant compte de la fréquence de l'évènement, de la probabilité de ses conditions de matérialisation en accident réel, et du niveau de gravité résultant des conséquences potentielles de cet accident.

D'une manière générale, l'estimation du risque doit être faite selon une approche prudente analysant le pire cas raisonnablement prévisible. Lorsqu'un même évènement peut donner lieu à différents scénarios, il convient de privilégier le scénario présentant le niveau de risque le plus élevé.

Il n'est pas tenu compte dans l'estimation du risque du nombre de véhicules intégrés dans le système. Le risque est estimé pour un véhicule du système en considérant qu'un usager est présent dans un seul véhicule à un instant donné, et en considérant les situations possiblement rencontrées par ce véhicule sur son parcours.

Il n'est pas tenu compte dans l'estimation du risque du nombre d'instanciations de chaque configuration d'infrastructure physique dans le système. Par exemple, le risque est estimé pour chaque carrefour présent sur le parcours en considérant qu'un usager est présent en un seul endroit du parcours à un instant donné.

La phase d'analyse détaillée des risques STRA nécessite donc de pouvoir graduer la gravité et la fréquence d'occurrence.

6.2 Estimation de la gravité

La gravité (ou « sévérité ») représente le niveau des dommages résultant d'un accident.

L'estimation de la gravité doit être faite en considérant le cas où l'accident est matérialisé et en prenant en compte le pire cas raisonnablement prévisible, et ce en tenant compte des conditions fixées dans le scénario (pour une collision par exemple : nature des tiers impliqués, nature du choc, type de véhicule, vitesses, présence d'aménagements ou de protections, etc.)

L'estimation de la gravité doit être tracée et documentée.

La métrique de gravité est dérivée de l'échelle de sévérité utilisée par la norme ISO 26262:2018. Le niveau de gravité 0 correspond à des dommages uniquement matériels et est donné dans le tableau par souci de complétude. Du fait que la démonstration GAME ne porte que sur la sécurité des personnes, un scénario dont les conséquences dans le pire cas raisonnablement prévisible pourraient n'être que matérielles, ne sera pas analysé.

Niveau de gravité	Description du niveau de dommage(s)
G0	Pas de blessure
G1	Blessures légères et modérées
G2	Blessures graves (survie probable)
G3	Blessures mortelles (survie incertaine) ou décès (*)

Tableau 2 – Classes de gravité

(*) Classe G3 avec de très nombreuses équivalences en décès dans des cas particuliers

Au sein du niveau G3, un marqueur (*) est prévu afin de marquer les évènements associés à des configurations pouvant donner lieu à un scénario d'accident dans les cas de zones d'interaction routier-ferroviaire ou à un scénario de sur-accident dans certains cas particuliers, et dont les conséquences potentielles seraient catastrophiques de par le nombre de personnes potentiellement impliquées : nombre

de passagers importants avec risque de blessures mortelles généralisé ou conséquences de l'accident impliquant potentiellement un nombre important d'usagers de la route, ce qui conduirait à de très nombreuses équivalences en décès (probablement plus de 10 ; il convient de se rapporter notamment à l'annexe C de la norme EN 50126-1).

Le niveau de gravité et l'objectif de sécurité associés aux scénarios marqués (*) restent ceux du niveau G3, mais chacun de ces événements, associé à ces configurations de circulation, doit faire l'objet d'une analyse spécifique, laquelle peut amener à des mesures de réduction du risque complémentaires au-delà du véhicule.

Ces mesures de réduction du risque complémentaires pourront porter par exemple sur :

- Des conditions d'exploitation propres à la situation considérée ;
- Des équipements et aménagements routiers propres à la situation considérée ;
- Des mesures organisationnelles propres à la situation considérée.

Le tableau suivant donne une liste des configurations devant donner lieu à ce type d'analyse spécifique complémentaire. Cette liste n'est pas exhaustive et il appartient à l'entité responsable d'identifier les situations à risque concernées par le marqueur (*).

Tableau 3- Liste des situations concernées par le marqueur (*)

ACCIDENT	ID ⁽¹⁾	sous-type	conditions	Catégorie / classe véhicule ⁽³⁾				argumentaire justifiant le marquage (*)
				cat M1 (8p maxi)	cat M2/M3 classes A/B 9-22p	cat M2/M3 classes 1/2/3 >22p	NAVURB 9-16p	
Collision	1.2	Collision contre un obstacle massif (containers, animaux, chute d'arbres, etc.)	si circulation dans un tunnel ⁽²⁾ de longueur > 300 m (200m si TMD) avec vitesse véhicule ego > 30 km/h	NA	NA	OUI	NA	collision amenant à un incendie du véhicule dans le tunnel (dommages étendus uniquement pour les potentiels calorifiques classes 1/2/3)
			si circulation avec risque de chute de hauteur (circulation sur ouvrage, ravin, etc.) avec vitesse véhicule ego > 30 km/h	NA	NA	OUI	NA	collision, sortie de route et renversement avec nombreuses victimes suite à chute de hauteur
	1.3	Collision avec un autre véhicule routier	si circulation dans un tunnel ⁽²⁾ de longueur > 300 m (200m si TMD) et avec différentiel possible de vitesse entre ego et tiers > 30 km/h lors du choc	NA	NA	OUI	NA	collision avec un autre véhicule amenant à un incendie véhicule dans le tunnel (conséquences sur le véhicule ego lui-même et si choc avec poids-lourd, conséquences étendues suite à incendie du poids-lourd)
			si circulation avec risque de chute de hauteur (circulation sur ouvrage, ravin, etc.) et avec différentiel possible de vitesse entre ego et tiers > 30 km/h lors du choc	NA	NA	OUI	NA	collision avec un autre avec nombreuses victimes dans le véhicule ego suite à chute de hauteur
	1.4	Collision avec le véhicule d'un système de transport guidé à une intersection d'une voie double (ex : ligne tramway et tramway croiseur)	si vitesse ego > 15 km/h lors du choc	OUI	OUI	OUI	OUI	collision avec nombreuses victimes dans le véhicule ego et dans le tramway suite au déraillement du tramway l'amenant en collision avec le tramway en croisement
		Collision avec le véhicule d'un système de transport ferré (ferroviaire lourd) à un passage à niveau		NA	NA	OUI	NA	collision avec système ferroviaire avec nombreuses victimes dans le véhicule ego
Feu fumée explosion	5.1	Feu/fumée dans le véhicule	Cas du feu dont l'origine est le véhicule : si circulation dans un tunnel ⁽²⁾ de longueur > 300 m (200m si TMD)	NA	NA	OUI	NA	1 - feu dont l'origine est le véhicule (mesures de prévention): risques pour les usagers du tunnel uniquement si capacité calorifique du véhicule élevée (classes 1/2/3 ou énergie embarquée dans le véhicule instable) 2 - feu initié par un poids-lourd avec le véhicule ego en seconde position (évacuation du véhicule ego): risques pour les usagers du tunnel uniquement si capacité calorifique du véhicule élevée (classes 1/2/3)

⁽¹⁾ Le champ ID d'identification des situations fait référence à la numérotation du tableau 8.

⁽²⁾ sont considérés comme tunnels pour l'application du présent tableau toutes les voies routières couvertes, quel que soit leur mode de construction : ouvrages creusés ou immergés, tranchées couvertes, couvertures non transparentes à l'air, couvertures partielles présentant une surface d'ouverture vers l'extérieur inférieure à 1 m² par voie de circulation et par mètre linéaire

"longueur du tunnel" = la distance comprise entre les deux têtes du tunnel ou entre une tête du tunnel et le tympan d'une gare ou station souterraine adjacente ou entre les tympans de deux gares ou stations souterraines consécutives (Art 1 AM du 22/11/2005).

⁽³⁾ Les catégories de véhicules sont données en référence à l'article R. 3111-1 du code de la route.

6.3 Estimation de la fréquence d'occurrence de l'accident

Dans le contexte de l'analyse détaillée des risques décrite ici, l'estimation vise à évaluer la probabilité d'occurrence de chaque accident, vu comme la combinaison d'une situation dangereuse pré-accidentelle et d'une ou plusieurs conditions de réalisation construisant le scénario.

Il convient d'adopter une démarche prudente pour l'estimation de la fréquence d'occurrence de chaque accident, en choisissant le pire cas raisonnablement prévisible.

La fréquence d'occurrence d'un accident (F) intègre la probabilité de survenue de la situation dangereuse et la probabilité des conditions de réalisation (FRR), tel que schématisé dans la figure ci-dessous.

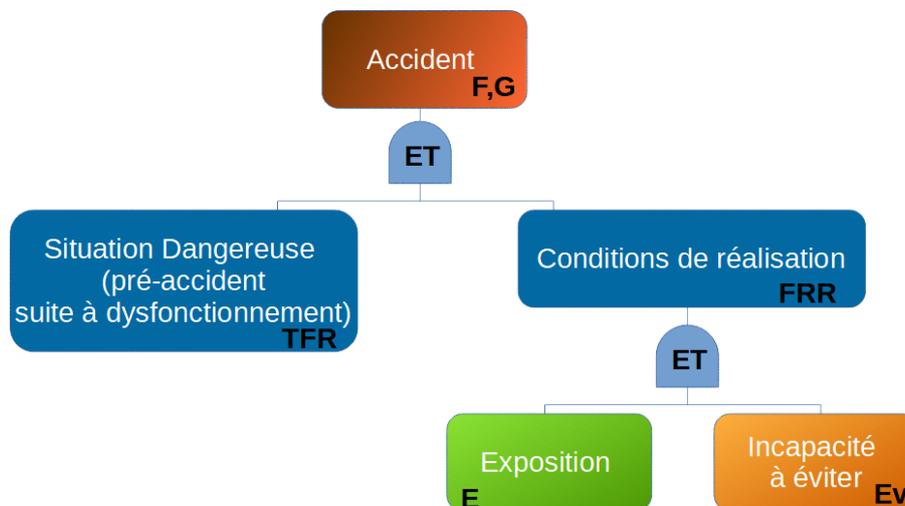


Figure 4 – Schéma des paramètres d'estimation du risque

La probabilité de réalisation des conditions de circulation est représentée par le facteur de réduction du risque (FRR). Celui-ci est la combinaison de l'exposition (E) au contexte nécessaire à la réalisation de l'accident (situation opérationnelle de conduite), et de l'incapacité des personnes impliquées à éviter l'accident (Ev).

Le facteur de réduction de risque (FRR) est le produit de l'exposition (E) et de l'évitabilité (Ev).

La fréquence d'occurrence d'un accident permet ainsi de graduer l'estimation du niveau de risque en ce qui concerne les événements aléatoires nécessaires à la réalisation de l'accident :

- L'estimation du risque associé à un scénario d'accident intégrant la défaillance aléatoire d'un équipement pourra ainsi intégrer la probabilité de dysfonctionnement de cet équipement (TFR). Par exemple, la diminution de la probabilité horaire de défaillance d'une carte électronique critique intégrée dans un feu de circulation communiquant permet de réduire le risque associé aux scénarios d'accident intégrant la défaillance du feu ;
- L'estimation du risque associé à un scénario d'accident intégrant un comportement spécifique d'un tiers pourra ainsi intégrer un paramètre traduisant le caractère « courant » ou « exceptionnel » de ce comportement au vu des données issues des observations (E). Par exemple, la probabilité que le conducteur d'un véhicule tiers en croisement perde le contrôle de son véhicule peut être estimée inférieure à la probabilité de non-respect d'une limitation de vitesse maximale autorisée.

Les niveaux des différents facteurs intervenant dans la fréquence d'occurrence doivent être estimés sur la base des données issues des circulations de véhicules routiers dans des conditions comparables, ou des données issues de situations comparables, en privilégiant l'estimation la plus prudente.

Les estimations conduisant à l'estimation de la fréquence d'occurrence doivent être tracées et documentées.

Prise en compte de l'exposition à la situation opérationnelle (E)

La métrique d'estimation de l'exposition est dérivée de l'échelle spécifiée par la norme ISO 26262:2018.

Classe d'exposition (E)	Description	Quantification dans le FRR ⁽¹⁾
E1	Très faible probabilité ou Moins d'une fois par an pour la majorité des véhicules	0,001
E2	Faible probabilité <1% du temps de circulation ou Quelques fois / an pour la majorité des véhicules	0,01
E3	Probabilité moyenne Entre 1 et 10 % du temps de circulation ou Une fois par mois ou plus pour la majorité des véhicules	0,1
E4	Probabilité élevée >10% du temps de circulation ou En moyenne presque à chaque trajet	1

Tableau 4 – classes d'exposition

⁽¹⁾ les valeurs de quantification du FRR données ici sont des valeurs standard liées aux seuils des classes d'exposition. Des valeurs de quantification plus précises peuvent être utilisées s'il existe des données significatives issues du REX (e.g. une exposition E4 pourrait être quantifiée à 0,33 pour le calcul du FRR, sur la base de l'analyse des données du REX)

L'exposition (E) traduit la probabilité que la situation opérationnelle nécessaire à la réalisation de l'accident, soit présente lors de la survenue de la situation dangereuse. Elle permet d'apprécier la concomitance temporelle entre une situation dangereuse et une situation opérationnelle, dont la combinaison peut conduire à un accident.

Selon le contexte de la situation analysée, l'exposition (E) peut être estimée en termes de durée d'exposition à la situation opérationnelle (proportion de temps où le véhicule du système est exposée à la situation) ou en terme de fréquence d'exposition à la situation (nombre de fois où le véhicule du système est exposé à la situation). Il convient d'utiliser l'approche la plus appropriée à la situation analysée.

La notion d'exposition ne s'applique que dans les cas où la concomitance temporelle de plusieurs événements indépendants a du sens (i.e. la concomitance entre l'instant d'apparition de la situation dangereuse et l'exposition à la situation opérationnelle).

Par conséquent, dans les cas où la situation dangereuse n'est pas limitée dans la durée, la classe d'exposition retenue doit être E4 (valeur d'exposition = 1) ; dans ce cas-là, il faut considérer qu'il y aura tôt ou tard concomitance entre situation dangereuse et situation opérationnelle.

Ceci peut être notamment le cas des situations dangereuses suivantes :

- Insuffisances fonctionnelles ;
- Cas où l'exposition à la situation opérationnelle génère de fait la situation dangereuse (par exemple, l'exposition doit être prise à 1 lors de l'analyse d'un accident « collision par temps de brouillard » dans le cas d'un véhicule qui n'est pas adapté pour circuler en condition de brouillard car dans ce cas, la condition « brouillard » est à la fois la situation dangereuse et la situation opérationnelle nécessaires à l'accident), etc.

Les valeurs d'exposition aux situations sont des éléments clé de l'estimation du risque et les valeurs retenues doivent être couvrantes par rapport aux conditions de circulation réelles rencontrées sur le parcours, que ce soit le parcours générique au stade du DCST ou le parcours réel au stade du DPS/DS.

La fixation des valeurs d'exposition devra ainsi être tracée et documentée pour permettre de vérifier au stade de l'analyse de sécurité du parcours (phases DPS/DS) que les valeurs d'exposition retenues au stade du système technique (phase DCST) sont bien couvrantes.

Prise en compte de l'évitabilité (Ev)

L'évitabilité (Ev) représente la capacité des personnes impliquées dans un scénario à éviter un accident, du fait de leur réaction opportune à la situation, c'est-à-dire la réalisation d'une action adaptée et réalisée à temps.

Les personnes impliquées dans le scénario d'accident d'un STRA peuvent être l'intervenant à distance du véhicule, les conducteurs éventuels des véhicules tiers éventuels, les personnes situées au voisinage du véhicule, et dans certains cas les personnes transportées.

Les moyens d'éviter l'accident peuvent notamment consister dans l'évitement ou l'arrêt.

L'évitabilité doit être estimée de manière prudente en traduisant la capacité réaliste des personnes impliquées à éviter l'accident, au vu notamment de leurs capacités et de leur situation.

Les critères permettant d'estimer l'évitabilité dépendent du scénario analysé et traduisent la capacité des personnes impliquées à mettre en place une parade. Sont à prendre par exemple en compte :

- La vitesse de survenue de l'évènement ;
- La perceptibilité de l'évènement (angles et distance de vision, masquages, signalisation, ...) ;
- La lisibilité de l'évènement (évènement classique ou improbable, anticipable ou non) ;
- La possibilité d'évitement (existe-t-il une parade réaliste au vu du scénario) ;
- Le profil des personnes impliquées (professionnels ou non, personnes formées ou non, capacités physiques, âge, niveau de vigilance, niveau de disponibilité, etc.).

Pour chaque scénario, la classe d'évitabilité prise en compte doit être cohérente avec le contexte des conditions de circulation réelles rencontrées sur le parcours, que ce soit le parcours générique au stade du DCST ou le parcours réel au stade du DPS/DS.

La métrique d'estimation de l'évitabilité est dérivée de l'échelle spécifiée pour la contrôlabilité par la norme ISO 26262:2018.

Classe d'évitabilité (Ev)	Description	Quantification dans le FRR
Ev0	Evitable en général	0
Ev1	Facilement évitable Evitable plus de 99 fois sur 100 en moyenne	0,01
Ev2	Normalement évitable Evitable plus de 90 à 99 fois sur 100 en moyenne	0,1
Ev3	Difficilement évitable Evitable moins de 90 fois sur 100 en moyenne	1

Tableau 5 – classes d'évitabilité

Si la notion d'évitabilité dérive de la notion de contrôlabilité définie par la norme ISO 26262:2018, il est important d'en souligner la principale différence. Celle-ci est liée à l'absence de conducteur dans le véhicule du STRA, voire également dans les véhicules tiers dans le cas des interactions entre les véhicules d'une flotte de véhicules automatisés par exemple.

Le conducteur du véhicule étant le vecteur essentiel de la contrôlabilité, sa suppression du scénario aura des conséquences importantes sur la capacité des personnes impliquées à éviter un accident.

7 Exigences de haut niveau

Les exigences de haut niveau sont des exigences génériques essentielles que doit respecter le STRA dans son ensemble.

Ces exigences s'appliquent en dehors de tout contexte d'accident ou de toute situation dangereuse, et sont complémentaires des exigences de sécurité spécifiques issues des analyses déductives et inductives présentées aux chapitres 8 et 9.

- Ces exigences doivent être prises en compte d'une part lors de la spécification du comportement attendu de la part du système, lors des analyses déductives et inductives ;
- D'autre part, ces exigences de haut niveau doivent être déclinées en une liste d'exigences détaillées, adaptées au système et à son contexte (parcours, conditions d'exploitation, conditions de circulation, etc.). Le respect de chacune de ces exigences doit faire l'objet d'une démonstration basée sur des éléments de preuve, issus d'analyses spécifiques et des différentes activités de la démonstration (analyses de sécurité, approche scénarios).

Les exigences de haut niveau présentées ici se veulent génériques et indépendantes des technologies mises en œuvre dans le système, ou des parcours de circulation. Elles sont déclinées à toutes les phases du projet en exigences spécifiques qui peuvent être de nature technique ou organisationnelle et qui peuvent donner lieu à des contraintes sur le parcours ou les conditions d'exploitation.

Le tableau ci-dessous dresse la liste des exigences de haut niveau applicables à un système de transport routier automatisé. Le respect de ces exigences ne préjuge pas du respect des éventuelles autres exigences applicables au système ou à ses équipements, comme par exemple celles qui seraient portées par le règlement UE 2019/2144 relatif aux prescriptions applicables à la réception par type des véhicules à moteur.

Les règles d'utilisation suivantes sont à prendre en compte :

- La liste ne peut pas être exhaustive et peut être enrichie dans le cadre du déroulement d'un projet spécifique.

- A l'inverse, même si les exigences présentées se veulent génériques, certaines peuvent ne pas être applicables sur un projet spécifique ; il convient dans ce cas de le tracer et de le justifier.
- Les exigences de haut niveau listées ici sont de niveau système ; néanmoins, certaines peuvent être déjà remplies par les exigences liées à l'homologation du véhicule intégré dans le système. Le choix a été fait de couvrir un périmètre plus large que le périmètre éventuellement strictement nécessaire.
- De manière générale, il a été vérifié que ces exigences de haut niveau ne sont pas en contradiction avec la réglementation applicable aux véhicules sans délégation de conduite.
- L'exigence de haut niveau n°11 concernant le « respect des règles de circulation applicables » est déclinée en différentes exigences qui visent uniquement à illustrer le contenu de l'exigence par des éléments plus concrets. Chacune de ces déclinaisons fait référence à un ensemble d'articles du code de la route. Il est important de noter que la liste de ces déclinaisons, donnée pour illustration, n'est pas exhaustive. De même il est important de noter que la liste des articles du code de la route précisée comme source n'est pas exhaustive. Le respect du code de la route qui définit les règles de circulation applicables est une exigence essentielle et celui-ci doit être respecté par les véhicules du système dans son intégralité. Il appartient à l'entité responsable de respecter cette exigence.

Guide de lecture du tableau ci-dessous

- Les exigences sont classées par grandes familles et par domaine ;
- L'intitulé se veut général et est décliné en une ou plusieurs exigences selon les cas ;
- La source est donnée à titre d'information pour remettre l'exigence dans son contexte. Les sources peuvent être issues de réglementations à l'état de projet dans l'attente de la publication des textes définitifs ;
- L'intitulé « Règlement UE ADS » fait référence au règlement d'exécution (UE) 2022/1426 de la commission du 5 août 2022 établissant des règles relatives à l'application du règlement (UE) 2019/2144 du Parlement européen et du Conseil en ce qui concerne les procédures uniformes et les spécifications techniques pour la réception par type des systèmes de conduite automatisée (ADS) des véhicules entièrement automatisés ;
- Des précisions sont données en dernière colonne pour guider la lecture.

Tableau 6.1 - Liste des exigences de haut de niveau - Exigences générales

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES GENERALES						
Conditions d'utilisation	1	Le système ne doit pas permettre la circulation des véhicules en mode de délégation de conduite si ce système est hors de son domaine d'emploi	1.1	Le système doit reconnaître la sortie de son domaine d'emploi	Code des transports Art. R. 3152-2 II	<p>On distingue les 2 cas :</p> <p>1 - sortie ODD ou défaillance entraînant incapacité à conduite en sécurité --> arrêt via MRM obligatoire.</p> <p>2 -dégradation des conditions de circulation ou défaillance n'entraînant pas une incapacité à conduire mais la nécessité de passage en fonctionnement dégradé (vitesse réduite). Ce fonctionnement dégradé a bien été évalué, et ce n'est donc pas une sortie de l'ODD. Les tâches de conduite restent assurées en sécurité moyennant ces conditions dégradées. Alors l'arrêt via MRM n'est pas obligatoire. L'exigence s'applique uniquement au cas n°1. Le domaine d'emploi est formalisé par différentes conditions de circulation telles que par exemple la localisation, les conditions météorologiques, les conditions de luminosité, l'état de la chaussée, le nombre de passagers et leurs conditions de transport, etc.</p> <p>On considère que le système sort de son domaine d'emploi "pour" (en raison d') un véhicule. Seul ce véhicule doit alors quitter le mode de délégation de conduite. L'arrêt du mode de délégation de conduite se fait selon une séquence qui débute par une MRM.</p> <p>Cf. règlement UE ADS Annexe II "3.1.5. Lorsque le système ADS atteint les limites de l'ODD, il effectue une MRM pour atteindre une MRC et en avertit l'opérateur à bord (le cas échéant)/l'opérateur à distance (le cas échéant)."</p>
			1.2	le système ne doit permettre l'activation du mode de délégation de conduite des véhicules que lorsque il est dans son domaine d'emploi	Code des transports Art. R. 3152-2 II	
			1.3	Lorsque le système sort de son domaine d'emploi, les véhicules concernés par la perte des condition d'emploi en sécurité doivent quitter le mode de délégation de conduite après avoir réalisé une MRM.		
			1.4	Le système doit informer l'exploitant de toute sortie de son domaine d'emploi, dans tous ses modes de fonctionnement	Code des transports Art. R. 3152-2 II	

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES GENERALES						
Conditions d'utilisation	2	Le système technique ne doit pas permettre la circulation des véhicules en mode de délégation de conduite si il est hors de son domaine de conception technique	2.1	Le système technique doit reconnaître la sortie de son domaine de conception technique	Code des transports Art. R. 3152-2 III	La sortie de son domaine de conception technique doit être détectée en priorité par des mesures techniques; s'il est démontré que cette exigence s'avère techniquement impossible, l'exigence de l'Art R. 3152-2 III doit être couverte par l'exigence de l'Art R. 3152-2 II relative à la détection de la sortie du domaine d'emploi.
			2.2	Le système technique doit informer l'exploitant de toute sortie de son domaine de conception technique, dans tous ses modes de fonctionnement	Code des transports Art. R. 3152-2 III	
	3	Le système doit être capable d'anticiper des sorties prévisibles des conditions d'utilisation	3.1	Le système technique doit être capable d'anticiper les sorties prévisibles de son domaine de conception technique		Il faut pouvoir anticiper et gérer correctement une sortie du domaine d'emploi lorsque celle-ci est prévisible. Cf. Règlement UE ADS Annexe II "3.1.3. Le système ADS doit pouvoir anticiper les sorties de l'ODD "
			3.2	Le système doit être capable d'anticiper les sorties prévisibles de son domaine d'emploi.		
Intégrité du système	4	Le système doit assurer que tout véhicule en mode de délégation de conduite respecte les règles du code de la route qui sont applicables, en tout lieu, et à tout instant.	4.1	Le système doit détecter les défaillances impactant potentiellement la sécurité.	Code des transports Art. R. 3152-2 II et III	
			4.2	Le système doit informer l'exploitant de toute défaillance impactant potentiellement la sécurité.		
			4.3	Le système ne doit pas permettre la circulation des véhicules en mode de délégation de conduite si une défaillance impactant la sécurité pour ces véhicules est survenue		La défaillance peut concerner un équipement du système technique situé hors du véhicule
			4.4	Le système ne doit pas permettre la circulation des véhicules en mode de délégation de conduite si une altération des équipements du système technique impactant la sécurité pour ces véhicules est survenue		Cas par exemple de collision sur un capteur du système technique qui modifierait son réglage

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES GENERALES						
Réponses du système	5	Le système doit être conçu pour éviter les accidents pouvant résulter de situations raisonnablement prévisibles dans son domaine d'emploi.			Code des transports Art. R. 3152-2 II	Le respect de cette exigence se traduit par les analyses de sécurité identifiant les risques raisonnablement prévisibles dans le domaine d'emploi et la définition des mesures les rendant acceptables.
	6	Le système technique doit être conçu pour éviter les accidents pouvant résulter de situations raisonnablement prévisibles dans son domaine de conception technique			Code des transports Art. R. 3152-2 III	
	7	Les réponses du système (actions incluant notamment les manœuvres à risque minimal, les manœuvres d'urgence, les manœuvres éligibles à l'intervention à distance, ..) ne doivent pas générer de risques supplémentaires inacceptables.			Code des transports Art. R. 3152-2 III	Réalisation par le système d'une action appropriée pour chaque situation visant à minimiser le risque global
	8	Lorsque le système détecte que les conditions permettant d'assurer son fonctionnement en sécurité ne sont plus remplies suite à une défaillance d'un équipement ou une sortie de son domaine d'emploi, le système doit assurer l'exécution d'une MRM par les véhicules concernés.				On distingue les 2 cas: 1 - sortie ODD ou défaillance entraînant incapacité à conduite en sécurité --> arrêt via MRM obligatoire. 2 -dégradation des conditions de circulation ou défaillance n'entraînant pas une incapacité à conduire mais la nécessité de passage en fonctionnement dégradé (vitesse réduite). Ce fonctionnement dégradé a bien été évalué, et ce n'est donc pas une sortie de l'ODD. Les tâches de conduite restent assurées en sécurité moyennant ces conditions dégradées. Alors l'arrêt via MRM n'est pas obligatoire. <u>L'exigence s'applique uniquement au cas n°1.</u>

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES GENERALES						
Réponses du système	9	Un véhicule ne peut quitter le mode de délégation de conduite que lorsqu'il est à l'arrêt.			Règlement UE ADS annexe 2 §4.1.2.2	Capacité du système à commander l'arrêt du véhicule et à quitter le mode de délégation de conduite, même en cas de défaillance. NB : on parle ici des défaillance uniquement car les insuffisances fonctionnelles impactant la sécurité du système sont considérées comme correspondant à des sorties d'ODD, et donc conduisant à des MRM. UE ADS annexe 2 §4.1.2.2 " Le système ADS exécute une MRM pour atteindre une MRC dans le cas d'une défaillance du système ADS et/ou d'un autre système du véhicule qui empêche le système ADS d'accomplir la DDT. "
	10	Le véhicule doit conserver la capacité de s'arrêter même en cas de défaillance sévère.			Règlement UE ADS annexe 1 §17.6.5 + annexe 2 §4	
Respect des règles de circulation applicables	11	Le système doit assurer que tout véhicule en mode de délégation de conduite respecte les règles du code de la route qui lui sont applicables, en tout lieu, et à tout instant.	11.1	Surveiller la situation du véhicule : respect PTAC, gabarit maxi, etc.	Code de la route R312-2, R312-10, R312-20, R313-21, etc.	Chaque déclinaison fait référence à un ensemble d'articles du code de la route. Il est important de noter que la liste de ces exigences donnée pour illustration n'est pas exhaustive. De même il est important de noter que le liste des articles du code de la route n'est pas exhaustive. Le respect du code de la route qui définit les règles de circulation applicables est une exigence essentielle et celui-ci doit être quoiqu'il en soit respecté dans son intégralité. Il appartient au porteur de projet de respecter cette exigence.
			11.2	Contrôler régulièrement l'état du véhicule: éclairage, pneumatiques, freins, etc.	Code de la route R313-1 à R313-19, R314-1, R315-1, etc.	
			11.3	Mettre en service l'éclairage du véhicule: par exemple les feux de route, les feux de croisement, etc.	Code de la route R416-4 R416-5 R416-6 R416-7 R416-8 R416-9	

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES GENERALES						
Respect des règles de circulation applicables			11.4	Se signaler vis-à-vis des tiers : par exemple en cas de freinage d'urgence, en cas de circulation à vitesse réduite, en cas d'arrêt dans une zone dangereuse, en cas de changement de direction, etc.	Code de la route R313-17-1 R416-18 R416-19 R412-10, etc.	<p>Le respect du code de la route du pays de circulation est l'une des exigences portées au niveau véhicule dans le cadre de l'homologation, éventuellement via des exigences exportées (cf. règlement UE ADS Annexe II 1.3. " Le système ADS doit respecter les règles de circulation du pays d'utilisation ").</p> <p>La Liste d'exigences finales au niveau STRA se veut de niveau général système. Peu importe par quelle partie du process c'est porté. Par exemple : certaines seront couvert via HOMOLOGATION ADS (celles pour lesquelles le véhicule automatisé est auto-suffisant). Toutes celles pour lesquelles le véhicule automatisé n'est pas autosuffisant, doivent être évaluées sur les couches SYSTEME TECHNIQUE et STRA. Donc l'évaluateur est soit l'HOMOLOGATEUR, soit l'OQA STRA.</p> <p>Toute évolution du Code de la route devra être prise en compte.</p>
			11.5	Adopter un comportement adapté: respecter les distances de sécurité, adapter le comportement en cas de feux de détresse ou d'usage de gyrophare par les tiers, adapter sa vitesse aux circonstances et à l'environnement sans gêner la marche normale des autres véhicules, etc.	Code de la route R412-12, R412-11-1, R413-17 R413-18 R413-19, etc.	
			11.6	Se soumettre aux contrôles routiers: respecter les injonctions, mettre à disposition les documents du véhicule, etc.	Code de la route L233-1 R233-1 R233-2 R233-3	
			11.7	Circuler uniquement sur les voies autorisées : respecter les marquages au sol des voies de circulation, ne pas circuler sur les voies interdites, respecter les sens de circulation interdits ou obligatoires, etc.	Code de la route R412-7 R412-8 R412-19 R412-22 R412-23 R412-24 R412-26 R411-17 R412-28 R412-26, etc.	
			11.8	Se positionner latéralement sur la voie de circulation de manière adaptée: en nominal, en croisement	Code de la route R412-9 R414-1, etc.	
			11.9	Respecter les priorités : intersections avec priorités à droite, avec STOP, avec céder le passage, sortie de stationnement, entrée sur giratoire, etc.	Code de la route R415-5, R415-6 R415-7 R415-9 R415-10 etc.	
			11.10	Respecter les feux tricolores	Code de la route R412-30 R412-31	

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES GENERALES						
Respect des règles de circulation applicables			11.11	Respecter les règles de franchissement des passages à niveau	Code de la route R422-3	
			11.12	Respecter la priorité des piétons	Code de la route R415-11	
			11.13	Respecter la priorité dans les cas particuliers : croisement des véhicules d'intérêt général, croisement si voies de largeur insuffisante, véhicules prioritaires en toutes circonstances, véhicule de TC quittant son arrêt, cortèges, etc.	Code de la route R414-2 R414-3 R415-12 R412-11 R412-15 etc.	
			11.14	Respecter les limitations de vitesses	Code de la route R413-1 R413-2 R413-5 R413-10 etc.	
			11.15	Respecter les règles de comportement sur les configurations spécifiques: intersections, TAD, TAG, aux entrées/sorties d'autoroute, etc.	Code de la route R415-1 R415-2 R415-3 R415-4 R421-3 R421-4, etc.	
			11.16	Respecter les règles lors du dépassement	Code de la route R414-4 R414-5 R414-6 R414-7 R414-8 R414-10 R414-12 R414-16 etc.	
			11.17	Arrêter le véhicule uniquement sur les emplacements adaptés: sur accotement ou sur voie de droite, hors des passages piétons, hors des zones de danger ou gênantes, hors autoroute, etc.	Code de la route R417-1 R417-4 R417-5 R417-9- R417-10 R417-11 R421-7	
			11.18	S'arrêter et alerter en cas d'accident de la circulation impliquant le véhicule	Code de la route R231-1	

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES GENERALES						
Respect des règles de circulation applicables			11.19	Respecter toute autre règle applicable	Code de la route	
Respect des règles d'aménagement et de signalisation applicables	12	Les équipements et les aménagements de la voirie issus d'exigences exportées par le système (soit spécifiques au système, soit spécifiés pour le système mais d'un usage partagé avec les autres usagers) doivent respecter les règles localement applicables.				Exemple : la géométrie d'un carrefour modifié dans le cadre du déploiement d'un STRA doit respecter les règles afin de ne pas induire de risque pour les autres usagers ; un feu pour les autres usagers ajouté spécifiquement pour le STRA doit être implanté de manière à être perceptible par ces usagers.
Protection d'accès	13	Les parties du système STRA auxquelles l'accès par des tiers peut présenter un enjeu pour la sécurité, ne doivent être accessibles qu'aux personnes autorisées.			FRAV-23-05 Rev2 GRVA §4.4.2.	FRAV-23-05 Rev2 GRVA "4.4.2. The ADS shall be designed to protect against unauthorized access." FRAV-23-05 Rev2 GRVA Table 1-17 "The measures ensuring protection from an authorized access should be provided in alignment with engineering best practices."

Tableau 6.2 - Liste des exigences de haut de niveau - Exigences relatives aux manœuvres des véhicules

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES RELATIVES AUX MANOEUVRES DES VEHICULES						
Comportement des véhicules	14	Les véhicules du système doivent avoir un comportement de conduite compréhensible par les autres usagers de la route			Cf. également exigences 11.4 et 11.8 du code de la route	- signalisation : cf. code de la route (lumineuse, sonore, etc.) - qualité des trajectoires: anticipées, fluides - fluidité du contrôle longitudinal - positionnement dans la voie
	15	Les véhicules du système doivent avoir un comportement de conduite prudent respectant les distances de sécurité appropriées	-		Règlement UE ADS Annexe II §1.1.2. Cf. également exigence 11.5 du code de la route	Règlement UE ADS Annexe II "1.1.2. Dans le cadre de la DDT, le système ADS doit pouvoir: ... (b) maintenir des distances appropriées avec les autres usagers de la route en contrôlant le déplacement longitudinal et latéral du véhicule; ;..."
	16	Les véhicules du système doivent avoir une vitesse adaptée et homogène vis-à-vis des autres usagers, et de leur environnement de conduite.			Règlement UE ADS Annexe II §1.1.2. Cf. également exigence 11.5 du code de la route	Règlement UE ADS Annexe II "1.1.2. Dans le cadre de la DDT, le système ADS doit pouvoir: (a) fonctionner à des vitesses sûres et respecter les limitations de vitesse applicables au véhicule; ..."
	17	Les véhicules du système doivent adapter leur comportement au contexte en privilégiant la sécurité des personnes			Règlement UE ADS Annexe II §1.1.2.	Règlement UE ADS Annexe II "1.1.2. Dans le cadre de la DDT, le système ADS doit pouvoir:... c) adapter son comportement aux conditions de trafic environnantes (par exemple, en évitant de perturber le flux du trafic) d'une manière appropriée privilégiant la sécurité; d) adapter son comportement en fonction des risques pour la sécurité et en accordant la plus haute priorité à la protection de la vie humaine.

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES RELATIVES AUX MANOEUVRES DES VEHICULES						
Gestion des cas d'accident de la circulation	18	En cas d'accident de la circulation impliquant un véhicule, - le véhicule doit détecter le choc en dynamique ou en statique (qu'il soit ou non à l'arrêt) - les actions adéquates doivent être mises en œuvre : - arrêt du véhicule (MRM par exemple) ou maintien de l'arrêt du véhicule; - une fois à l'arrêt, le véhicule doit quitter le mode de délégation de conduite. - alerter la supervision - interdiction du retour en mode délégation de conduite tant que les vérifications nécessaires n'ont pas été conduites - permettre l'accès aux données (ordonnance 2021-442 du 14 Avril 2021)			Règlement UE ADS Annexe II §2.1.5	Cas de collision à l'arrêt à prendre en compte Règlement UE ADS Annexe II "2.1.5 Dans le cas d'un accident de circulation impliquant le véhicule entièrement automatisé, le système ADS doit viser à arrêter le véhicule entièrement automatisé et à effectuer une manœuvre de risque minimal pour atteindre l'état de risque minimal. La reprise du fonctionnement normal du système ADS ne doit pas être possible avant que l'état de fonctionnement sûr du véhicule entièrement automatisé ait été confirmé par les autocontrôles du système ADS et/ou l'opérateur à bord (le cas échéant) ou l'opérateur d'intervention à distance (le cas échéant). "
MRM	19	Toute MRM engagée par un véhicule, doit être signalée aux passagers du véhicule, aux autres usagers de la route et à l'exploitant.			Règlement UE ADS Annexe II 5.2	Règlement UE ADS Annexe II 5.2 " Le système ADS signale son intention de placer le véhicule entièrement automatisé dans une MRC aux occupants du véhicule entièrement automatisé ainsi qu'aux autres usagers de la route conformément aux règles de circulation (par exemple, en activant les feux de détresse). "
	20	Après l'exécution d'une manœuvre à risque minimal, la remise en mouvement véhicule en mode de délégation de conduite ne peut se faire qu'après vérification que les conditions ayant conduit à la manœuvre à risque minimal ont disparu .			Règlement UE ADS annexe II 5.3	Règlement UE ADS annexe II 5.3 : " Le véhicule entièrement automatisé ne quitte la MRC qu'après confirmation par les autocontrôles du système ADS ou/et par l'opérateur à bord (le cas échéant) ou l'opérateur d'intervention à distance (le cas échéant) que la ou les causes de la MRM ne sont plus présentes. "

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES RELATIVES AUX MANOEUVRES DES VEHICULES						
Arrêt d'urgence	21	Toute manœuvre d'urgence engagée par un véhicule, doit être signalée aux passagers du véhicule, aux autres usagers de la route et à l'exploitant.			-	Le retour en mode délégation de conduite exige une procédure. Signalisation spécifique / autres usagers Information de l'exploitant
	22	Suite à une manœuvre d'urgence conduisant à un arrêt du véhicule, le véhicule doit se signaler aux autres usagers de la route ainsi qu'à la supervision du système			-	

Tableau 6.3 - Liste des exigences de haut de niveau - Exigences pour les passagers

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES POUR LES PASSAGERS						
Evacuation	23	Le système doit assurer que les passagers sont en mesure d'évacuer le véhicule dans les meilleures conditions possibles et ce dans toutes les situations prévisibles pour le parcours.				<p>Note : lorsque des zones du parcours / zone dégradent la capacité à assurer l'évacuation en sécurité, alors une stratégie d'évacuation doit être définie et formalisée via le SGS</p> <p>Les aspects suivants doivent notamment être pris en compte :</p> <ul style="list-style-type: none"> - cas de l'occurrence d'un autre danger empêchant l'évacuation (ex. incendie, collision ayant bloqué les ouvrants, etc.) - évacuation difficile suite à un dimensionnement insuffisant ou nombre insuffisant des issues de secours ou ouvrants - mauvaise d'information sur les possibilités d'ouverture des portes et/ou issues de secours - évacuation des PMR, même isolés - mouvement panique dans le véhicule du système rendant l'évacuation difficile - évacuation impossible en raison de poteaux ou d'obstacles - défaillance du système de communication avec la supervision - défaillance de l'information de position du véhicule envoyée à la supervision suite à un choc <p>A noter que dans le cadre de cette exigence, il faut que le véhicule permette des évacuations en dehors des portes (vitre et marteau à disposition). Voir la réglementation à ce sujet (notamment l'arrêté du 2 juillet 1982 relatif aux transports en commun de personnes, pour</p>

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES POUR LES PASSAGERS						
Evacuation						<p>dans le cas du transport de passagers au moyen d'un véhicule qui comporte plus de neuf places assises, y compris celle du conducteur).</p> <p>Les conditions d'évacuation doivent être adaptées selon que le véhicule a conservé ou non sa capacité à circuler.</p>
	24	Chaque véhicule du système doit permettre l'évacuation de ses passagers par les secours ou le personnel d'exploitation depuis l'extérieur du véhicule				<p>Permettre l'ouverture des ouvrants depuis l'extérieur par les secours ou du personnel d'exploitation</p> <p>Gérer la protection contre les actes de malveillance</p>
Demande d'arrêt passager	25	Chaque véhicule du système doit donner la possibilité à ses passagers de demander l'arrêt du véhicule en cas d'urgence.			Règlement UE ADS Annexe II § 6.3	<p>Les aspects suivants doivent notamment être pris en compte :</p> <ul style="list-style-type: none"> - accessibilité de la commande - informations sur la commande - traitement de la commande - gestion de la phase d'arrêt <p>règlement UE ADS Annexe II 6.3 "</p> <p>Le système ADS doit fournir aux occupants du véhicule le moyen de demander une manœuvre de risque minimal pour arrêter le véhicule entièrement automatisé. En cas d'urgence:</p> <ul style="list-style-type: none"> a) pour les véhicules équipés de portes à ouverture automatique, le déverrouillage des portes s'effectue automatiquement dès que cela peut se faire en toute sécurité; b) un moyen doit être donné aux passagers pour sortir d'un véhicule à l'arrêt (ouverture des portes ou via une sortie d'urgence).

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES POUR LES PASSAGERS						
Communication passager	26	Chaque véhicule du système doit donner la possibilité à ses passagers du véhicule du système de communiquer avec la supervision du système			Règlement UE ADS annexe II §6.2	<p>Les exigences suivantes doivent notamment être prises en compte :</p> <p>possibilité d'alerte par les passagers en cas de situation critique (malaise passager, incendie à bord, ...)</p> <p>Peut être complété pour les cas de défaillance du système de communication par une signalétique et n° de téléphone à appeler en cas d'urgence</p> <p>UE ADS annexe II §6.2 " Si un opérateur d'intervention à distance fait partie du concept de sécurité du système ADS, le véhicule entièrement automatisé doit fournir aux occupants du véhicule les moyens d'appeler un opérateur d'intervention à distance via une interface audiovisuelle à bord du véhicule entièrement automatisé. Des signes non ambigus doivent être utilisés pour l'interface audiovisuelle (par exemple, ISO 7010 E004). »</p>

Tableau 6.4 - Liste des exigences de haut de niveau - Exigences pour le personnel opérateur à distance / supervision

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES POUR LE PERSONNEL OPERATEUR INTERVENANT A DISTANCE / SUPERVISION						
Commandes opérateur	27	Le système doit donner la possibilité au personnel opérateur intervenant à distance , de commander une MRM d'un véhicule selon des modalités prédéfinies adaptées.				Les modalités de mise à l'arrêt sont définies au niveau du SGS du STRA
	28	Le système doit donner la possibilité au personnel opérateur intervenant à distance, de commander la mise à l'arrêt de l'ensemble des véhicules du système selon des modalités prédéfinies adaptées.				On pense ici par exemple aux exigences de haut niveau associées à des situations concernant l'ensemble du système: cas d'attaque cyber , cas d'évènement météo de grande ampleur et soudain. La mise à l'arrêt inclut la réalisation d'une MRM ou un autre type d'arrêt.
	29	Le système doit donner la possibilité au personnel opérateur intervenant à distance de commander l'ouverture des portes motorisées du véhicule, dans des conditions adaptées.				cf règlement UE ADS annexe II 6.5 " Si un opérateur d'intervention à distance fait partie du concept de sécurité du système ADS, il doit être possible, pour l'opérateur d'intervention à distance, d'ouvrir à distance la porte de service à commande électrique. "

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES POUR LE PERSONNEL OPERATEUR INTERVENANT A DISTANCE / SUPERVISION						
Communication depuis la supervision	30	Le système doit donner la possibilité au personnel opérateur intervenant à distance de communiquer avec les passagers du véhicule du système				<p>Les exigences suivantes doivent notamment être prises en compte : possibilité de transmission de consigne aux passagers en cas de besoin, notamment :</p> <ul style="list-style-type: none"> - sortie du système de son domaine d'emploi - interruption ou modification du service - .. <p>Cf. également règlement UE ADS annexe II 6.4 "</p> <p>Si un opérateur d'intervention à distance fait partie du concept de sécurité de l'ADS, le véhicule entièrement automatisé doit fournir des moyens de vision (par exemple, des caméras conformément au chapitre 6 de ISO16505:2019) de l'espace occupants à l'intérieur du véhicule et des alentours du véhicule afin de permettre à l'opérateur d'intervention à distance d'évaluer la situation à l'intérieur et à l'extérieur du véhicule.."</p>

Tableau 6.5 - Liste des exigences de haut de niveau - Exigences pour l'IHM supervision

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES POUR L'IHM SUPERVISION						
IHM	31	L'IHM du système doit être conçue de manière à limiter les risques de mésusages par le personnel d'exploitation.				<ul style="list-style-type: none"> - lecture rapide de la situation du système, d'un véhicule - pertinence des informations, priorisation - champ de vision <p>Concerne à la fois l'affichage des informations (volume et présentation des informations, priorisation, etc.) et les procédures de commande (par exemple : principe de double saisie ou d'acquiescement)</p> <ul style="list-style-type: none"> - seule une action délibérée de la part de l'opérateur doit permettre d'effectuer, modifier, interrompre une manœuvre (cf. définition intervention à distance) - seule une action délibérée de la part de l'opérateur doit permettre d'acquiescer des manœuvres proposées par le système (cf. définition intervention à distance)
	32	La mise en service ou la remise en service du mode de délégation de conduite doit requérir une action spécifique et non ambiguë de la part de l'opérateur.				Y compris suite à un arrêt d'urgence ou suite à une MRM (reprise en mode automatique) <ul style="list-style-type: none"> - seule une action délibérée de la part de l'opérateur doit permettre d'activer le mode de conduite automatique (cf. "Automated driving safety validation: proposals from the French Eco-system" janv 2020 - TR-01)
Information pour le personnel opérateur	33	Le personnel opérateur intervenant à distance doit pouvoir disposer des informations nécessaires concernant l'état du système.				<p>L'état du système comprend toutes les informations pertinentes relatives au système: état de la délégation de conduite, vitesse, état des portes, etc.</p> <ul style="list-style-type: none"> - connaissance du mode de conduite (cf. "Automated driving safety validation: proposals from the French Eco-system" janv 2020 - T03)

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES POUR L'IHM SUPERVISION						
Information pour le personnel opérateur	34	Le personnel opérateur intervenant à distance doit avoir les moyens de percevoir l'environnement du véhicule avec une qualité (précision, portée, latence) compatible avec ses missions d'intervention à distance.			Règlement UE ADS annexe II § 6.4	Règlement UE ADS annexe II : "6.4. Si un opérateur d'intervention à distance fait partie du concept de sécurité de l'ADS, le véhicule entièrement automatisé doit fournir des moyens de vision (par exemple, des caméras conformément au chapitre 6 de ISO16505:2019) de l'espace occupants à l'intérieur du véhicule et des alentours du véhicule afin de permettre à l'opérateur d'intervention à distance d'évaluer la situation à l'intérieur et à l'extérieur du véhicule."
	35	La supervision doit recevoir une information : - en cas de sortie du domaine d'emploi (cf. 1.4) - en cas de sortie de son domaine de conception technique (cf. 2.2) - en cas de défaillance impactant potentiellement la sécurité (cf. 4.1) - en cas d'accident de la circulation impliquant un véhicule du système (cf. 18) - en cas d'engagement d'une MRM par un véhicule (cf. 19) - en cas d'arrêt d'urgence d'un véhicule (cf. 21) - en cas de demande d'arrêt d'un véhicule par un passager (cf. 25) - en cas de demande communication par un passager (cf. 26)				Règlement UE ADS Annexe II "3.1.5. Lorsque le système ADS atteint les limites de l'ODD, il effectue une MRM pour atteindre une MRC et en avertit l'opérateur à bord (le cas échéant)/l'opérateur à distance (le cas échéant). L'arrêt d'urgence est l'arrêt du véhicule suite à une manœuvre d'urgence : cf. règlement d'homologation (seuil de gamma à définir).
Information des tiers	36	Le système doit permettre aux tiers, aux forces de l'ordre, aux services de secours de connaître l'état de délégation de conduite d'un véhicule			FRAV-23-05 Rev2 GRVA Table1-5	- y compris pour les véhicules suiveurs - FRAV-23-05 Rev2 GRVA Table1-5 "The ADS shall signal its operational status (active/inactive) as needed."

Domaine	N°	Intitulé	n°	Déclinaisons	source	Précisions
EXIGENCES POUR L'IHM SUPERVISION						
Information des tiers	37	Il doit être possible pour les forces de l'ordre en présence d'un véhicule de communiquer avec la supervision du système			Projet d'arrêté Navettes Urbaines Automatisées	Projet arrêté Navettes Urbaines Automatisées : "7.7.9.6 En cas de besoin, la navette doit : 7.7.9.6.2 porter, à l'extérieur et de façon clairement visible le pictogramme ci-dessous permettant aux forces de l'ordre ou à tous passagers de communiquer avec l'opérateur depuis l'extérieur "

8 Analyse déductive (analyse préliminaire des dangers)

8.1 Présentation

L'analyse déductive met en œuvre une démarche partant des effets vers les causes. Elle a pour but d'identifier les combinaisons de causes possibles d'un accident. Cette analyse part des dangers pour en déterminer les causes possibles (type Analyse préliminaire des dangers ou APD)

Le point de départ de l'analyse déductive est l'accident. L'analyse explore par une approche descendante toutes les causes et combinaisons de causes pouvant conduire à cet accident (analyse des causes). L'analyse déductive n'analyse pas les causes d'accident de type cyber-attaque. La prise en compte de ces événements fait l'objet d'un guide spécifique.

Chaque scénario conduisant à l'accident fait alors l'objet d'une analyse et d'une estimation de la gravité de ses conséquences. Cette analyse tient compte des éventuels facteurs liés au contexte (situation, facteurs aggravants éventuels liés par exemple à l'absence de conducteur et de personnel et au caractère collectif du système de transport, etc.).

Cette analyse permet de définir un ensemble d'exigences de sécurité, techniques et/ou organisationnelles, qui doivent être cohérentes avec les exigences de haut niveau présentées au chapitre 7.

Ces exigences peuvent consister dans l'application d'un référentiel externe pour lequel il a été démontré qu'il couvrait le risque considéré et son contexte (démonstration de type 3a du guide d'application GAME) ou dans la mise en œuvre de mesures spécifiques après avoir démontré que leur combinaison permettait de ramener le risque résiduel à un niveau acceptable (démonstration de type 3b du guide d'application GAME).

- Dans le cas de l'application d'un référentiel externe (démonstration de type 3a), les exigences de sécurité à mettre en œuvre sont celles issues du référentiel externe ;
- Dans le cas d'une analyse explicite (démonstration de type 3b), l'évaluation de la fréquence d'occurrence de chaque scénario permet d'estimer sa criticité et de définir les exigences de sécurité à mettre en œuvre.

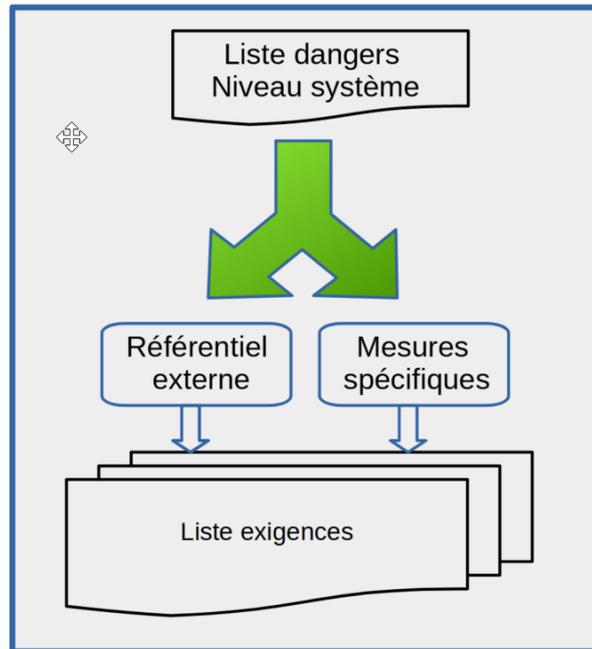


Figure 5 – Schéma de l'analyse déductive

Objectifs

- L'analyse déductive permet de construire les scénarios, d'estimer les risques au niveau du système, et d'explicitier leur prise en compte.
- L'analyse déductive permet d'estimer chaque risque et de spécifier la liste des exigences à mettre en œuvre.
- En décrivant les arbres des causes amenant à chaque accident de niveau système, l'analyse déductive est un outil permettant d'identifier et de tracer les scénarios pour lesquels il est nécessaire de démontrer le respect des objectifs de sécurité quantitatifs, globaux ou spécifiques.

Phases du projet

- L'analyse déductive est une démarche de haut niveau, globale au système qui est mise en œuvre d'abord au stade du DCST pour un système technique générique associé à un domaine de conception technique connu. Les exigences qu'elle permet de spécifier touchent à la conception et à l'architecture du système technique, aux contraintes exportées par le système technique vers le type de parcours visé et vers ses conditions d'exploitation. Ces différents éléments définissent le domaine de conception technique du système technique repris dans la déclaration de fonctionnalités et de sécurité prévue par le décret STRA (2021-873 du 29 juin 2021).
- Ensuite, au stade du DPS et du DS, les spécificités liées au déploiement de niveau système sur le parcours réel sont analysées au travers de l'analyse de sécurité du parcours. L'analyse déductive doit alors être complétée au vu des conditions de circulation sur le parcours spécifique sur lequel le système technique est déployé, afin de prendre en compte les scénarios spécifiques.

L'approche doit permettre in fine de vérifier que l'ensemble des risques spécifiques au projet réel a bien été pris en compte dans l'analyse faite au niveau générique et que les objectifs de sécurité sont bien respectés pour le système déployé.

8.2 Trame

Les tableaux suivants fournissent à titre uniquement illustratif un exemple de trame décrivant les différents éléments de l'analyse déductive.

ACCIDENT POTENTIEL DE NIVEAU STRA				IDENTIFICATION DE LA SITUATION DANGEREUSE						
#	Type	#	Sous-type	Type de section d'infrastructure	Dynamique (des acteurs de la situation)	Eléments complémentaires de contexte	Illustration(s) de la situation étudiée	SYNTHESE de la situation dangereuse (SD) de niveau système		Personne(s) exposée(s)
								Ref	Description	
1	Collision	1.1	Collision avec usager vulnérable de la voirie (cycliste, piéton, etc.)	Section courante avec zone de travaux		Circulation d'un véhicule du système sur une zone à risque qui aggrave les conséquences potentielles d'un événement redouté	Collision avec piéton traversant la chaussée sur un passage piéton suite à sa perception tardive (masquage par engin de chantier). La distance de freinage a de plus été allongée du fait de la chaussée localement déformée par les travaux en cours.			
en lien avec Tableau 8				en lien avec tableaux 9 et 10						

CAUSE(S) POSSIBLE(S)			EVALUATION INITIALE DES RISQUES						TYPE D'APPROCHE GAME		
Contributeur potentiel = Composant(s) concerné(s) du STRA	Type de cause(s) possible(s)	Description	Gravité		Exposition		Evitabilité		Estimation du risque <i>(optionnel)</i>	Type	Description
			Classe	Commentaire(s)	Classe	Commentaire(s)	Classe	Commentaire(s)			
SGS	Particularités de parcours, c'est à dire les caractéristiques spécifiques d'un parcours/zone (ou d'un type de parcours) qui génèreraient ou amplifieraient des possibilités d'accidents, ou qui nécessiteraient une réponse particulière du système	Circulation d'un véhicule du système sur une zone de travaux									
en lien avec Tableau 8											

Tableau 7.1 – trame analyse déductive

EXIGENCES DE SECURITE		EVALUATION FINALE DES RISQUES						
Catégorie	Description	Gravité		Exposition		Evitabilité		Evaluation du risque
		Classe	Commentaire(s)	Classe	Commentaire(s)	Classe	Commentaire(s)	
- vis à vis angle de perception	- spécifier des aménagements type compatibles avec les capacités du système							
- vis-à-vis de la gestion des zones de travaux	- encadrer l'organisation des zones de travaux au voisinage du parcours							
	- exigences pour le gestionnaire de voirie							
	- réduire la vitesse sur les zones de travaux							
- vis à vis de l'état de la chaussée	- contrôle quotidien de l'état du parcours avant la première circulation							
	- spécifier des seuils de déformation maximale de la chaussée							

Tableau 7.2 – trame analyse déductive

8.3 Éléments d'entrée de l'analyse déductive

Les différents tableaux suivants fournissent des éléments d'entrée de l'analyse déductive :

- Tableau 8 : Liste des accidents de niveau système ;
- Tableau 9 : Liste de points d'attention pour les causes, à prendre en compte lors de la détermination des causes possibles des accidents (arbres de cause) ;
- Tableau 10 : Liste de situations de vie pouvant être rencontrées au sein d'un système et qui doivent être prises en compte dans les scénarios ;
- Tableau 11 : Liste des éléments de contexte d'un système et pouvant influencer sur les exigences de réponse aux dangers.

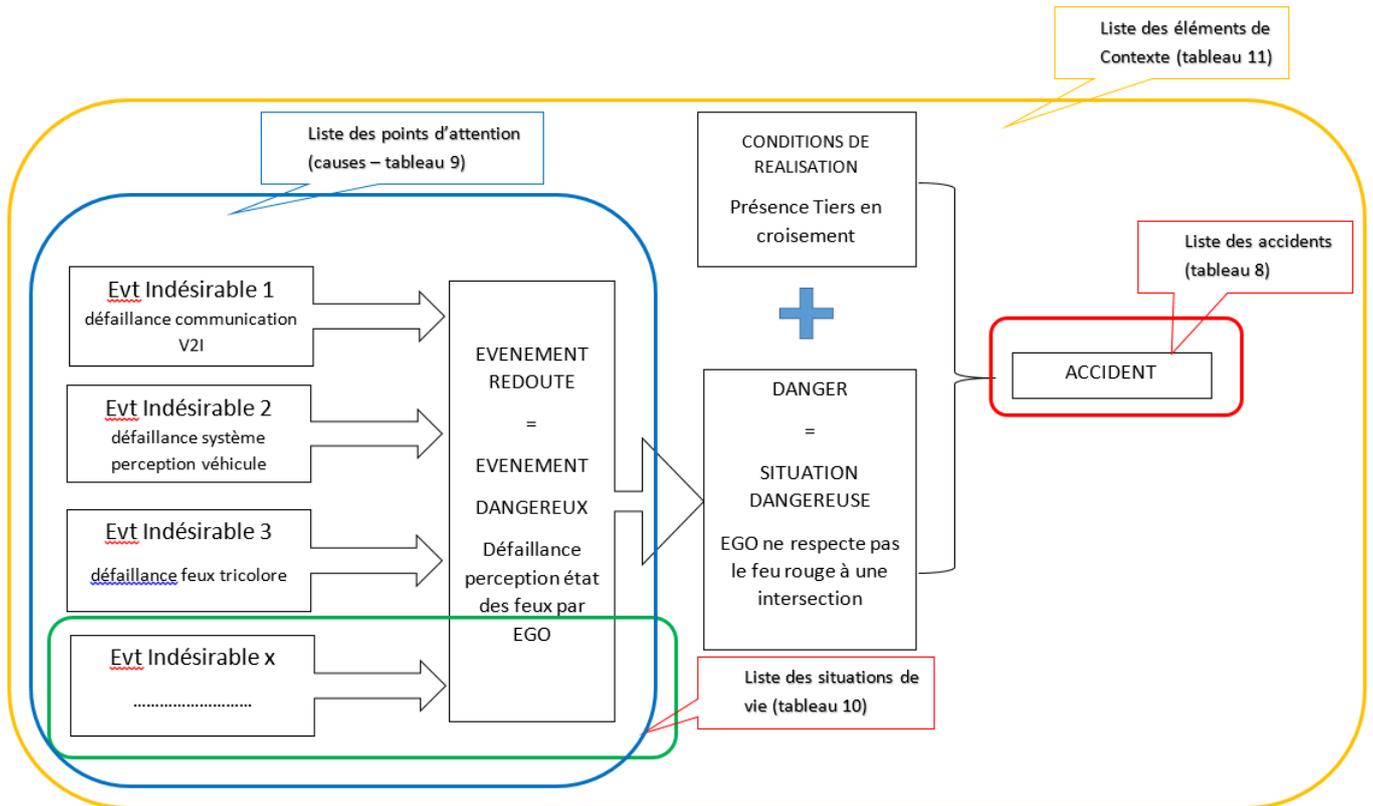


Figure 6 - Organisation des tableaux guides de l'analyse déductive

Les tableaux suivants donnent des listes génériques des différents éléments à prendre en compte qui se veulent indépendants des technologies mises en œuvre dans le système et des types de parcours de circulation.

Ces tableaux ont pour objectif de favoriser la recherche d'exhaustivité lors des analyses de risques, ainsi que la structuration de ces analyses. Elles doivent toutefois être adaptées et complétées si nécessaire par les porteurs de projet au vu des spécificités de chaque système.

L'analyse construite sur la base de ces 4 tableaux doit couvrir l'ensemble du domaine d'emploi du STRA, en prenant en compte :

- Toutes les typologies d'objets en interaction prévisibles avec les composants du système au vu du domaine d'emploi du STRA, comme notamment :
 - o Les usagers du système (ex. piétons, personnes à mobilité réduite, avec poussette, avec bagages lourds, avec engin de déplacement personnel, etc.) présents dans les véhicules du système ou les stations ;

- Les usagers de la route vulnérables (ex. piétons, personnes à mobilité réduite, avec poussette, avec bagages lourds, avec engin de déplacement personnel, avec cycle, cyclistes, etc.) présents dans l'environnement de circulation des véhicules du système ;
 - Les usagers de route (ex. les différents types de véhicules routiers) ;
 - Les autres systèmes de transports (transports guidés ou ferrés, ...) ;
 - Les obstacles / objets du parcours (permanent et non permanent) ;
 - Les masques à la visibilité ;
- Toutes les typologies d'évènements en interaction prévisibles avec les composants du système au vu du domaine d'emploi du STRA (en lien avec ses descripteurs) :
 - Les conditions météorologiques ;
 - Les conditions de luminosité ;
 - L'état de l'infrastructure ;
 - Etc.
 - Tous les modes de fonctionnement des différents composants du système (ex. pour les véhicules : phase d'utilisation en mode manuel (le cas échéant), phase de conduite en mode automatisé, phase d'intervention à distance (le cas échéant), etc.)
 - Toutes les situations de vie du système au vu de son domaine d'emploi (cf. tableau 10)

Les règles suivantes doivent être respectées lors de l'utilisation des tableaux :

- Les listes ne sont pas exhaustives et ont vocation à être enrichies dans le cadre du déroulement d'un projet.
- A l'inverse, même si les éléments présentés se veulent génériques, certaines peuvent ne pas être applicables sur un projet spécifique ; il conviendra dans ce cas de le tracer et de le justifier.
- Un type d'accident peut être la conséquence d'un autre type d'accident dans le cadre d'un scénario : par exemple, une collision peut survenir suite à une sortie de route du véhicule, un incendie peut survenir suite à une collision, etc. L'analyse peut alors prioriser le traitement de l'accident initial de manière à mettre en place les mesures de réduction du risque visant à s'en prémunir.
- Certains accidents présentés dans le tableau 8 pourront faire l'objet d'un regroupement si l'analyse montre que leur traitement est identique.

Tableau 8
Liste des accidents de niveau système

TYPOLOGIE	ID	ACCIDENTS POTENTIELS	COMPLEMENTS (éventuels)	EXEMPLES (non exhaustifs)
Collision	1.1	Collision avec usager vulnérable de la voirie (cycliste, piéton, etc.)	Les cas de collision active "collision du véhicule du système contre" et passive "collision du véhicule du système par ..." doivent notamment être envisagés	
	1.2	Collision (latérale/frontale) contre un obstacle massif (containers, animaux, chute d'arbres, etc.)	Les cas suivants doivent notamment être envisagés : - collision avec des obstacles fixes et permanents - collision avec des obstacles non-permanents fixes ou mobiles	Collision avec obstacles fixes permanents : murs, barrières, ... Collision avec obstacles fixes non-permanents : branche d'arbre, containers, ... Collision avec obstacles mobiles : animaux
	1.3	Collision avec un autre véhicule routier	Toutes les catégories pertinentes de véhicules doivent être envisagées Les cas de collision active "collision du véhicule du système contre" et passive "collision du véhicule du système par ..." doivent notamment être envisagés La collision passive regroupe l'ensemble des configurations où la collision n'est pas causée par le véhicule du système mais par un véhicule tiers (collision par rattrapage, latéral à une intersection par un autre véhicule qui refuse une priorité, pendant une manœuvre de l'autre véhicule (e.g. marche arrière), etc.	
	1.4	Collision avec le véhicule d'un système de transport guidé (tramways, ..) ou ferré (ferroviaire lourd)	Pour le cas de la collision avec un système de transport guidés, les cas de collision active "collision du véhicule du système contre" et passive "collision du véhicule du système par ..." doivent notamment être envisagés	
	1.5	Collision avec un autre type de véhicule		Collision avec véhicules non homologués pour la route (engins de chantier par ex)
Chute de personnes	2.1	Chute de personne à l'intérieur du véhicule		Perte d'équilibre et chute d'un passager suite freinage du VA Chute d'un passager suite rupture élément d'appui du mobilier

TYPOLOGIE	ID	ACCIDENTS POTENTIELS	COMPLEMENTS (éventuels)	EXEMPLES (non exhaustifs)
Chute de personnes	2.2	Chute de personne depuis le véhicule du système vers l'extérieur en station	Le terme "en station" regroupe les phases - d'approche et de départ de la station au cours desquelles le véhicule est en mouvement - d'arrêt en station, incluant les phases de transfert des passagers du véhicule	Chute de passagers à l'extérieur en approche station suite ouverture portes avant l'arrêt ou en ligne Chute de passagers à l'extérieur en départ station suite redémarrage portes ouvertes Chute de passagers quittant ou accédant au véhicule l'extérieur suite mouvement intempestif rampe PMR Chute de passagers quittant ou accédant au véhicule suite fermeture portes intempestive Chute de passagers quittant ou accédant au véhicule suite rupture d'élément d'appui pour les passagers
	2.3	Chute de personne depuis le véhicule du système vers l'extérieur en ligne	Le terme "en ligne" regroupe les phases - de circulation du véhicule - d'arrêt du véhicule hors des stations	Chute de passagers à l'extérieur en ligne suite à ouverture intempestive des portes Chute de passagers à l'extérieur en ligne suite à rupture mécanique d'un élément de retenue des passagers (vitrage par exemple)
Renversement	3.1	Renversement véhicule	Le renversement peut résulter - d'une instabilité du véhicule - d'un excès de vitesse en courbe - ...	Renversement suite à une sortie de route Renversement suite à vitesse excessive et heurt d'un obstacle Renversement suite à sortie de route sur une zone de travaux Renversement suite à un chargement excessif et mal réparti Renversement suite à une défaillance mécanique (freinage, ..) Renversement suite à la collision avec un obstacle sur la chaussée Renversement suite à l'arrivée sur une zone de chaussée déformée
Electrisation/Électrocution	4.1	Electrisation/Electrocution dans le véhicule		
	4.2	Electrisation/Electrocution dans une station		

TYPOLOGIE	ID	ACCIDENTS POTENTIELS	COMPLEMENTS (éventuels)	EXEMPLES (non exhaustifs)
Electrisation/Électrocution	4.3	Electrisation/Electrocution sur le parcours au niveau d'un équipement du système		Electrisation au niveau d'une armoire électrique dédiée spécifiquement au système Electrisation au niveau d'une borne de recharge sur le parcours
Feu/fumée/explosion	5.1	Feu/fumée dans le véhicule	Le cas où le feu dans le véhicule du système ferait suite à un incendie situé à proximité immédiate du véhicule du système doit notamment être pris en compte	
	5.2	Feu/fumée au niveau d'une station		
	5.3	Feu/fumée sur le parcours au niveau d'un équipement du système		Incendie dans une armoire électrique située sur le parcours et dédiée spécifiquement au système
	5.4	Explosion dans le véhicule		
	5.5	Explosion au niveau d'une station		
	5.6	Explosion sur le parcours au niveau d'un équipement du système		
Autres accidents de voyageurs	6.1	Passagers coincés/pincés par les ouvrants (fenêtres, portes, etc.) d'un composant du système	Les cas de coincement dans les ouvrants du véhicule et les portes palières des stations doivent notamment être pris en compte.	
	6.2	Passagers coincés/pincés par une partie mobile d'un composant du système		Coincement d'un passager dans la rampe d'accès mobile Coincement d'un passager dans un tripode d'accès
	6.3	Entraînement de personne par le véhicule (en particulier entraînement de personnes lors de la sortie de la station ou suite à un coincement de vêtement)		entraînement d'une personne lors de la sortie de la station suite au redémarrage du véhicule entraînement d'une personne suite au coincement du vêtement d'un passager resté sur le quai

TYPOLOGIE	ID	ACCIDENTS POTENTIELS	COMPLEMENTS (éventuels)	EXEMPLES (non exhaustifs)
Autres accidents de voyageurs	6.4	Contact avec un élément agressif d'un composant du système (blessure suite à contact avec / par les parties saillantes, coupantes, pointues, etc.)		
	6.5	Contact avec une partie chaude ou froide d'un des composant du système		
	6.6	contact avec un liquide dangereux (toxique, corrosive, etc.) d'un des composant du système		
	6.7	contact avec un gaz dangereux (toxique, etc.) d'un des composant du système		
Chute /projection ou perte d'objet	7.1	Chute / projection / perte d'éléments d'un véhicule du système vers la voirie	Note : pouvant entrer en collision avec un tiers ou un usager du système sur le parcours (ex. autre véhicule, piéton, etc.) ou provoquer sa sortie de route	- un obstacle laissé sur la voirie par un élément d'un véhicule du système entraine la sortie de route/collision du véhicule d'un tiers - un élément issu d'un véhicule du système heurte un usager vulnérable
	7.2	Passagers heurtés suite à la chute / projection / perte d'élément d'un véhicule dans son habitacle	Ce cas correspond à la perte d'une pièce/élément du véhicule, déclenchement intempestif d'un équipement de sécurité (e.g. airbag), etc.)	
	7.3	Passagers heurtés suite à la chute d'objets transportés dans l'habitacle d'un véhicule du système d'un objet transporté (ex. bagages, colis, etc.)		
	7.4	Chute d'objets de l'infrastructure du système (e.g. feux de trafic, panneaux ou éclairage en station, etc.)	Note : pouvant entrer en collision avec un tiers ou un usager du système sur le parcours (ex. autre véhicule, piéton, etc.) ou provoquer sa sortie de route	- un feu de trafic dédié au système tombé sur la voirie entraine la sortie de route/collision d'un tiers - une caméra dédiée au système tombe sur la voirie et heurte un usager vulnérable

Tableau 9

Liste informative de points d'attention à ne pas omettre dans les analyses de risques lors de l'identification des causes possibles pouvant mener à l'un des dangers de niveau STRA

ID	Intitulé	Compléments	Commentaire
1	Absence d'exécution / ou exécution erronée d'une exigence / règle / procédure d'exploitation	erreur opérateur défaut entretien absence contrôle etc.	
2	Absence de règle ou inadéquation de la règle avec l'utilisation visée	procédure d'exploitation non adaptée ...	En lien avec contrainte exportée vers le SGS
3	Caractéristique(s) du parcours ou d'un composant du système non compatibles ou plus compatible avec l'utilisation visée	dégradation des performances d'un capteur suite à variation luminosité dégradation de la chaussée ...	En lien avec analyse de sécurité parcours (ou type de parcours)
4	particularités de parcours, c'est à dire les caractéristiques spécifiques d'un parcours/zone (ou d'un type de parcours) qui génèreraient ou amplifieraient des possibilités d'accidents, ou qui nécessiteraient une réponse particulière du système	présence de masques à la visibilité présence d'un chantier non prévu sur le parcours marquage au sol effacé sur le parcours type de bâtiment au voisinage présence de places de stationnement au voisinage immédiat	En lien avec analyse de sécurité parcours (ou type de parcours)
5	Défaillance équipement électrique/électronique	défaillance capteur défaillance carte électronique défaillance systématique logiciel	Les défaillances envisagées sont celles qui font partie de la chaîne des causes conduisant à l'accident La granularité de l'analyse doit être de niveau système STRA. Ce sont les analyses spécifiques dédiées qui traduiront ces exigences de niveau système en exigences de niveau composant.
6	Insuffisance fonctionnelle (SOTIF)	erreur de classification des objets ...	Analyse au niveau système, amenant à identifier les analyses de la sécurité fonctionnelle

ID	Intitulé	Compléments	Commentaire
7	Conception inadaptée des dispositifs et moyens d'interface (affichages, marquages, signalisation visuelle ou sonore, etc.) avec les tiers (usagers du système, autres usagers de la route, forces de l'ordre, services de secours, personnel d'exploitation, ...) favorisant des mésusages	erreur d'appréciation opérateur déporté suite IHM pas claire ou incomplète passager incapable de prendre contact avec le PCC suite à manque d'information dans le véhicule erreur opérateur suite non information défaillance élément du système	L'IHM est à considérer vis-à-vis des usagers du système et des tiers, y compris les services de secours et les forces de l'ordre.
8	Contraintes de l'environnement extérieur vers le composant (ex. CEM, thermique, vibrations, produits chimiques, etc.)	- les éventuelles contraintes de type "risque industriel" liées aux zones de circulation des véhicules seront à prendre en compte dans l'analyse de sécurité du parcours	
9	Menaces du composant vers son environnement (ex. combustibles, catalyseurs chimiques, condensateurs, batteries, réservoir sous pression, ressorts de tension, fluides sous pression, mécanisme de déplacement, objets susceptibles d'être catapultés, pompes, matériaux émettant de l'électricité statique, énergie sous toutes ses formes, interrupteurs, appareil pyrotechnique, appareil de chauffage, générateurs électriques, CEM, etc.)	- exemple: dégagement gazeux batterie suite choc mécanique - les éventuelles contraintes de type "risque industriel" créées par le système vis à vis des zones de circulation des véhicules seront à prendre en compte dans l'analyse de sécurité du parcours	
10	Conception imparfaite / inadaptée vis-à-vis d'une utilisation prévisible, des principes ergonomiques (e.g. sous-dimensionnement mécanique, durabilité insuffisante, électrique, matériau glissant, angles saillants, coupants, etc.)	temps de latence important de la liaison entre le véhicule et l'opérateur déporté entraînant erreur d'appréciation de l'opérateur ...	L'homologation faite au niveau du véhicule couvre plusieurs aspects de la liste donnée dans l'intitulé.
11	Risques liés aux nouvelles technologies intégrées dans le système		- risque lié à une technologie innovante intégrée dans le système (ex : hydrogène, ..) - les risques liés aux cyberattaques ne sont pas à aborder à ce niveau car traités par des exigences globales dédiées
12	défaillance mécanique	crevaison échauffement freins suite défaillance ...	
13	incendie au voisinage du système	incendie d'un véhicule tiers devant le véhicule du système incendie dans un tunnel sur le parcours ...	
14	comportement dangereux des usagers du système	non-respect des interdictions de fumer déstabilisation du véhicule du système personnes se plaçant volontairement devant le véhicule ...	

ID	Intitulé	Compléments	Commentaire
15	comportement malveillant et intentionnel des usagers	<ul style="list-style-type: none">- personnes se plaçant volontairement devant le véhicule- personnes s'accrochant au véhicule- flamme sur les sièges	On s'intéresse aux comportements des usagers du système qui sont prévisibles sur ce type de système automatisé car ayant déjà été observé sur des systèmes de transport public

Tableau 10**Liste informative de scénarios et manœuvres à ne pas omettre dans les analyses de risques lors de l'identification des situations pouvant mener à l'un des accidents de niveau système**

Lors de l'analyse des dangers identifiés au niveau système, certaines situations dans lesquelles ces dangers peuvent survenir méritent une prise en compte et une analyse particulière. Le tableau suivant donne pour information une liste non exhaustive de ces circonstances particulières.

ID	situations	exemple d'accident en relation
1	Interaction entre un véhicule du système et un agent des force de l'ordre	Collision avec un véhicule sur une zone d'accident suite à la non-compréhension de l'injonction d'un agent des forces de l'ordre
2	Interaction entre un véhicule du système et un véhicule prioritaire	A une intersection, collision du véhicule avec un véhicule prioritaire non reconnu comme tel
3	Circulation d'un véhicule du système sur une zone de travaux	Sortie de route du véhicule suite à un cheminement modifié par une zone de travaux
4	Arrêt non voulu d'un véhicule du système au sein d'une zone à risque (ex. intersection routière, passage à niveau ferroviaire, tunnel, viaduc, etc.)	Immobilisation du véhicule au milieu d'un passage à niveau
5	Situation générant un mouvement de panique à l'intérieur d'un véhicule du système	Passagers coincés suite à un mouvement de panique lié à un dégagement de fumée soudain dans le véhicule
6	Situation générant un mouvement de panique sur le parcours ou en station du système	Mouvement de foule soudain suite à panique liée à une explosion aux abords du parcours
7	Incendie survenant au voisinage du système	Incendie du véhicule système suite au feu du véhicule tiers derrière lequel le véhicule système est en attente en cas de congestion du trafic Feu dans un bâtiment à proximité immédiate du véhicule système

Tableau 11
Liste des éléments de contexte pouvant influencer sur l'analyse des accidents

Lors de l'analyse des accidents identifiés au niveau système, l'analyse des conséquences de ces accidents peut être modifiée par des éléments de contexte particulier.

Le tableau suivant donne une liste minimale de situations de contexte à prendre en compte. Cette liste non exhaustive est adaptable au vu du domaine d'emploi du système.

ID	situations	exemples
1	Circulation d'un véhicule du système sur une zone à risque qui aggrave les conséquences potentielles d'un évènement redouté	<ul style="list-style-type: none"> - tunnel - viaduc - ravin - ..
2	Circulation d'un véhicule du système sur une zone dont la configuration rend les manœuvres à risque minimal complexes	<ul style="list-style-type: none"> - tunnel - viaduc - voie étroite - ..
3	Circulation d'un véhicule du système sur une zone dont la configuration rend l'évacuation des passagers dangereuse	<ul style="list-style-type: none"> - tunnel -viaduc - ..

9 Analyse inductive (analyse préliminaire des risques)

9.1 Présentation

Une analyse dite inductive analyse de manière systématique les conséquences des dysfonctionnements potentiels du système. Cette analyse part des fonctions du système pour déterminer l'ensemble des conséquences possibles de leur dysfonctionnement (type Analyse préliminaire des risques ou APR).

L'analyse inductive met en œuvre une démarche partant des causes vers les effets. Elle a pour but d'investiguer les dysfonctionnements (défaillances et insuffisances fonctionnelles) et de déterminer les situations dangereuses et les scénarios qui en résultent, et l'ensemble de leurs conséquences possibles.

Le point de départ de l'analyse inductive est la décomposition fonctionnelle du système. Le principe de la décomposition fonctionnelle est d'identifier des fonctions dites « racines », les sous-fonctions qui y sont attachées ainsi que leurs propres sous-fonctions. Le processus itératif de recherche de sous-fonctions se poursuit autant que nécessaire et conduit à une représentation de type arborescence où la position d'une sous fonction dans l'arbre déductif ne préjuge pas de son importance pour le système.

Sur la base de cette décomposition, une analyse systématique des dysfonctionnements possibles de chaque fonction élémentaire et de leurs conséquences est conduite afin de construire l'ensemble des scénarios dysfonctionnels.

L'analyse inductive n'intègre pas les dysfonctionnements dus à des cyber-attaques, la prise en compte de ces événements font l'objet d'un guide spécifique.

Chaque scénario résultant d'un dysfonctionnement fait l'objet d'une estimation de la gravité de ses conséquences (et de sa fréquence d'occurrence pour la démonstration de type 3b) permettant d'estimer son niveau de risque et de graduer les exigences à mettre en œuvre pour s'en protéger (AMDEC fonctionnelle).

Ces exigences peuvent consister dans l'application d'un référentiel externe pour lequel il a été démontré qu'il couvrait le risque considéré et son contexte (démonstration de type 3a du guide d'application GAME) ou dans la mise en œuvre de mesures spécifiques après avoir démontré que leur combinaison permettait de ramener le risque résiduel à un niveau acceptable (démonstration de type 3b du guide d'application GAME). Ces mesures peuvent être à la fois qualitatives et quantitatives : architecture des fonctions, spécifications fonctionnelles, fiabilité des composants, etc.

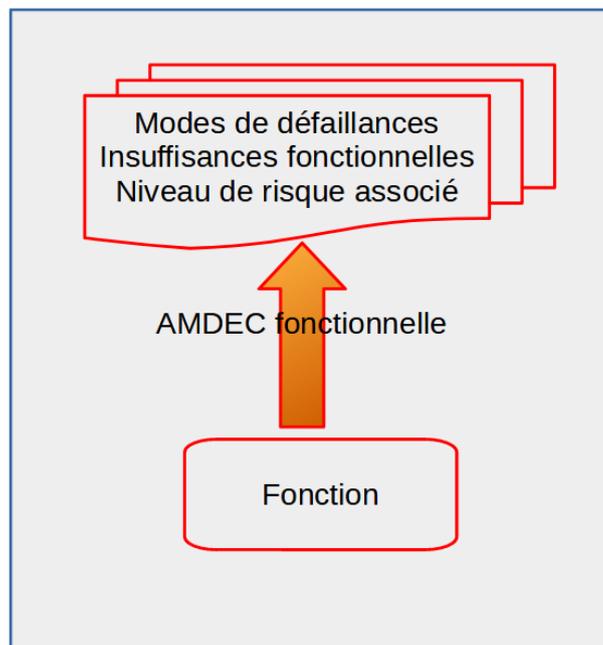


Figure 7 - Analyse inductive

L'analyse inductive concerne l'ensemble des composants du système et peut être conduite à différents niveaux. L'analyse présentée ici est déroulée au niveau du système global et permet de déterminer des exigences globales portant d'abord sur les différentes fonctions du système.

Dans un second temps, ces exigences devront être déclinées au niveau des différentes sous-fonctions, puis des différents équipements et composants, au vu des architectures supportant les fonctions.

Objectifs

- Identifier toutes les défaillances et insuffisances fonctionnelles du système impactant la sécurité
- L'analyse inductive permet d'estimer et de tracer chaque risque issu de l'approche dysfonctionnelle, en lien avec les accidents de niveau système.

Note : L'analyse inductive constitue une activité préalable à la phase d'allocation des objectifs de sécurité (Cf. § 5.4).

Phase du projet

- L'analyse inductive est une démarche de haut niveau, globale au système qui est mise en œuvre d'abord au stade du DCST pour un système technique générique associé à un domaine de conception technique connu. Les exigences qu'elle permet de spécifier touchent à la conception et l'architecture du système technique, aux contraintes exportées par le système technique vers le type de parcours visé et vers ses conditions d'exploitation. Ces différents éléments définissent le domaine de conception technique du système technique repris dans la déclaration de fonctionnalités et de sécurité prévue par le décret STRA.
- Au stade du DPS et du DS, les spécificités liées au déploiement de niveau système sur le parcours réel seront analysées au travers de l'analyse de sécurité du parcours. L'analyse inductive doit ensuite être complétée afin de prendre en compte les conséquences des dysfonctionnements dans le contexte des scénarios spécifiques au parcours de déploiement.

9.2 Trame

Les tableaux suivants fournissent à titre uniquement illustratif un exemple de trame décrivant les différents éléments de l'analyse inductive.

FONCTION			IDENTIFICATION DE LA SITUATION DANGEREUSE						
Fonction étudiée			Mode de défaillance ou d'Insuffisance fonctionnelle	SYNTHESE de la situation dangereuse (SD) de niveau système		Type de section d'infrastructure	Dynamique (des acteurs de la situation)	Eléments complémentaires de contexte	Illustration(s) de la situation étudiée
#	Intitulé	Description		Ref	Description				
3.2.1	Empêcher l'autorisation d'ouverture de portes hors des phases de transfert ou d'évacuation	Autorise l'ouverture des portes ssi l'ensemble des conditions {C1&C2} sont remplies C1 = véhicule immobilisé C2 = zone répertoriée ou si commande urgence	autorisation d'ouverture intempestive			station ou zone répertoriée			Autorisation d'ouverture alors que le véhicule n'est pas immobilisé en station
						section courante			Autorisation d'ouverture alors que le véhicule n'est pas immobilisé en ligne
						section courante			Autorisation d'ouverture alors que le véhicule est immobilisé mais n'est pas dans une zone autorisée.
			absence d'autorisation d'ouverture			section courante			Absence d'autorisation d'ouverture en zone autorisée
						section courante			Absence d'autorisation d'ouverture en situation d'urgence

Tableau 12.1- trame de l'analyse inductive

ACCIDENT POTENTIEL DE NIVEAU STRA					AUTRES EFFETS POTENTIELS		
DESCRIPTION	EFFET = ACCIDENT POTENTIEL DE NIVEAU STRA				Personne(s) exposée(s)		
	#	Type	#	Sous-type		1er niveau	conséquences possibles
chute de passagers		Chute de personnes	2.2	Chute de personne depuis le véhicule du système vers l'extérieur en station			
			2.3	Chute de personne depuis le véhicule du système vers l'extérieur en ligne			
chute de passagers / débarquement de passagers sur des zones non adaptées		Chute de personnes	2.3	Chute de personne depuis le véhicule du système vers l'extérieur en ligne			
						Service non assuré	panique des passagers
						Exigence de haut niveau n°23 relative à l'évacuation non respectée	auto-évacuation des passagers impossible en situation d'urgence

EVALUATION INITIALE DES RISQUES							EXIGENCE(S) DE SECURITE DE NIVEAU STRA					
Gravité		Exposition		Evitabilité		Evaluation du risque <i>(optionnel)</i>	TYPE D'APPROCHE GAME			Part de l'Objectif de Sécurité quantitatif alloué à la fonction étudiée, pour le mode de défaillance ou d'insuffisance fonctionnelle étudiée		Niveau d'intégrité requis
Classe	Commentaire(s)	Classe	Commentaire(s)	Classe	Commentaire(s)		Type	Référence(s) utilisée(s)	Description	Document d'argumentation de la déclinaison	Valeur	

Tableau 12.2- trame de l'analyse inductive

9.3 Eléments d'entrée de l'analyse déductive

La décomposition fonctionnelle proposée est structurée selon une arborescence en 4 niveaux, dont les 2 premiers sont présentés dans la figure ci-dessous.

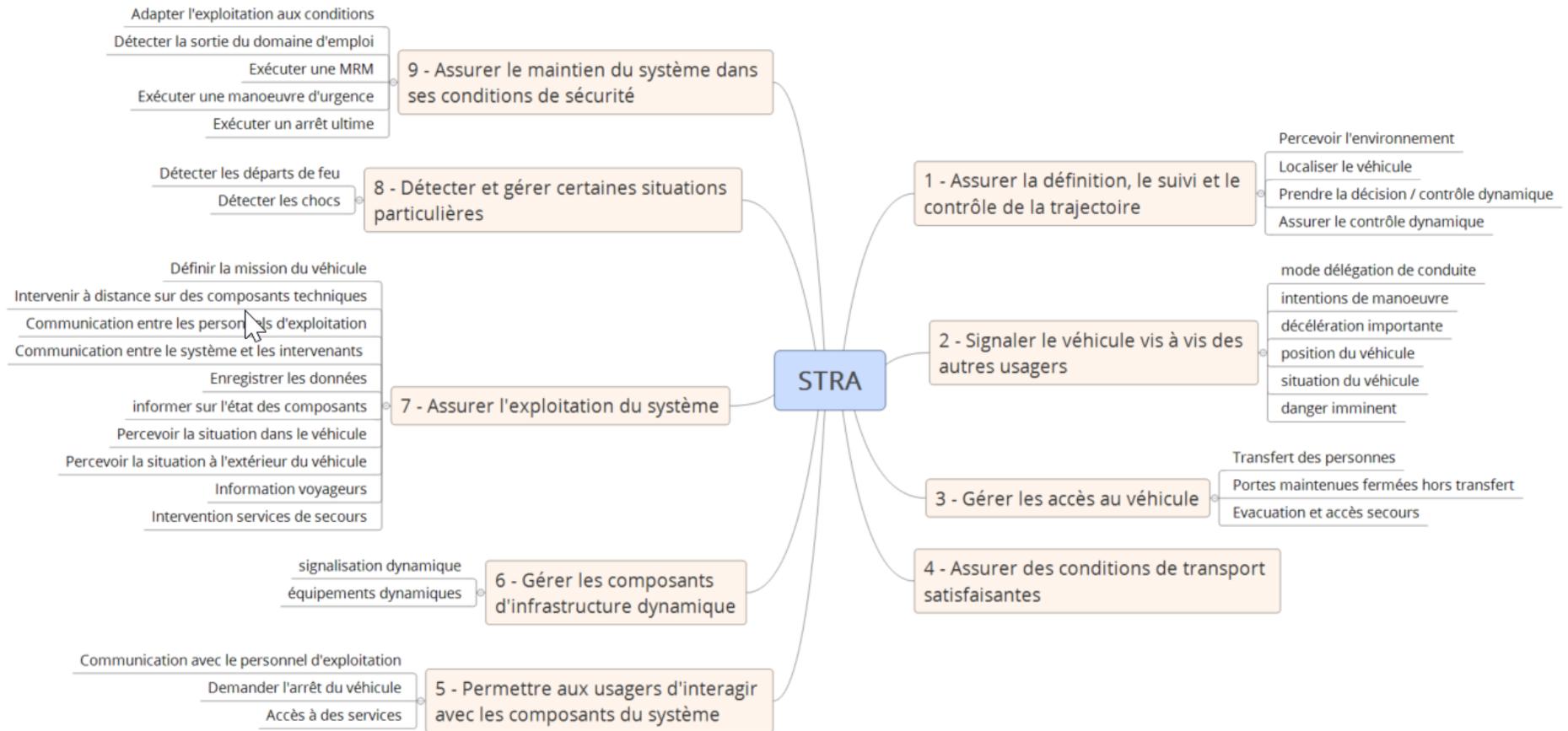


Figure 8 - Arborescence décomposition fonctionnelle

Le tableau suivant fournit une décomposition fonctionnelle générique d'un STRA. Cette décomposition se veut indépendante des technologies mises en œuvre dans le système et des types de parcours de circulation.

Ce tableau doit être adapté et complété par les porteurs de projet au vu des spécificités de chaque système.

Les règles suivantes sont à prendre en compte lors de l'utilisation des tableaux :

- La liste des fonctions ne saurait être exhaustive et a vocation à être enrichie dans le cadre du déroulement d'un projet.
- A l'inverse, même si les fonctions présentées se veulent génériques, certaines peuvent ne pas être présentes sur un projet spécifique ; il conviendra dans ce cas de le tracer et de le justifier.
- La décomposition des fonctions suit une arborescence purement fonctionnelle. Le rang de la fonction ne préjuge aucunement de son poids vis à vis des enjeux de sécurité ou des obligations réglementaires.
Une fonction (quel que soit son rang) peut contribuer par la transmission du flux (ex. données, matière, énergie, etc.) à plusieurs fonctions de rang équivalent ou supérieur (par exemple : la fonction 1.1 "Percevoir l'environnement" peut transmettre des données utiles aux fonctions : 1.2; 1.3; 2; 3...)
- Les fonctions listées dans le tableau ne comportent pas les fonctions "techniques" telles que l'alimentation électrique, les liaisons de communication, etc. Celles-ci doivent être prises en compte au stade de l'analyse de chaque fonction auxquelles elles contribuent.
- Les fonctions des groupes 7.2, 7.7 et 7.8 seront détaillées dans les compléments au présent guide relatifs aux interventions à distance.

Tableau 13
Canevas de décomposition fonctionnelle d'un STRA

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
1-Assurer la définition, le suivi et le contrôle de la trajectoire du véhicule		1.1-Percevoir l'environnement (sense)	La fonction 1.1 permet d'assurer la perception des données, par exemples: la détection d'objets (statiques, dynamiques, êtres vivants...), des événements de circulation, de conditions (météo,...) et les éléments de l'infrastructure Peut être assurée par des capteurs : ex. caméras, lidars, radars, par exemple (embarqué/débarqué)	1.1.1-Percevoir/traiter les objets	Obstacles statiques/mobiles et/ou autres usagers de la route	1.1.1.1-Détecter les objets	Savoir détecter un objet sur la trajectoire ou proche
						1.1.1.2-Caractériser les objets	Savoir identifier un objet (vélo, moto, camion, animal, obstacle, piéton, agent des FO, véhicule prioritaire...)
						1.1.1.3-Prédire/interpréter le comportement des objets	Anticiper la vitesse et la trajectoire des objets identifiés (en amont de la prise de décision : je double, je m'arrête...) Interpréter les gestes et injonctions des forces de l'ordre
				1.1.2-Percevoir/traiter les infrastructures	Connectées ou non (feux, panneau STOP, passage piéton, marquage au sol, ...), peut aussi être assurée par la localisation (a priori perception)	1.1.2.1-Détecter les infrastructures	Savoir détecter une infrastructure
						1.1.2.2-Caractériser les infrastructures	Savoir identifier une infrastructure statique ou dynamique (feu rouge, vert, STOP, marquage au sol...)
						1.1.2.3-Traiter le statut d'une infrastructure	Respecter la signalétique dynamique ou non (s'arrêter au feu rouge, avancer au feu vert, s'arrêter au STOP...)

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
1-Assurer la définition, le suivi et le contrôle de la trajectoire du véhicule				1.1.3-Percevoir/traiter les VP et AFO	-	1.1.3.1-Détecter les VP et les agents des FO	Détecter les véhicules d'intérêt général à caractère prioritaire ou bénéficiant de facilités de passages(VP) et les agents des forces de l'ordre (AFO)
						1.1.3.2-Caractériser les VP et les AFO	Identifier les types de VP en présence, et la nature des agents
						1.1.3.3-Interpréter les injonctions des AFO et intentions des VP	-
		1.2-Localiser le véhicule sur le parcours / zone par rapport à l'itinéraire défini	La fonction 1.2 permet d'assurer la localisation du véhicule sur un parcours/une zone L'itinéraire peut être défini à différents niveaux : - en amont de la mission (cas d'un STRA déployé sur un parcours prédéfini) - pendant la mission : cas d'un itinéraire calculé et remis à jour pendant la mission, par le système en fonction d'éléments	1.2.1 Connaître la mission (itinéraire défini)	Connaître l'itinéraire à suivre , relatif au service de transport alloué au véhicule, y compris les stations voyageurs, les points d'arrêt à la demande, les points d'évacuation possibles, ... par exemple, dans le cas d'un itinéraire prédéfini en amont, en flashant et mettant à jour la map et la mission (temps) dans le PC du système.	-	-

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
1-Assurer la définition, le suivi et le contrôle de la trajectoire du véhicule			extérieurs (trafic, informations supervision, etc.) (cas d'un STRA de type robot-taxi par exemple) -etc.	1.2.2 - Localiser le véhicule	Positionner le véhicule (coordonnées)	1.2.2.1-Charger la carte	Surveiller à distance la position et le déplacement du véhicule, et connaître à priori l'environnement dans lequel va circuler le véhicule. Prendre des mesures si la position ou le déplacement s'écarte de certaines valeurs fixées d'avance. => 1.3
						1.2.2.2-Localiser le véhicule sur la carte	La localisation peut être assurée par des signaux GPS et/ou des capteurs embarqués, : ex. IMU/odométrie, accompagnés ou non d'équipements déployés sur l'infrastructure.
		1.3-Prendre la décision concernant le contrôle dynamique (plan)	En fonction de la perception (1.1) et la localisation (1.2), décider des mouvements et de la dynamique du véhicule, en tenant compte de la mission, des manœuvres et des contraintes réglementaires.	1.3.1- Décider des actions opérationnelles pour le déplacement longitudinal et latéral du véhicule.	Décider de la prochaine séquence de manœuvres "nominales" (avec ses composantes longitudinale et latérale) à réaliser à court terme (par exemple tourner à gauche et changer de file, en ralentissant à x km/h etc.	-	-

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
1-Assurer la définition, le suivi et le contrôle de la trajectoire du véhicule				1.3.2- Décider des actions tactiques pour le déplacement longitudinal et latéral du véhicule.	Décider de la manœuvre en temps réel (avec ses composantes longitudinale et latérale) à réaliser immédiatement (par exemple décélérer, freiner et tourner à gauche d'un angle de 10°)	-	-
		1.4-Assurer le contrôle dynamique (act)	La fonction 1.4 permet d'assurer les commandes du mouvement latéral (direction) et longitudinal (freinage et accélération) en tenant compte l'énergie servant à la traction/freinage.	1.4.1-Assurer le contrôle longitudinal	Va permettre de répondre aux exigences de niveau service de type "respecter la limitation de vitesse", "respecter l'interdistance" ...	1.4.1.1- Gérer l'accélération	- inclut les actions sur la traction et le frein - inclut la prise en compte des valeurs du gamma + et du jerk
						1.4.1.2-Gérer la décélération	- inclut les actions sur la traction et le frein - inclut la prise en compte des valeurs du gamma - et du jerk
						1.4.1.3-Immobiliser	- arrêt prolongé - assurer l'immobilisation du véhicule
		1.4.2-Assurer le contrôle latéral (direction)	Fonction élémentaire permettant de se positionner sur la voie en Y (se centrer sur la voie, prendre un virage, changer de voie,...)	-	-		

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
2-Signaler le véhicule vis-à-vis des autres usagers de la route (signalisation sonore, visuel, etc.)	En fonction de la fonction 1, se signaler aux autres usagers de la route via des avertisseurs sonores (klaxon, cloche,...) ,via des avertisseurs visuels (les feux de croisement, de route, bouillard, clignotant,...), ou via des communications V2X. Cette fonction peut être supportée par le véhicule et/ou des équipements d'infrastructure (intentions de manœuvre à l'arrivée/départ de station par ex)	2.1 - signaler le mode délégation de conduite	-	-	-	-	-
		2.2 - signaler les intentions de manœuvre du véhicule	- vers les autres véhicules - vers les piétons - vers les VRU - lors de phases spécifiques (entrées/sorties de station)	-	-	-	-
		2.3 - signaler une décélération importante du véhicule	cf. homologation: signalisation si gamma > seuil	-	-	-	-
		2.4 - signaler la position du véhicule	- situations nominales - situations avec manque de visibilité	-	-	-	-
		2.5 - signaler la situation du véhicule	- signalisation suite à MRM - signalisation suite à incident (feux de détresse)	-	-	-	-
		2.6 - signaler un danger imminent	- en cas de danger imminent détecté par le véhicule ego (feux de détresse, avertisseur sonore, appel de phares, etc.)	-	-	-	-

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
3-Gérer les accès aux véhicules automatisés	-	3.1-Gérer le transfert des personnes aux points autorisés	La fonction 3.1 permet d'assurer le transfert des personnes (montée/descente des passagers/personnel d'urgence/employés du service...) aux points autorisés (station, point d'arrêt à la demande,..)	3.1.1-Assurer un accostage avec espacement limité véhicule/trottoir	- cas de TC : lacune horizontale et verticale < 50 mm (cf. arrêté accessibilité 13/07/2009) - A traiter le cas du point d'arrêt à la demande / robot-taxi Déployer les dispositifs dédiés en station ou dans le véhicule (emmarchements mobiles, baraquage, ..)	3.1.1.1 - Respecter une lacune verticale limitée	-
						3.1.1.2 - Respecter une lacune horizontale limitée	-
				3.1.2- Gérer l'ouverture et la fermeture des portes pour faire entrer/sortir les personnes	- ouverture des portes aux points autorisés - non-ouverture des portes hors des points autorisés et des cas d'évacuation - ...	-	-
				3.1.3-Gérer l'E/S des PMR	Déployer les dispositifs dédiés en station ou dans le véhicule (emmarchements mobiles, rampe PMR, baraquage, ..)	-	-
		3.1.4- Surveillance du dépassement de la capacité maxi du véhicule	-	3.1.4 .1 - surveiller le nombre de passagers debout et/ou assis	-	3.1.4.2 - surveiller le PTAC	-

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
3-Gérer les accès aux véhicules automatisés				3.1.5- surveiller les conditions de redémarrage du véhicule en ce qui concerne les dispositifs mobiles d'accès et d'embarquement	- position des dispositifs portes, élévateur, rampe, système de baraquage,... - absence de coincement - absence d'entraînement d'un usager	-	-
		3.2-Maintenir le véhicule automatisé fermé hors transfert personnes/évacuation	En dehors des points autorisés, la fonction 3.2 permet d'assurer le maintien des portes en position fermée.	3.2.1 - Empêcher l'autorisation d'ouverture de portes hors des phases de transfert ou d'évacuation	-	-	-
				3.2.2 - Surveiller l'état des portes	surveillance du verrouillage et de la position fermée des portes hors des phases de transfert ou d'évacuation	-	-

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
3-Gérer les accès aux véhicules automatisés		3.3-Permettre l'évacuation et l'accès des secours	En complément des fonctions 3.1 et 3.2, la fonction 3.3 permet l'évacuation des passagers et l'accès de secours en cas d'urgence.	3.3.1- Donner moyen aux passagers d'évacuer l'habitacle du véhicule dans	Issues de secours suffisantes et accessibles. Moyens d'ouverture accessibles et adaptés. Cas des PMR à prendre en compte Pour les cat M2 et M3, l'homologation fixe le nb d'issues de secours présentes (cf. UNR 107). Cas de commande automatique d'ouverture des portes automatiques dans les situations d'urgence.	-	-
				3.3.2 - Donner moyen au personnel technique et aux services de secours d'accéder à l'habitacle du véhicule		-	-
				3.3.3 - Informer l'opérateur distant en cas d'actionnement des systèmes d'ouverture prévus des issues de secours pour l'évacuation		-	-

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
4- Assurer des conditions de transport satisfaisantes pour les passagers	Ces fonctions permettent d'assurer le confort des passagers (thermique, acoustique, vibratoire, maintien, luminosité et visibilité,...) Néanmoins, certaines de ces fonctions peuvent présenter un enjeu en terme de sécurité, et doivent alors être prises en compte dans la démonstration de sécurité. Par exemple, l'éclairage de l'habitacle du véhicule peut être nécessaire pour prévenir le risque de chute des passagers; le désembuage des vitres permettant la perception de l'environnement par les passagers peut être important dans le contexte d'une évacuation.						
5- Permettre aux usagers d'interagir avec des composants du système	-	5.1-Permettre la communication des usagers vers le personnel d'exploitation (COM)	La fonction 5.1 permet d'assurer la communication sonore et visuelle entre les usagers (à bords du véhicule et en station) et le personnel d'exploitation.	5.1.1 - Permettre aux usagers du système de dialoguer avec le personnel d'exploitation	Interphonie véhicule, interphonie station, etc.	-	-
				5.1.2 - Permettre aux usagers du système d'alerter le personnel d'exploitation	par ex Système de demande d'assistance passagers (projet NAVURB AUT)	-	-
		5-2 Permettre aux passagers de demander l'arrêt du véhicule	Système de demande d'arrêt sécurité passagers (projet NAV URB AUT)	-	-	-	-

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
5- Permettre aux usagers d'interagir avec des composants du système		5.3-Permettre aux usagers l'accès à des services	La fonction 5.3 permet d'assurer l'accès à des services pour les usagers en station/ sur smartphone/ dans les véhicules, ... (ex. Horaire, tickets, réservation, ...). Certaines de ces fonctions peuvent éventuellement présenter des risques liés à la sécurité	-	-	-	-
6-Gérer les composants d'infrastructure dynamiques pilotés par le système	La fonction 7 permet de gérer la signalisation dynamique (gestion des priorités avec feux de signalisation, vitesse, ...), les composants de ségrégation dynamique (barrières, potelets, etc.), etc.	6-1 commander la signalisation dynamique	par exemple, pilotage des feux connectés	-	-	-	-
		6-2 commander les équipements dynamiques mobiles	par exemple, pilotage des barrières mobiles, bornes escamotables, etc.	-	-	-	-

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
7- Assurer l'exploitation 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)...	7.1 - définir la mission de chaque véhicule	<p>- Définir les contraintes d'itinéraire , relatif au service de transport alloué au véhicule, y compris les stations voyageurs, les points d'arrêt à la demande, les points d'évacuation possibles</p> <p>- Définir les contraintes temporelles (date, heure de départ, heure d'arrivée, heures de passage, fréquence, ...)</p> <p>La mission peut être définie au préalable en fonction des conditions prévues sur le parcours, ou être éventuellement modifiée en cours d'exploitation au vu des évènements rencontrés ou connus. (nécessite une communication avec les services extérieurs cf 8.4)</p>	-	-	-	-

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
7- Assurer l'exploitation du système		7.2- Intervenir à distance sur des composants techniques du système	<p>La fonction 9.1 permet d'assurer les différents types d'intervention à distance prévus par le système.</p> <p>Intervention à distance : Action exercée par une personne habilitée située à l'extérieur d'un système de transport routier automatisé, aux fins :</p> <ul style="list-style-type: none"> d'activer ou de désactiver le système, ou de donner l'instruction d'effectuer, modifier, interrompre une manœuvre, d'acquitter des manœuvres proposées par le système, de donner instruction au système de choisir ou de modifier la planification d'un itinéraire ou des points d'arrêt pour les usagers (notamment en réponse à des aléas ou des défaillances). 	7.2.1 - arrêter le(s) véhicules	immédiat en zone station, next stop, ASAP, etc.	-	-
				7.2.2 - activer/désactiver le mode délégation de conduite		-	-
				7.2.3 - donner une consigne au(x) véhicule(s)	réduction de vitesse, consigne de vitesse maximale	-	-
				7.2.4 - acquitter une manœuvre proposée		-	-
				7.2.5 - commander une manœuvre du véhicule		-	-
				7.2.6 - interrompre une manœuvre	Définir l'état suite à interruption manœuvre	-	-
				7.2.7 - modifier une manœuvre		-	-
				7.2.8 - commander des équipements du véhicule	essuie-glaces, éclairage, etc. rampes portes etc.	-	-

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
7- Assurer l'exploitation du système				7.2.9 - percevoir l'environnement de circulation au voisinage du véhicule	Perception des tiers à proximité selon manœuvre à acquitter ou commande à effectuer pour être en capacité de le faire	-	-
				7.2.10 - percevoir l'environnement de l'équipement commandé, pour donner les autorisations de manœuvre ou de démarrage	environnement des portes si commande des portes à distance ou en cas de défaut, environnement de la rampe PMR si commandée à distance	-	-
		7.3-Permettre la communication entre les personnels d'exploitation	La fonction 9.2 permet d'assurer la communication entre les personnels d'exploitation. Par exemple, communication entre le personnel d'exploitation situé au poste de supervision et le personnel d'exploitation sur site ou dans le véhicule	-	-	-	-
		7.4-Permettre la communication entre le système et des intervenants extérieurs	La fonction 9.3 permet d'assurer la communication entre les personnels d'exploitation et les intervenants extérieurs (ex. Force de l'Ordre, les opérateurs PCC, Préfet dans le cas d'un plan ORSEC ou	7.4.1 - permettre l'initiation de la communication avec le système à la demande de l'intervenant extérieur	moyen pour l'intervenant d'établir la communication	-	-

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
7- Assurer l'exploitation du système			équivalent service de secours comme les pompiers, SAMU, les fournisseurs de service (EDF, télécom), la ville et les acteurs intervenant sur la voirie (Gaz, DDE, EDF,...)).	7.4.2 - permettre la communication entre le personnel d'exploitation et les intervenants extérieurs	communication à l'initiative du personnel ou à l'initiative de l'intervenant extérieur (agent des forces de l'ordre, services de secours par exemple)	-	-
				7.4.3 - permettre la communication des informations nécessaires à l'intervenant extérieur	par exemple, documents du véhicule à destination des agents des forces de l'ordre	-	-
		7.5-Enregistrer les données	La fonction 7.5 permet d'enregistrer les données pour répondre aux besoins de l'exploitation.	7.5.1 - Enregistrer les données des différents sous-systèmes pour l'amélioration continue du système	-	-	-
				7.5.2 - Enregistrer les données des différents sous-systèmes pour l'analyse des accidents	Cf. décret STRA art R3152-22	-	-

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
7- Assurer l'exploitation du système		7.6- informer sur l'état des composants du système	La fonction 7.6 permet la supervision / l'exploitation (afficher les états des composants, des alertes, des évènements, des conditions (météo, etc.), etc.)	7.6.1 - informer sur l'état du véhicule	Y compris niveau de charge batterie Y compris ceintures de sécurité Y compris état des portes Y compris état des issues de secours Y compris vitesse instantanée, etc.	-	-
		7.6.2 - informer sur les conditions de fonctionnement du véhicule		par exemple véhicule en situation d'évacuation, véhicule en attente, état de délégation de conduite du véhicule, arrêt suite manœuvre d'urgence, arrêt suite à MRM, arrêt suite à collision, évènement	-	-	
		7.6.3 - Informer sur l'état des équipements du système, ou participant à la sécurité du système.		Y compris la supervision Y compris les équipements du système préexistants et participant à la sécurité	-	-	
		7.7- permettre à l'opérateur de percevoir la situation dans le véhicule	écoute passive visio sur passagers	7.7.1 - Percevoir l'ambiance sonore dans l'habitacle du véhicule	-	-	-
				7.7.2 - Pouvoir avoir une vision de l'intérieur véhicule	-	7.7.2 - Pouvoir avoir une vision générale de l'habitacle du véhicule	par ex gérer les demandes d'arrêt passagers

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
7- Assurer l'exploitation du système					-	7.7.3 - Pouvoir avoir une vision sur des points particuliers de l'habitacle	par exemple pour réaliser des identifications ou des levées de doute (zones de coincement portes, incendie, ..)
		7.8 - permettre à l'opérateur de percevoir la situation à l'extérieur du véhicule	-	7.8.1 - percevoir le voisinage du véhicule		7.8.1.1 - percevoir l'environnement de circulation au voisinage du véhicule	Perception des conditions d'une évacuation ou d'une manœuvre, y compris des conditions météo
						7.8.1.2 - Pouvoir avoir une vision sur des points particuliers situés hors de l'habitacle	par exemple pour réaliser des identifications ou des levées de doute: zones portes côté quai, zone rampe, incendie Vérification d'absence de coincement, d'absence d'entraînement d'un passager, etc.
				7.8.2 -permettre à l'opérateur de connaître la situation sur le parcours		7.8.2.1 -connaître les conditions de circulation prévisibles sur le parcours	conditions trafic et météo afin d'adapter les consignes d'exploitation (cf. 10.1)
						7.8.2.2 -connaître les conditions de circulation en des points particuliers du parcours	par exemple, vision déportée sur un PN ou zone accidentogène
		7.9 -Permettre la transmission de l'information voyageurs	La fonction 5.2 permet d'assurer la transmission d'informations sonores ou	7.9.1- Donner des informations aux usagers en station	messages audio ou affichage	-	-

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
7- Assurer l'exploitation du système			visuelles aux usagers (à bord du véhicule et en station).	7.9.2 - Donner des informations aux passagers du véhicules	messages audio ou affichage	-	-
		7.10 - permettre l'intervention en sécurité des services de secours	Existence de moyens d'immobilisation du véhicule, protection / risque électrique, etc. existants, connus et accessibles pour secours	-	-	-	-
8- Détecter et gérer certaines situations particulières	-	8.1 - détecter et gérer les départs de feu	-	8.1.1 - détecter et gérer les départs de feu dans les véhicules	-	-	-
				8.1.2 - détecter et gérer les départs de feu dans les stations	-	-	-
				8.1.3 -détecter et gérer les départs de feu dans les équipements du parcours	Y compris équipements dédiés à la supervision	-	-
				8.1.4 -détecter et gérer les départs de feu dans les équipements de la supervision	-	-	-
		8.2- détecter les chocs contre le véhicule	cas de collision impactant la sécurité des passagers ou des tiers (tiers, obstacles fixes, etc..)	-	-	-	-

rang 1		rang 2		rang 3		rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
9 - Assurer le maintien du système dans ses conditions de sécurité	-	9.1 - Adapter les consignes d'exploitation aux conditions de circulation	réduction de vitesse, arrêt préventif du service en cas de conditions de circulation dégradées > seuil (trafic et/ou météo)	-	-	-	-
		9.2 - Détecter la sortie du système de son domaine d'emploi	Y compris dysfonctionnement équipements extérieurs participant à la sécurité	-	-	-	-
		9.3 - Exécuter une MRM adaptée à la situation	adaptée au contexte, à la situation de parcours, etc. (y compris en cas de défaut d'acquittement de la part de l'opérateur)	-	-	-	-
		9.4 - Exécuter une manœuvre d'urgence adaptée à la situation	-	-	-	-	-
		9.5 - Exécuter un arrêt "ultime"	fonction(s) liée(s) à la réponse à l'exigence de conserver la capacité d'arrêter le véhicule même en cas de défaillance profonde du système entraînant l'incapacité du système à effectuer une MRM (FAILURE MITIGATION STRATEGY cf. SAE J3016_202104 3.11)	-	-	-	-

10 Annexe

Conformément au décret n° 2010-1580 du 17 décembre 2010, portant création du Service technique des remontées mécaniques et des transports guidés, le STRMTG est chargé de produire des guides et référentiels.

Le présent document a été élaboré par le groupe de travail national GAME-STRA mis en place par le STRMTG.

Pilote : M. Pierre Jouve - STRMTG – département transports publics automatisés
Secrétaire : M. Florent Sovignet - STRMTG – département transports publics automatisés

M.	Courtet	Alstom
M.	Guesdon	Alstom
M.	Poisson	Alstom
Mme	Quiney	Alstom
M.	Alliouche	Bureau Veritas
M.	Boniakowski	Bureau Veritas
M.	Clarissou	Bureau Veritas
Mme	Dam	Bureau Veritas
M.	Travers	Cara
M.	Belloche	Cerema
M.	Sautel	Cerema
M.	Russo	Certifer
M.	Testemale	Certifer
M.	Willmann	CETU
M.	Audige	DGITM
M.	Delache	DGITM
M.	Diez	DGITM
Mme	Lanaud	DGITM
M.	Launay	DSR
M.	Dupont	Easymile
M.	Pagliero	Easymile
M.	Chauvin	GART
M.	Lesot	Ile-de-France Mobilités
Mme	Brini	IRT System X
M.	Aubourg	Keolis
Mme	Benmhalla	Navya
Mme	Hu	Navya
M.	Renaud	Ramsai
Mme	Berthault	RATP

M.	Boulineau	RATP
M.	Arnoux	Renault
M.	Rousseau	Renault
M.	Sencerin	Renault
M.	Geronimi	Stellantis
M.	Lenti	Stellantis
M.	Brun	STRMTG
M.	Dusserre	STRMTG
M.	Maisonobe	STRMTG
Mme	Torelli	Systra
M.	Tran	Systra
M.	Dadou	SYTRAL
M.	Negrier	SYTRAL
M.	Bakadal	Transdev
M.	Desmoineaux	Transdev
M.	Baranowski	Université Gustave Eiffel
Mme	Cuvelier	Université Gustave Eiffel
M.	Herveleu	UTAC
M.	De Sousa Fernandes	UTAC

A également contribué à la relecture du guide :

M. Ludovic Brun, chargé de mission juridique du STRMTG