GUIDE
TECHNIQUE

STRMTG
SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

SYSTÈMES DE TRANSPORT ROUTIER AUTOMATISES

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

MINISTÈRE CHARGÉ DES TRANSPORTS
Liberté
Égalité
Fraternité

Version 3 – novembre 2025

Objet – Domaine d'application – Destinataires

Ce guide technique est un complément au guide d'application GAME du STRMTG qui explicite une méthodologie de démonstration du principe « GAME » (Globalement au moins équivalent) prévu par l'article R. 3152-2 du titre V du livre I^{er} de la troisième partie de la partie règlementaire du code des transports. Le présent guide technique précise les éléments permettant de guider la démarche GAME décrite dans le guide d'application GAME.

Comme ce dernier, il est applicable aux STRA de personnes relevant du titre V du livre I^{er} de la troisième partie de la partie règlementaire du code des transports (articles R. 3151-1 à R. 3153-1) et aux STRA de marchandises relevant du titre V du livre II de la troisième partie de la partie réglementaire du code des transports (articles R. 3251-1 à R. 3253-1).
Il est destiné à l'ensemble des acteurs professionnels du secteur des transports routiers automatisés : organisateurs de service, maitres 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. 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 usagers et des tiers vis-à-vis du fonctionnement du système, et d'autre part 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 usagers, lorsqu'ils sont transportés à bord des véhicules du système ou en attente de l'être,
- 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) ;
- des opérations de chargement et de déchargement des marchandises ;
– 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 présentée dans le guide d'application GAME (approche de type 3).

Le présent guide a vocation à être complété et mis à jour au fur et à mesure de l'enrichissement des travaux relatifs à la démonstration de sécurité des STRA.

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)
2	Pierre Jouve	10/10/2024	Compléments à la version 1 apportés par le groupe de travail GAME (STRA)
3	Pierre Jouve	14/11/2025	Intégration du transport routier automatisé de marchandises

RÉDACTEUR	VÉRIFICATEUR	APPROBATEUR
Pierre Jouve Chef du département transports routiers automatisés	**Alexandre Dusserre** Chef du département métros et systèmes ferroviaires	**Daniel Pfeiffer** Directeur
Pierre JOUVE pierre.jouve Signature numérique de Pierre JOUVE pierre.jouve Date : 2025.11.14 16:35:12 +01'00'	Alexandre DUSSERRE alexandre.dusserre 2025.11.14 17:11:01 +01'00'	Le Directeur du Service Technique des Remontées Mécaniques et de Transports Guidés Daniel PFEIFFER Date : 2025.11.14 17:44:12 +01'00'

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

Le titre V du livre I^er^ de la troisième partie de la partie règlementaire du code des transports fixe les exigences de sécurité applicables aux systèmes de transport routier automatisés fournissant un service de transport de personnes, et notamment le principe « Globalement au moins équivalent ».

Ces mêmes exigences sont applicables aux systèmes de transport routier automatisés de marchandises relevant du titre V du livre II de la troisième partie de la partie réglementaire du code des transports (en application de l'article R. 3251-1 du code des transports).

En complément du guide d'application GAME[1] qui présente les différentes approches de la démonstration de sécurité dans le cadre du principe GAME, le présent guide technique 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 » ;*
- *Décrire les différents cas de mise en œuvre de la démarche de type 3 ;*
- *Décrire les principes de l'estimation des risques pour les systèmes de transport routier automatisés ;*
- *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.

Enfin, ce guide ne vise pas à préciser le rôle de chaque partie dans la production des différents éléments et documents constituant les dossiers, sur la base desquels la démonstration de sécurité est conduite.

[1] Guide du STRMTG : Guide d'application relatif au principe GAME pour les STRA (« STRA - Principe « GAME » Globalement au moins équivalent ») - https://www.strmtg.developpement-durable.gouv.fr/guide-d-application-game-pour-les-systemes-de-a769.html

2 Définitions

« 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.

« Accident mortel » : accident ayant entraîné le décès d'au moins une personne sur le coup ou dans les trente jours qui suivent l'accident.

« 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.

« 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 *(article R. 311-1-1 du code de la route).*

« 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).*

« Domaine de conception technique du système » : conditions d'opération dans lesquelles un système technique de transport routier automatisé est spécifiquement conçu pour fonctionner, à l'exclusion, pour les systèmes de transport routier automatisé de marchandises, des opérations de chargement et de déchargement des marchandises.

« 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 *(article R. 3151-1 du code des transports).*

« 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 ») : Événement 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 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 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.

« 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'acquitter 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 *(article R. 3151-1 du code des transports).*

« 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'acquittement de manœuvre demandé par le système *(article R. 3151-1 du code des transports).*

« 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 *(article R. 3151-1 du code des transports).*

« 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.

« 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 *(article R. 3151-1 du code des transports)*

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

« 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 *(article R. 3151-1 du code des transports).*

« 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 *(article R. 3151-1 du code des transports).*
Note : dans la suite du document, le terme "parcours" est communément utilisé en lieu et place de "parcours ou zone de circulation prédéfinie ».

« Passager » : catégorie d'usager 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.

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

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

« Station » : point d'arrêt prédéfini des véhicules destiné à permettre l'accès des usagers aux véhicules dans un système de transport routier automatisé de personnes. Par extension, ce terme désigne également un point d'arrêt destiné à permettre le chargement ou le déchargement des marchandises dans un système de transport routier automatisé de marchandises.

« 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

« Système de conduite automatisé » : système associant des éléments matériels et logiciels, permettant d'exercer le contrôle dynamique d'un véhicule de façon prolongée *(article R. 311-1-1 du code de la route).*

« 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 *(article R. 3151-1 du code des transports).*
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 de marchandises » : 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 réaliser une activité de transport routier de marchandises » *(article R. 3251-2 du code des transports).*

« Système de transport routier automatisé de personnes » : 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.

« Système de transport routier automatisé » : système de transport routier automatisé de personnes ou système de transport routier automatisé de marchandises.
Note : la définition de « système de transport routier automatisé » utilisée dans ce guide est volontairement plus large que celle de l'article R.3151-1 du code des transports. Elle recouvre à la fois les systèmes de transport routier automatisés de personnes qui relèvent du titre V du livre I^er^ de la troisième partie de la partie réglementaire du code des transports et les systèmes de transport routier automatisés de marchandises qui relèvent du titre V du livre II de la troisième partie de la partie réglementaire du code des transports.

« Usager » (du système) : terme général faisant référence au rôle de l'humain par rapport à la délégation de conduite (*SAE J3016*).
Note : Dans ce document, le terme « usager » est employé pour désigner l'usager du système, par opposition aux « autres usagers » de la route (ou de la voirie).
L'usager du système peut être par exemple le passager à bord d'un véhicule du système, la personne en attente d'être prise en charge, les personnes en charge du chargement et du déchargement des marchandises[2], etc.
Par ailleurs, même si elle peut être rattachée à l'usager, la notion de personnel d'exploitation est préférée à celle d'usager du système pour désigner les personnels en charge de l'exploitation et de la maintenance du système : opérateur d'intervention à distance, opérateur d'intervention locale, etc.

« 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 aux usagers du système, les « autres » usagers de la route représentent les tiers.

[2] Les opérations de chargement et de déchargement des marchandises n'entrent pas dans le périmètre du présent guide.

« 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 1° de l'article R. 3151-1 du code des transports *(article R. 311-1 du code de la route).*

« 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 *(article R. 311-1 du code de la route).*

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)*
AUGT : Transports guidés urbains automatiques
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 : Evènement redouté
ERP : Etablissement recevant du public
E/E : Electriques et électroniques
FO : Forces de l'ordre
FRR : Facteur de réduction du risque
G : Classe de gravité
GAME : Globalement au moins équivalent
ID : Identifiant
IHM : Interface homme-machine
MRM : Manœuvre à risque minimal
MRC : Situation de risque minimal
MRR : Mesure de réduction du risque
NA : Non applicable
OGS : Objectif global de sécurité
OQA : Organisme qualifié agréé
OSS : Objectif spécifique de sécurité
PCC : Poste de commande centralisé
PMR : Personne à mobilité réduite
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
STRA-M : Système de transport routier automatisé de marchandises

STRA-P : Système de transport routier automatisé de personnes
TFDR : Taux d'occurrence de dysfonctionnements des fonctions du système (« Tolerable functional dysfunction Rate »)
TFFR : Taux de défaillance fonctionnelle acceptable (« Tolerable functional failure rate »)
TFIR : Taux d'occurrence d'insuffisances fonctionnelles acceptable (« Tolerable functional insuffisencies rate »)
TFR : Taux de dysfonctionnement acceptable (« Tolerable fail rate »)
TMD : Transport de marchandises dangereuses
VP : Véhicule prioritaire
VRU : Voie rapide urbaine

4 Contexte réglementaire

Le présent guide est applicable aux systèmes de transport routier automatisés de personnes relevant du titre V du livre I^{er} de la troisième partie de la partie règlementaire du code des transports (articles R. 3151-1 à R. 3153-1) et aux systèmes de transport routier automatisés de marchandises relevant du titre V du livre II de la troisième partie de la partie réglementaire du code des transports (articles R. 3251-1 à R. 3253-1).

Le code des transports introduit l'obligation, pour les systèmes de transport routiers automatisés de respecter le principe « GAME » en ce qui concerne leur niveau de sécurité.
Pour les systèmes de transport routier automatisés de personnes (STRA-P), cette exigence est formalisée par l'article R. 3152-2 du code des transports :
« 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. […] »

Cette même exigence est ensuite transposée pour les systèmes de transport routier automatisé de marchandises (STRA-M) par l'article R. 3251-1 du code des transports :
« Art. R. 3251-1. – Les dispositions du titre V du livre premier de la troisième partie du présent code sont applicables au transport routier de marchandises, lorsqu'il est effectué au moyen d'un système de transport routier automatisé, sous réserve des dispositions prévues au présent titre. »

En complément, l'article R. 3152-2 précité 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.

Opérations de chargement et de déchargement des marchandises

Dans le cas des systèmes de transport routier automatisé de marchandises (STRA-M), les opérations de chargement et de déchargement des marchandises, y compris les opérations d'arrimage des marchandises, sont exclues du domaine de conception technique du système et ne font pas partie du périmètre de la démonstration GAME (2. de l'article R. 3251-2. du code des transports).
Seules leurs interfaces avec les fonctions de conduite automatisée sont prises en compte et décrites dans le dossier de conception du système technique (article R. 3252-2 du code des transports).

Transports interdits

Le transport, dans le cadre d'un STRA, de marchandises dangereuses et de marchandises dont le transport est soumis à l'obtention d'un agrément en application des dispositions particulières qui leur sont applicables, est interdit. *(*Article. R.3252-11 du code des transports)

De même, le transport, dans le cadre d'un STRA, d'engins ou de véhicules présentant un caractère exceptionnel en raison de leurs dimensions ou de leur masse, est interdit sauf autorisation spécifique. (Article R.3252-10 du code des transports)

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 pourront être détaillés dans les mises à jour 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.

Exigences selon la nature du service de transport
Par défaut, les éléments présentés dans la suite de ce document concernent les STRA au sens général.

Lorsque pertinent, le document précise pour certains éléments s'ils concernent plus spécifiquement les STRA-P ou plus spécifiquement les STRA-M.

Cette précision reste indicative, en particulier pour les systèmes prévoyant un transport effectué à titre accessoire. En application de l'article R. 3252-12 du code des transports, ces systèmes sont concernés par l'ensemble des éléments :
- Le transport routier automatisé de marchandise effectué à titre accessoire au moyen d'un STRA-P est également concerné par les éléments du guide spécifiques aux STRA-M ;
- Le transport routier automatisé de personnes effectué à titre accessoire au moyen d'un STRA-M est également concerné par les éléments du guide spécifiques aux STRA-P.

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 système de gestion de la sécurité 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 autres 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.

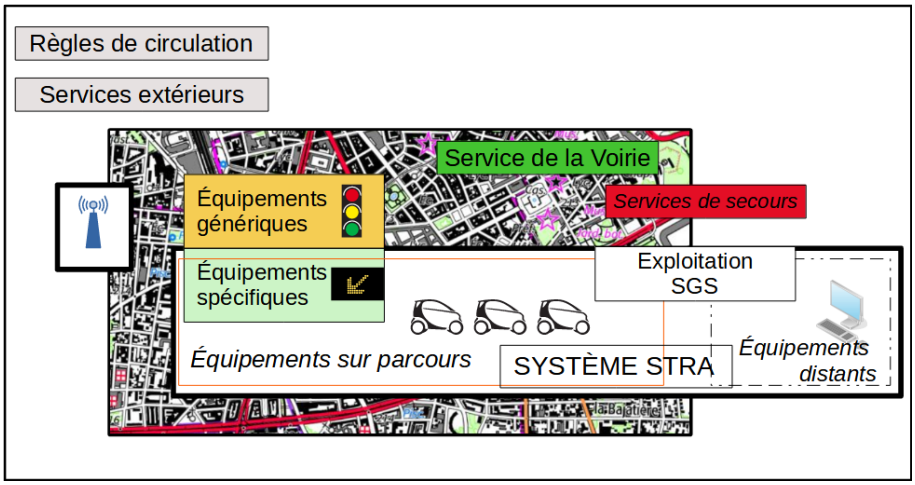


Figure 1 - Décomposition organique d'un STRA

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.

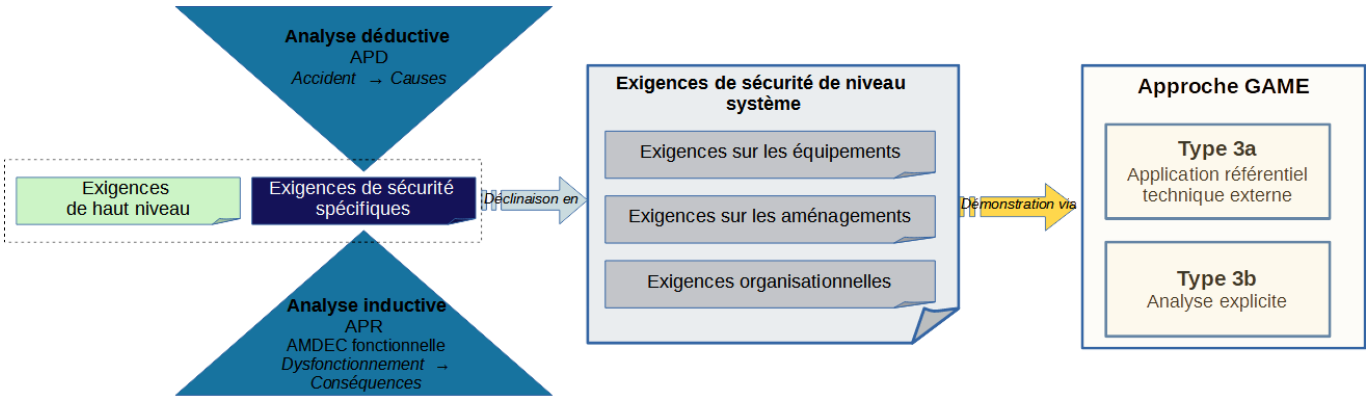


Figure 2 - Analyse détaillée type 3

On distingue 2 types d'exigences :

- <u>Les exigences de haut niveau :</u>

Les exigences de haut niveau présentées au chapitre 9 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.

- <u>Les exigences spécifiques :</u>

Les exigences spécifiques sont définies pour le projet au moyen de 2 analyses complémentaires présentées aux chapitres 10 et 11 :

- 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.

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.

6 Cas de l'application d'un référentiel technique hors-STRA (type 3a)

6.1 Généralités

L'approche de type 3a consiste à identifier un référentiel hors-STRA et à analyser ce référentiel afin de démontrer son aptitude à couvrir le danger identifié dans le contexte STRA. Les exigences du référentiel doivent alors être respectées en prenant en compte les éventuelles contraintes liées à l'application du référentiel.

Comme expliqué au chapitre précédent, l'analyse détaillée nécessite la réalisation d'une analyse exhaustive des dangers, au moyen de 2 analyses complémentaires :

- Une analyse déductive type analyse préliminaire des dangers qui explore pour chaque accident toutes les causes et combinaisons de causes pouvant conduire à cet accident (cf. § 10) ;
- Une analyse inductive type analyse préliminaire des risques qui analyse les dysfonctionnements possibles de chaque fonction et leurs conséquences (cf. § 11).

Cette analyse permet d'identifier l'opportunité d'utilisation de référentiels techniques issus d'un domaine autre que celui des STRA, spécifiant les moyens aptes à traiter chaque danger identifié par l'analyse exhaustive des dangers et pouvant être transposés dans le contexte STRA.

Les conditions de l'acceptabilité d'un référentiel externe concernent les points suivants (cf. Guide d'application relatif au principe GAME pour les STRA v1 §4 .2) :

- Référentiel reconnu ;
- Champ d'application compatible ;
- Prise en compte des éléments de contexte du référentiel ;
- Formalisation des hypothèses et contraintes exportées attachées au référentiel ;
- Compatibilité entre les exigences issues des différents référentiels couvrant les différents dangers[3];
- Couverture précise du danger à travers toutes les exigences issues de l'analyse dans le contexte STRA.

Cette dernière condition conduit à ce que l'approche type « application d'un référentiel technique hors-STRA » (type 3a) concerne uniquement les cas où l'application d'un unique référentiel hors-STRA permet de couvrir le danger identifié dans le contexte STRA.
Dès lors qu'il est nécessaire de juxtaposer plusieurs référentiels pour couvrir une même situation dangereuse, ou de combiner un référentiel et des mesures complémentaires, une analyse explicite est nécessaire (démarche de type 3b).

Le tableau suivant synthétise les principales étapes de la démarche d'application d'un référentiel technique hors-STRA (type 3a).

[3] Par exemple, le référentiel mis en œuvre pour traiter le danger « Chute de personne à l'intérieur du véhicule » pourrait fixer une valeur de décélération maximale, qui serait incompatible avec les exigences visant à traiter le danger de type « collision ».

	Activité	Observations et commentaires	Renvoi
1	Rappeler les situations dangereuses via une APD (Analyse préliminaire des dangers).	- Identification des situations dangereuses (SD) pour un scénario d'accident donné.	Cf. chapitre 10
2	APR (Analyse préliminaire de risques)	- Identification des causes des SD. - L'APR permet de faciliter l'identification des dysfonctionnements du système STRA en les liant aux SD.	Cf. chapitre 11
3	Identification et démonstration de l'acceptabilité d'un référentiel technique hors-STRA pour une SD	- Analyse des points communs entre les domaines pour la SD. - Analyse de la couverture du référentiel proposé. - Analyse des éléments de contexte du référentiel proposé. - Analyse des spécificités propres aux STRA. - Vérification de la compatibilité entre les référentiels mis en œuvre pour les différentes SD.	*Non traité dans le présent guide.* (Cf. guide application relatif au principe GAME pour les STRA version 1 §4.2)
4	Mise en œuvre du référentiel et prise en compte de ses contraintes exportées		*Non traité dans le présent guide*

Tableau 1 – Canevas de l'application d'un référentiel technique hors-STRA (type 3a)

6.2 Exemples d'application

Sur la base des accidents potentiels listés dans le tableau 11, le tableau suivant propose des exemples de référentiels pouvant être identifiés pour traiter différentes situations dangereuses issues de l'analyse exhaustive d'un STRA.

La colonne de droite « Type 3a possible » illustre pour exemple la limitation de l'approche de type 3a aux situations dangereuses pour lesquelles l'application d'un unique référentiel hors-STRA est suffisante.
A contrario, les exemples pour lesquels plusieurs référentiels, ou la combinaison de référentiels et de mesures complémentaires, est nécessaire, devront faire l'objet d'une analyse explicite (type 3b) telle que présentée au chapitre suivant.

Les référentiels proposés dans le tableau sont donnés à titre d'exemple pour guider la démarche de démonstration, sans préjuger de leur acceptabilité qui doit être démontrée.
Lorsqu'ils s'appliquent au véhicule lui-même, les éléments de référentiels proposés dans ce tableau peuvent uniquement compléter les exigences issues des référentiels d'homologation applicables au véhicule mais ne peuvent s'y substituer.

D'autre part, ces référentiels pourront faire l'objet de mises à jour ou être remplacés par de nouveaux référentiels.

Tableau 2 – Exemples de référentiels hors-STRA et analyse de la possibilité de l'approche de type 3a

Caractéristiques Accidents (cf Tableau 11 « Liste des accidents de niveau système »)			**Eléments d'analyse**				**Type 3a possible**
TYPOLOGIE	**ID**	**ACCIDENTS POTENTIELS**	**SD potentielle issue des analyses**	**Comparaison entre STRA et autres systèmes**	**Exemple de référentiels potentiels en lien avec la SD**	**Compléments**	
Chute de personnes (STRA-P)	2.1	Chute de personne à l'intérieur du véhicule dans le cas des véhicules avec passagers debout	Chute suite application freinage - décélération excessive	Les véhicules sont conformes aux prescriptions relatives au freinage dans le cadre de leur homologation. En complément, des éléments relatifs aux décélérations des véhicules avec passagers debout, peuvent être issus des systèmes tramways .	EN 13452-1 § 6.2.3. « Performances de confort »		Oui
			Chute du fait des sols (glissants, marche, obstacle…)	Référence transport en commun de personnes (véhicules M2/M3)	Règlement UN R107 Application des clauses adéquates concernant les revêtements du sol		Oui
			Chute du fait de manque de moyen de maintien pour les passagers debout	Référence transport en commun de personnes (véhicules M2/M3)	Règlement UN R107 clause 7.11 « Barres et poignées de maintien »		Oui
	2.2	Chute de personne depuis le véhicule du système vers l'extérieur en station	Chute suite défaillance mécanique ou mouvement intempestif de rétractation rampe PMR (STRA-P)	Référence transport en commun de personnes (véhicules M2/M3)	Règlement UN R107 annexe 8 « stationnement et accessibilité des voyageurs à mobilité réduite »		Oui
			Chute lors de l'entrée sortie du véhicule (à quai ou hors quai)		Règlement UN R107 § 7.7.7 « marches » et fig. 8 annexe 4 + Guide du CERTU § 4.2.1 pour les lacunes		Non
	2.3	Chute de personne depuis le véhicule du système vers l'extérieur en ligne	Chute depuis un véhicule suite à l'ouverture intempestive d'une porte	Différents référentiels pouvant être considérés : - transport en commun de personnes (véhicules M2/M3) - tramway avec une détection ouverture intempestive de porte	{Règlement UN R107 Point 7.6.5 + analyse FMDS des fonctions selon ISO 26262 ou IEC 61508} ou EN14752 « Applications ferroviaires – Systèmes d'accès latéraux pour matériel roulant »		Non
Renversement	3.1	Renversement véhicule	Renversement en roulage ou lors de présence de vent latéral ou de défaillance mécanique (possible blessures et écrasements passagers	Exigences issues des référentiels d'homologation en termes de stabilité et de renversement	Règlement UN R107 : Annexe 3, Point 7.4: Essai de stabilité statique (Angle de 28° véhicule en charge)		Oui

Caractéristiques Accidents (cf Tableau 11 « Liste des accidents de niveau système »)			**Eléments d'analyse**				**Type 3a possible**
TYPOLOGIE	**ID**	**ACCIDENTS POTENTIELS**	**SD potentielle issue des analyses**	**Comparaison entre STRA et autres systèmes**	**Exemple de référentiels potentiels en lien avec la SD**	**Compléments**	
Electrisation/Électrocution	4.1	Electrisation/Electrocution dans le véhicule	Dans le véhicule ou à l'extérieur au contact du véhicule	Exigences issues des véhicules électriques (voiture ou bus selon catégorie)	{Règlement UN R100 : Annexe 3 « Protection contre les contacts directs avec des pièces sous tension » + surveillance de la résistance d'isolement + alerte PCC sur détection de défaut et arrêt de la mission au plus tôt}		Non
Feu/fumée/ explosion	5.1	Feu/fumée dans le véhicule	Non prise en compte d'un incendie (Non détection, détection tardive ou absence d'action résultant de la détection)	Comparaison avec un système « métro automatique » du fait de la non présence de conducteur ou personnel pour gérer la situation à bord : - Système de communication et d'alarme des passagers vers le PCC (STRA-P), - détection feu/fumée et alarme au PCC, - Arrêt automatique du véhicule.	{Norme IEC EN 62267 clause 8.5.12 à adapter : - alarme feu ou fumée reportée automatiquement au PCC - action d'arrêt sur les trains (véhicule) Norme IEC 62267 clause 8.5.10 à adapter (STRA-P) : - poignée (ou autre dispositif) d'urgence avec alerte PCC. - action d'arrêt sur les trains (véhicule) Norme IEC 62267 clause 8.5.11 en totalité (STRA-P): - communication audio (voir IEC 62267 clause 8.5.8) et vidéo surveillance (voir IEC 62267 clause 8.5.7 + EN 45545 (feu fumées) + EN 16334 (Systèmes d'alarme)}	La priorité doit être l'évacuation immédiate. Toutefois une étude du site est nécessaire pour définir des éventuelles zones nécessitant (du fait de dangers spécifiques comme tunnel, fleuve) une temporisation sur l'arrêt. - Particularités éventuelles de parcours à prendre en compte : cf. Tableau 12 point 4. - « Arrêt non voulu sur zone à risque type PN » : cf. Tableau 13 point 4 - Aptitude au roulement en cas d'incendie (EN 50553) pour atteinte zone "refuge" (cas tunnels)	Non
			Asphyxie / suffocation / brulure du fait de l'apparition d'un incendie et de la non possibilité de traitement local (absence de moyen de lutte) (STRA-P)	Comparable à un véhicule de transport en commun M2/M3 => conception vis-à-vis de l'incendie en considérant les exigences pour les catégories M2/M3 Ou Peut être comparé à un métro automatique du fait de la non présence de conducteur ou personne	{Application des clauses adéquates de UN R107 pour les moyens de lutte contre l'incendie - Annexe 3, Point 7.5 « Prévention des risques d'incendie » + absence de personnel à bord à traiter} ou référentiels AUGT	Absence de personnel à bord à traiter : - Présence effective des moyens de lutte - Information sur l'utilisation - cas de PMR ou personne isolée	Non

Caractéristiques Accidents (cf Tableau 11 « Liste des accidents de niveau système »)			**Eléments d'analyse**				**Type 3a possible**
TYPOLOGIE	**ID**	**ACCIDENTS POTENTIELS**	**SD potentielle issue des analyses**	**Comparaison entre STRA et autres systèmes**	**Exemple de référentiels potentiels en lien avec la SD**	**Compléments**	
Autres accidents de personnes	6.1	Personnes coincées/pincées par les ouvrants (fenêtres, portes, etc.) d'un composant du système	Coincement dans mécanismes portes dû à des forces de fermeture trop élevées	Porte motorisée du véhicule à considérer de la même manière que les portes motorisées et rampe PMR des véhicules de catégories M2/M3	Règlement UN R107 pour le dimensionnement et la conception de la porte		Oui
	6.2	Personnes coincées/pincées par une partie mobile d'un composant du système	Coincement par la rampe PMR dû à des forces de fermeture trop élevées	Rampe PMR (cas STRA-P) à considérer de la même manière que la rampe PMR des véhicules de catégories M2/M3	Règlement UN R107 Annexe 8 pour la conception de la rampe PMR		Oui

7 Cas de l’analyse explicite (type 3b)

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

Ce chapitre présente les 2 déclinaisons possibles de l’analyse explicite de type 3b :

- Analyse explicite avec objectif quantitatif : un objectif de sécurité quantitatif peut être déterminé, puis alloué de manière successive aux différentes fonctions (cf. §7.1) ;
- Analyse explicite sans objectif quantitatif : à défaut, lorsqu’il n’est pas possible de déterminer un objectif quantitatif, une démarche qualitative permet de définir les mesures permettant de ramener le risque résiduel à un niveau acceptable (cf. §7.2).

7.1 Analyse explicite avec objectif quantitatif

Dans le cas d’une catégorie d’accidents pour laquelle il existe des données issues du retour d’expérience, suffisantes et cohérentes avec le domaine d’emploi du système, un objectif de sécurité quantitatif peut être déterminé. La stratégie de traitement du risque repose alors sur la déclinaison de cet objectif quantitatif aux différents éléments qui peuvent conduire à cette catégorie d’accidents.

Le tableau suivant présente les étapes de cette démarche d’analyse explicite avec objectif quantitatif (type 3b).

	Activité	Observations et commentaires	Renvoi
1	Déterminer le ou les objectifs quantitatifs : - Objectif global de sécurité (OGS) pour des catégories d'accidents (exemple : collision). - Eventuellement, les objectifs spécifiques de sécurité (OSS) pour chaque type d'accident dans la catégorie (exemple : collision avec différents tiers, ou collision sans tiers).	- Le critère d'acceptation du risque peut être défini en termes de taux d'occurrence maximal acceptable d'accident (OGS). - Eventuellement, associer pour chaque type d'accident l'OSS qui lui correspond.	Cf. §7.1.1
2	Rappeler les situations dangereuses (SD) via une analyse préliminaire des dangers (APD).	- Identification des situations dangereuses (SD) pour un scénario d'accident donné. - Identification des SD concernées par l'OSS.	Cf. chapitre 10
3	Allouer le ou les objectifs quantitatifs de sécurité sur les situations dangereuses (SD). Calculer un objectif TFR relatif aux SD qui intègre l'expression de contexte propice à l'accident.	- 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). - (Le TFR représente le taux de dysfonctionnements, i.e. le taux des défaillances et des insuffisances fonctionnelles.)	Cf. §7.1.2
4	Réaliser une analyse préliminaire de risques (APR)	- Identification des causes des SD. - L'APR permet de faciliter l'identification des dysfonctionnements du système STRA en les liant aux SD.	Cf. chapitre 11
5	Répartir les objectifs de TFR (relatif aux SD) sur les fonctions du système STRA : le TFR est réparti sur les dysfonctionnements des fonctions techniques (TFDR). Ces dysfonctionnements constituent les ER (événements redoutés).	- Cette répartition en TFDR 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. - L'objectif de cette étape permet de vérifier que TFR < Σ_i TFDR(i).	Cf. §7.1.2
5	Répartir le taux de dysfonctionnements (TFDR) de chaque fonction entre le taux de défaillance (TFFR) et le taux d'insuffisances fonctionnelles (TFIR).	- Pour chaque fonction, TFDR = TFFR + TFIR.	Cf. §7.1.2
6	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*
7	Traduire le TFIR en objectifs concernant les insuffisances fonctionnelles.	- A partir de l'objectif TFIR, graduer les moyens mis en œuvre pour réduire les insuffisances fonctionnelles	*Non traité dans le présent guide*

Tableau 3 – Etapes de la démarche d'analyse explicite avec objectif quantitatif

7.1.1 Détermination d'objectifs de sécurité quantitatifs

7.1.1.1 Périmètre des objectifs de sécurité quantitatifs

Les objectifs de sécurité quantitatifs peuvent s'appliquer à différents périmètres :

- Périmètre global : l'objectif concerne le système pour la globalité de son domaine d'emploi pour une typologie d'accident, et constitue un objectif global de sécurité (OGS);
- Périmètre spécifique, i.e. catégorie d'accidents, types de configurations, etc. : l'objectif concerne un sous-domaine au sein du domaine d'emploi du système et constitue un objectif spécifique de sécurité (OSS).
  Un tel objectif spécifique de sécurité peut être défini lorsque des données suffisamment précises et significatives permettent de répartir l'objectif global sur les différentes sous-catégories d'accidents.

Par exemple, dans le cas des accidents de type « collision », des objectifs quantitatifs peuvent être déterminés sur la base des données d'accidentalité des véhicules conventionnels utilisées comme références d'accidentalité :

- Un objectif global fixera la probabilité maximale admissible pour le système d'être impliqué dans une collision, quelles que soient les circonstances ;
- Un ou des objectifs spécifiques complémentaires pourront fixer la probabilité maximale admissible pour le système d'être impliqué dans une collision à une intersection.

7.1.1.2 Expression des objectifs de sécurité quantitatifs

Un objectif de sécurité quantitatif est exprimé en termes de nombre d'accidents[4] rapporté à la dimension caractérisant le « volume d'exploitation » du système.

De manière à prendre également en considération la gravité de l'accident, un objectif quantitatif est décliné selon le niveau de gravité potentiel de l'accident en distinguant 2 catégories :

- Accident mortel : accident pouvant conduire à au moins 1 décès (gravité G=3)[5,6]
- Accident non mortel : accident pouvant conduire uniquement à des blessés (gravité G=1 et G=2).

Pour les accidents de type collision par exemple, le volume d'exploitation du système pour ce qui concerne les fonctions embarquées, peut être mesuré par le nombre de km parcourus par l'ensemble des véhicules du système ou par le nombre d'heures d'exploitation cumulées pour l'ensemble des véhicules du système. Les différents objectifs quantitatifs, objectif global ou objectifs spécifiques, s'expriment alors sous forme du ratio,

- Du nombre de collisions mortelles, i.e. ayant entraîné au moins 1 décès, par heure de circulation ou par km parcouru ;
- Du nombre de collisions non mortelles, i.e. ayant causé au moins une victime mais n'ayant pas entraîné de décès, par heure de circulation ou par km parcouru.

7.1.1.3 Elaboration d'objectifs de sécurité quantitatifs

Des objectifs de sécurité quantitatifs peuvent être déterminés sur la base des données issues du retour d'expérience lorsque celles-ci sont considérées comme fiables, suffisantes et représentatives pour le type d'accident et pour le système sur lesquels porte l'analyse.

[4] Les exigences issues de l'analyse explicite visent à réduire la survenue des accidents. L'objectif quantitatif est donc exprimé en termes de nombre d'accidents et non en termes de nombre de victimes potentielles.
[5] L'échelle de cotation de la gravité est définie au §8.2.
[6] Y compris les accidents marqués (*) au sein de la classe G3 (cf. §8.2)

Par exemple, pour les accidents de type collision, le fichier national de l'accidentalité routière constitué des Bulletins d'analyse des accidents corporels (BAAC)[7] recense pour la France les accidents corporels de la circulation des véhicules conduits manuellement, portés à la connaissance des forces de l'ordre. Les données de ce fichier peuvent permettre de construire des références d'accidentalité pour l'analyse de sécurité des STRA. Celles-ci peuvent être utilisées pour élaborer les objectifs quantitatifs de sécurité représentatifs du domaine d'emploi du système.

Le processus d'élaboration des objectifs quantitatifs doit refléter la prudence nécessaire en prenant en compte des hypothèses conservatives et en intégrant les marges de sécurité suffisantes, liées au caractère innovant des STRA et aux attentes sociétales fortes quant à leur sécurité.

Par exemple, pour les accidents de type collision, les objectifs quantitatifs doivent refléter l'exigence de prendre pour référence les véhicules conduits manuellement de façon compétente et prudente[8], en cohérence avec les exigences issues du règlement UE 2022/1426 du 5 août 2022 pour la réception par type des systèmes de conduite automatisée (ADS) des véhicules entièrement automatisés. Dans le contexte des STRA, cette exigence de se référer à un conducteur compétent et prudent, est encore renforcée par la qualité de « professionnel de la conduite » du conducteur assurant un service de transport routier.

Des références d'accidentalité issues de l'analyse du fichier national de l'accidentalité routière sont présentées en annexe 2.

7.1.1.4 Raffinement des objectifs de sécurité quantitatifs

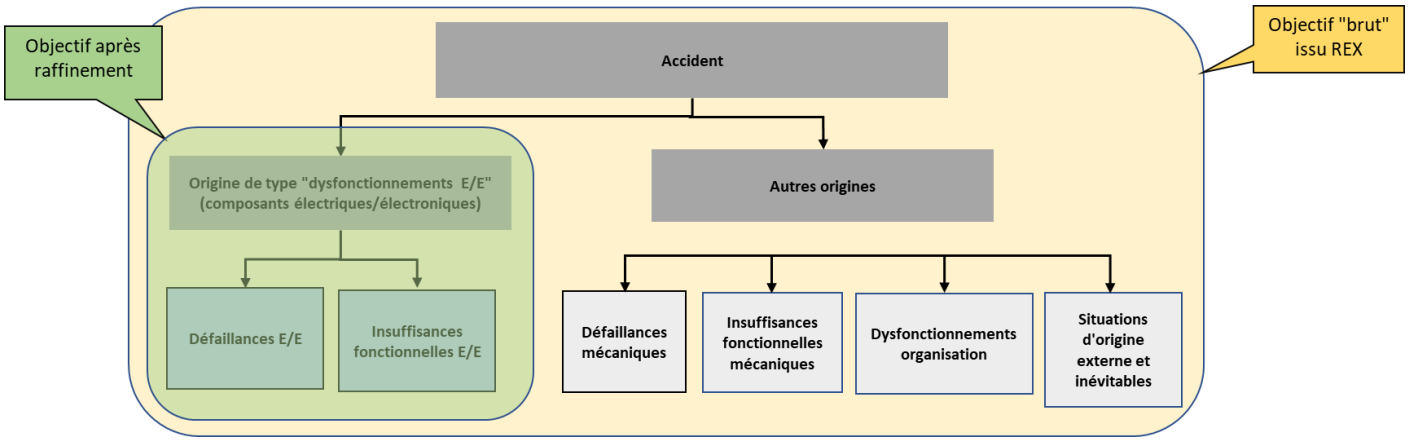


Figure 3 – Raffinement de l'objectif quantitatif

Lorsque les objectifs de sécurité quantitatifs sont basés sur des données du retour d'expérience qui englobent toutes les causes possibles des accidents, il est nécessaire de raffiner les valeurs cibles de ces

[7] Pour tout accident corporel (soit un accident survenu sur une voie ouverte à la circulation publique, impliquant au moins un véhicule et ayant fait au moins une victime ayant nécessité des soins), des saisies d'information décrivant l'accident sont effectuées par l'unité des forces de l'ordre (police, gendarmerie, etc.) qui est intervenue sur le lieu de l'accident. Ces saisies sont rassemblées dans une fiche intitulée bulletin d'analyse des accidents corporels. L'ensemble de ces fiches constitue le fichier national des accidents corporels de la circulation dit « Fichier BAAC » administré par l'Observatoire national interministériel de la sécurité routière "ONISR". Cf. https://www.data.gouv.fr/fr/datasets/bases-de-donnees-annuelles-des-accidents-corporels-de-la-circulation-routiere-annees-de-2005-a-2022/

[8] L'annexe II du règlement UE 2022/1426 prévoit en 7.1.1 que « le constructeur doit définir les critères d'acceptation à partir desquels les cibles de validation du système ADS sont dérivées afin d'évaluer le risque résiduel pour l'ODD en prenant en compte, si disponibles, des données d'accident existantes, des données sur les performances de véhicules conduits manuellement de façon compétente et prudente et de l'état de l'art technologique ».

objectifs quantitatifs en soustrayant la fraction[9] des accidents dont l'origine n'est pas compatible avec une analyse quantitative.

Ces accidents dont l'origine n'est pas compatible avec une analyse quantitative, doivent faire l'objet d'un ensemble d'exigences qualitatives et organisationnelles relatives aux moyens mis en œuvre. Celles-ci visent à en diminuer l'occurrence et/ou à en réduire les effets, mais ne permettent pas de les éliminer complètement.
En pratique, il s'agit des accidents dont l'analyse montre que l'origine n'est pas due au dysfonctionnement des composants électriques et électroniques (E/E), qu'il s'agisse de défaillances E/E ou d'insuffisances fonctionnelles E/E. Il est possible de répartir cette catégorie d'accidents en plusieurs sous-catégories selon leur origine :

- Accidents dus aux défaillances des composants mécaniques : ils ne sont pas traités à l'aide d'objectifs probabilistes, mais via le respect de principes de conception, de procédures de contrôle et des codes de pratique.
  La démonstration vise à démontrer que les mesures mises en œuvre en matière de conception, de contrôles, et de surveillance permettent de prévenir la défaillance d'origine mécanique conduisant à chaque situation dangereuse analysée.
  Ces mesures peuvent par exemple intégrer la mise en œuvre de principes de redondance, la réalisation de tests, la mise en place de contrôles internes, la surveillance en exploitation, les contrôles périodiques, des règles de maintenance, etc. Lorsque ces mesures concernent les véhicules, elles peuvent s'appuyer sur les exigences démontrées dans le cadre de la réception des véhicules, si celles-ci restent suffisantes dans le contexte des véhicules à délégation de conduite.

- Accidents dus aux insuffisances fonctionnelles des composants mécaniques, qui représentent les cas où les composants mécaniques implémentés ne remplissent pas la fonctionnalité souhaitée en raison d'une insuffisance dans leurs spécifications ou dans leurs performances.
  En pratique, il est considéré que la problématique des insuffisances fonctionnelles de composants mécaniques doit être traitée par des mesures qualitatives permettant de minimiser leur occurrence : les véhicules font l'objet d'une réception, le système fait l'objet d'une démonstration de sécurité spécifique et d'essais préalables à sa mise en service, les règles d'exploitation et de maintenance sont formalisées et évaluées, etc.

- Accidents dus à des facteurs humains et organisationnels : les différents acteurs du système peuvent également être à l'origine de dysfonctionnements du système. Par exemple, le non-respect d'une règle d'exploitation ou de maintenance peut amener le système dans une situation dangereuse. Ces dysfonctionnements doivent être traités par des mesures qualitatives permettant de réduire leur occurrence. Les moyens mis en œuvre dans le cadre de l'évaluation de la sécurité et du suivi en exploitation visent à ce que les principes d'exploitation et de maintenance définis soient adaptés, cohérents et appliqués : le système de gestion de la sécurité en exploitation est évalué préalablement à la mise en service, son application et son adéquation à l'évolution des enjeux de sécurité font l'objet d'un audit périodique, etc.

- Accidents pouvant être considérés comme inévitables : ce sont les accidents liés aux situations dangereuses d'origine extérieure au système et raisonnablement non évitables, i.e. pour lesquelles il est acceptable de dire que le système ne peut raisonnablement pas les éviter[10], en prenant pour référence les capacités d'un conducteur humain compétent et prudent [11]. C'est par exemple le cas de la collision par l'arrière d'un véhicule du système arrêté à un feu rouge, pour laquelle des mesures de réduction du risque de signalisation et de protection passive peuvent être spécifiées, mais qui ne seront opérantes que dans certaines limites.

[9] La valeur de la fraction à soustraire doit faire l'objet d'estimations à dire d'expert dans un premier temps. Cette estimation devra ensuite faire l'objet d'un suivi dans le cadre des activités de surveillance en service.
[10] L'ensemble des autres situations dangereuses d'origine extérieure sont bien par ailleurs traitées dans les autres volets de la démonstration de sécurité.
[11] Cf. annexe II §7.1.1. du règlement UE 2022/1426 qui prévoit la référence aux « véhicules conduits manuellement de façon compétente et prudente. ».

Ces accidents dont l'origine n'est pas compatible avec une analyse quantitative font l'objet d'exigences de respect de référentiels de bonnes pratiques, de mise en œuvre de règles de conception et de mise en place de mesures organisationnelles, ou font l'objet d'une analyse explicite sans objectif quantitatif (cf. §7.2).

7.1.2 Allocation des objectifs de sécurité quantitatifs

Dans le cas d'une analyse explicite (type 3b), les objectifs 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 est faite selon le canevas suivant :

7.1.2.1 Déclinaison de l'objectif au TFR sur chaque situation dangereuse

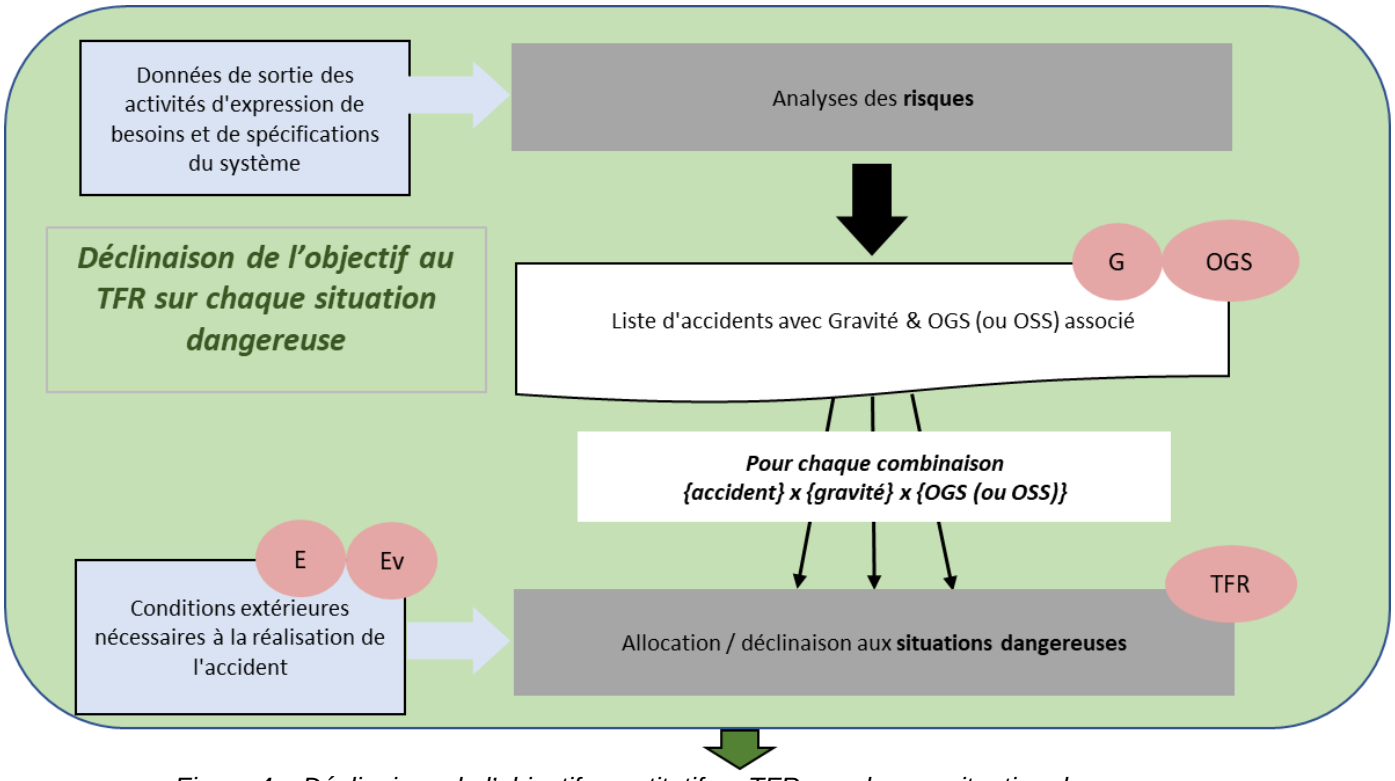


Figure 4 – Déclinaison de l'objectif quantitatif au TFR sur chaque situation dangereuse

L'analyse préliminaire des dangers (analyse déductive – cf. §10) identifie pour chaque accident du système les différents scénarios conduisant possiblement à cet accident, et décrit pour chacun son contexte et les actions des différents acteurs (tiers et ego).

L'accident est considéré comme la conséquence d'un dysfonctionnement (situation dangereuse), qui se concrétise dès lors que ses « conditions de réalisation » sont remplies (cf. §8.3).
L'analyse déductive détermine ensuite pour chaque situation dangereuse, la gravité de l'accident qui peut en résulter d'une part, et la probabilité de survenue de ses conditions de réalisation d'autre part :

- Le niveau de gravité distingue les scénarios pouvant conduire à des accidents mortels, des scénarios pouvant conduire à des accidents non mortels pour lesquels les circonstances et les

protections mises en place permettent d'éliminer le risque de décès. Chaque scénario sera ainsi « aiguillé » vers l'objectif relatifs aux collision mortelles, ou non mortelles.
Le niveau de gravité est estimé en fonction des caractéristiques du parcours, des tiers présents et de leur vitesse, des trajectoires possibles, de l'environnement et des obstacles, des protections existantes pour les personnes impliquées, etc.
A noter qu'une même situation dangereuse peut donner lieu selon le contexte (classe de vitesse par exemple) à plusieurs scénarios, conduisant à des accidents de gravité différentes ;

- La probabilité de survenue des conditions de réalisation est le produit de l'exposition à la situation nécessaire à la réalisation (E) et de l'évitabilité de l'accident par les personnes impliquées (Ev).

Pour chaque scénario rattaché à chaque situation dangereuse, la probabilité de survenue de l'accident est facteur de la probabilité de la situation dangereuse (TFR) et de la probabilité de survenue des conditions de réalisation propres au scénario considéré (FRR).
La probabilité de survenue des conditions de réalisation propres à chaque scénario est estimée en fonction du domaine d'emploi du système, que ce soit les configurations rencontrées sur le parcours envisagé, les conditions extérieures, les conditions de trafic etc.

Au final, la probabilité qu'un accident mortel (resp. un accident non mortel) survienne est alors la somme des probabilités de survenue de tous les scénarios pouvant conduire à un accident mortel (resp. à un accident non mortel). Ces probabilités, calculées au niveau global système, ou de manière spécifique, doivent respecter l'objectif quantitatif de sécurité global ou spécifique.

$$soit\ i\ la\ situation\ dangereuse, \sum_{i=1}^{n} (TFRi\ \times FRRi) \leq OGS(ou\ OSS)$$

L'exigence de respect de chaque objectif de sécurité quantifié (OGS ou OSS), se traduit donc pour chaque situation dangereuse par des exigences portant sur sa probabilité d'apparition (TFR_i), et/ou sur les éléments de contexte (FRR_i) permettant d'influer sur la gravité de l'accident résultant et sur la probabilité de survenue des conditions de réalisation.
In fine, le TFR_i de chaque situation dangereuse devra respecter l'exigence la plus contraignante parmi celles issues des différents objectifs de sécurité qui l'impactent.

Les situations dangereuses identifiées à ce stade de l'analyse doivent être tracées dans un registre des situations dangereuses, en lien avec les scénarios qui y conduisent.

7.1.2.2 Déclinaison de l'objectif pour chaque fonction

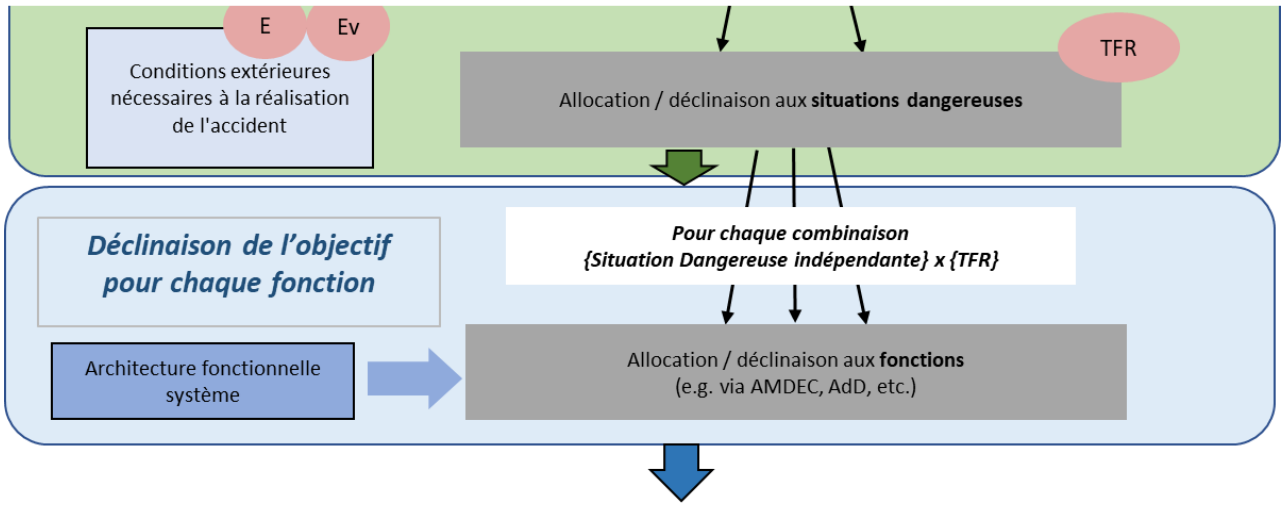


Figure 5 – Déclinaison de l'objectif quantitatif pour chaque fonction

L'exigence relative à la probabilité de survenue des situations dangereuses (dysfonctionnement) (TFR_i), doit ensuite être déclinée en exigences portant sur le taux d'occurrence de dysfonctionnement des fonctions du système ($TFDR_j$).

L'analyse préliminaire des risques (analyse inductive – cf. §11) qui analyse de manière systématique les dysfonctionnements possibles de chaque fonction et leurs conséquences au niveau système, permet de rattacher chaque situation dangereuse à la (ou aux) fonction(s) dont le dysfonctionnement conduit à cette situation dangereuse.

Au final, la probabilité de survenue d'une situation dangereuse TFR_i sera égale à la somme des taux d'occurrence de dysfonctionnement $TFDR_j$ de toutes les fonctions dont le dysfonctionnement conduit à cette situation dangereuse, à condition toutefois que ces fonctions soient bien indépendantes, i.e que le dysfonctionnement d'une fonction n'ait pas d'influence sur le dysfonctionnement d'une autre fonction. A contrario, si le dysfonctionnement d'une fonction A peut entraîner le dysfonctionnement d'une fonction B, seule la fonction A doit être prise en compte lors de la déclinaison de l'objectif.

$$Pour\ toute\ situation\ dangereuse\ i\ et\ et\ toute\ fonction\ indépendante\ j, \quad \sum_{j=1}^{m}(TFDRi,j) = TFRi$$

Cette condition d'indépendance nécessite une vérification conduite au travers de l'analyse de l'architecture fonctionnelle du système, et qui peut conduire à affiner la décomposition fonctionnelle.

A noter qu'un même dysfonctionnement d'une fonction peut conduire à plusieurs situations dangereuses. Cette fonction devra alors respecter le TFDR lié à la situation dangereuse la plus contraignante l'impliquant.

7.1.2.3 Déclinaison de l'objectif quantitatif par origine des dysfonctionnements

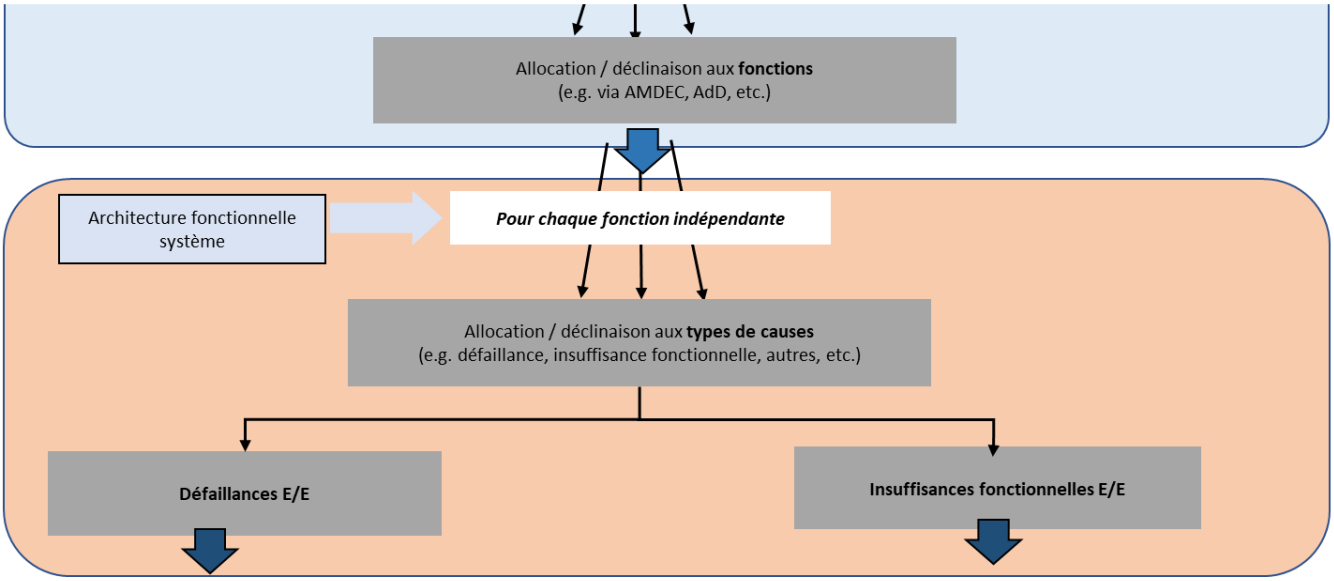


Figure 6 – Déclinaison en termes de défaillances et d'insuffisances fonctionnelles pour chaque fonction

Un dysfonctionnement est une mauvaise réponse du système en raison d'une défaillance, ou de conditions de fonctionnement qui ne sont pas correctement gérées en raison de limitations fonctionnelles (insuffisances fonctionnelles).

L'analyse distingue d'une part les dysfonctionnements des composants électriques et électroniques (E/E), répartis entre défaillances E/E et insuffisances fonctionnelles E/E, et d'autre part les dysfonctionnements des composants d'autre nature, comme par exemple les composants mécaniques.

L'exigence de respect d'un ou de plusieurs objectifs quantifiés implique de répartir préalablement, pour chaque fonction indépendante, l'objectif quantitatif du taux d'occurrence de dysfonctionnement, sur les différentes origines possibles de ces dysfonctionnements, i.e. sur un objectif quantitatif en termes de défaillances E/E ($TFFR_j$), combiné avec un objectif en termes d'insuffisances fonctionnelles E/E ($TFIR_j$).

$$TFDR\ j = TFFR\ j + TFIR\ j$$

La somme de la probabilité de défaillance de chaque fonction et de la « probabilité d'insuffisance fonctionnelle » ne doit pas dépasser la probabilité de dysfonctionnement maximale issue de l'analyse précédente.

Nota :

- Comme précisé au §7.1.1.4, les dysfonctionnements des composants autres que électriques ou électroniques ne sont pas traités par un objectif quantitatif dans l'analyse.

La notion de « probabilité d'insuffisance fonctionnelle » est utilisée à ce stade par commodité de langage (cf. §7.1.2.5).

7.1.2.4 Déclinaison de l'objectif quantitatif vis-à-vis des défaillances E/E

Les défaillances sont définies par la « cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou à fonctionner comme prévu ».
L'ensemble des composants de type électrique ou électronique qui participent à la sécurité du système STRA doivent faire l'objet d'une analyse de leurs défaillances, afin de leur fixer un objectif quantitatif relatif à leur probabilité de défaillance.

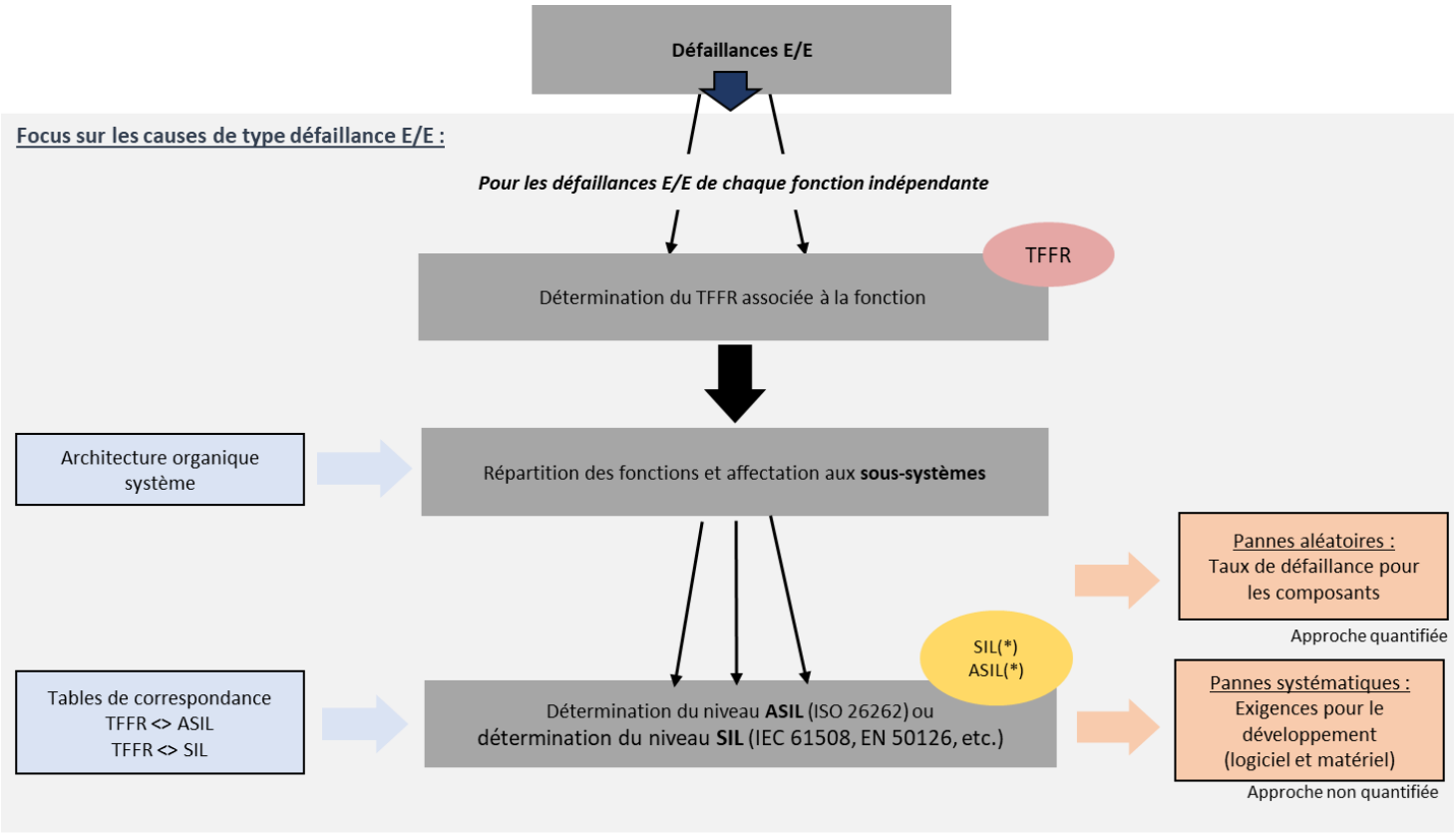


Figure 7 – Déclinaison aux défaillances des sous-systèmes E/E

Les méthodes décrites dans les référentiels de sécurité (IEC 61508, EN 50126, ISO 26262, …) analysent les défaillances possibles des composants électriques ou électroniques, et allouent à chaque fonction un objectif d'intégrité de sécurité.
Les défaillances aléatoires telles que les défaillances d'un composant électronique sont traitées par une approche quantifiée ; les défaillances systématiques comme par exemple les défaillances dues au logiciel sont traitées par une approche non quantifiée basée sur des exigences organisationnelles.

L'analyse de l'architecture du système et de chaque fonction permet d'allouer l'objectif quantitatif de la fonction vers les différents sous-systèmes.
Selon les cas et la nature des sous-systèmes, cette allocation peut être faite en fonction du TFFR

- Au moyen des tableaux de correspondance de la norme ISO 26262, permettant de spécifier le niveau d'intégrité de sécurité ASIL requis pour chaque équipement ;
- Ou au moyen des normes IEC 61508 ou EN 50126, permettant de spécifier le niveau d'intégrité de sécurité SIL requis pour chaque équipement.[12]

7.1.2.5 Déclinaison de l'objectif quantitatif vis-à-vis des insuffisances fonctionnelles E/E

Les insuffisances fonctionnelles désignent les causes, hors défaillance, menant à un danger. Celles-ci peuvent être dues :

a) À des insuffisances de spécification de la fonctionnalité prévue au niveau du système ;
ou
b) À des insuffisances de spécification ou de performance dans la mise en œuvre des éléments électriques et/ou électroniques (E/E) dans le système.

[12] L'analyse doit veiller à traiter les éventuelles incohérences issues de l'application de référentiels différents pour allouer l'objectif quantitatif sur les différents sous-systèmes.

Seules les insuffisances des fonctions intégrant des composants E/E (particulièrement des composants logiciels) sont considérées ici.
Elles englobent les cas de robustesse insuffisante de certains équipements en raison de l'environnement, les cas de mauvaise interprétation par le système de la situation qu'il rencontre et également les cas de mésusages prévisibles des équipements et des systèmes.

Le TFIR désigne le « taux d'occurrence d'insuffisance fonctionnelle E/E » de la fonction, notion qui est utilisée ici par commodité de langage. Le traitement des insuffisances fonctionnelles E/E repose sur des exigences vis-à-vis des moyens mis en œuvre pour les réduire de manière suffisante par rapport à l'objectif du TFIR.

Pour chaque fonction, l'atteinte du TFIR fixé doit être démontrée en s'appuyant sur les référentiels pertinents tel que par exemple la norme ISO 21448. Les exigences de cette norme reposent sur des analyses, des vérifications et des tests. Les analyses permettent notamment de définir puis de démontrer le respect d'un critère d'acceptation du risque résiduel SOTIF[13], en définissant une stratégie de vérification et de validation.

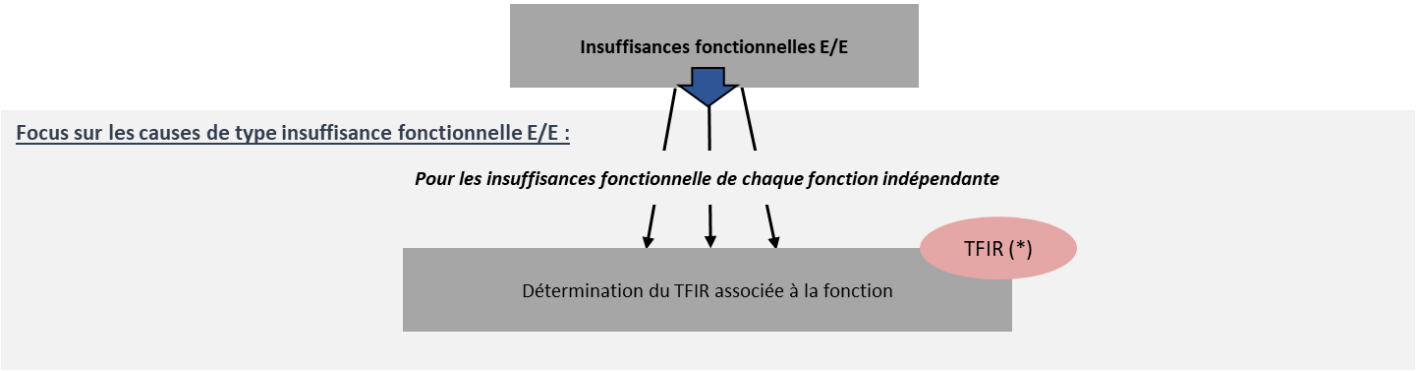


Figure 8 – Déclinaison aux insuffisances fonctionnelles des sous-systèmes E/E

7.2 Analyse explicite sans objectif quantitatif

7.2.1 Généralités

Lorsque par manque de données exploitables, il n'est pas possible d'élaborer un objectif quantitatif, l'objectif est alors de vérifier que chaque risque représenté par chaque situation dangereuse est bien acceptable. Si tel n'est pas le cas suite à l'évaluation initiale, une stratégie de réduction doit être mise en œuvre permettant in fine de ramener chaque risque à un niveau jugé acceptable.

Le tableau suivant présente le canevas de cette démarche.

	Activité	Observations et commentaires	Renvoi
1	Rappeler les situations dangereuses via une APD (Analyse préliminaire des dangers).	- Identification des situations dangereuses (SD) pour un scénario d'accident donné.	Cf. chapitre 10

[13] ISO 21448:2022 « Véhicules routiers — Sécurité de la fonction attendue » - §6.5 6.5 « Specification of acceptance criteria for the residual risk.»

2	APR (Analyse préliminaire de risques)	- Identification des causes des SD. - L'APR permet de faciliter l'identification des dysfonctionnements du système STRA en les liant aux SD.	Cf. chapitre 11
4	Evaluation des risques : Evaluation initiale	Pour chaque scénario d'accident : - Estimation du niveau de risque associé à chaque SD - Evaluation du risque associé à chaque SD (matrice de risques)	Cf chapitre 7.3.2
5	Evaluation des risques : Stratégie de réduction des risques	Pour chaque scénario d'accident : - Spécification des Mesures de réduction - Evaluation du risque résiduel associé à chaque SD	Cf chapitre 7.3.3

Tableau 4 – Etapes de la démarche d'analyse explicite sans objectif quantitatif

7.2.2 Principes d'évaluation du risque

Le risque associé à chaque situation dangereuse est estimé selon les principes définis dans le §8, dans le contexte des scénarios d'accident.

Catégories d'acceptation

3 catégories d'acceptation du risque sont définies :

- Risque acceptable : le risque peut être accepté sans mesure de réduction supplémentaire
- Risque tolérable : le risque doit autant que faire se peut être ramené à un niveau acceptable
- Risque inacceptable : le risque doit être éliminé ou a minima réduit par des mesures réduction des risques

Critères d'acceptation

L'évaluation du risque associé à chaque situation dangereuse consiste à classifier chaque risque selon les 3 catégories d'acceptation, en estimant le niveau de chaque risque au vu de critères d'acceptation, et au vu de principes d'acceptation formalisés dans une matrice de risques.

Ces critères d'acceptation du risque doivent refléter les objectifs de sécurité quantitatifs élaborés lorsqu'il existe des données issues du retour d'expérience et mis en œuvre dans le cadre de la « démarche d'analyse explicite avec objectif quantitatif » (cf. §7.1).

Ces critères d'acceptation doivent être définis de manière à ce que le niveau de probabilité d'occurrence d'un scénario d'accident pouvant conduire à un décès soit globalement cohérent avec les objectifs de sécurité quantitatifs donnés par les normes pertinentes sur le champ de la sécurité [14] (ISO 26262, EN 50126 ou IEC 61508).

Un exemple de matrice de risques est donné pour information à l'annexe 3 de ce document.

[14] Par exemple :

- Pour les systèmes ferroviaires, la norme EN 50126-1 donne par exemple pour information un objectif quantitatif de 1×10^{-9} par heure d'exploitation pour les défaillances fonctionnelles pouvant avoir une conséquence catastrophique (cf. également R UE 402/2013) ;
- La norme IEC 61508-5 Annexe E donne pour exemple un exemple d'étalonnage de graphe de risque, déterminant un niveau d'intégrité de sécurité en fonction des paramètres de risque.

Processus d'évaluation

L'évaluation des risques est un processus itératif, visant au travers de la définition de mesures successives de réduction des risques, à amener chaque risque à la catégorie « acceptable ».
Ce processus débute par une évaluation initiale.

Exigence générale

Suite à cette évaluation initiale, tous les risques qui n'ont pas été classifiés comme « acceptables » doivent, sauf exception détaillée ci-dessous, être réduits en respectant une stratégie de réduction du risque afin d'être ramenés à la catégorie « acceptable ».

Exception

La seule exception possible à l'exigence précédente est le cas d'un risque de catégorie « tolérable » pour lequel il est démontré qu'il est raisonnablement impossible de le réduire davantage, i.e. que les mesures de réduction des risques à mettre en œuvre remettraient en cause l'existence même du système, en raison par exemple de leur faisabilité.
A ces conditions et par exception, il peut alors être décidé d'accepter ce risque. Cette acceptation doit alors faire l'objet d'une décision étayée dans le cadre de la démonstration de sécurité et doit apparaître dans les conclusions de cette démonstration de sécurité.
Le risque considéré doit ensuite faire l'objet d'un suivi particulier dans le cadre des activités de surveillance en service.

7.2.3 Stratégie de réduction du risque

Une stratégie de réduction des risques doit être mise en œuvre, visant à réduire chaque risque jusqu'à un niveau permettant de l'accepter selon les principes définis ci-dessus.

La stratégie de réduction des risques peut combiner plusieurs mesures :

- La stratégie de réduction du risque doit avoir pour premier objectif de déterminer si les situations dangereuses peuvent être évitées dans la pratique ;
- S'il n'est pas possible de les éviter, il convient alors d'examiner si la fréquence d'occurrence de ces situations dangereuses peut être réduite à un niveau permettant de rendre le risque acceptable ;
- Si la fréquence d'occurrence des situations dangereuses ne peut être suffisamment réduite, la dernière mesure consiste alors en complément, à réduire la gravité de l'accident (conséquence du danger) de manière à rendre le risque acceptable.

La capacité des mesures de réduction des risques successives à réduire suffisamment la fréquence d'occurrence d'une situation dangereuse et/ou la gravité de l'accident doit être estimée de manière prudente. L'analyse associée doit être tracée et documentée.

8 Principes d'estimation du risque

8.1 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 11 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. A titre d'exemple, un évènement survenant sur un STRA-M et conduisant uniquement à la dégradation du chargement (panne du système de réfrigération sur un véhicule réfrigéré entraînant la rupture de la chaîne du froid et rendant la marchandise impropre à la consommation) n'est pas considéré comme un accident dans le cadre de cette analyse.

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.

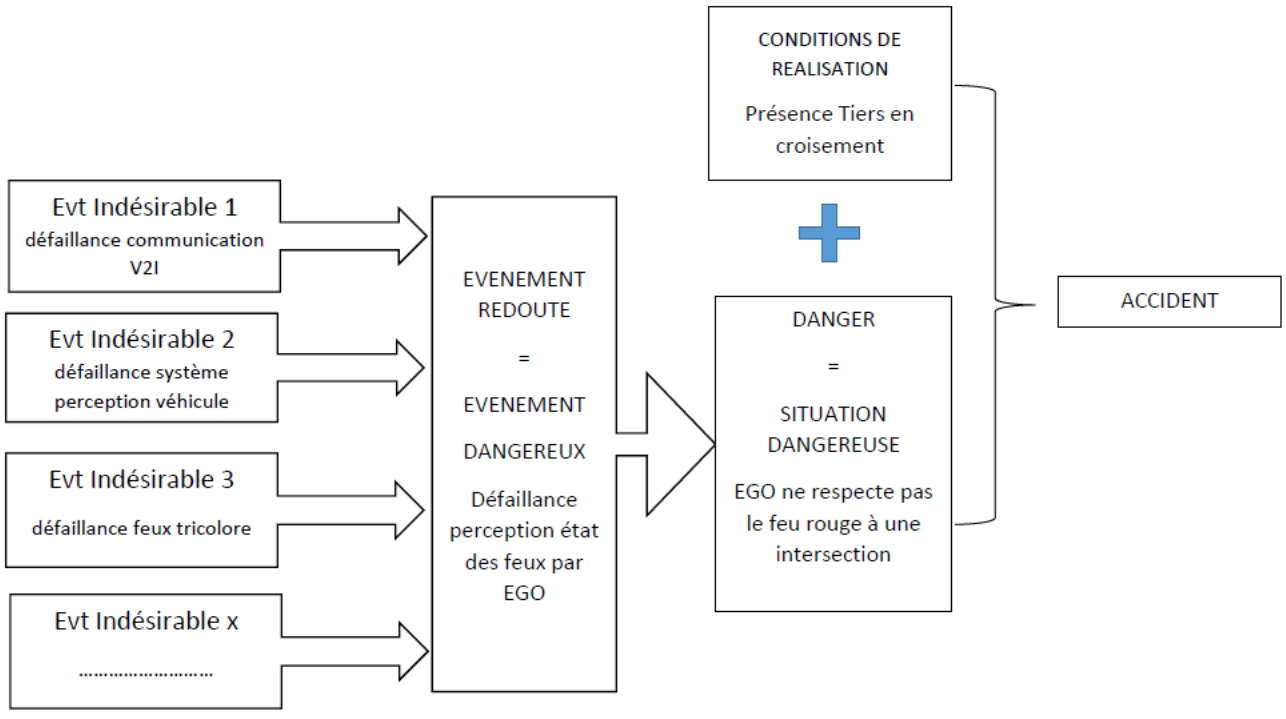


Figure 9 – Déroulement d'un accident

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.

Le 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.

8.2 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, dégâts matériels uniquement[15]
G1	Blessures légères et modérées
G2	Blessures graves (survie probable)
G3	Blessures mortelles (survie incertaine) ou décès (*)

Tableau 5 – 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 suraccident 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

[15] Si les dégâts concernent des éléments du système, des mesures d'exploitation doivent permettre de traiter la situation de manière à ce qu'elle ne conduise pas à un nouvel évènement de gravité supérieure.

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 évènements, 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 6 - Liste des situations concernées par le marqueur (*)

Accident	ID[16]	Sous-type	Conditions	Catégorie / classe véhicule[17]					Argumentaire justifiant le marquage (*)
				M1 (8p maxi)	M2/M3 classe A/B 9-22p	M2/M3 classe 1/2/3 >22p	Navette urbaine 9-16p	L, N, O	
Collision	1.2	Collision contre un obstacle massif (containers, animaux, chute d'arbres, etc.)	Si circulation dans un tunnel [18] de longueur > 300 m (200m si tunnel avec TMD possible) avec vitesse véhicule ego > 30 km/h	NA	NA	OUI	NA	OUI (N3, O4[19])	Collision amenant à un incendie du véhicule dans le tunnel (dommages étendus uniquement pour les potentiels calorifiques M2/M3 classes 1/2/3 ou N3/O4)
			Si circulation avec risque de chute de hauteur (circulation sur ouvrage, ravin, etc.) avec vitesse véhicule ego > 30 km/h	NA	NA	OUI	NA	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 [15] de longueur > 300 m (200m si tunnel avec TMD possible) et avec différentiel possible de vitesse entre ego et tiers > 30 km/h lors du choc	NA	NA	OUI	NA	OUI (N3, O4[19])	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	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	OUI (N,O[19])	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

[16] Le champ ID d'identification des situations fait référence à la numérotation du tableau 11.
[17] Les catégories de véhicules sont données en référence à l'article R. 311-1 du code de la route.
[18] 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 m^2 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 A.M. du 22/11/2005).
[19] La mention de la catégorie O signifie ici « véhicule articulé avec une remorque de catégorie O »

Accident	ID[16]	Sous-type	Conditions	Catégorie / classe véhicule[17]					Argumentaire justifiant le marquage (*)
				M1 (8p maxi)	M2/M3 classe A/B 9-22p	M2/M3 classe 1/2/3 >22p	Navette urbaine 9-16p	L, N, O	
		Collision avec le véhicule d'un système de transport ferré (ferroviaire lourd) à un passage à niveau		NA	NA	OUI	NA	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 [15] de longueur > 300 m (200m si tunnel avec TMD possible)	NA	NA	OUI	NA	OUI (N3, O4[19])	1 - feu dont l'origine est le véhicule (mesures de prévention): risques pour les usagers du tunnel uniquement si capacité calorifique du véhicule élevée (M2/M3 classes 1/2/3, catégories N3, catégories O4 remorqué 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)

8.3 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.

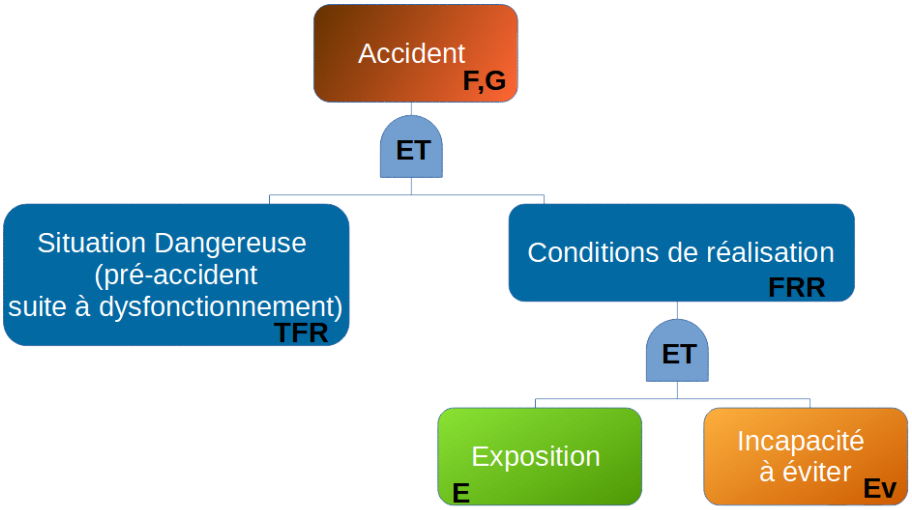


Figure 10 – Schéma des paramètres d'estimation du risque

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 évènements 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 [20]
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 7 – classes d'exposition

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 exposé à la situation) ou en termes 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 ;

[20] 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)

- 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, 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 8 – 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.

9 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 10 et 11

- 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.

Les différentes parties du tableau ci-dessous dressent 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 règlementation 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.

<u>Guide de lecture du tableau 9 parties 1 à 5 ci-dessous</u>

- Chaque partie du tableau rassemble une famille d'exigences ;
- Dans chaque famille, les exigences sont classées par domaine ;
- Chaque exigence est spécifiée sous la forme d'un intitulé général qui fait pour certaines l'objet de déclinaisons plus détaillées ;
- La source des exigences est donnée à titre d'information pour remettre chaque exigence générale ou déclinée dans son contexte ;
- 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.

Tableau 9 / Partie 1 - Liste des exigences de haut de niveau : exigences générales

Partie 1 : EXIGENCES GENERALES						
Domaine	**ID**	**Intitulé**	**ID**	**Déclinaisons**	**Source**	**Précisions**
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 article R. 3152-2 II	On distingue les 2 cas : 1 - sortie ODD ou défaillance entrainant 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. 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. 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. 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)."
			1.2	Le système ne doit permettre l'activation du mode de délégation de conduite des véhicules que lorsqu'il est dans son domaine d'emploi	Code des transports article R. 3152-2 II	
			1.3	Lorsque le système sort de son domaine d'emploi, les véhicules concernés par la perte des conditions 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 article R. 3152-2 II	

Partie 1 : EXIGENCES GENERALES						
Domaine	**ID**	**Intitulé**	**ID**	**Déclinaisons**	**Source**	**Précisions**
Conditions d'utilisation	2	Le système technique ne doit pas permettre la circulation des véhicules en mode de délégation de conduite s'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 article 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'article R. 3152-2 III doit être couverte par l'exigence de l'article 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 article 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 être en mesure de surveiller son intégrité.	4.1	Le système doit détecter les défaillances impactant potentiellement la sécurité.	Code des transports article 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

Partie 1 : EXIGENCES GENERALES						
Domaine	**ID**	**Intitulé**	**ID**	**Déclinaisons**	**Source**	**Précisions**
			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
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 article 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 article 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 article R. 3152-2 III	Réalisation par le système d'une action appropriée pour chaque situation visant à minimiser le risque global

Partie 1 : EXIGENCES GENERALES						
Domaine	**ID**	**Intitulé**	**ID**	**Déclinaisons**	**Source**	**Précisions**
Réponses du système	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 entrainant 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. L'exigence s'applique uniquement au cas n°1.
	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 défaillances 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	

Partie 1 : EXIGENCES GENERALES						
Domaine	**ID**	**Intitulé**	**ID**	**Déclinaisons**	**Source**	**Précisions**
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, R312-3, R312-4, R312-10, R312-12, 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. 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 "). Toute évolution du Code de la route devra être prise en compte.
			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, etc.	
			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.	
			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	

Partie 1 : EXIGENCES GENERALES						
Domaine	**ID**	**Intitulé**	**ID**	**Déclinaisons**	**Source**	**Précisions**
Respect des règles de circulation applicables			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	
			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.	

Partie 1 : EXIGENCES GENERALES						
Domaine	**ID**	**Intitulé**	**ID**	**Déclinaisons**	**Source**	**Précisions**
Respect des règles de circulation applicables			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	
			11.19	Respecter toute autre règle applicable	Code de la route	

Partie 1 : EXIGENCES GENERALES						
Domaine	**ID**	**Intitulé**	**ID**	**Déclinaisons**	**Source**	**Précisions**
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 auxquelles l'accès par des tiers peut présenter un enjeu pour la sécurité, ne doivent être accessibles qu'aux personnes autorisées.				

Tableau 9 / Partie 2 - Liste des exigences de haut de niveau : exigences relatives aux manœuvres des véhicules

Partie 2 : EXIGENCES RELATIVES AUX MANŒUVRES DES VEHICULES				
Domaine	**ID**	**Intitulé**	**Source**	**Précisions**
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. »

Partie 2 : EXIGENCES RELATIVES AUX MANŒUVRES DES VEHICULES				
Domaine	**ID**	**Intitulé**	**Source**	**Précisions**
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 autres usagers de la route, à l'exploitant, et le cas échéant aux passagers du véhicule.	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. "

Partie 2 : EXIGENCES RELATIVES AUX MANŒUVRES DES VEHICULES				
Domaine	**ID**	**Intitulé**	**Source**	**Précisions**
Arrêt d'urgence	21	Toute manœuvre d'urgence engagée par un véhicule, doit être signalée aux autres usagers de la route, à l'exploitant, et le cas échéant aux passagers du véhicule.		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 9 / Partie 3 - Liste des exigences de haut de niveau : exigences pour les passagers

Partie 3 : EXIGENCES POUR LES PASSAGERS				
Domaine	**ID**	**Intitulé**	**Source**	**Précisions**
Evacuation (STRA-P)	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.		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 Les aspects suivants doivent notamment être pris en compte : - 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 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 dans le cas du transport de passagers au moyen d'un véhicule qui comporte plus de neuf places assises, y compris celle du conducteur). Les conditions d'évacuation doivent être adaptées selon que le véhicule a conservé ou non sa capacité à circuler.

Partie 3 : EXIGENCES POUR LES PASSAGERS				
Domaine	**ID**	**Intitulé**	**Source**	**Précisions**
Evacuation (STRA-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		Permettre l'ouverture des ouvrants depuis l'extérieur par les secours ou du personnel d'exploitation Gérer la protection contre les actes de malveillance
Demande d'arrêt passager (STRA-P)	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	Les aspects suivants doivent notamment être pris en compte : - accessibilité de la commande - informations sur la commande - traitement de la commande - gestion de la phase d'arrêt règlement UE ADS Annexe II 6.3 « 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 : 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). »
Immobilisation pour les personnes ou le personnel chargé des opérations de chargement/déchargement (STRA-M)	26	Le système doit garantir l'immobilisation de chaque véhicule du système durant les opérations chargement ou du déchargement des marchandises.		L'immobilisation doit garantir l'absence de mouvement du système pour toute personne en interaction avec le véhicule.

Partie 3 : EXIGENCES POUR LES PASSAGERS				
Domaine	**ID**	**Intitulé**	**Source**	**Précisions**
Communication passager (STRA-P)	27	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	Les exigences suivantes doivent notamment être prises en compte : possibilité d'alerte par les passagers en cas de situation critique (malaise passager, incendie à bord, …) 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. 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). »
Communication avec les tiers (STRA-M)	28	Chaque véhicule du système doit donner la possibilité aux tiers situés à proximité du véhicule de communiquer avec la supervision du système.		Communication bidirectionnelle activable depuis l'extérieur du véhicule à l'arrêt, à destination des personnes en interaction avec le véhicule (personnes ou personnel chargé des opérations, agents des forces de l'ordre, etc.)

Tableau 9 / Partie 4 - Liste des exigences de haut de niveau : exigences pour le personnel opérateur à distance / supervision

Partie 4 - EXIGENCES POUR LE PERSONNEL OPERATEUR A DISTANCE / SUPERVISION				
Domaine	**ID**	**Intitulé**	**Source**	**Précisions**
Commandes opérateur	29	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
	30	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.
	31	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. "

Partie 4 - EXIGENCES POUR LE PERSONNEL OPERATEUR A DISTANCE / SUPERVISION				
Domaine	**ID**	**Intitulé**	**Source**	**Précisions**
Communication depuis la supervision (STRA-P)	32	Le système doit donner la possibilité au personnel opérateur intervenant à distance de communiquer avec les passagers du véhicule du système		Les exigences suivantes doivent notamment être prises en compte : possibilité de transmission de consigne aux passagers en cas de besoin, notamment : - sortie du système de son domaine d'emploi - interruption ou modification du service. Cf. également 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 ISO 16505:2019) 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..."

Tableau 9 / Partie 5 - Liste des exigences de haut de niveau : exigences pour l'IHM supervision

Partie 5 - EXIGENCES POUR L'IHM SUPERVISION				
Domaine	**ID**	**Intitulé**	**Source**	**Précisions**
IHM	33	L'IHM du système doit être conçue de manière à limiter les risques de mésusages par le personnel d'exploitation.		- lecture rapide de la situation du système, d'un véhicule - pertinence des informations, priorisation - champ de vision 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'acquittement) - 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'acquitter des manœuvres proposées par le système (cf. définition intervention à distance)
	34	La mise en service ou la remise en service du mode de délégation de conduite doit requérir une action spécifique et non ambigüe de la part de l'opérateur.		Y compris suite à un arrêt d'urgence ou suite à une MRM (reprise en mode automatique) - 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	35	Le personnel opérateur intervenant à distance doit pouvoir disposer des informations nécessaires concernant l'état du système.		L'état du système comprend toutes les informations pertinentes relatives au système : état de la délégation de conduite, vitesse, état des portes, etc. - connaissance du mode de conduite (cf. "Automated driving safety validation: proposals from the French Eco-system" janv. 2020 - T03)

Partie 5 - EXIGENCES POUR L'IHM SUPERVISION				
Domaine	**ID**	**Intitulé**	**Source**	**Précisions**
Information pour le personnel opérateur	36	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 ISO 16505:2019) 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."
	37	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	38	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	Travaux du GRVA (UNECE WP on Automated/Autonomous and Connected Vehicles)	

Partie 5 - EXIGENCES POUR L'IHM SUPERVISION				
Domaine	**ID**	**Intitulé**	**Source**	**Précisions**
Information des tiers	39	Il doit être possible pour les forces de l'ordre en présence d'un véhicule de communiquer avec la supervision du système	Travaux FR sur le projet d'arrêté « Navettes Urbaines Automatisées » Travaux FR sur les interactions entre les véhicules automatisés, les forces de l'ordre et les services de secours.	

10 Analyse déductive (analyse préliminaire des dangers)

10.1 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, dont la prise en compte fait l'objet du guide d'application relatif à la cybersécurité pour les STRA .

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 9.

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 (cf. chapitre 6 - Cas de l'application d'un référentiel technique hors-STRA (type 3a)) 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 (cf. chapitre 7 - Cas de l'analyse explicite (type 3b)) :

- 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.

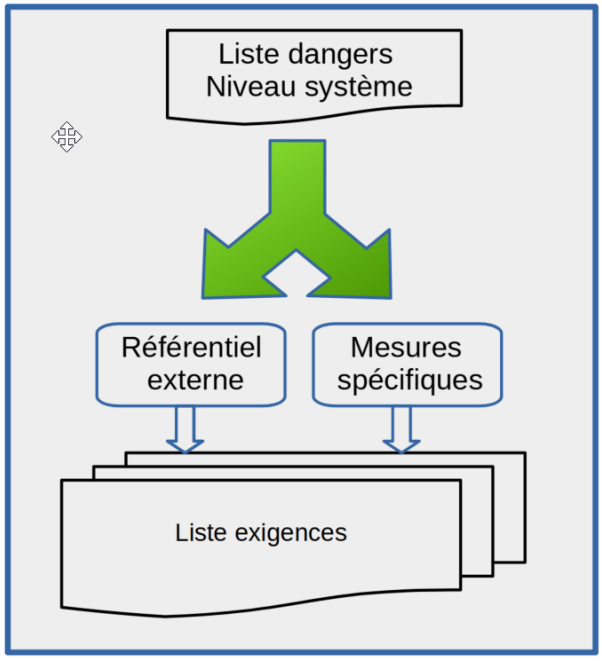


Figure 11 – Analyse déductive

Objectifs

- L'analyse déductive permet de construire les scénarios, d'estimer les risques au niveau du système, et d'expliciter 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 l'article R. 3152-6 II du code des transports.
- 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.

10.2 **Trame**

Le tableau suivant en 3 parties fournit à titre uniquement illustratif un exemple de trame décrivant les différents éléments de l'analyse déductive.

Tableau 10 – Trame de l'analyse déductive – Partie 1

PARTIE 1										
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 évènement 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.			***Partie 2***
En lien avec Tableau 11				En lien avec tableaux 13 et 14						

Tableau 10 – Trame de l'analyse déductive – Partie 2

PARTIE 2												
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 *(optionnel)*		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 12												

Partie 3

Tableau 10 – Trame de l'analyse déductive – Partie 3

PARTIE 3									
EXIGENCES DE SECURITE		**EVALUATION FINALE DES RISQUES**							
Catégorie	Description	Gravité		Exposition		Evitabilité		Evaluation du risque *(optionnel)*
		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							

10.3 Eléments d'entrée de l'analyse déductive

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

- Tableau 11 : Liste des accidents de niveau système ;
- Tableau 12 : 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 13 : Liste de situations de vie pouvant être rencontrées au sein d'un système et qui doivent être prises en compte dans les scénarios ;
- Tableau 14 : Liste des éléments de contexte d'un système et pouvant influer sur les exigences de réponse aux dangers.

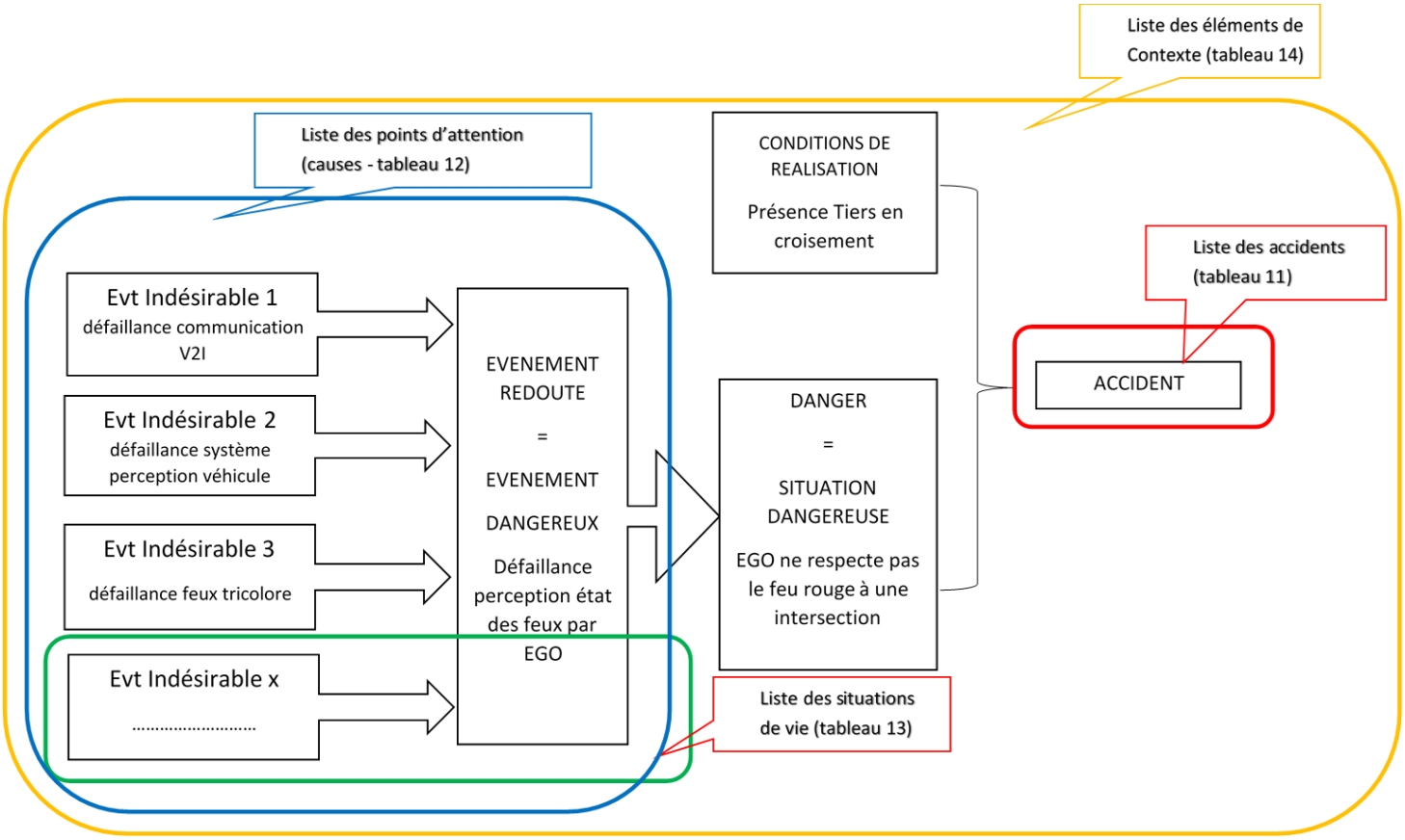


Figure 12 - Organisation des tableaux guides de l'analyse déductive

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 :
  - Les usagers du système (ex. piétons, personnes à mobilité réduite, avec poussette, avec bagages lourds, avec engin de déplacement personnel, personnes en charge du

chargement et du déchargement des marchandises, etc.) présents dans les véhicules du système ou les stations ;
NB : Dans le cas des STRA-M, les personnes en charge du chargement et du déchargement des marchandises sont considérées comme des usagers du système lors de leurs interactions avec le système à l'exclusion des opérations de chargement et de déchargement.
- Le chargement présent à bord des véhicules dans le cas des STRA-M ;
- 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 autres usagers de la route (ex. les différents types de véhicules routiers) ;
- Les personnels d'exploitation, au titre des usagers lorsqu'ils sont transportés à bord des véhicules du système ou en attente de l'être, et au titre de tiers, lorsqu'ils sont présents sur le parcours ;
- 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 types 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.).
  Dans le cas des STRA-M, les modes de fonctionnement liés aux opérations de chargement et de déchargement des marchandises pour les STRA-M, y compris les opérations d'arrimage des marchandises, sont exclus du périmètre de l'analyse, et seules leurs interfaces (informations échangées, autorisations, commandes, etc.) avec les fonctions de conduite automatisée sont prises en compte.

- Toutes les situations de vie du système au vu de son domaine d'emploi (cf. tableau 13).

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 11 - Liste des accidents de niveau système

Type	ID	Accidents Potentiels	Compléments (éventuels)	Exemples (non exhaustifs)
Collision[21]	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)

[21] La collision peut concerner également la collision avec un élément dépassant du gabarit du véhicule : collision avec la partie mobile du véhicule dont l'immobilisation serait inopérante ou collision avec un objet entraîné par le véhicule.

Type	ID	Accidents Potentiels	Compléments (éventuels)	Exemples (non exhaustifs)
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
	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 Chute d'une personne en charge du déchargement en départ station suite redémarrage intempestif (STRA-M)
	2.3	Chute de personne depuis le véhicule du système vers l'extérieur en ligne (STRA-P)	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

Type	ID	Accidents Potentiels	Compléments (éventuels)	Exemples (non exhaustifs)
Electrisation/ Électrocution	4.1	Electrisation/Electrocution dans le véhicule		
	4.2	Electrisation/Electrocution dans une station		
	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 personnes	6.1	Personnes coincées/pincées 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	Personnes coincées/pincées/heurtées par une partie mobile d'un composant du système	Les phases d'utilisation des éventuels équipements mobiles de chargement et de déchargement ne font pas partie du périmètre de l'analyse.	Coincement d'un passager dans la rampe d'accès PMR (STRA-P) Coincement d'un passager dans un tripode d'accès (STRA-P)

Type	ID	Accidents Potentiels	Compléments (éventuels)	Exemples (non exhaustifs)
				Heurt d'un usager ou d'un tiers par un équipement mobile dédié au chargement/déchargement (STRA-M)
	6.3	Entrainement de personne par le véhicule (en particulier entrainement de personnes lors de la sortie de la station ou suite à un coincement de vêtement)		Entrainement d'une personne lors de la sortie de la station suite au redémarrage du véhicule Entrainement d'une personne suite au coincement du vêtement d'un passager resté sur le quai Entrainement d'une personne en charge du chargement (STRA-M)
Autres accidents de personnes	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 Chute d'un élément du chargement du véhicule (STRA-M) entraine la sortie de route/collision d'un véhicule tiers

Type	ID	Accidents Potentiels	Compléments (éventuels)	Exemples (non exhaustifs)
	7.2	Personnes heurtées 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	Personnes heurtées suite à la chute d'objets transportés dans l'habitacle d'un véhicule du système d'un objet transporté (ex. bagages, colis, etc.)		Chute d'une valise sur un passager (STRA-P) Chute d'un élément du chargement du véhicule sur un passager transporté à titre accessoire (STRA-M)
	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 12 - 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.	Les erreurs éventuelles d'une personne en charge du chargement et du déchargement des marchandises, lors des opérations de chargement et de déchargement ne sont pas prises en compte (STRA-M).
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 l'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 l'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 chaine 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 un manque d'information dans le véhicule Erreur opérateur suite à l'absence d'information sur la défaillance d'un élément du système	L'IHM dédiée aux opérations de chargement et de déchargement n'est pas prise en compte (STRA-M).
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)

ID	Intitulé	Compléments	Commentaire
12	Défaillance mécanique	Crevaison Echauffement 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 …	
15	Comportement malveillant et intentionnel des usagers	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 13 - 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 forces 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 14 - Liste des éléments de contexte pouvant influer 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	- tunnel - viaduc - ravin - ...
2	Circulation d'un véhicule du système sur une zone dont la configuration rend les manœuvres à risque minimal complexes	- tunnel - viaduc - voie étroite - ...
3	Circulation d'un véhicule du système sur une zone dont la configuration rend l'évacuation des passagers dangereuse	- tunnel -viaduc - ...

11 Analyse inductive (analyse préliminaire des risques)

11.1 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 évènements font l'objet d'un guide spécifique [22].

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 (cf. chapitre 6 - Cas de l'application d'un référentiel technique hors-STRA (type 3a)) 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 (cf. chapitre 7- Cas de l'analyse explicite (type 3b)). Ces mesures peuvent être à la fois qualitatives et quantitatives : architecture des fonctions, spécifications fonctionnelles, fiabilité des composants, etc.

[22] STRMTG - Guide d'application relatif à la cybersécurité pour les STRA

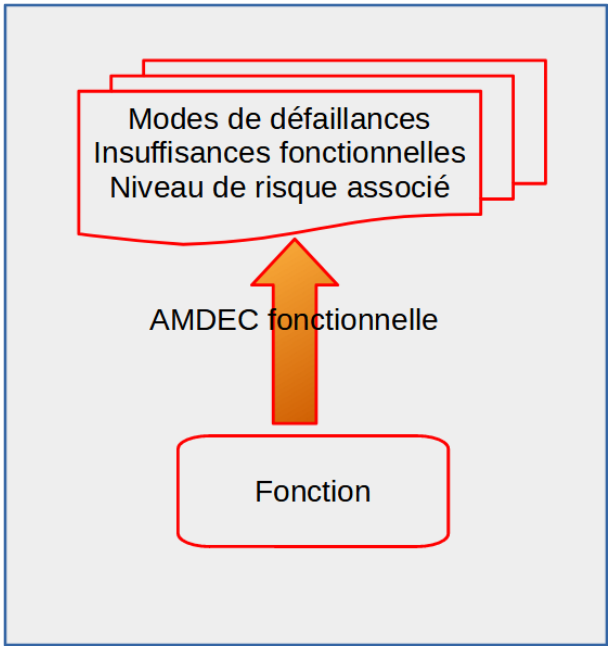


Figure 13 - Analyse inductive

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 ;
- Estimer et 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. §7.1 - Analyse explicite avec objectif quantitatif).

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.

11.2 **Trame**

Le tableau suivant en 3 parties fournit à titre uniquement illustratif un exemple de trame décrivant les différents éléments de l'analyse inductive.

Tableau 15- trame de l'analyse inductive – Partie 1

PARTIE 1									
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 si 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

Partie 2

Tableau 15- trame de l'analyse inductive – Partie 2

PARTIE 2							
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			***Partie 3***
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

Tableau 15- trame de l'analyse inductive – Partie 3

PARTIE 3												
EVALUATION INITIALE DES RISQUES							**EXIGENCE(S) DE SECURITE DE NIVEAU STRA**					
Gravité		Exposition		Evitabilité		**Evaluation du risque** ***(optionnel)***	**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	

11.3 **Eléments d'entrée de l'analyse inductive**

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

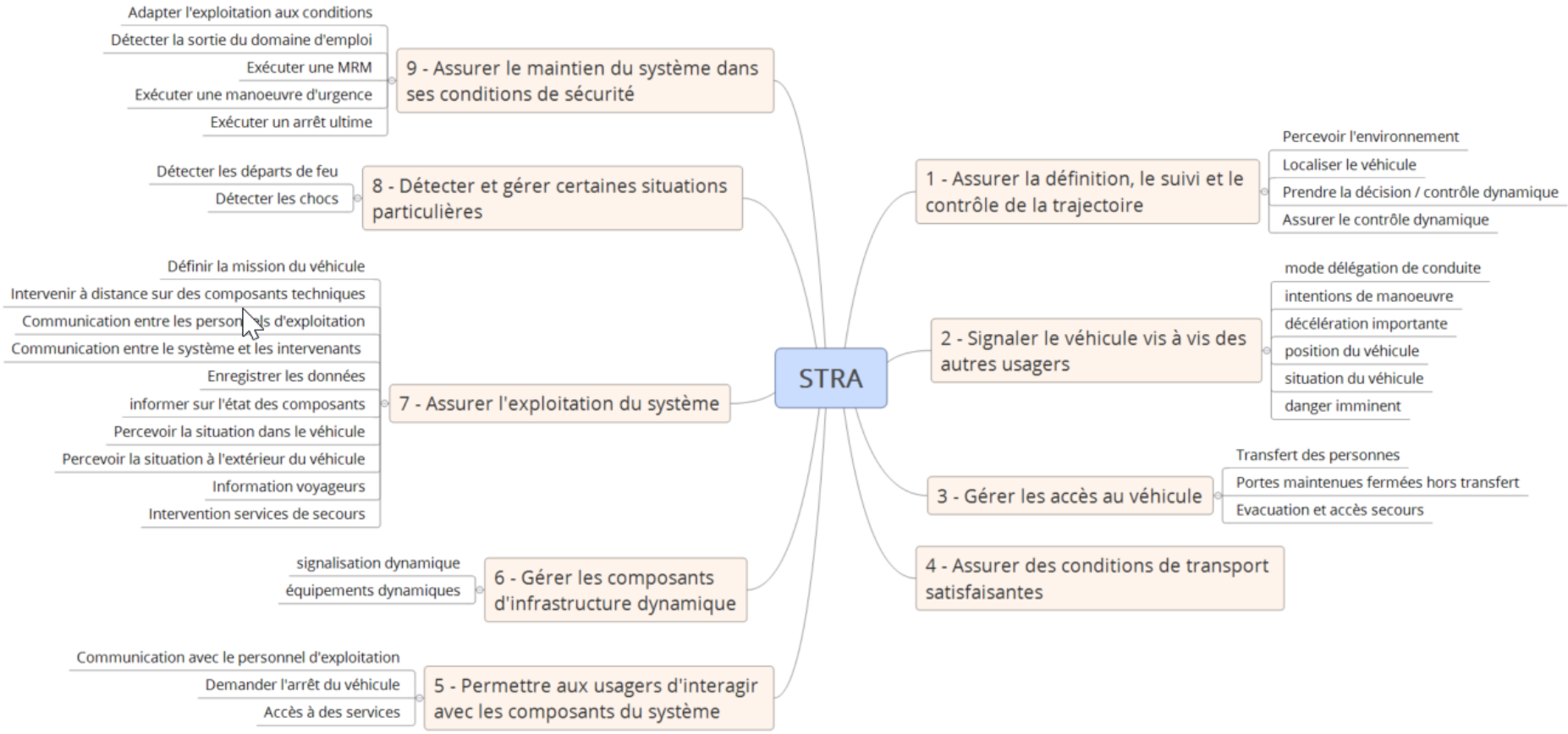


Figure 14 - Arborescence simplifiée de la décomposition fonctionnelle

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 pourront faire l'objet de compléments dans le cadre des documents relatifs aux interventions à distance.

Tableau 16 – 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 exemple : 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 les agents des FO	-	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
						1.1.3.2-Caractériser les VP et les agents des FO	Identifier les types de VP en présence, et la nature des agents
						1.1.3.3-Interpréter les injonctions des agents des FO et les 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, les points d'arrêt à la demande, les points d'évacuation possibles, ...	-	-

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 connaitre 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. => fonction 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 (fonction 1.1) et la localisation (fonction 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 de l'énergie servant à la traction/freinage.	1.4.1-Assurer le contrôle longitudinal	Permettre de répondre aux exigences de niveau service de type "respecter la limitation de vitesse", "respecter l'inter-distance"…	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 latéralement « 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 (STRA-P)	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'entrainement d'un usager	-	-
		3.2-Maintenir le véhicule automatisé fermé hors transfert personnes/ évacuation (STRA-P)	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 (STRA-P)	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	Issues de secours suffisantes et accessibles. Moyens d'ouverture accessibles et adaptés. Cas des PMR à prendre en compte Pour les catégories M2 et M3, l'homologation fixe le nb d'issues de secours présentes (cf. Règlement UN R107). 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
3-Gérer les accès aux véhicules automatisés		3.4-Gérer les interfaces avec les opérations de chargement/déchargement (STRA-M)	La fonction 3.4 permet d'assurer les interfaces entre les opérations de chargement et de déchargement, y compris d'arrimage des marchandises, et les fonctions de conduite automatisée.				
		3.5 -Maintenir le véhicule automatisé fermé hors des phases de chargement/déchargement (STRA-M)	En dehors des points autorisés, la fonction 3.5 permet d'assurer le maintien des portes en position fermée.				
4- Assurer des conditions de transport satisfaisantes pour les passagers (STRA-P)	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.	-	-

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				5.1.2 - Permettre aux usagers du système d'alerter le personnel d'exploitation	Cf. par exemple : Système de demande d'assistance passagers (projet d'arrêté Navette Urbaine Automatisée)	-	-
		5-2-Permettre aux passagers de demander l'arrêt du véhicule (STRA-P)	Cf. par exemple : système de demande d'arrêt sécurité passagers (projet d'arrêté Navette Urbaine Automatisée)	-	-	-	-
		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 6 permet de gérer la signalisation dynamique (gestion des priorités avec feux de signalisation, vitesse, …), les	6-1- Commander la signalisation dynamique	Par exemple, pilotage des feux connectés	-	-	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
6-Gérer les composants d'infrastructure dynamiques pilotés par le système	composants de ségrégation dynamique (barrières, potelets, etc.), etc.	6-2- Commander les équipements dynamiques mobiles	Par exemple, pilotage des barrières mobiles, bornes escamotables, etc.	-	-	-	-
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	- Définir les contraintes d'itinéraire , relatif au service de transport alloué au véhicule, y compris les stations, les points d'arrêt à la demande, les points d'évacuation possibles - Définir les contraintes temporelles (date, heure de départ, heure d'arrivée, heures de passage, fréquence, ...) 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. fonction 8.4)	-	-	-	-

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	La fonction 7.2 permet d'assurer les différents types d'intervention à distance prévus par le système. (Intervention à distance au sens R.3151-1 du Code des Transports : Action exercée par une personne habilitée située à l'extérieur d'un système de transport routier automatisé, aux fins : • 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, immédiat en station, « au prochain arrêt », « aussitôt que possible », 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 - donner l'instruction d'effectuer une manœuvre		-	-
				7.2.6 - - donner l'instruction d'interrompre une manœuvre	-	-	-
				7.2.7 - - donner l'instruction de modifier une manœuvre		-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires	Fonctions	Commentaires
7- Assurer l'exploitation du système				7.2.8 - commander des équipements du véhicule	Essuie-glaces, éclairage, etc. rampes portes etc.	-	-
				7.2.9 - percevoir l'environnement de l'équipement commandé, pour donner les autorisations de manœuvre ou de démarrage	Percevoir l'environnement des portes si commande des portes à distance ou en cas de défaut, percevoir l'environnement de la rampe PMR si commandée à distance	-	-
		7.3-Permettre la communication entre les personnels d'exploitation	La fonction 7.3 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 7.4 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	7.4.1 - permettre l'initiation de la communication avec le système à la demande de l'intervenant extérieur	Définition du 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			ORSEC ou équivalemment 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. notamment art. R.3152-22 du Code des Transports	-	-

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	Niveau de charge batterie, bouclage des ceintures de sécurité, état des portes, état des issues de secours, 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 ou 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 et vision des passagers	7.7.1 - Percevoir l'ambiance sonore dans l'habitacle du véhicule	-	-	-
				7.7.2 - Pouvoir avoir une vision de l'intérieur véhicule	-	7.7.2.1 - 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					-	7.7.2.2 - 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'entrainement 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. fonction 9.1)
						7.8.2.2 -connaître les conditions de circulation en des points particuliers du parcours	Par exemple, vision déportée sur un passage à niveau ou une zone accidentogène
		7.9 -Permettre la transmission de l'information	La fonction 7.9 permet d'assurer la transmission d'informations sonores ou visuelles aux usagers (à	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		voyageurs (STRA-P)	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 entrainant l'incapacité du système à effectuer une MRM (cf. document SAE J3016_202104 « Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles » §3.11)	-	-	-	-

12 Annexes

Annexe 1 – Liste des participants

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 routiers automatisés
Secrétaire : M. Florent Sovignet - STRMTG – département transports routiers automatisés

Pour les versions 1 et 2 (transport de personnes) :

M.	Guesdon	Alstom
M.	Lebdiri	Alstom
M.	Chodorge	Auditsafe
M.	Guillemin	Auditsafe
M.	Alliouche	Bureau Veritas
M.	Clarissou	Bureau Veritas
Mme	Dam	Bureau Veritas
M.	Travers	CEREMA
M.	Testemale	Certifer
M.	Toilliez	Certifer
M.	Willmann	CETU
M.	Audige	DGITM
Mme	Lanaud	DGITM
M.	Launay	DSR
M.	Dupont	Easymile
M.	Russo	Geste Engineering
M.	Bohn	IRT System X
Mme	Brini	IRT System X
M.	Renaud	Ramsai
Mme	Berthault	RATP
M.	Boulineau	RATP
M.	Caire	RATP
M.	Fiorot	RATP
M.	Arnoux	Renault
M.	Lenti	Stellantis
M.	Brun	STRMTG
M.	Dusserre	STRMTG

M.	Maisonobe	STRMTG
M.	Parent	Suburvan
Mme	Torelli	Systra
M.	Tran	Systra
M.	Smal	Transdev
M.	Baranowski	Université Gustave Eiffel
M.	De Sousa Fernandes	UTAC
M.	Pauron	UTAC
M.	Savona	UTAC

Pour la version 3 (transport de marchandises) :

M.	Chehwan	Beti
Mme	Thomasson	CARA
M.	Travers	CEREMA
M.	Willmann	CETU
Mme	Gallay	DGITM
M.	Launay	DSR
M.	Breau	Eurovia
M.	Celerier	FNTR
M.	Goux	FNTR
Mme	Moustahy	Geste Engineering
M.	Russo	Geste Engineering
M.	Coget	Konboi One
M.	Renaud	Ramsai
M.	Kamoshida	Renault
M.	Lenti	Stellantis
M.	Brun	STRMTG
M.	Maisonobe	STRMTG
M.	Fauchet	Taur
Mme	Chateauroux	Transpolis
M.	Talon	Twinswheel
M.	Boussif	Université Gustave Eiffel
M.	Pauron	UTAC
M.	Savona	UTAC
Mme	Torelli	/

A également contribué à la relecture du guide :

M. Ludovic Brun, chargé de mission juridique du STRMTG

Annexe 2 : références d'accidentalité pour l'analyse de sécurité des STRA

Sur la base de l'accidentologie et des travaux connus des experts rassemblés, des références d'accidentalité indicatives sont présentées dans le tableau suivant pour différents cas d'usage. Ces références brutes permettent :

- Aux concepteurs et aux organisateurs de service d'établir l'objectif global de sécurité pour la démonstration de sécurité d'un STRA assurant des services comparables à des services non automatisés,
- Aux évaluateurs d'évaluer cet objectif global de sécurité.

Il est possible de combiner ces références d'accidentalité pour représenter au mieux le domaine d'emploi (resp. le domaine de conception technique) du système (resp. du système technique) objet de la démonstration.

Si le concepteur, ou l'organisateur du service, justifie que d'autres données d'accidentologie, reconnues et statistiquement représentatives, sont mieux adaptées au cas d'usage du système objet de la démonstration, ces données peuvent servir de base à l'établissement de références d'accidentalité alternatives pour ce système.

Ces références d'accidentalité ont été établies sur la base

- Des données d'accidentalité issues du fichier national de l'accidentalité routière constitué des Bulletins d'Analyse des Accidents Corporels (BAAC) sur une durée de 5 ans (2015 à 2019). Ces données concernent les accidents corporels de la circulation routière survenus sur une voie publique ou privée, ouverte à la circulation publique, ayant impliqué au moins un véhicule et ayant causé au moins une victime.
  Ces données ont été affinées selon les cas d'usage suivants :
  - Autoroutes et voies à caractéristiques autoroutières[23] : accidents corporels impliquant des véhicules de tous types, survenus sur le réseau autoroutier, et sur les routes des autres catégories présentant des caractéristiques autoroutières ;
  - Routes nationales : accidents corporels impliquant des véhicules de tous types, survenus sur les routes nationales à l'exclusion de celles présentant des caractéristiques autoroutières ;
  - Autres routes : accidents corporels impliquant des véhicules de tous types, survenus sur les routes des autres catégories (routes métropolitaines, routes départementales et voies communales) à l'exclusion de celles présentant des caractéristiques autoroutières ;
  - Transports en commun en zone urbaine (TCU) : accidents survenus sur les réseaux de transport en commun urbain de 52 EPCI de plus de 100 000 habitants situés en France métropolitaine, et sur ceux de l'Ile de France ;
- Des données de trafic du SDES[24] pour les 3 premiers cas d'usage de type mobilité individuelle ; des données fournies par les exploitants dans le cadre des enquêtes annuelles d'une part et des données de l'OMNIL[25] pour l'Ile de France d'autre part, pour le cas d'usage TCU.

[23] Routes à chaussées séparées par un terre-plein central, comportant au moins deux voies par sens de circulation en section courante, isolées de leur environnement et dont les carrefours sont dénivelés (Catalogue des types de route pour l'aménagement du réseau routier national – CEREMA – Octobre 2018)
[24] Service des données et études statistiques
[25] Observatoire de la mobilité en Île-de-France

Références d'accidentalité brutes	Taux d'accidents mortels[26]/km parcouru	Taux d'accidents corporels non mortels/km parcouru
Autoroutes et voies à caractéristiques autoroutières	$1{,}89.10^{-9}$	$3{,}89.10^{-8}$
Routes nationales	$7{,}92.10^{-9}$	$9{,}18.10^{-8}$
Autres routes	$6{,}31.10^{-9}$	$1{,}07.10^{-7}$
Transports en commun en zone urbaine (TCU)	$2{,}84.10^{-8}$	$5{,}77.10^{-7}$

Pour déterminer un objectif global de sécurité qui puisse être utilisé par le concepteur du système dans le cadre de l'analyse de sécurité (cf. chapitre 7.1), celles-ci doivent faire l'objet des corrections suivantes, liées notamment à leur méthode d'élaboration :

- Prise en compte de la sous-déclaration des accidents non-mortels

A l'exception du cas d'usage des transports en commun en zone urbaine (TCU) pour lequel celle-ci n'est pas pertinente, les références brutes doivent être corrigées de la sous-déclaration des évènements non mortels observée dans les BAAC. Cette sous-déclaration a été analysée par comparaison avec le Registre du Rhône, et documentée par l'ONISR[27]. Il est possible sur cette base d'estimer le niveau de sous-déclaration propre à chaque macro-cas d'usage.

Le tableau ci-dessous donne le coefficient de correction à appliquer aux références brutes relatives au taux d'accidents corporels non mortels, pour les différents cas d'usage.

Correction de la sous-déclaration	Facteur de correction du taux d'accidents corporels non mortels /km parcouru
Autoroutes et voies à caractéristiques autoroutières	2,9
Routes nationales	3,4
Autres routes	3,4
Transports en commun en zone urbaine (TCU)	1

[26] Un accident est considéré comme mortel s'il a causé un ou plusieurs décès (personnes qui décèdent du fait de l'accident, sur le coup ou dans les trente jours qui suivent l'accident).

[27] Cf. document ONISR « Estimation du nombre de blessés graves et de blessés légers en France métropolitaine selon l'échelle internationale des blessures AIS »

- Prise en compte du contexte des objectifs de sécurité routière

Les références brutes doivent être corrigées afin de prendre en compte le contexte des objectifs de sécurité routière déclinés aux STRA : ces objectifs doivent traduire la référence à un conducteur conduisant de façon compétente et prudente[28] et la prise en compte de l'objectif de réduction de l'accidentalité routière à moyen terme fixé par l'UE (Towards « Vision Zero »)[29].

La prise en compte de ces éléments se traduit par l'application d'un facteur de correction global de 0,2 sur les références d'accidentalité.

Prise en compte du contexte des objectifs de sécurité routière	Facteur de correction du taux d'accidents corporels /km parcouru	
	Accidents mortels	Accidents non mortels
Autoroutes et voies à caractéristiques autoroutières	0,2	0,2
Routes nationales		
Autres routes		
Transports en commun en zone urbaine		

- Marges de sécurité

Au-delà des corrections ci-dessus, différentes marges de sécurité peuvent être intégrées par les concepteurs et les organisateurs de service afin de prendre en compte tout élément de contexte intéressant la sécurité, comme par exemple les incertitudes liées au caractère innovant du système.

NB : il convient de rappeler que ces références d'accidentalité sont construites sur la base des valeurs moyennes de l'accidentalité observée. L'objectif quantitatif issu de ces références reste donc un objectif moyenné, dont l'atteinte ne dispense pas de traiter de manière spécifique toute situation ponctuelle particulièrement accidentogène pour le système considéré. Cela peut consister par exemple à :

- Modifier une configuration de circulation présente sur le parcours de manière ponctuelle et pour laquelle le système est insuffisamment sûr ;
- Exclure du domaine d'emploi du système des conditions météorologiques trop défavorables.

[28] Cf. notamment annexe II 7.1.1 du règlement UE 2022/1426.

[29] Cf. document CADRE POLITIQUE DE L'UE EN MATIÈRE DE SÉCURITÉ ROUTIÈRE POUR LA DÉCENNIE D'ACTION 2021-2030

Annexe 3 : exemple de matrice de risque

La matrice de risque suivante propose un exemple de principes d'acceptation des risques selon 3 catégories d'acceptation comme définies au §7.2.2.

Elle est basée en entrée sur les niveaux de gravité (G), d'exposition (E) et d'évitabilité (Ev) du scénario d'accident résultant de la situation dangereuse envisagée.

Pour rappel, un risque évalué dans la catégorie « tolérable » ne peut être accepté que par exception et selon les conditions détaillées dans le §7.2.2.

Gravité	Exposition	Ev0	Ev1	Ev2	Ev3
G0	E0	Acceptable	Acceptable	Acceptable	Acceptable
	E1	Acceptable	Acceptable	Acceptable	Acceptable
	E2	Acceptable	Acceptable	Acceptable	**Tolérable**
	E3	Acceptable	Acceptable	**Tolérable**	**Inacceptable**
	E4	Acceptable	**Tolérable**	**Inacceptable**	**Inacceptable**
G1	E0	Acceptable	Acceptable	Acceptable	**Tolérable**
	E1	Acceptable	Acceptable	**Tolérable**	**Tolérable**
	E2	Acceptable	**Tolérable**	**Tolérable**	**Inacceptable**
	E3	Acceptable	**Tolérable**	**Inacceptable**	**Inacceptable**
	E4	**Tolérable**	**Inacceptable**	**Inacceptable**	**Inacceptable**
G2	E0	Acceptable	Acceptable	**Tolérable**	**Tolérable**
	E1	Acceptable	**Tolérable**	**Tolérable**	**Inacceptable**
	E2	Acceptable	**Tolérable**	**Inacceptable**	**Inacceptable**
	E3	**Tolérable**	**Inacceptable**	**Inacceptable**	**Inacceptable**
	E4	**Tolérable**	**Inacceptable**	**Inacceptable**	**Inacceptable**
G3	E0	Acceptable	**Tolérable**	**Tolérable**	**Inacceptable**
	E1	Acceptable	**Tolérable**	**Inacceptable**	**Inacceptable**
	E2	**Tolérable**	**Inacceptable**	**Inacceptable**	**Inacceptable**
	E3	**Tolérable**	**Inacceptable**	**Inacceptable**	**Inacceptable**
	E4	**Inacceptable**	**Inacceptable**	**Inacceptable**	**Inacceptable**

Annexe 4 : exemple analyse déductive type APD

Les exemples sont donnés uniquement pour illustration des analyses présentées au chapitre 10.
Les analyses des accidents ne sont aucunement exhaustives.
Les cotations faites des différentes situations dangereuses ne constituent en aucun cas des références.
L'analyse type APD de chaque exemple est présentée sur 3 tableaux à la suite parties 1/2/3.

Dans les tableaux suivants :

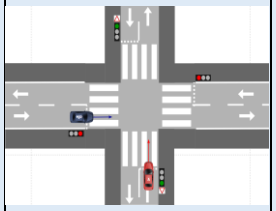
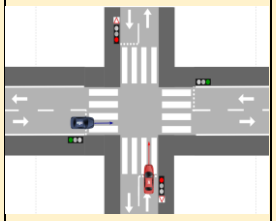
- « VHC » = véhicule
- « VA » = véhicule automatisé

ACCIDENT POTENTIEL DE NIVEAU STRA[30]				**IDENTIFICATION DE LA SITUATION DANGEREUSE**							**Type de cause(s) possible(s)**[31]	**Type GAME**	**EVALUATION INITIALE DES RISQUES**[32]								**EXIGENCES DE SECURITE**
								SYNTHESE de la situation dangereuse (SD) de niveau système					Gravité		Exposition		Evitabilité				
#	Type	#	Sous-type	Type de section d'infrastructures	Dynamique (des acteurs de la situation)	Eléments complémentaires de contexte	Illustration(s) de la situation étudiée	Réf.	Description	Personne(s) exposée(s)			Classe	Comm.	Classe	Comm.	Classe	Comm.	Référence(s) utilisée(s)	Description	Description

Partie 1 Partie 2 Partie 3

[30] Les # renvoient au tableau 11
[31] Le tableau 12 liste des points d'attention à prendre en compte pour identifier les causes
[32] L'évaluation du risque résiduel doit également prendre en compte la fréquence de la situation dangereuse (FSD) – cf. §8.3 Estimation de la fréquence d'occurrence de l'accident.

Exemple 1 : franchissement d'une intersection à feu tricolore – Partie 1

Réf exemple	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	
A	1	Collision	1.3	Collision avec un autre véhicule routier	Intersection à feux (sur Chaussée à 2x1 voie à sens opposé non séparée)	Vmax VA = 30 km/h Vmax Autre VHC = 50 km/h	<u>Le feu de signalisation est en fonctionnement nominal :</u> - ROUGE pour le VA - VERT pour l'autre VHC		SD-xx	Le VA s'insère alors que son feu est rouge menant à collision (lat/front/etc.) avec tiers	Passagers du VA Passagers de l'autre VHC
B	1	Collision	1.3	Collision avec un autre véhicule routier	Intersection à feux (sur Chaussée à 2x1 voie à sens opposé non séparée)	Vmax VA = 30 km/h Vmax Autre VHC = 50 km/h	<u>Le feu de signalisation est en fonctionnement nominal :</u> - VERT pour le VA - ROUGE pour l'autre VHC		SD-xx	Un tiers s'insère alors que son feu est rouge menant à collision (lat/front/etc.) avec tiers	Passagers du VA Passagers de l'autre VHC

Exemple 1 : franchissement d'une intersection à feu tricolore – Partie 2

Ref exemple	Type de cause(s) possible(s)	Type GAME	EVALUATION INITIALE DES RISQUES					
			Gravité		Exposition		Evitabilité	
			Classe	Commentaire(s)	Classe	Commentaire(s)	Classe	Commentaire(s)
A	#5 : Défaillance équipement électrique/électronique #6 : Insuffisance fonctionnelle (SOTIF) #12 : Défaillance mécanique	Type 3b Avec objectif	**G3**	Collision FRONTALE OU collision LATERALE Cas pire LATERAL : Δv = 50 km/h Plateforme VA M1, passagers assis et ceinturés, systèmes pyrotechniques actifs Δv latéral à expliciter	**E3**	Arrivée du VA à une intersection à feu COMBINE A Absence de VHC le précédant COMBINE A Un autre VHC arrive au même moment à l'intersection (par la gauche ou par la droite) COMBINE A Un autre VHC arrive à une vitesse max Δv = 50 km/h[33] ==> 1 % à 10 % du temps d'exploitation moyen.	**EV3**	Difficilement évitable (par les autres usagers de gérer une insertion soudaine du VA dans l'intersection alors que la priorité est à l'autre véhicule)
B	Le point de départ de la situation est le non-respect d'une règle de trafic par un tiers / accident causé par un tiers CAUSE INTERNE AU SYSTÈME ETUDIE DEGRADANT LA REPONSE DU SYSTEME A LA SITUATION INITIALE: #5 : Défaillance équipement électrique/électronique #6 : Insuffisance fonctionnelle (SOTIF) #12 : Défaillance mécanique	Type 3b Avec objectif	**G3**	Collision FRONTALE OU collision LATERALE Cas pire LATERAL : Δv = 50 km/h Plateforme VA M1, passagers assis et ceinturés, systèmes pyrotechniques actifs Δv latéral à expliciter	**E3**	Arrivée du VA à une intersection à feu COMBINE A Absence de VHC le précédant COMBINE A Un autre VHC arrive au même moment à l'intersection (par la gauche ou par la droite) COMBINE A Un autre VHC arrive à une vitesse max Δv = 50 km/h ==> 1 % à 10 % du temps d'exploitation moyen.	**EV3**	Difficilement évitable (par les autres usagers)

[33] Cette dernière condition porte sur le cas du pire Δv latéral avec vitesse VHC = 50 km/h et doit être adaptée. Selon les configurations de choc et les protections, la collision peut être de gravité G3 pour un Δv plus faible que 50 km/h et donc avoir un valeur d'Exposition plus élevée.

Exemple 1 : franchissement d'une intersection à feu tricolore – Partie 3

Ref exemple	Traitement envisagé de la situation		EXIGENCES DE SECURITE
	Référence(s) utilisée(s)[34]	Description[35]	Description des exigences[36]
A	Cf. § « Déclinaison des objectifs de sécurité » décrivant la déclinaison OGS > TFR	Objectif à répartir sur chaque fonction participant à la gestion de priorité carrefour : fonction embarquées, fonctions de l'équipement connecté, communication, etc. NB : au-delà de la perception et du respect de l'état du feu, le périmètre des fonctions liées à la situation dangereuse intègre aussi les fonctions de décision et de réalisation de la trajectoire du VA. + {* sécurité passive du VA * aménagement intérieur du VA * détection collision (immobilisation, alerte supervision, etc.) * moyens d'évacuation du VA}	…..
B	Cf. § « Déclinaison des objectifs de sécurité » décrivant la déclinaison OGS > TFR	Le comportement visé pour le VA est l'évitement ou la manœuvre d'urgence lorsque l'autre véhicule arrive en face du VA Objectif à répartir sur chaque fonction participant à la perception de la trajectoire du tiers et à la décision et réalisation de la trajectoire du VA. + {* sécurité passive du VA * aménagement intérieur du VA * détection collision (immobilisation, alerte supervision, etc.) * moyens d'évacuation du VA}	…..

[34] Les référentiels généraux sous-jacents à la démonstration tels que les référentiels d'homologation, les exigences de haut niveau, la référence du véhicule à conduite conventionnel en termes de comportement, ne sont pas listés dans ce tableau car de niveau général

[35] Les éléments listés comprennent les mesures pour éviter la situation dangereuse d'une part, et celles entre {} visant à en réduire les conséquences d'autre part si la situation dangereuse se matérialise en accident malgré les premières mesures.

[36] La description des exigences vise à définir les concepts de sécurité. L'évaluation finale des risques doit ensuite évaluer le risque résiduel suite à la mise en œuvre de ces exigences de sécurité.

Exemple 2 feu/fumées explosion – Partie 1

Ref exemple	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	SYNTHESE de la situation dangereuse (SD) de niveau système		Personne(s) exposée(s)
									Réf.	Description	
C	5	Feu/fumée/explosion	5.3 5.6	Feu/fumée sur le parcours Explosion sur le parcours	Une chaussée routière à 2 voies, limitée à 30 km/h	Le VA se déplace à une vitesse maximale de 30 km/h tandis que n véhicule accidenté en feu se trouve sur le parcours du VA	Le véhicule en feu se trouve sur le bas-côté de la chaussée - Possibilité pour le VA de contourner l'obstacle cependant, le véhicule en feu peut exploser lors du passage à proximité de la VA	SO	SD-xx	Le VA détecte le véhicule mais pas la présence de l'incendie à l'intérieur du véhicule qui est amené à exploser. Il opère un contournement de l'obstacle Explosion du véhicule projetant des débris sur les passagers	Passagers VA
D	5	Feu/fumée/explosion	5.1	Feu/fumée dans le véhicule	Une chaussée routière à 2 voies, limitée à 30 km/h	Le VA se déplace à une vitesse maximale de 30 km/h.	Le véhicule circule sur une chaussée à double sens bordée de trottoirs et d'arbres. Un dégagement de fumée survient dans l'habitacle au niveau d'un moteur de porte.	SO	SD-xx	Asphyxie des passagers par les fumées. Départ de feu se propageant à l'habitacle	Passagers VA
E	5	Feu/fumée/explosion	5.1	Feu/fumée dans le véhicule	Une chaussée routière à 2 voies, limitée à 30 km/h	Le VA se déplace à une vitesse maximale de 30 km/h.	Le véhicule circule sur une chaussée à double sens bordée de trottoirs et d'arbres. Un dégagement de fumée survient dans l'habitacle au niveau d'un habillage de siège.	SO	SD-xx	Asphyxie des passagers par les fumées. Départ de feu se propageant à l'habitacle	Passagers VA

Exemple 2 feu/fumées explosion – Partie 2

Ref exemple	Type de cause(s) possible(s)	Type GAME	EVALUATION INITIALE DES RISQUES					
			Gravité		Exposition		Evitabilité	
			Classe	Commentaire(s)	Classe	Commentaire(s)	Classe	Commentaire(s)
C	#13 : incendie au voisinage du système	Type 3b sans objectif	**G3**	Propagation incendie sur la VA / explosion Plateforme NAVURB M2, passagers assis non ceinturés et debout,	**E1**	Situation plutôt rare Moins d'une fois / an en moyenne	**Ev3**	Pas de possibilité d'évitement pour les personnes impliquées
D	#5 : défaillance équipement électrique	Type 3b sans objectif	**G3**	Personne âgée seule. PMR	**…**	Fonction du taux de défaillance de l'équipement électrique	**Ev3**	Pas de possibilité d'évitement pour les personnes impliquées
E	#14 comportement dangereux usagers #15 comportement malveillant	Type 3b sans objectif	**G3**	Personne âgée seule. PMR	**E2**	Quelques fois / an, moins d'une fois / mois	**Ev3**	Pas de possibilité d'évitement pour les personnes impliquées

Ref exemple	Traitement envisagé de la situation		EXIGENCES DE SECURITE
	Référence(s) utilisée(s)[37]	Description[38]	Description des exigences[39]
C	*Conformité au R107 (spécifique véhicule de type M2) concernant les évacuations de secours Nécessité en amont d'une fonction de détection d'un incendie au voisinage évaluée en référence à norme IEC 61508 --> exigences par rapport aux fonctions de détection, de pilotage d'un arrêt MRM ou dégradé (macro-fonction)	Mise en œuvre d'une stratégie de réduction des risques	Le VA doit disposer d'un système d'évacuation de secours accessible aux passagers en cas d'urgence. Ce moyen doit permettre en cas d'activation, l'arrêt du véhicule afin que les passagers puissent évacuer. Le VA doit détecter l'incendie dans le voisinage de sa trajectoire + analyse spécifique si équipement E/E Le VA doit effectuer un arrêt dès qu'il détecte l'incendie : MRM, arrêt en voie …
D	Référentiel relatif aux règles de dimensionnement et aux protections électriques pour le véhicule Moyens de détection et d'alerte incendie dans le véhicule. Rôle de l'intervenant à distance. Prise en compte de l'absence de personnel à bord	Mise en œuvre d'une stratégie de réduction des risques	…..
E	Par exemple, prise en compte d'un référentiel couvrant un système HORS STRA avec des enjeux comparables vis-à-vis de l'évènement étudié. Prise en compte de l'absence de personnel à bord	Mise en œuvre d'une stratégie de réduction des risques	……

[37] Les référentiels généraux sous-jacents à la démonstration tels que les référentiels d'homologation, les exigences de haut niveau, la référence du véhicule à conduite conventionnel en termes de comportement, ne sont pas listés dans ce tableau car de niveau général

[38] Les éléments listés comprennent les mesures pour éviter la situation dangereuse d'une part, et celles entre {} visant à en réduire les conséquences d'autre part si la situation dangereuse se matérialise en accident malgré les premières mesures.

[39] La description des exigences vise à définir les concepts de sécurité. L'évaluation finale des risques doit ensuite évaluer le risque résiduel suite à la mise en œuvre de ces exigences de sécurité.

Annexe 5 : exemples analyse inductive type APR

Les exemples sont donnés uniquement pour illustration des analyses présentées au chapitre 10.
Les analyses des accidents ne sont aucunement exhaustives.
Les cotations faites des différentes situations dangereuses ne constituent en aucun cas des références.
L'analyse type APD de chaque exemple est présentée sur 3 tableaux à la suite parties 1/2/3.

Dans les tableaux suivants :

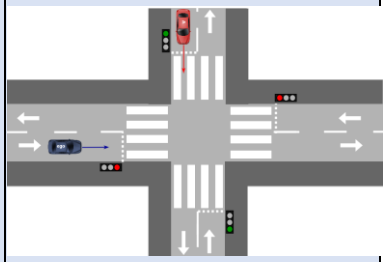
- « VHC » = véhicule
- « VA » = véhicule automatisé

FONCTION		IDENTIFICATION DE LA SITUATION DANGEREUSE					EVENEMENT REDOUTE / ACCIDENT POTENTIEL DE NIVEAU STRA[40]			EVALUATION INITIALE DES RISQUES[41]			EXIGENCE(S) DE SECURITE DE NIVEAU STRA						
Fonction étudiée [42]	Mode de défaillance ou d'Insuffisance fonctionnelle	SYNTHESE 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	Description	EFFET	Personne(s) exposée(s)	Gravité	Exposition	Evitabilité	Type d'approche GAME	Description	PartOGS	Niveau d'intégrité requis	Etat sûr	Exigence de sécurité	Caractérisation de l'exigence de sécurité

Partie 1 Partie 2 Partie 3

[40] En lien avec tableau 11
[41] L'évaluation du risque résiduel doit également prendre en compte la fréquence de la situation dangereuse (FSD) – cf. §8.3 Estimation de la fréquence d'occurrence de l'accident.
[42] cf. tableau 16

Exemple « Définition, le suivi et le contrôle de trajectoire » – Partie 1

Ref exemple	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 du rang1	Intitulé du rang étudié		Réf.	Description				
A	1	**1-Assurer la définition, le suivi et le contrôle de la trajectoire du véhicule**	1.4.1.2-Gérer la décélération	Défaillance : Absence / Perte / Erroné Absence de décélération ou décélération insuffisante à l'arrivée sur un feu rouge	SD-xx	Le VA ne décélère pas, ou décélère insuffisamment, et ne respecte pas la priorité vis-à-vis des autres véhicules à l'intersection, alors qu'un autre véhicule arrive à l'intersection	Intersection entre : - la chaussée à 2 voies, dédiée aux véhicules automatisés du STRA, limitée à 30 km/h ; - et une chaussée routière à 2 voies, dédiée aux autres usagers de la route, limitée à 50 km/h ; avec des feux de circulation connectés avec les véhicules automatisés.	Le VA se déplace à une vitesse maximale de 30 km/h **TANDIS QUE** Un autre VHC routier arrive à l'intersection (par la gauche ou par la droite) à vitesse maximale de 50 km/h	Le feu de signalisation est en fonctionnement nominal : - ROUGE pour le VA - VERT pour l'autre VHC Plateforme VA M1, passagers assis et ceinturés, systèmes pyrotechniques actifs	 $V_{max\ VA}$ = 30 km/h $V_{max\ Autre}$ = 50 km/h
B	1	**1-Assurer la définition, le suivi et le contrôle de la trajectoire du véhicule**	1.4.1.2-Gérer la décélération	Décélération trop forte (au-delà des seuils nominaux)	SD-xx	Le VA décélère très fort alors que le véhicule est suivi par un autre véhicule	Tout type de section d'infrastructure	Le VA se déplace à une vitesse maximale de 30 km/h. Il est suivi par un autre véhicule au moment où il commence à décélérer.	Le véhicule suiveur est en conduite manuelle.	Zone urbaine limitée à 30 Km/h  $V_{max\ VA}$ = 30 km/h
C	1	**1-Assurer la définition, le suivi et le contrôle de la trajectoire du véhicule**	1.4.1.2-Gérer la décélération	Décélération trop forte (au-delà des seuils nominaux)	SD-xx	Le VA décélère très fort alors que le véhicule est suivi par un autre véhicule	Tout type de section d'infrastructure	Le VA se déplace à une vitesse maximale de 30 km/h. Il est suivi par un autre véhicule au moment où il commence à décélérer.	Le véhicule suiveur est en conduite manuelle.	Zone urbaine limitée à 30 Km/h  $V_{max\ VA}$ = 30 km/h

Exemple « Définition, le suivi et le contrôle de trajectoire » – Partie 2

Ref exemple	EVENEMENT REDOUTE / ACCIDENT POTENTIEL DE NIVEAU STRA						EVALUATION INITIALE DES RISQUES					
	Description	EFFET = ACCIDENT POTENTIEL DE NIVEAU STRA				Personne(s) exposée(s)	Gravité		Exposition		Evitabilité	
		#	Type	#	Sous-type		Classe	Commentaire(s)	Classe	Commentaire(s)	Classe	Commentaire(s)
A	Absence de décélération ou décélération insuffisante à l'arrivée sur un feu rouge ==> Le VA ne respecte pas la priorité vis-à-vis des autres véhicules à l'intersection	1	Collision	1.3	Collision avec un autre véhicule routier	Passagers du VA Passagers de l'autre VHC	**G3**	Collision FRONTALE OU collision LATERALE Cas pire LATERAL : Δv ⩽ 50 km/h Plateforme VA M1, passagers assis et ceinturés, systèmes pyrotechniques actifs	**E3**	[43]Arrivée du VA à une intersection à feu COMBINE A Absence de VHC le précédant COMBINE A Un autre VHC arrive au même moment à l'intersection (par la gauche ou par la droite) ==> 1 % à 10 % du temps d'exploitation moyen NB : < 10% semble peu en zone urbaine	**EV3**	Difficilement contrôlable (par les autres usagers de gérer une insertion soudaine du VA dans l'intersection alors que la priorité est à l'autre véhicule)
B	Décélération intempestive (trop forte)	1	Collision	1.3	Collision avec un autre véhicule routier	Passagers du VA, Passagers du VHC suiveur	**G1**	Collision arrière : Cas pire arrière : Δv proche de 30 km/h Plateforme VA M1, passagers assis et ceinturés, systèmes pyrotechniques actifs,	**E4**	Présence des véhicules suiveurs dans une zone urbaine, avec interdistance nominale	**EV2**	Normalement contrôlable pour le conducteur du VHC suiveur d'éviter la collision arrière
C	Décélération intempestive (trop forte)	1	Collision	1.3	Collision avec un autre véhicule routier	Passagers du VA, Passagers du VHC suiveur	**G1**	Collision arrière : Cas pire arrière : Δv proche de 30 km/h Plateforme VA M1, passagers assis et ceinturés, systèmes pyrotechniques actifs,	**E3**	Présence des véhicules suiveurs dans une zone urbaine, avec interdistance anormalement courte	**EV3**	Difficilement contrôlable pour le conducteur du VHC suiveur d'éviter la collision arrière

[43] En complément de ce cas-ci, l'autre cas à envisager est le cas similaire mais avec présence d'un VHC précédant le VA et collision par l'AR avec ce VHC précédant.

Exemple « Définition, le suivi et le contrôle de trajectoire » – Partie 3

Ref exemple	EXIGENCE(S) DE SECURITE DE NIVEAU STRA								
	TYPE D'APPROCHE GAME		Description	Part de l'Objectif Global de Sécurité quantitatif alloué à la fonction étudiée, pour le mode de défaillance ou d'insuffisance fonctionnelle étudiée		Niveau d'intégrité requis *via Table de correspondance TFFR <> ASIL, SIL*	Etat sûr	Exigence de sécurité	Caractérisation de l'exigence de sécurité
	Type	Référence(s) utilisée(s)	Description	Document d'argumentation de la déclinaison	Valeur				
A	Type 3b Avec objectif	Objectif Global de Sécurité quantitatif = 1.00E-08 / h[44]	OGS = 1.00E-08 / h FRR = E3 x Ev3 = 0,1 x 1 THR = OGS / FRR THR < 1.00E-07 / h (en liaison avec d'autres causes[45])	Document xxx	à définir	**ASIL C** (si référentiel ISO 26262)	Arrêt du VA avant d'entrer dans l'intersection	Le VA doit s'assurer de ne pas entrer dans une intersection avec des feux de circulation si l'état du feu est ROUGE	À définir
B	Type 3b Avec objectif	Objectif Global de Sécurité quantitatif = 1.00E-06 / h[35] (gravité G1)	OGS = 1.00E-06 / h FRR = E4 x Ev2 = 1 x 0.1 THR = OGS / FRR THR < 1.00E-05 (en liaison avec d'autres causes[36])	Document xxx	à définir	**ASIL A** (si référentiel ISO 26262)	Sans objet	Limiter la décélération à un niveau contrôlable par le véhicule suiveur (e.g. 4m/s²)	À définir
C	Type 3b Avec objectif	Objectif Global de Sécurité quantitatif = 1.00E-06 / h[35] (gravité G1)	OGS = 1.00E-06 / h FRR = E3 x Ev3 = 0.1 x 1 FSD = OGS / FRR FSD < 1.00E-05 (en liaison avec d'autres causes[36])	Document xxx	à définir	**ASIL A** (si référentiel ISO 26262)	Sans objet	Limiter la décélération à un niveau contrôlable par le véhicule suiveur (e.g. 4m/s²)	À définir

[44] La valeur de 1.00E-08 /h est donnée ici pour illustration. Il faudra éventuellement considérer en plus l'Objectif Spécifique de Sécurité éventuel pour les collisions aux intersections.

[45] La somme des TFRi X FRRi doit respecter le ou les objectifs quantitatifs. La déclinaison doit ensuite être poursuivie jusqu'à la fonction (TFFRi) (Cf. §7.1.2)