GUIDE D'APPLICATION

STRMTG
SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

SYSTÈMES DE TRANSPORT ROUTIER AUTOMATISES

PRINCIPE « GAME »
Globalement Au Moins Équivalent

MINISTÈRE CHARGÉ DES TRANSPORTS
Liberté
Égalité
Fraternité

Version 1 du 20 décembre 2021

Objet – Domaine d'application – Destinataires

Le présent guide d'application explicite une méthodologie de démonstration du principe « GAME » (Globalement au moins équivalent) prévue par le décret n°2021-873 du 29 juin 2021 portant application de l'ordonnance n° 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation (décret « STRA »).

Il est applicable à un système de transport routier automatisé défini par l'article R.31151-1 du code des transports (ajouté par article 6 du décret STRA), comme étant un *« système technique de transport routier automatisé, déployé sur des parcours ou zones de circulation prédéfinis, et complété de règles d'exploitation, d'entretien et de maintenance, aux fins de fournir un service de transport routier public collectif ou particulier de personnes, ou de service privé de transport de personnes, à l'exclusion des transports soumis au décret no 2017-440 du 30 mars 2017 relatif à la sécurité des transports publics guidés »*.

Il est destiné à l'ensemble des acteurs professionnels du secteur des transports routiers automatisés : Autorité organisatrice de mobilité (AOM), maitres d'ouvrage, exploitants, maîtres d'œuvre, bureaux d'études, Organismes qualifiés agréés (OQA), concepteurs de systèmes de transports routiers automatisés, constructeurs de matériels.

Les dispositions du présent guide visent à expliciter et décliner la réglementation de sécurité applicable. Elles formalisent les attentes concertées du STRMTG et de la profession, offrant ainsi 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.

Elles sont limitées à la sécurité des personnes transportées (passagers, conducteurs…) et des tiers vis-à-vis du fonctionnement du système.

Elles ne traitent pas :

– des problématiques relatives à la sûreté publique (colis suspect, acte de vandalisme…) ou à l'accessibilité, à proprement parler, du système de transport ;
– 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 ERP de type gare en tant que tel, hormis pour leurs interfaces avec le système de transport ;
– des problématiques liées à la Défense extérieure contre l'incendie (DECI) ;
– de la prise en compte des éventuels risques engendrés par les travaux de réalisation du projet lorsque ceux-ci n'ont pas d'impacts sur un système de transport routier automatisé existant.

Historique des mises à jour

N° version	Rédacteur	Date	Nature de la version
1	P.Jouve	20/12/2021	Création par GT GAME (STRA)

RÉDACTEUR	VÉRIFICATEUR	APPROBATEUR
Pierre Jouve Chef du département transports publics automatisés	**Alexandre Dusserre** Chef du département métros et systèmes ferroviaires	**Daniel Pfeiffer** Directeur
Pierre JOUVE pierre.jouve Signature numérique de Pierre JOUVE pierre.jouve Date : 2021.12.20 15:49:13 +01'00'	Alexandre DUSSERRE alexandre.dusserre 2021.12.21 10:23:08 +01'00'	Le Directeur du Service Technique des Remontées Mécaniques et des Transports Guidés Daniel PFEIFFER Signature numérique de Daniel PFEIFFER daniel.pfeiffer Date : 2021.12.21 10:34:08 +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

Préambule

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

La démonstration du respect de ces exigences est composée de plusieurs démonstrations imbriquées dont l'articulation se fait entre les niveaux sous-système et système. Le présent document ne développe que la démonstration des exigences relatives au principe GAME.

En préalable, les véhicules intégrés dans le STRA doivent faire l'objet d'une réception préalable au titre du Code de la route. La réception (ou homologation) est la certification administrative de la conformité du véhicule aux exigences des règlementations techniques en vue de permettre son immatriculation et sa circulation. Ce processus n'est pas abordé dans le présent guide. La réception est un prérequis à la démonstration de sécurité mais elle ne suffit pas à démontrer la sécurité des systèmes vis-à-vis de tous les évènements redoutés. Par définition, le périmètre de l'homologation est limité au véhicule. Aussi, si les résultats de l'homologation et ses référentiels associés servent de données d'entrée à la démonstration de sécurité des STRA, les analyses faites dans le cadre de l'homologation ne sauraient dispenser des analyses de niveau système décrites dans le présent guide.

La démonstration du respect des exigences de sécurité applicables au STRA est réalisée au niveau du système. Elle est réalisée pour chaque système dans son domaine d'emploi et pour un parcours ou une zone prédéfini et vise à s'assurer de son fonctionnement en sécurité, dans les conditions de circulation raisonnablement prévisibles. La validation de la sécurité du STRA est un processus complexe au sein duquel coexistent plusieurs approches imbriquées et complémentaires.

- La démonstration de la sécurité, au sens de l'approche GAME, a pour objectif de démontrer que le niveau global de sécurité à l'égard des usagers, des personnels d'exploitation et des tiers est 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 démonstration permet de combiner plusieurs types d'approches au niveau des systèmes ou des sous-systèmes considérés : respect des réglementations et des référentiels techniques existants, comparaison avec des systèmes de référence existants (approche par écarts), analyse détaillée des risques combinant analyses inductives et déductives.
La démonstration GAME concerne le périmètre global du système et vise à couvrir l'ensemble des risques relatifs à la sécurité des personnes transportées et des tiers, sans se limiter à ceux liés à la collision des véhicules ou aux dysfonctionnements du système. Elle définit les exigences quantitatives comme qualitatives, portant aussi bien sur la conception que sur l'exploitation du système. Ces exigences sont ensuite déclinées sur les différents sous-systèmes et composants ainsi que dans le SGS. Seule cette démonstration est l'objet du présent guide d'application.

- « L'approche par scénarios » vise à construire un ensemble de scénarios de circulation représentatifs du domaine d'emploi d'un système : elle alimente certaines étapes de la démonstration de sécurité de l'approche GAME, qui sont amenées à utiliser ou générer des scénarios. L'approche par scénarios vise en premier lieu à harmoniser les descripteurs des

contextes de conduite ainsi que des objets et des événements de circulation potentiellement rencontrés dans le domaine d'emploi du système technique. L'approche par scénarios peut, par une combinaison la plus systématique possible des descripteurs d'environnements de conduite et d'aléas, et, le cas échéant, de sur-aléas, contribuer à limiter le risque d'omission de scénarios critiques dans la démonstration de sécurité. L'approche par scénarios est également susceptible, pour le domaine de conception fonctionnelle (ODD) a*fférent au système, d'extraire un jeu de scénarios de circulation dont la démonstration de sécurité pourrait être amenée à tracer la prise en compte, ou les motifs pour lesquels ce scenario n'est pas pertinent pour le système étudié, ce qui fournirait une information utile sur la façon dont le risque d'omission de scénarios a été traité. L'approche par scénario reste à élaborer au moment de la rédaction du présent guide et n'y est donc pas décrite.*

*- L'analyse de sécurité du parcours vise à démontrer la compatibilité du parcours avec le domaine de conception technique du système technique et la capacité du système technique à fonctionner en sécurité sur le parcours pour les situations de circulation qu'il pourra rencontrer. Chaque parcours sur lequel est déployé un STRA étant unique et comportant des risques qui lui sont propres, l'analyse de sécurité de chaque parcours est systématiquement nécessaire. Cette analyse permet notamment l'identification de scénarios de circulation spécifiques à chaque parcours, complémentaires de l'approche GAME et de l'approche par scé*narios*. Les exigences propres à l'analyse de sécurité du parcours ne sont pas décrites dans le présent guide.*

- L'analyse cyber-sécurité définit les exigences relatives à la protection des systèmes numériques vis-à-vis des agressions, qui doivent être prises en compte aux différents stades de la conception des systèmes, ainsi que durant leurs différentes phases de vie. La cyber-sécurité n'est pas abordée dans le présent guide.

La démonstration de sécurité d'un STRA regroupe donc un ensemble de démonstrations, en interface les unes avec les autres. Si le présent guide d'application tend à définir le cadre général de démonstration, il ne décrit pas l'ensemble des éléments de la démonstration.

Enfin, la méthode de démonstration du principe GAME présentée dans ce guide d'application n'est en rien exclusive. Pour tout nouveau système ou pour toute partie de système existant modifié, d'autres méthodes de démonstration peuvent ainsi être utilisées, dans la mesure où elles présenteraient des objectifs similaires. Dans ce cas, la méthode de démonstration alternative suivie fera également l'objet d'une évaluation par l'OQA.

Définitions

Les définitions ci-dessous proviennent de l'article R.3151-1. du code des transports créé par l'article 6 du décret STRA:

« 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 ;

« Système de transport routier automatisé » : système technique de transport routier automatisé, déployé sur des parcours ou zones de circulation prédéfinis, et complété de règles d'exploitation, d'entretien et de maintenance, aux fins de fournir un service de transport routier public collectif ou particulier de personnes, ou de service privé de transport de personnes, à

l'exclusion des transports soumis au décret no 2017-440 du 30 mars 2017 relatif à la sécurité des transports publics guidés ;

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

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

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

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

En complément, il semble utile de préciser les termes suivant sur la base des définitions issues de publication existantes ou élaborées dans le cadre spécifique de ce guide :

« Danger » : circonstance pouvant mener à un accident (règlement UE 402/2013 du 30 avril 2013).

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

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

Liste des abréviations

AOM : Autorité organisatrice de la mobilité
DCST : Dossier de conception du système technique
DECI : Défense extérieure contre l'incendie
DPS : Dossier préliminaire de sécurité
DS : Dossier de sécurité
ERP : Etablissement recevant du public
GAME : Globalement au moins équivalent
ODD : Domaine de conception fonctionnelle (« Operational design domain »)
OQA : Organisme qualifié agréé
REX : Retour d'expérience
SGS : Système de gestion de la sécurité
SOTIF : Sécurité de la fonctionnalité attendue (« Safety of the intended functionality »)
STRA : Système de transport routier automatisé

1. Champ d'application

Le présent guide est applicable aux systèmes de transport visés par l'article R.3152-2. du code des transports créé par l'article 6 du décret STRA n° 2021-873 du 29 juin 2021. Il est donc applicable aux systèmes techniques de transport routier automatisés, déployés sur des parcours ou zones de circulation prédéfinis, 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.

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

Cette exigence est introduite dans les termes suivants à l'article R.3152-2. du code des transports créé par l'article 6 du décret STRA :

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

La notion de GAME prend en compte notamment :

- les différentes parties d'un système existant ;
- l'évolution des règles de l'art (normes, guides techniques, recommandations, …) ;
- le retour d'expérience.

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

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

Le présent guide vise donc à expliciter les conditions de la démonstration par comparaison avec un système de référence et son articulation avec les cas où il n'existe pas de système de référence.

Préalablement à la présentation de la méthodologie de démonstration du respect de ce principe, il convient d'apporter des précisions relatives au champ d'application de ce principe.

1.1. Périmètre du système faisant l'objet de l'analyse

La méthodologie proposée dans les chapitres suivants s'appuie sur les constats et analyses suivants :

Un système de transport routier automatisé est composé de différents sous-systèmes structurels et opérationnels interfacés.

Chaque sous-système est lui-même constitué de différents sous-ensembles, éventuellement interfacés.

Au fur et à mesure de la maturation des systèmes, un système de transport routier automatisé de personnes pourra être constitué de sous-ensembles « standards » déjà utilisés sur des systèmes similaires. Certains sous-ensembles pourront donc avoir déjà fait l'objet d'une démonstration de sécurité, au moins pour des conditions d'utilisation et d'environnement données.

Pour autant, chaque système de transport routier automatisé est unique. En effet, les interfaces entre les différents sous-ensembles le constituant, les caractéristiques de son environnement, le parcours ou la zone prédéfinie où il circule notamment sont, de fait, spécifiques. Ce constat justifie l'élaboration de démonstrations de sécurité et leur évaluation au cas par cas, préalablement à la décision de mise en service pour les STRA, en complément à la logique de réception nationale par type mise en œuvre dans le domaine des véhicules routiers par exemple.

Il est dès lors impératif de s'assurer de l'aptitude des différents sous-ensembles à fonctionner ensemble en sécurité et de la capacité du système à fonctionner en sécurité dans son environnement sur son parcours (ou sa zone) prédéfini.

La justification du niveau de sécurité à l'échelle du système ne peut donc pas être apportée par la seule démonstration, sans autre forme de garantie, du niveau de sécurité de ses différents sous-ensembles.

Aussi, le décret STRA définit la notion de système de transport routier automatisé comme intégrant les véhicules et installations techniques hors véhicules, le parcours ou la zone où ces composantes sont déployées et les règles d'exploitation et de maintenance.

Au sens du présent document, la notion de système est employée de manière générique. Elle peut ainsi faire référence à un système complet de transport routier automatisé, à un système technique, à un sous-système ou à une composante.

Le principe GAME s'applique donc au système considéré, qui doit toutefois être appréhendé en tant qu'élément du système de transport routier automatisé complet. Ceci signifie que la démonstration de la sécurité doit être faite in fine au niveau du système de transport routier automatisé complet considéré, c'est à dire d'un système technique déployé sur un parcours donné et sujet à des règles d'exploitation, d'entretien et de maintenance.

Il en résulte que même si une modification ne concerne qu'un composant d'un système de transport routier automatisé, la démonstration du GAME devra être faite au niveau du système de transport routier automatisé complet considéré.

1.2. Opérations concernées

Le principe « GAME » est un principe général qui, selon les termes du décret, doit être mis en œuvre dans le cadre de tout nouveau système de transport routier automatisé ou de toute modification, même non substantielle d'un système existant.

Le principe « GAME » est donc à respecter en toutes circonstances.

Si une modification n'est pas substantielle (c'est à dire l'évaluation de la sécurité du système n'est pas modifiée), le niveau de sécurité du système n'est pas impacté par la modification. L'analyse montrant que la modification n'est pas substantielle démontre donc le respect du principe GAME.

Dès lors qu'une modification entraîne la modification de l'évaluation de la sécurité du système, alors cette modification est considérée comme substantielle.

1.3. Périmètre de la sécurité

L'article R.3152-2. du code des transports créé par l'article 6 du décret STRA, définit 3 grandes « populations » :

- les usagers du système de transport,
- les personnels d'exploitation,
- les tiers,

à l'égard desquelles il convient de respecter le principe « GAME » dans le cadre de tout nouveau système et de toute modification d'un système existant.

Dans le cadre du processus de décision de mise en service des systèmes de transport routier automatisés (et des dossiers de sécurité afférents), sans préjudice des exigences de sécurité découlant d'autres réglementations, la démonstration du « GAME » n'est cependant explicitée dans le présent guide qu'en 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.

2. Objectifs et limites du principe « GAME »

2.1. Notion de globalité

La notion de globalité associée au principe « GAME » peut a priori être appréhendée à différents niveaux (système complet, sous-système, par événement redouté, pour un ensemble d'évènements redoutés, pour la totalité des évènements redoutés, …).

Elle implique qu'une « insuffisance » structurelle du système peut sous réserves de justifications, être « compensée » par un « gain » au niveau d'un (ou plusieurs) autre(s) dispositif(s) structurel(s) ou bien être rendue « acceptable » par le biais d'une (ou plusieurs) mesure(s) d'ordre opérationnel (critère de maintenance ou d'exploitation particulier par exemple).

En tout état de cause, il est exclu d'intégrer dans la démonstration du « GAME » les éventuels gains de sécurité dus aux reports modaux (des modes routiers classiques vers le transport automatisé notamment) liés à l'arrivée du nouveau système de transport.

En conclusion, si le principe « GAME » introduit une certaine souplesse à travers la possibilité de poursuivre une approche « système » de la sécurité, la notion de « globalité » qui lui est associée doit être entendue dans les limites évoquées ci-dessus.

2.2. Notion d'équivalence

La notion d'équivalence introduite par le décret traduit l'objectif de non-régression du niveau de sécurité par rapport au niveau de sécurité des systèmes existants comparables.

Il est à noter que cette équivalence lorsqu'elle est démontrée par rapport à un système ou un sous-système comparable doit également prendre en compte l'évolution des règles de l'art et le retour d'expérience pour le système ou le sous-système concerné en application de l'article R.3152-2. du code des transports créé par l'article 6 du décret STRA. Ainsi, dans le cas de la modification d'une partie d'un système, la prise en compte de l'évolution des règles de l'art et du retour d'expérience ne s'appliquera qu'à la partie modifiée du système.

2.3. Articulation des différentes approches de démonstration

Il existe, schématiquement, trois approches de démonstration de sécurité applicables, appliquées danger par danger :

- Approche de type 1 : respect de la réglementation technique et de sécurité ou la conformité à un référentiel technique ;
- Approche de type 2 : comparaison avec un système existant, aussi appelée approche par écarts ;
- Approche de type 3 : analyse détaillée des risques vis-à-vis de chaque événement redouté suivant une méthode reconnue.

La démonstration de sécurité doit s'appuyer sur l'une de ces approches ou une combinaison des trois, en donnant la priorité à l'approche de type 1 :

Type 1	En premier lieu, dans la mesure où un référentiel réglementaire applicable existe, il s'impose. La référence est, de fait, déclinée et imposée par les dispositions réglementaires en vigueur. Dans le même esprit, bien qu'à un autre niveau (puisque non opposable juridiquement), on peut également considérer que la question de la référence est résolue dès lors qu'il existe un référentiel technique reconnu et pertinent (ex : norme, guide technique du STRMTG, recommandation, ...). Le référentiel pris en compte doit être celui en vigueur au moment où la méthodologie de démonstration de la sécurité pour le parcours ou la zone sur lequel le système technique est déployé, est arrêtée (i.e. à la date de l'avis favorable de l'OQA portant sur le DPS, à condition toutefois que la décision de mise en service soit prise dans un délai raisonnable suivant cette date). Ces référentiels techniques constituent le niveau de sécurité minimum admissible sans justification. Cependant, d'autres démonstrations peuvent être proposées, dans la mesure où l'équivalence des exigences par rapport au référentiel énoncé au deuxième paragraphe serait justifiée.
Type 2	Lorsqu'il n'existe ni référentiel réglementaire applicable, ni référentiel technique applicable, la démarche de comparaison avec un système existant de référence, appelée « approche par écarts », peut être envisagée. Le système pris en référence doit alors satisfaire aux différents critères explicités dans le chapitre 3. L'évolution des règles de l'art par rapport à celles du système de référence et son retour d'expérience, doivent être prise en compte au moment où les référentiels sont figés, à la date de l'avis favorable de l'OQA portant sur le DPS.
Type 3	Lorsqu'il n'existe ni référentiel réglementaire applicable, ni référentiel technique applicable, l'approche de type 2 peut ne pas être retenue, soit par choix, soit parce que les critères qui s'y rattachent ne peuvent être satisfaits et qu'il n'existe donc pas de système de référence (cas des innovations et des nouvelles conceptions par exemple). Une analyse détaillée des risques doit alors être réalisée. Celle-ci pourra conduire à la définition d'objectifs de sécurité déclinés sur les fonctions du système et/ou à la mise en œuvre de référentiels reconnus d'autres domaines, et en vigueur à la date de l'avis favorable de l'OQA portant sur le DPS.

Pour les approches de types 2 et 3, plusieurs méthodologies d'analyse sont envisageables (quantitative, qualitative…). La nature de l'analyse dépend directement des spécificités et de l'ampleur du projet (à l'échelle d'un système, d'un sous-système, d'une fonction, d'un composant…). Aussi, il est impossible de définir une règle absolue en la matière.

En tout état de cause, pour les opérations faisant l'objet d'une décision de mise en service, les modalités de démonstration de la sécurité font l'objet d'une évaluation par un OQA, prévue par le décret STRA, à l'occasion de l'évaluation des dossiers de sécurité (DCST, DPS et DS).

Spécificité de l'analyse du parcours

Quelle que soit l'approche retenue, l'analyse du parcours sur lequel est déployé le STRA est nécessaire et est une composante obligatoire de la démonstration de la sécurité du système. En effet, chaque parcours est unique et les risques associés à un aménagement urbain dépendent de différents paramètres souvent liés au contexte local (trafic, vitesses, types d'usagers routiers). Il est donc toujours nécessaire de réaliser l'analyse de sécurité de chaque parcours où un système technique est déployé, afin de démontrer la compatibilité de ce parcours avec le domaine de conception technique du système technique et la capacité du système technique à fonctionner en sécurité sur le parcours pour les situations qu'il y rencontrera.

A titre d'illustration, cette démonstration pourra nécessiter par exemple la réalisation d'aménagements sur le parcours, l'adaptation des conditions de circulation en certains points du parcours, voire des modifications du système technique.

Dans tous les cas, il est nécessaire de prendre en compte le retour d'expérience associé à un risque clairement identifié sur une configuration de circulation donnée.

3. Exigences propres à l'approche par écarts (Type 2)

3.1. Présentation générale

Un système nouveau peut être (exception faite des innovations ou des nouvelles conceptions) constitué de plusieurs sous-ensembles « standards », éventuellement modifiés et/ou adaptés, déjà mis en place sur d'autres systèmes en exploitation.

Ce constat conduit légitimement les concepteurs de systèmes techniques et les organisateurs de service à souhaiter la mise en œuvre d'une approche de la sécurité dite « par écart », permettant de ne pas réitérer des démonstrations de sécurité lorsque celles-ci ont déjà pu être apportées.

Ce type d'approche peut parfaitement être envisagé mais uniquement dans les conditions suivantes :

- le système de référence doit respecter les conditions présentées au paragraphe 3.2 ;
- le système de référence doit être parfaitement appréhendé (configuration, identification, …), de même que ses limites (domaine de conception technique du système notamment) et conditions d'utilisation (conditions d'exploitation requises, exigences exportées, …), de manière à permettre le recensement des écarts éventuels avec le nouveau système, tant au plan technique qu'au plan des conditions d'utilisation et de maintenance ;
- la justification de l'identification exhaustive des écarts entre le nouveau système et le système de référence doit pouvoir être apportée ;
- pour chaque écart identifié, la démonstration doit être faite que les mesures mises en œuvre garantissent la non régression du niveau de sécurité du nouveau système par rapport au système pris en référence.

Nonobstant les éléments précédents, la mise en œuvre d'une démonstration par écart ne dispense pas de la fourniture des éléments descriptifs du système considéré ni des justificatifs relatifs à la sécurité du système de référence et, le cas échéant, du système considéré.

Ainsi, la documentation concernant la démonstration et la description du système considéré telle que demandée dans les dossiers de sécurité (DCST, DPS, DS) ne saurait être limitée qu'aux seuls écarts avec le système de référence.

3.2. Choix de la référence

Si la démarche de comparaison avec un système existant est retenue, le choix de la référence est essentiel dans la mesure où celle-ci fixe le niveau de sécurité à atteindre.

Ce peut être par exemple le cas lorsqu'il n'existe aucun référentiel technique applicable ou à l'occasion de la reconduction à l'identique (ou presque) d'un système déjà en exploitation.

Le décret STRA fixe pour exigence que tout nouveau système (ou modification d'un système existant) offre un niveau de sécurité globalement au moins équivalent au niveau de sécurité des systèmes assurant des services comparables. L'obligation faite par le décret porte donc sur la comparaison des niveaux de sécurité et non (nécessairement) sur la comparaison des systèmes entre eux.

3.2.1. Possibilité de références multiples

Le décret STRA définit comme référence générale le niveau de sécurité des systèmes existants assurant des services comparables.

Il n'impose donc pas l'unicité du système de référence, qui peut être retenu selon les différents sous-systèmes du système de transport. Dans le cas où il y a plusieurs systèmes de référence, la compatibilité entre les sous-systèmes et la gestion des interfaces exigent une attention particulière.

Pour autant, lorsque la démonstration de la sécurité d'un nouveau système ou d'un système existant modifié est faite par comparaison avec des systèmes existants, il apparaît souhaitable de limiter autant que faire se peut le nombre de systèmes de référence.

3.2.2. Règles de choix du système de référence

S'il est délicat de définir des règles absolues concernant le choix du système de référence, un certain nombre de principes doivent, néanmoins, être respectés :

- En application des dispositions du décret STRA, le système de référence peut être le système concerné (cas d'une modification du système) ou bien un système existant assurant des services comparables. Dans tous les cas, il doit s'agir d'un système en exploitation depuis au moins deux ans ou ayant été en exploitation pendant au moins deux ans avec un retour d'expérience positif. Le système de référence doit être identifié au stade où les principes de démonstration de la sécurité sont actés (au stade du DPS ou DCST).

- Au stade où le système de référence est identifié, l'évolution des règles de l'art par rapport aux règles de l'art retenues pour la conception du système de référence, doit également être prise en compte. Les écarts vis-à-vis de ces règles de l'art (normes, guides techniques, recommandations, …) doivent être identifiés, et leur acceptabilité justifiée.

- Le système de référence doit être un système existant en France ou, à défaut, dans un pays de l'Union Européenne (ou dans un État appliquant des règles techniques et de sécurité équivalentes à celles de l'Union Européenne).

    - <u>A - Lorsque le système de référence est en France :</u>

    Le système a fait l'objet de l'évaluation prévue par la section 3 du décret STRA et est réputé constituer une référence acceptable au plan de la sécurité, sous condition de ne pas avoir mis en évidence une insuffisance en matière de sécurité à travers son REX.

    En effet, la démonstration de l'équivalence du niveau de sécurité d'un système nouveau à un système non satisfaisant au plan de la sécurité ne saurait permettre la mise en exploitation du nouveau système.

    Ainsi, la conformité d'un nouveau système à un système déjà en exploitation ne constitue pas nécessairement une condition suffisante pour l'obtention de l'autorisation de mise en exploitation.

- B - Lorsque le système de référence est situé dans un autre pays de l'Union européenne (ou dans un état appliquant des règles techniques et de sécurité équivalentes à celles de l'Union européenne) :

  Deux cas de figure sont envisageables :

Cas 1 :	Le système de référence proposé satisfait aux conditions suivantes : • il a fait l'objet d'une évaluation (au sens de la mission d'évaluation prévue par la section 3 du décret STRA) ; • cette évaluation a été menée par un organisme : ◦ indépendant (au sens de la section 3 décret STRA) ; ◦ agréé par le STRMTG en qualité d'Organisme qualifié (OQA) ; • le référentiel d'évaluation est reconnu par le STRMTG Dans ce cas, le système proposé constitue une référence acceptable à défaut de mise en évidence d'une insuffisance en matière de sécurité, à travers le REX sur le système.
Cas 2 :	Le système proposé ne satisfait pas à l'une (au moins) des conditions précédentes. Dans ce cas, l'acceptabilité du système comme référence pour la démonstration de la sécurité est appréciée au cas par cas par l'OQA.

- Le système de référence doit être d'un type identique à celui du système évalué. La démonstration de la sécurité d'un système type STRA sera donc à faire par comparaison avec un système référence de type STRA. Des adaptations sont envisageables pour des fonctions communes avec un système de transport différent. L'acceptabilité de la référence devra dans ce cas être examinée par l'OQA.

- Le système de référence doit être comparable au système évalué, tant au plan fonctionnel que dans ses conditions d'exploitation.

- Le système de référence doit être pertinent en terme d'objectif de sécurité.

- Pour les parcours ou les zones sur lesquels un système technique est déployé, la notion de système comparable n'a pas réellement de sens. Comme expliqué au §2.3 chaque parcours est unique et il est donc toujours nécessaire de réaliser l'analyse du parcours où un système technique est déployé, afin de démontrer la compatibilité de ce parcours avec le domaine de conception technique de ce système technique.

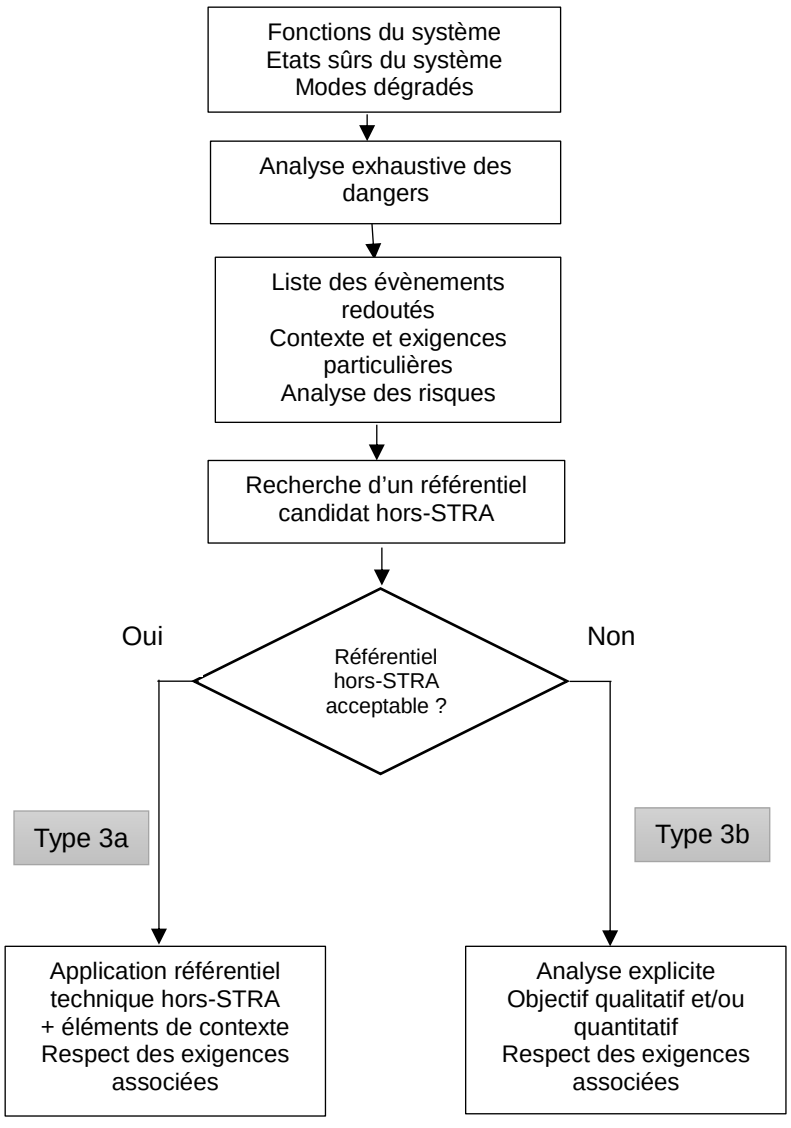
- En tout état de cause, le choix de la référence fait l'objet d'une évaluation par l'organisme qualifié en charge de l'évaluation. Cette évaluation sera formalisée dans l'avis de l'organisme qualifié agréé transmis au STRMTG, tel que prévu par le décret STRA.

4. Exigences propres à l'analyse détaillée des risques (Type 3)

4.1. Présentation générale

Dans le cas d'un système intégrant des équipements ou des fonctions innovants, l'approche par écarts peut être impossible s'il n'existe ni référentiel réglementaire ou technique applicable au système complet, ni système de référence acceptable. Il est alors nécessaire d'analyser de manière précise et globale les risques induits par ces nouvelles fonctions ou ces nouveaux équipements, dans le contexte du système (en application du 2nd paragraphe de l'Art. R. 3152-2. – I. du Code des Transports).
D'autre part, même s'il existe un système de référence acceptable, cette même approche, dénommée analyse détaillée des risques (type 3), peut être choisie à la place de l'approche par écarts (type 2).

De manière à alléger ce travail d'analyse, il est intéressant de pouvoir utiliser dans cette analyse détaillée des référentiels techniques existants pour des systèmes autres que les STRA (« hors-STRA »). A titre d'illustration, un concepteur pourrait juger intéressant d'analyser la pertinence pour les STRA d'un référentiel reconnu de protection contre les incendies, issu du domaine ferroviaire.



Dans l'objectif de permettre l'utilisation de ces référentiels hors-STRA, l'analyse doit être faite à l'échelle des dangers, afin de pouvoir analyser pour chaque danger identifié s'il existe un référentiel hors-STRA, reconnu et apte à traiter ce danger, dans le contexte du système global.

La démarche d'analyse détaillée est construite en plusieurs étapes successives :

- Détermination des fonctions du système, des états sûrs du système, des modes dégradés possibles et des manœuvres permettant d'atteindre les états sûrs.

- Analyse exhaustive des dangers associés aux fonctions et équipements dans le contexte du système global. Le périmètre de cette analyse est large et vise à analyser l'ensemble des dangers que le système peut générer (à titre d'illustration, les familles de dangers analysés à ce stade peuvent conduire à des incendies, des collisions, des sorties de route, des coincements, etc.). Cette analyse pourra s'appuyer sur
    - une démarche déductive type analyse préliminaire des dangers faite au niveau du système analysant les différentes causes pouvant conduire au même danger;
    - des démarches inductives type AMDEC fonctionnelle du système analysant les défaillances possibles de chaque fonction et le danger potentiel associé.

- Pour chaque danger identifié à l'étape précédente,
    - Analyse de ses conséquences potentielles au niveau du système global
    - Définition des mesures de réduction permettant de rendre acceptable, le risque découlant de ce danger, dans le contexte du système global, en tenant compte notamment
        - du comportement attendu du système dans cette situation dangereuse ;
        - des éventuels facteurs aggravants liés par exemple à l'absence de conducteur et de personnel et au caractère collectif du système de transport.

    - Si un système hors du domaine STRA existe proposant un référentiel technique reconnu susceptible de justifier ces mesures de réduction de risque
        - Vérification rigoureuse de l'acceptabilité de ce référentiel hors-STRA (voir §4.2).

    - Si ce référentiel hors-STRA est jugé acceptable (type 3a) :
        - Formalisation des éventuelles contraintes exportées (limitations, exclusions, conditions, hypothèses, …) liées à l'application de ce référentiel hors-STRA ;
        - Vérification du respect des différentes exigences issues du référentiel hors-STRA complété des éventuels éléments de contexte.

    - Si aucun référentiel technique hors-STRA n'existe, ou n'est jugé acceptable au sens du §4.2 (type 3b),
        - Réalisation d'une analyse explicite afin de déterminer les mesures qualitatives et quantitatives applicable pour ce danger (voir §4.3) ;
        - Vérification de la mise en œuvre des mesures issues de cette analyse explicite.

La documentation concernant la démonstration et la description du système considéré telle que demandée dans les dossiers de sécurité (DCST, DPS, DS) devra expliciter pour chaque

danger l'analyse conduite et ses conclusions, ainsi que la prise en compte des éventuelles contraintes exportées.

4.2. Acceptabilité d'un référentiel hors du domaine STRA

S'il est délicat de définir des règles absolues concernant les critères d'acceptabilité d'un référentiel hors-STRA, un certain nombre de principes peuvent, néanmoins, être posés :

- Le référentiel hors-STRA envisagé doit être reconnu pour le domaine qu'il couvre en terme d'objectif de sécurité.
- Le champ d'application du référentiel hors-STRA doit être compatible avec le domaine des systèmes STRA pour le danger analysé. Ceci doit être démontré en analysant les points communs entre les domaines pour ce danger particulier, et en montrant qu'il n'existe pas à contrario de point rendant le référentiel hors-STRA incompatible.
- Le référentiel hors-STRA doit couvrir précisément le danger issu de l'analyse des dangers propres au système STRA, à travers toutes les exigences issues de l'analyse des dangers dans le contexte STRA, et notamment sa gravité potentielle, les éventuels facteurs aggravants, exigences liées au comportement attendu du système, etc.
- Chaque référentiel représente un ensemble cohérent d'exigences et il est important d'appliquer autant que possible chaque référentiel hors-STRA dans son intégralité.
  Cependant il est possible qu'en raison du périmètre trop vaste couvert par le référentiel hors-STRA, seule une partie du référentiel hors-STRA soit applicable et adaptée pour le danger considéré dans l'analyse.
  Dans ce cas, il est nécessaire de déterminer et de prendre en compte tous les éléments de contexte et les hypothèses qui sont attachées à la partie applicable du référentiel hors-STRA.
- Chaque référentiel repose sur des hypothèses, des contraintes ou des conditions d'application. Ces différentes contraintes doivent être formalisées et prises en compte pour chaque référentiel hors-STRA appliqué. La compatibilité de chacune de ces contraintes exportées entre elles d'une part et avec les spécificités du système STRA d'autre part doit être vérifiée.
- Comme expliqué précédemment, le choix du référentiel hors-STRA se fait pour chaque danger, ce qui amène à avoir une démonstration bâtie par la juxtaposition de plusieurs référentiels hors-STRA différents. Par conséquent :
  - La compatibilité entre les différents référentiels hors-STRA nécessite une attention particulière;
  - De manière à faciliter cette analyse, il apparaît souhaitable de limiter autant que faire se peut le nombre de référentiels hors-STRA.

La démonstration de l'acceptabilité des référentiels hors-STRA devra faire l'objet d'un soin particulier. Il s'agira notamment d'expliciter de manière rigoureuse l'argumentaire ayant permis de conclure à l'acceptabilité de chaque référentiel, les analyses conduites pour démontrer la compatibilité entre les différents référentiels, et la méthode suivie afin de prendre en compte des contraintes exportées.

Cette démonstration devra être évaluée par l'OQA. Cette évaluation sera formalisée dans l'avis de l'organisme qualifié agréé transmis au STRMTG, tel que prévu par le décret « STRA ».

4.3. Principes de l'analyse explicite

L'analyse explicite s'appuie sur une analyse de la situation dangereuse afin de déterminer un objectif de sécurité adapté à la situation et au système, puis de décliner cet objectif à la fois :

- sur le champ de la sécurité de fonctionnement ;
- et sur le champ « sécurité de la fonction attendue », afin de traiter les problématiques d'insuffisances fonctionnelles ou de mésusages raisonnablement prévisibles (en l'absence de toute défaillance) ;

au moyen de canevas de démonstration issus de normes reconnues dans le domaine de la sécurité (ex. EN 50126, IEC 61508, ISO 26262, ISO PAS21448 « SOTIF », ISO/TR 4804, etc.).

La démarche se décompose en plusieurs étapes successives :

- Détermination d'un objectif global de sécurité basé sur l'accidentologie et le REX de systèmes (ou de combinaisons de systèmes) « cibles » de transports différents déjà en service, et tenant compte des spécificités des systèmes STRA
    - Objectif qualitatif et ou quantitatif du type « nombre d'évènements par km » ou « nombre d'évènements par heure », qui pourra être également décliné pour chaque niveau de gravité et pour chaque scénario,
    - Prise en compte d'une marge de sécurité liée au caractère innovant des systèmes STRA et de la sensibilité sociétale à tout évènement lié à ces systèmes (conduite automatisée, transport collectif).

- Allocation successives de l'objectif de sécurité aux différents niveaux sur le principe des normes reconnues dans le domaine de la sécurité
    - au niveau des macro-fonctions sur la base de l'analyse exhaustive des dangers élaborée à l'étape initiale, au niveau des fonctions du système sur la base de l'architecture fonctionnelle du système,
    - au niveau des sous-systèmes et composants sur la base de l'architecture matérielle des fonctions.

5. Méthodologie

La démonstration du « GAME » doit être apportée événement redouté par événement redouté.

Le cas échéant, en particulier lorsque la sécurité ne sera pas assurée au niveau d'un ou plusieurs événements redoutés, des « arbitrages » à l'échelle d'un ensemble d'évènements redoutés pourront être mis en œuvre dans les limites évoquées au paragraphe 2.1, et en tenant compte d'acceptabilité sociétale de certains types d'évènements.

La méthodologie repose sur le schéma général à 2 niveaux suivant :

Globalement	1. Justification d'une approche globale de la sécurité : • Approche « système » de la sécurité s'appuyant sur la liste générique des évènements redoutés, permettant d'identifier les risques liés au fonctionnement du système dans son ensemble et de définir les exigences de sécurité à respecter au niveau de chaque sous-ensemble et de chaque interface interne (entre sous-ensembles) ou externe (contraintes exportées vers l'environnement), • Justification de la mise en place de dispositions pour répondre à chacune des exigences de sécurité définies pour garantir la sécurité d'ensemble du système, • Mise en place d'un processus de management de la sécurité à l'échelle du système permettant de garantir la traçabilité de ces exigences tout au long du développement du système (y compris au niveau des exigences exportées vers l'exploitation et la maintenance), • Justification de la pertinence du processus de construction et de démonstration de la sécurité à l'échelle du système en regard des référentiels et règles de l'art en vigueur, évalué par l'OQA.
Au Moins Équivalent	2. Justification des dispositions de couverture des risques (= caractère « au moins équivalent » à) : • Justification de la « suffisance » de chacune des dispositions mises en œuvre pour répondre aux exigences de sécurité définies au niveau de chaque sous-ensemble et chaque interface par démonstration de leur conformité : o Préférentiellement à un référentiel technique reconnu et pertinent (réglementation technique, normes, guides techniques du STRMTG, recommandations, …). C'est l'approche de type 1, ou s'il n'existe pas de référentiel technique reconnu et pertinent, o soit à des dispositions techniques ou opérationnelles déjà mises en œuvre sur des systèmes similaires existants et justifiées du point de vue de la sécurité. Cette approche peut se révéler intéressante pour justifier globalement de la sécurité d'un sous-ensemble donné exploité à l'identique (ou quasiment) sur un système similaire Les conditions encadrant cette approche dite « par écart » ou de type 2 sont précisées au chapitre 3, o soit aux niveaux et exigences de sécurité déterminés par une analyse détaillée des risques. Cette approche peut s'appliquer au cas d'un équipement ou d'une fonction innovante. Les conditions encadrant cette approche dite « analyse détaillée des risques » ou de type 3 sont précisées au chapitre 4

Ces deux niveaux de démonstration sont indissociables, en ce sens qu'ils sont tous deux nécessaires mais non suffisants pris individuellement pour justifier de la sécurité du système.

La démonstration du « GAME » pour le système considéré sera établie dès lors que :

- La mise en œuvre d'une approche globale de la sécurité conforme aux référentiels et aux règles de l'art en vigueur pourra être justifiée

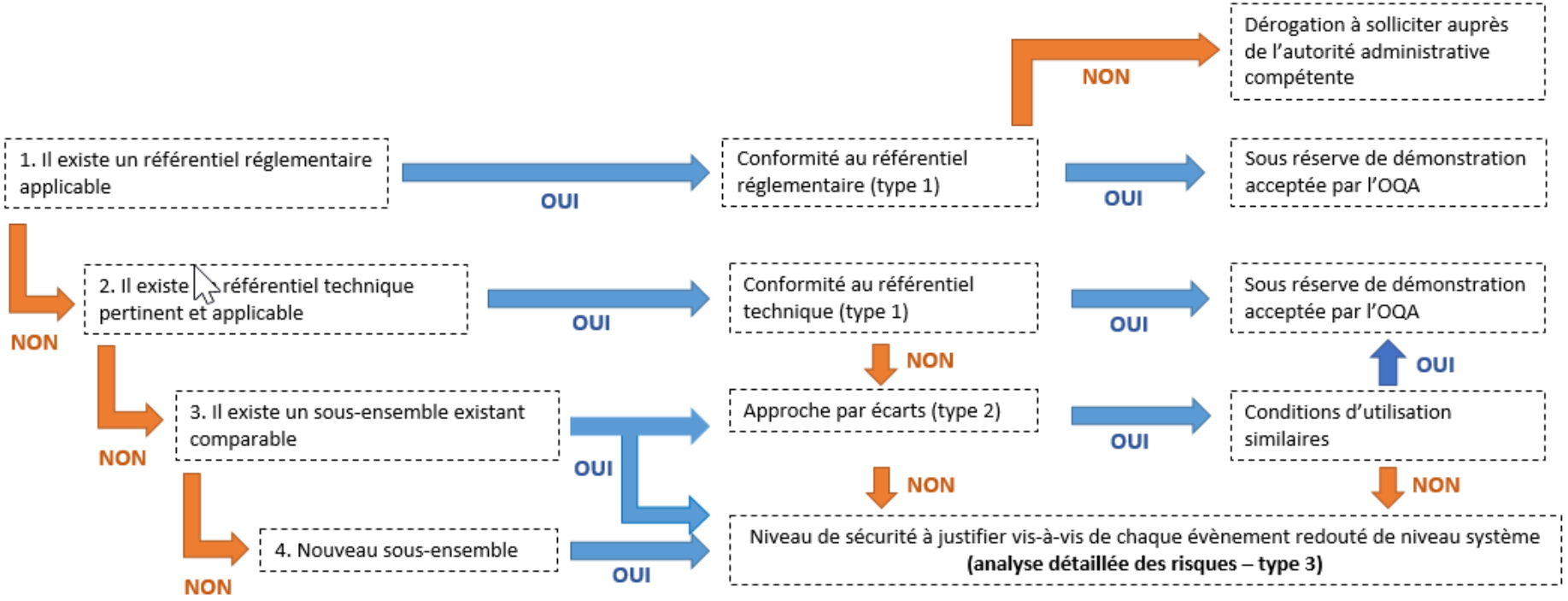
et

- La mise en œuvre de dispositions pertinentes pour couvrir l'ensemble des risques identifiés pourra être justifiée.

À défaut, des dispositions compensatoires devront être prises pour démontrer la sécurité du système à l'égard de chacun des évènements redoutés « génériques ».

En tout état de cause, la démonstration GAME devra être tracée dans des documents présentant les différents éléments justifiant la couverture des risques au niveau système.

Schéma de principe de la démonstration de la sécurité d'un sous-ensemble :



Annexe - Élaboration du guide

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

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

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

M.	Pagliero	Alstom
M.	Guesdon	Alstom
M.	Alliouche	Bureau Veritas
M.	Boniakowski	Bureau Veritas
M.	Clarissou	Bureau Veritas
Mme	Dam	Bureau Veritas
M.	Travers	Cara
M.	Belloche	Cerema
M.	Sautel	Cerema
M.	Russo	Certifer
M.	Testemale	Certifer
M.	Willmann	CETU
M.	Delache	DGITM
M.	Diez	DGITM
Mme	Lanaud	DGITM
M.	Kleinman	DSR
M.	Dupont	Easymile
M.	Chauvin	GART
M.	Lesot	Ile de France Mobilités
M.	Le Cornec	Navya
Mme	Crepat	Navya
M.	Nyina Mvondo	Navya
M.	Renaud	Ramsai
Mme	Berthault	RATP
M.	Boulineau	RATP
M.	Arnoux	Renault
M.	Martinez	Renault
M.	Rousseau	Renault
M.	Sencerin	Renault
M.	Lenti	Stellantis
M.	Brun	STRMTG
M.	Dusserre	STRMTG
Mme	Torrelli	Systra

M.	Tran	Systra
M.	Dadou	SYTRAL
M.	Negrier	SYTRAL
Mme	Brini	System X
M.	Van Frank	System X
M.	Desmoineaux	Transdev
M.	Baranowski	Université Gustave Eiffel
Mme	Cuvelier	Université Gustave Eiffel
M.	Gruyer	Université Gustave Eiffel
M.	Hedhli	Université Gustave Eiffel
M.	Herveleu	UTAC
M.	De Sousa Fernandes	UTAC

A également contribué à la relecture du guide :

M. Brun Ludovic, chargé de mission juridique du STRMTG