

Méthodologie générale de démonstration de la sécurité d'un STRA

Contexte

Les activités Sécurité du projet SAM ont eu pour objectif de contribuer à la **définition du processus de validation de la sécurité des Systèmes de Transport Routiers Automatisés (STRA)**.

Les **aspects méthodologiques fondamentaux** ont été traités et s'inscrivent dans le contexte de la **démonstration de sécurité** relative au **déploiement du Véhicule Automatisé en France**. Ils ont permis d'établir et d'appliquer :

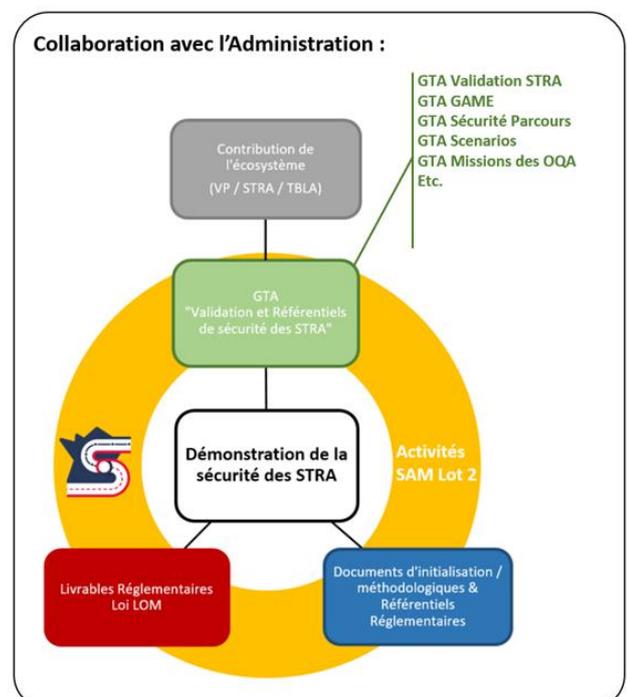
- la **réglementation internationale** relative aux dispositions techniques des véhicules routiers automatisés,
- les textes d'application de la **Loi LOM**, relative aux conditions de **mise en circulation sur la voie publique des véhicules automatisés**, en France.

Introduction

Ces travaux méthodologiques ont notamment pu être étayés de retours d'expérience pratiques issus des expérimentations SAM et de leurs pilotes ; et ont été présentés en tant que positions unifiées de l'ensemble du consortium, **représentatif de l'écosystème STRA français**, car constitué notamment de Concepteurs de Systèmes Techniques, de Constructeurs de véhicules automatisés, d'Organisateurs de Services, et d'Instituts.

D'un point de vue organisationnel, les activités Sécurité du projet SAM se sont structurées **de manière synchronisée et cohérente, avec les Groupes de Travail Administration (GTA)** « Validation et Référentiels de sécurité des STRA ». Ces GTA ont notamment donné lieu à différents référentiels, guides, et documents méthodologiques, au sein desquels les positions unifiées du projet SAM ont été soutenues et considérées.

Guides disponibles sur les sites dédiés à la mobilité automatisé du ministère en charge des transport (DGITM et STRMTG).



Portée de la méthodologie

La **méthodologie générale de démonstration de la sécurité** a été développée pour répondre aux besoins de systèmes de systèmes, multi périmètres techniques, multi parties-prenantes responsables (issus de secteurs différents – cf. : « Fiche de Synthèse Architecture Organique et Fonctionnelle au niveau des STRA »), qu'il s'agit d'encadrer par un processus de maîtrise des risques adapté, et qui répond aux attendus réglementaires.



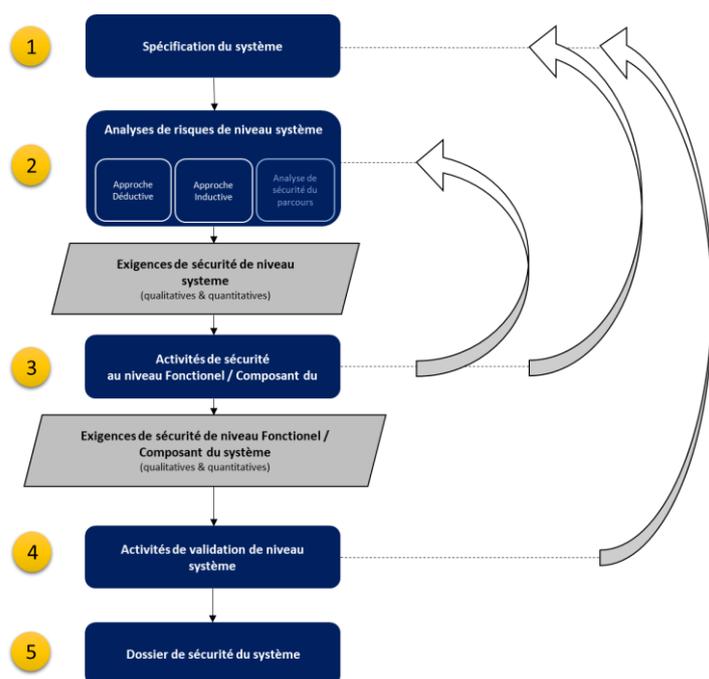
 Méthodologie SAM de démonstration de la sécurité des STRA

L'implémentation de cette méthodologie prend place lors des phases suivantes du cycle de vie d'un STRA :

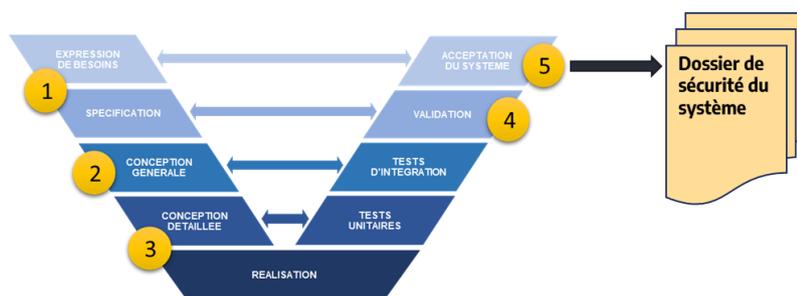
- La phase de **développement** : Activités de développement relatives au SYSTEME TECHNIQUE et de ses sous-systèmes.
- Et la phase **d'installation et de mise en service** : Installation du SYSTEME TECHNIQUE sur un parcours prédéfini aménagé.

Présentation synthétique de la méthodologie

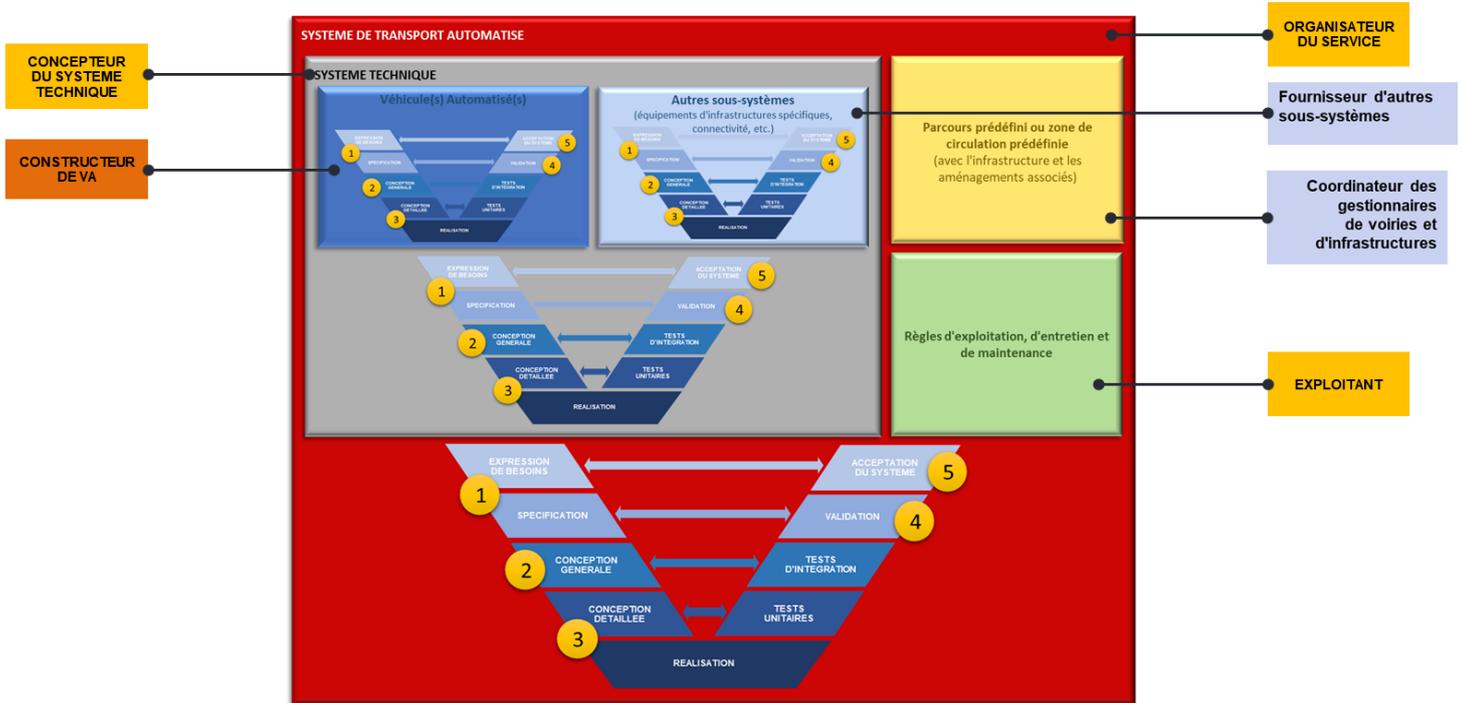
La **méthodologie de démonstration de la sécurité** développée par le projet SAM est un **processus itératif et structuré selon les 5 phases** suivantes :



Phase	1	: Spécification du système
Phase	2	: Analyses de Risques de niveau système
Phase	3	: Activités de sécurité au niveau « fonctionnel / composant » du système
Phase	4	: Activités de Validation
Phase	5	: Livrable final = Dossier de sécurité du système

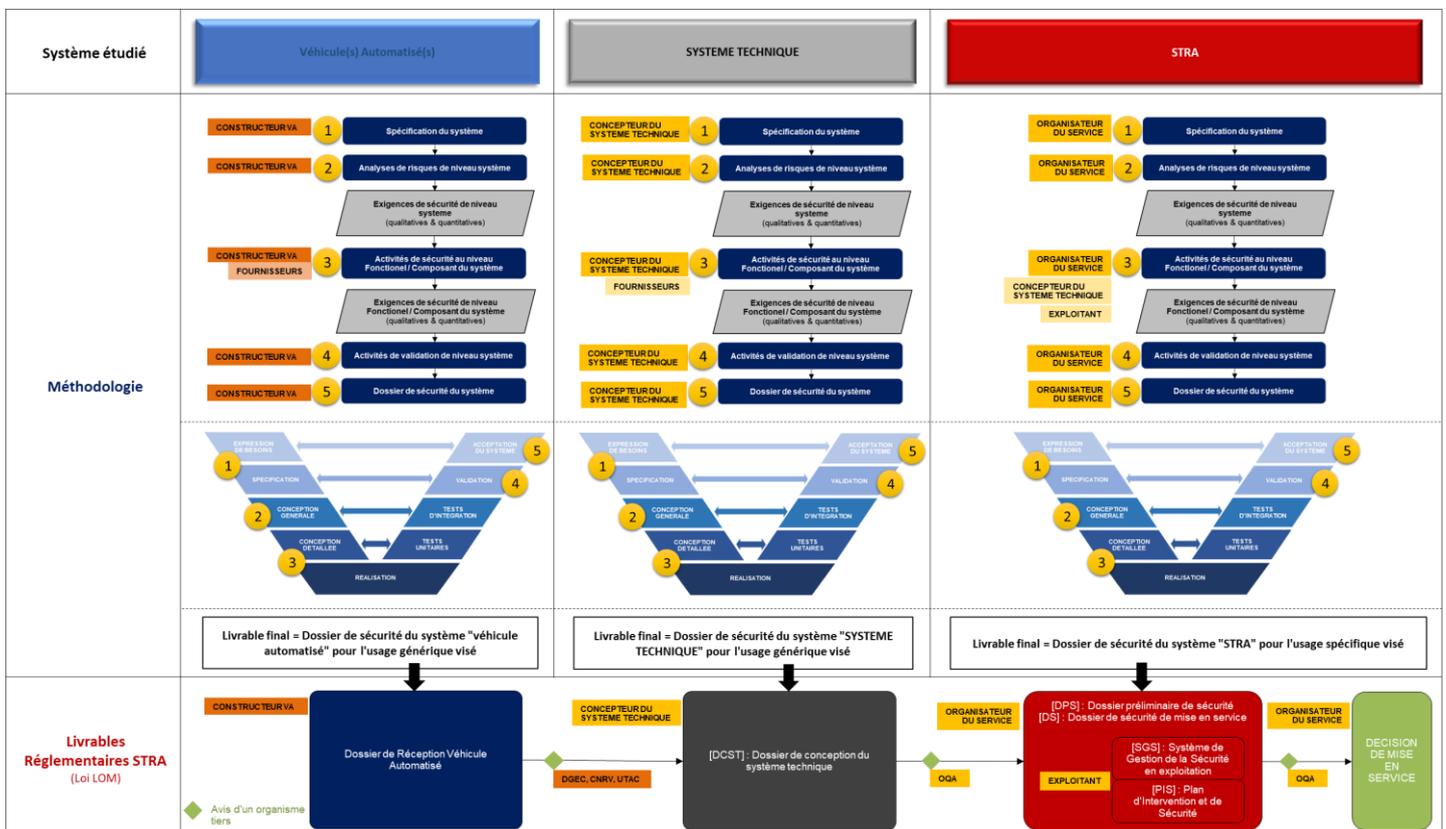


Cette méthodologie générale est pensée pour être **applicable au système STRA et ses sous-systèmes**. Il s'instancie donc au Système technique comprenant le Véhicule Automatisé (VA) et les Equipements externes au VA, ainsi qu'au Parcours prédéfini et aux Règles d'exploitation, mais avec des temporalités différentes, et mené par des parties-prenantes différentes :



Chaque sous-système aboutit à des Dossiers de Sécurité (VA, Système Technique) et alimente le Dossier de sécurité de niveau STRA.

Ces livrables sont réglementaires et issus de la loi LOM :



Thématiques techniques abordées pour chaque phase de la méthodologie

Ci-dessous la liste des thématiques techniques qui ont été travaillées dans le cadre des tâches Sécurité du projet SAM :

Phase 1 : Spécification du système

- Condition d'emploi en sécurité (ODD)
- Décomposition organique d'un système
- Décomposition fonctionnelle d'un système
- Description / caractérisation de parcours
- OEDR : Réponse à la Détection des Objets et des Evènements
- Approche basée sur les scénarios

Phase 2 : Analyses de risques de niveau système

- Liste générique des accidents de niveau STRA
- Critères d'évaluation des risques
- Objectif Globaux de Sécurité (OGS) quantitatifs
- Les types d'analyses de risques
- La définition des exigences de sécurité de niveau système

Phase 3 : Activités de sécurité au niveau fonctionnel / composant du système

- Etape de réduction des risques
- Définition des concepts de sécurité
- Déclinaison des exigences de sécurité quantitatives
- Acceptabilité des risques résiduels

Phase 4 : Activités de Validation

- Stratégie de validation via piliers NATM (New Assessment Test Method) : Catalogue scénarios, simulation et tests virtuels, audit et évaluation, essais sur site, marche à blanc et surveillance de l'exploitation.

Phase 5 : Dossier de sécurité du système

- Dossier de sécurité du système
- Exigences exportées.