

FOCUS SUR LA SURETÉ DE FONCTIONNEMENT

SESSION MENÉE PAR **STÉPHANE GERONIMI**, GROUPE PSA



Part 1 : Traitement de la sûreté de fonctionnement du VA,
Stéphane GERONIMI, Groupe PSA

Part 1.1 : Focus sur le projet SVA, simulation pour la sécurité du véhicule autonome
Jean VAN FRANK, SystemX

Part 1.2 : Focus sur le projet Moove, monitoring outillé pour le véhicule dans son environnement
Annie BRACQUEMOND, Vedecom

Part 2 : Sûreté de fonctionnement et transport public
Jean-Marc PAGLIERO, ALSTOM



TRAITEMENT DE LA SURETÉ DE FONCTIONNEMENT DU VA

STÉPHANE GERONIMI, GROUPE PSA



Traitement de la sûreté de fonctionnement du véhicule autonome

- > Travaux réalisés dans le cadre du « GT Sûreté de fonctionnement – Véhicule Autonome » du Plan NFI Véhicule Autonome et rattaché au CRA de la PFA
- > Pilotes : Bruno COMPIN (RSA) / Nicolas BECKER (Groupe PSA)
- > Participants : Michel LEEMAN (Valeo), Annie BRACQUEMOND (Vedecom), Jean VANFRANK (SystemX), Marc LAVABRE (RSA), Stéphane GERONIMI (Groupe PSA)

« Safety » et Véhicule Autonome

- > Objectifs de sécurité pour le véhicule autonome
 - Pourquoi se fixer des objectifs ?
 - Définition de ces objectifs
 - Utilisation de ces objectifs
 - Synthèse

POURQUOI se FIXER des OBJECTIFS ?

Eléments de contexte – Véhicule Autonome

« SAFETY » du VA

Trois causes possible de violation des objectifs de « safety » du VA

Cyber sécurité

Démarche
spécifique

Défaillances

Dysfonctionnel

Couvert par ISO26262
et pratiques
« standards »
constructeurs

Menaces / agressions

POURQUOI se FIXER des OBJECTIFS ?

Eléments de contexte – Véhicule Autonome

« SAFETY » du VA

Trois causes possible de violation des objectifs de « safety » du VA

Cyber sécurité

Fonctionnel sûr : « SOTIF »

Défaillances

“Reduce risks caused by every hazard, including those **not due to failures.**”

POURQUOI se FIXER des OBJECTIFS ?

« Safety » du VA et « SOTIF »

Limite du domaine fonctionnel



Mésusages spécifiques au
VA

Assurer un véhicule sûr

- Dans toutes les situations
- Malgré un environnement potentiellement perturbateur

Mais pas de cadre de référence applicable !!

Principes de la « safety » du VA

1. Le véhicule autonome doit améliorer la sécurité routière
 - Permet de fixer une référence quantitative « safety »



Principes de la « safety » du VA

1. Le véhicule autonome doit améliorer la sécurité routière
 - ▶ Permet de fixer une référence quantitative « safety »

2. Le véhicule autonome est sûr

- Démarche quantitative
 - Conformité à la référence quantitative « safety »
- Démarche qualitative
 - Application de règles fonctionnelles et techniques communes



« Safety » du VA – « SOTIF » : méthode

Contexte = SOTIF

Principes

Améliorer la sécurité routière : fixe les objectifs
VA est sûr : assure que l'on est conforme

Quelle méthode pour définir des
objectifs et appliquer ces principes ?

« Safety » du VA – « SOTIF » : méthode

Méthode pour fixer les objectifs : GAME
« Globalement Au Moins Equivalent »

Analyse effectuée par le GT :

- Méthode la plus adaptée à la problématique véhicule autonome
- Devient l'état de l'art ; consensus en cours ISO SOTIF

« Safety » du VA – « SOTIF »

Quelle référence ?

«Globalement Au Moins Equivalent » en terme d'accident

➡ **Données accidentologiques dans le « contexte d'utilisation »**

Utilisation des données issues des autoroutes (données ASFA)

- les données sont fiables
- Les autoroutes sont d'un très bon niveau de sécurité

« Safety » du VA – « SOTIF »

Quels objectifs quantitatifs ?

➡ Application d'un facteur d'amélioration à la référence

Pour prendre en compte :

- Situations critiques gérés par le conducteur
- Contexte d'utilisation qui peut être plus large que les seules autoroutes
- Situations critiques qui ne sont pas identifiées aujourd'hui

« Safety » du VA – « SOTIF »

Approche qualitative : exemples de règles communes

«Règles» de conception

- Définir une liste a minima de situations critiques d'un point de vue sécuritaire
- Définir des modes refuges communs si le conducteur ne reprend pas le contrôle malgré la demande du système ou en cas de défaillance
- Définir des règles de reprises en main, de surveillance conducteur, d'alertes, d'activation / désactivation

«Règles» post-commercialisation

- Mettre en place un mécanisme d'analyse et de traitement (mise à jour) des incidents/accidents en clientèle
- Partager au sein de la PFA, les situations critiques (accidents)

« Safety » du VA – « SOTIF »

Objectif quantitatif :

- Critères d'arrêt de la validation
 - Impact sur dimensionnement de la conception

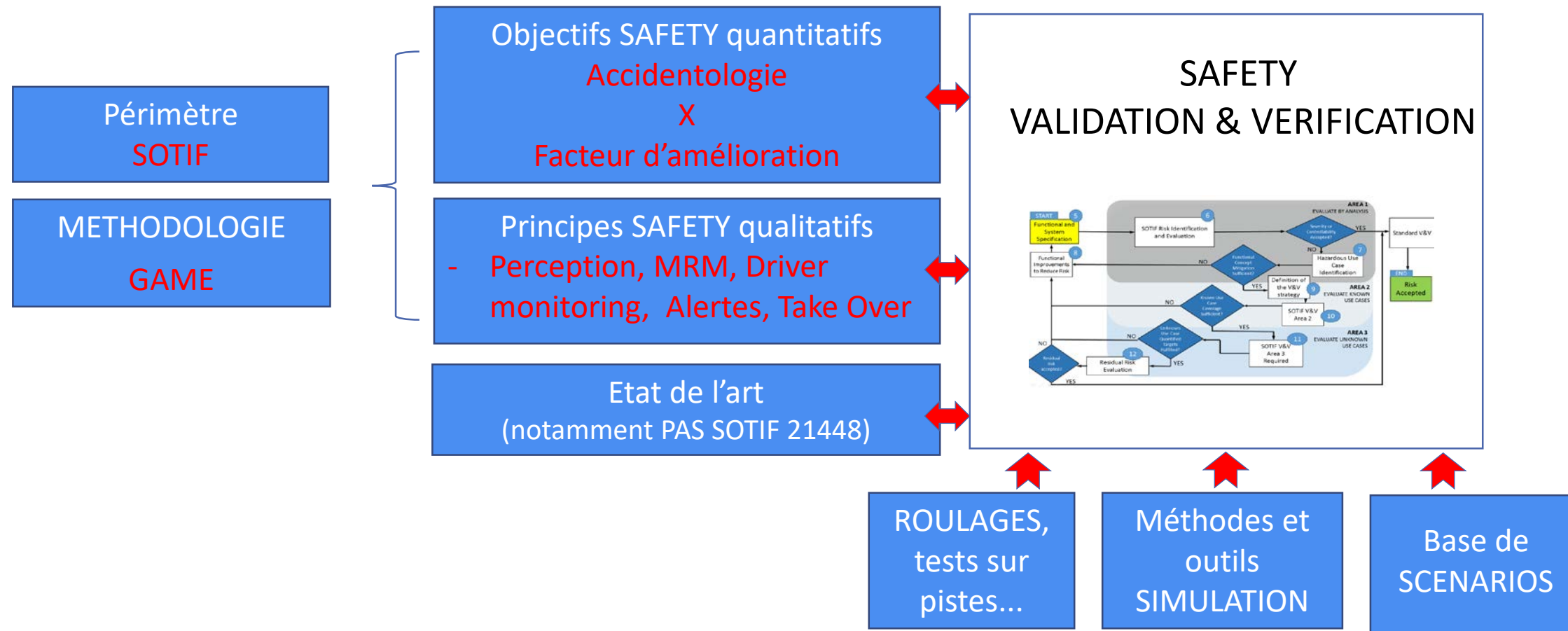
Contribue à montrer que le niveau de risque sur le véhicule autonome est maîtrisé au moment de son lancement

NB : tous les cas clientèles observés devront être analysés et traités afin d'améliorer continûment le niveau de sécurité du véhicule autonome

Objectif qualitatif :

- Les règles communes sont respectées

Approche « safety » du VA



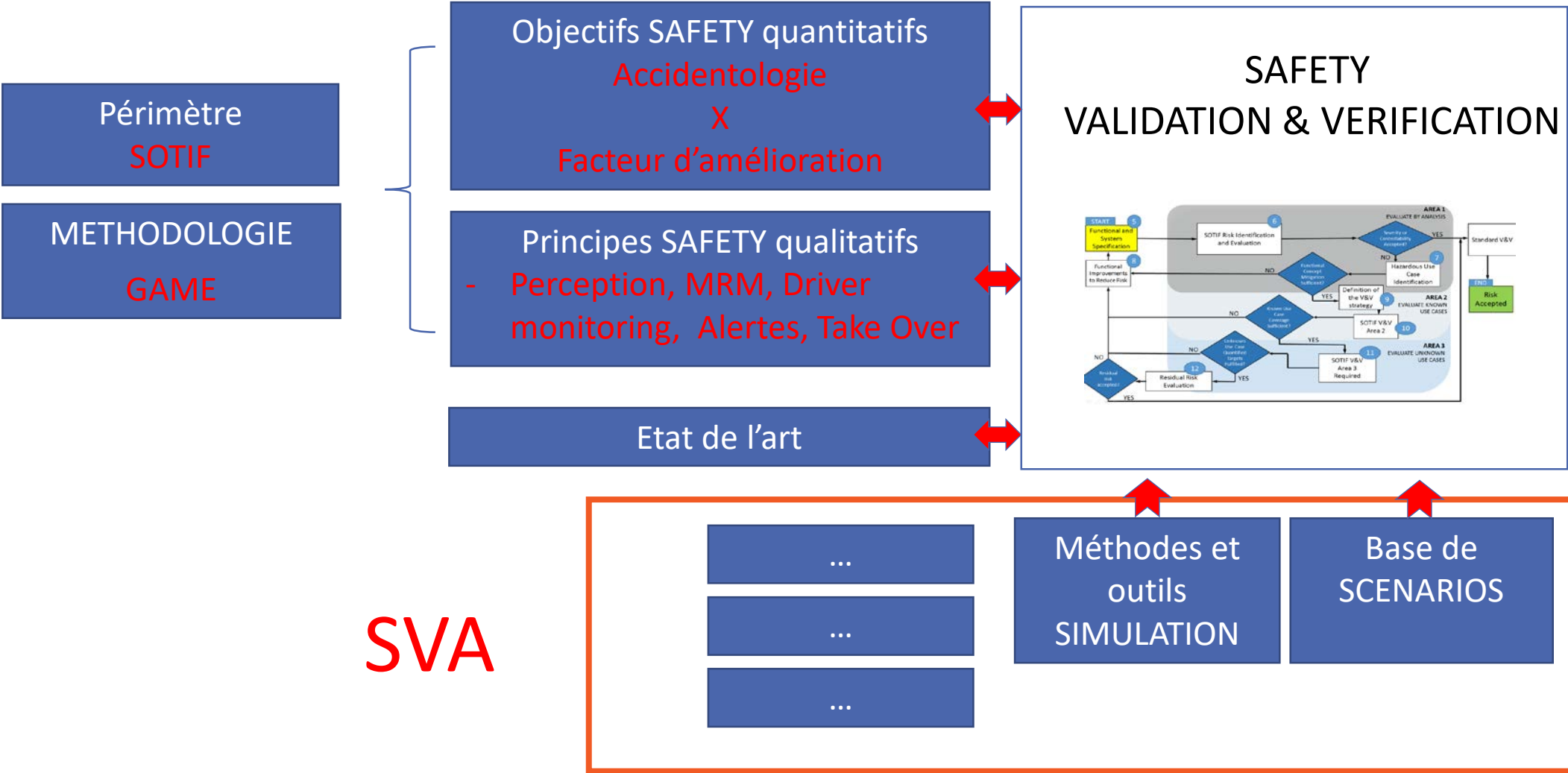
MERCI



FOCUS SUR LE PROJET SVA SIMULATION POUR LA SÉCURITÉ DU VÉHICULE AUTONOME

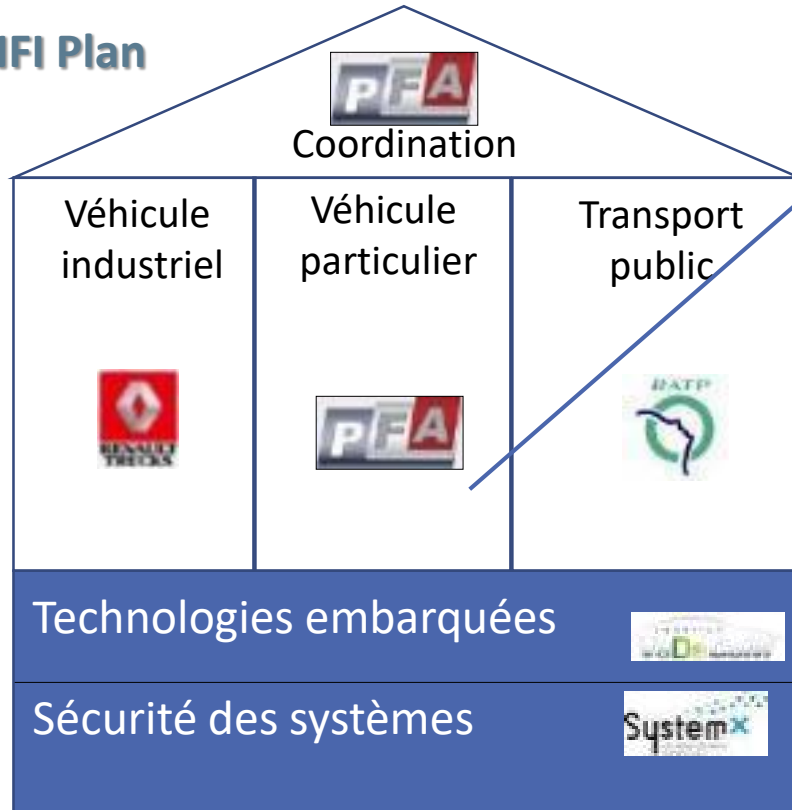
JEAN VAN FRANK, IRT-SYSTEMX

APPROCHE « SAFETY » du VA



Eco système et Partenaires

NFI Plan



SVA

Partenaires industriels (grands groupes et PME)



Partenaires académiques

université
PARIS-SACLAY

LNE
Le progrès, une passion à partager

lsu

cea

Validation d'un véhicule autonome par simulation

Système à tester (AD niveau 3 et 4)



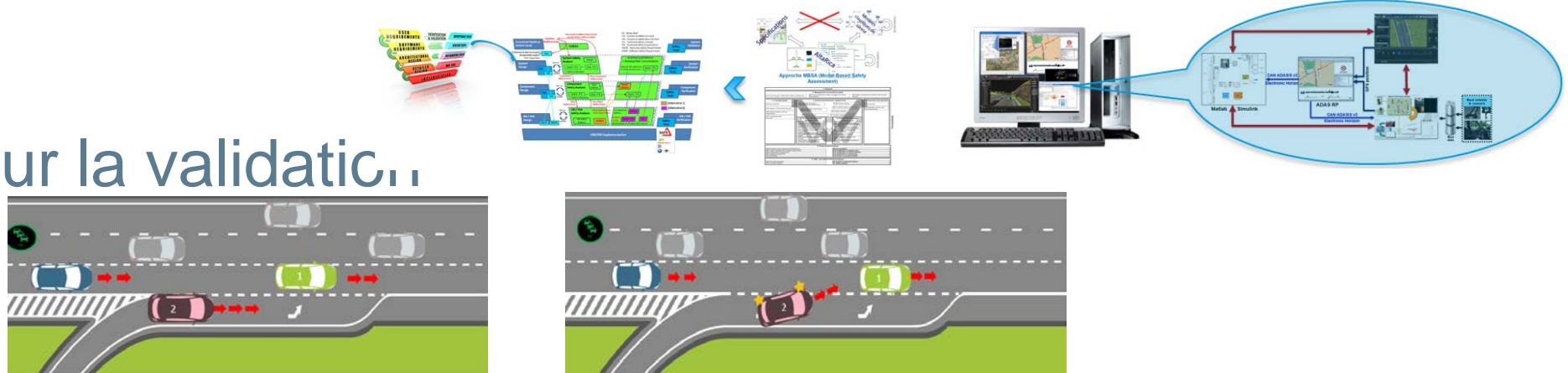
(Modèle Simulink
SVA d'une TJC)

Modèles de capteurs qui équipent le véhicule



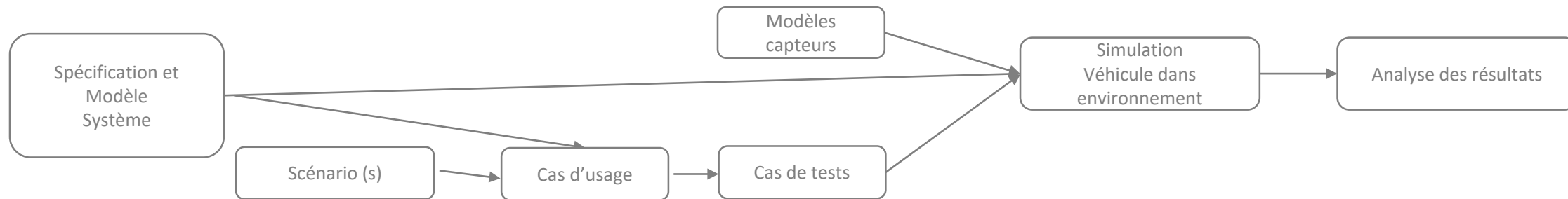
Méthodes et outils de validation

Scénarios pour la validation



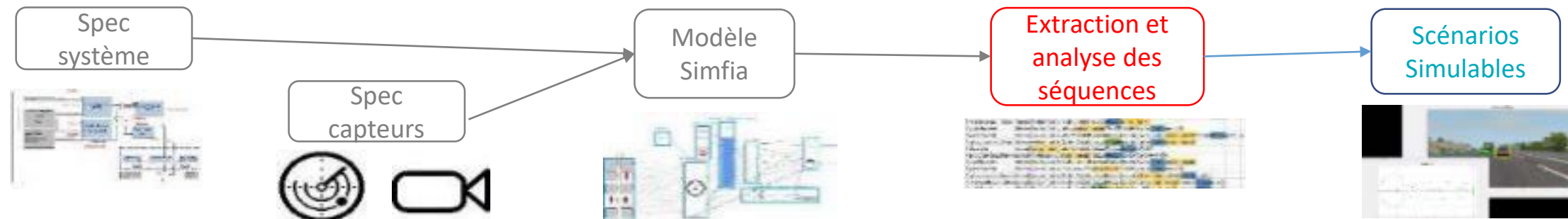
◆ Approche « classique »

- ◆ Dysfonctionnel (ISO 26262) → APR, SG, FSR/TSR, Arbres de défaillances
- ◆ Fonctionnel sûr / SOTIF (ISO/PAS 21448)
- ◆ Simulation fonctionnelle / simulation multi-physique



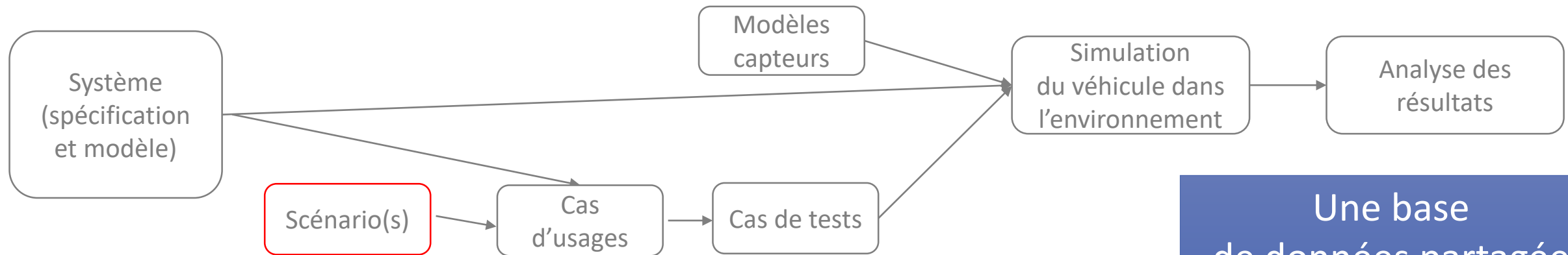
◆ Approche fondée sur la vérification formelle (Model checking)

- ◆ Conception et validation du VA à travers une modélisation comportementale (AltaRica)



Processus de validation

- ◆ **Approche « classique »** (simulation fonctionnelle ou simulation multi-physique)



Une base de données partagée



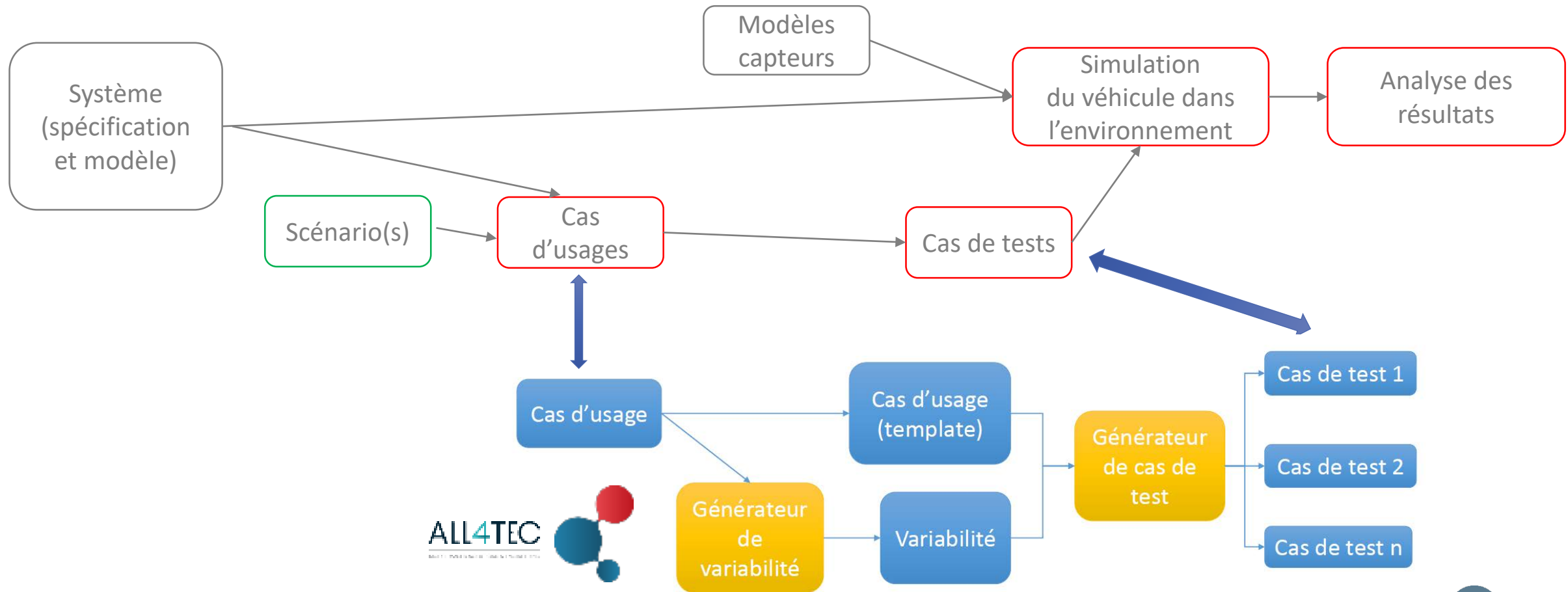
situation initiale



Événement

Processus de validation

- ◆ **Approche « classique »** (simulation fonctionnelle ou simulation multi-physique)



Scénario d'insertion



Résultats de simulation



MERCI



MOOVE :

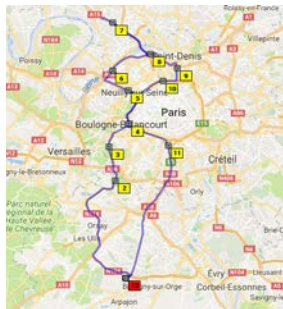
IDENTIFICATION DES SCÉNARIOS DE CONDUITE DU MONDE RÉEL POUR LA SÉCURITÉ FONCTIONNELLE DU VA

ANNIE BRACQUEMOND, VEDECOM

IDENTIFICATION des SCENARIOS de conduite

- **Safety critical scenarios (SCS) du monde réel**
- **SCS occurrence et statistiques**
- **New SCS**

1. Big data : Collecte de données spécifiques

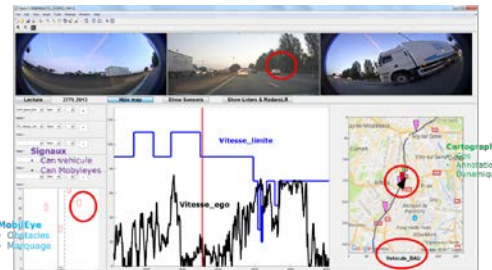


2. Preprocessing :

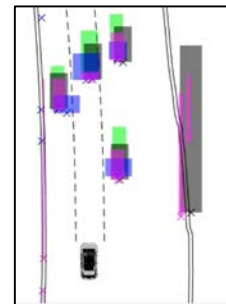
Déchargement, Decodage
& Transformation des
données

Format neutre

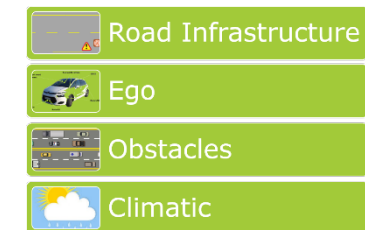
	2010	2009	2008	2007	2006	2005	2004	2003	2002	2001	2000	1999	1998	1997	1996	1995	1994	1993	1992	1991	1990	1989	1988	1987	1986	1985	1984	1983	1982	1981	1980	1979	1978	1977	1976	1975	1974	1973	1972	1971	1970	1969	1968	1967	1966	1965	1964	1963	1962	1961	1960	1959	1958	1957	1956	1955	1954	1953	1952	1951	1950	1949	1948	1947	1946	1945	1944	1943	1942	1941	1940	1939	1938	1937	1936	1935	1934	1933	1932	1931	1930	1929	1928	1927	1926	1925	1924	1923	1922	1921	1920	1919	1918	1917	1916	1915	1914	1913	1912	1911	1910	1909	1908	1907	1906	1905	1904	1903	1902	1901	1900	1899	1898	1897	1896	1895	1894	1893	1892	1891	1890	1889	1888	1887	1886	1885	1884	1883	1882	1881	1880	1879	1878	1877	1876	1875	1874	1873	1872	1871	1870	1869	1868	1867	1866	1865	1864	1863	1862	1861	1860	1859	1858	1857	1856	1855	1854	1853	1852	1851	1850	1849	1848	1847	1846	1845	1844	1843	1842	1841	1840	1839	1838	1837	1836	1835	1834	1833	1832	1831	1830	1829	1828	1827	1826	1825	1824	1823	1822	1821	1820	1819	1818	1817	1816	1815	1814	1813	1812	1811	1810	1809	1808	1807	1806	1805	1804	1803	1802	1801	1800	1799	1798	1797	1796	1795	1794	1793	1792	1791	1790	1789	1788	1787	1786	1785	1784	1783	1782	1781	1780	1779	1778	1777	1776	1775	1774	1773	1772	1771	1770	1769	1768	1767	1766	1765	1764	1763	1762	1761	1760	1759	1758	1757	1756	1755	1754	1753	1752	1751	1750	1749	1748	1747	1746	1745	1744	1743	1742	1741	1740	1739	1738	1737	1736	1735	1734	1733	1732	1731	1730	1729	1728	1727	1726	1725	1724	1723	1722	1721	1720	1719	1718	1717	1716	1715	1714	1713	1712	1711	1710	1709	1708	1707	1706	1705	1704	1703	1702	1701	1700	1699	1698	1697	1696	1695	1694	1693	1692	1691	1690	1689	1688	1687	1686	1685	1684	1683	1682	1681	1680	1679	1678	1677	1676	1675	1674	1673	1672	1671	1670	1669	1668	1667	1666	1665	1664	1663	1662	1661	1660	1659	1658	1657	1656	1655	1654	1653	1652	1651	1650	1649	1648	1647	1646	1645	1644	1643	1642	1641	1640	1639	1638	1637	1636	1635	1634	1633	1632	1631	1630	1629	1628	1627	1626	1625	1624	1623	1622	1621	1620	1619	1618	1617	1616	1615	1614	1613	1612	1611	1610	1609	1608	1607	1606	1605	1604	1603	1602	1601	1600	1599	1598	1597	1596	1595	1594	1593	1592	1591	1590	1589	1588	1587	1586	1585	1584	1583	1582	1581	1580	1579	1578	1577	1576	1575	1574	1573	1572	1571	1570	1569	1568	1567	1566	1565	1564	1563	1562	1561	1560	1559	1558	1
--	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	---



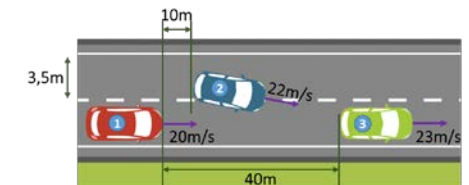
3. Algorithmes de perception pour l'identification des objets mobiles and statiques, et infrastructure



4. PHN - Paramètres de aut Niveau Modèle de l'environnement du Véhicule Autonome



5. Recherche des Scenarios : évènements de safety, variabilité (PHN) et Statistiques



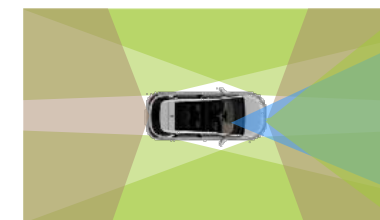
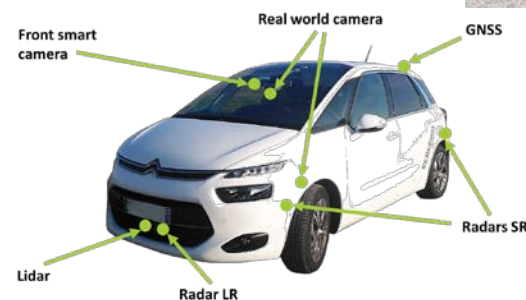
Six véhicules équipés



1.
Big data : Collecte de données spécifiques

Capteurs de perception en 360°

- 2 Lidars Avant et Arrirère
- 1 Long range radar avant
- 4 Short range radar aux coins
- 1 Smart Camera Avant
- 1 GNSS receiver
- IMU
- CAN vehicle



Videos de réalité terrain en 360°

- Avant
- Ariière
- Latérale
- Grand angle avant



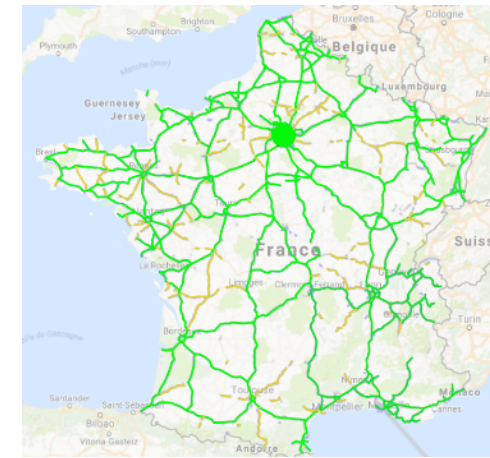
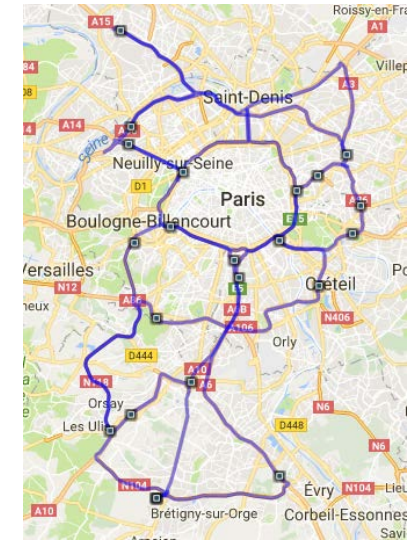
Professional Drivers

- Tête
- Pieds
- Mains
- Ecran d'annotation dynamique par le conducteur



Parcours Enregistrés

- ❑ Traffic JAM sur Voie à chaussée séparées autour de Paris, et autres grandes villes Européennes.
- ❑ Autoroutes de France, UK, Belgique, Allemagne, Italie, etc...
- ❑ Enregistrements de nuit, sous la pluie, la neige...
- ❑ Acquisition de :
 - ❑ 600.000 km
 - ❑ 12000 H



Data Organisation

2.

Preprocessing :

Déchargement, Decodage & Transformation des données

Format neutre

Data processing
and modeling

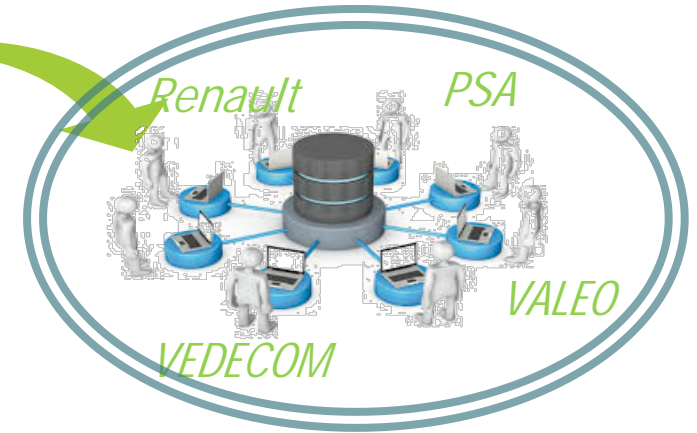
Data logger



SSD stockage

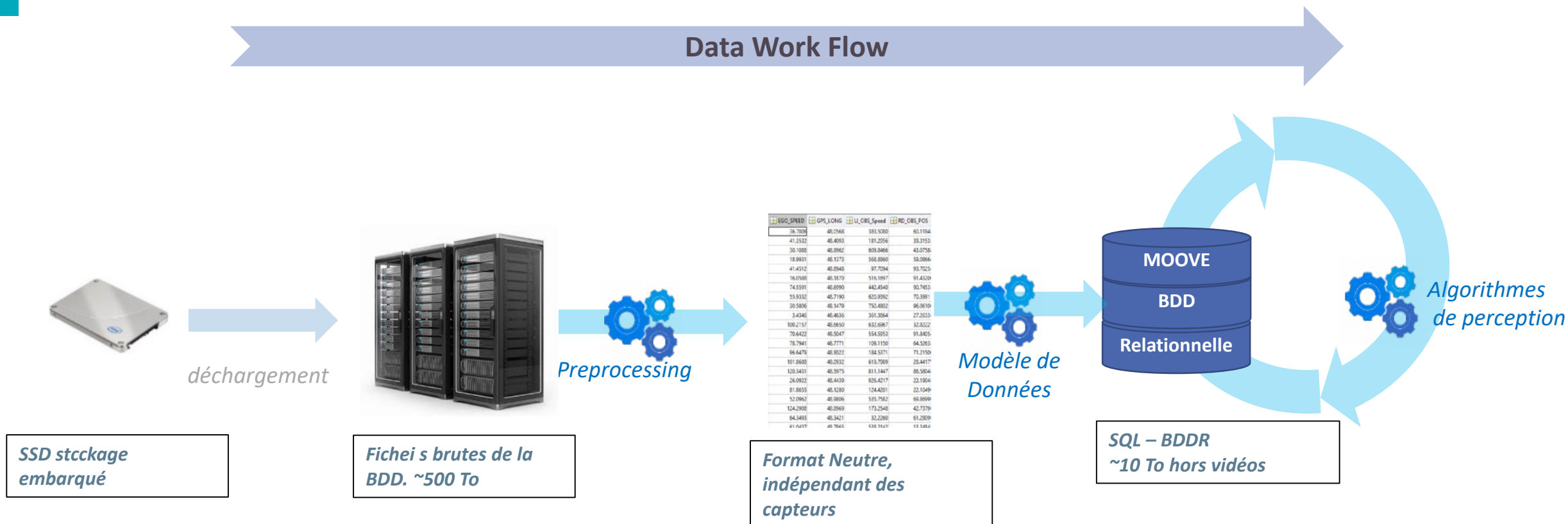


VEDECOM data
center

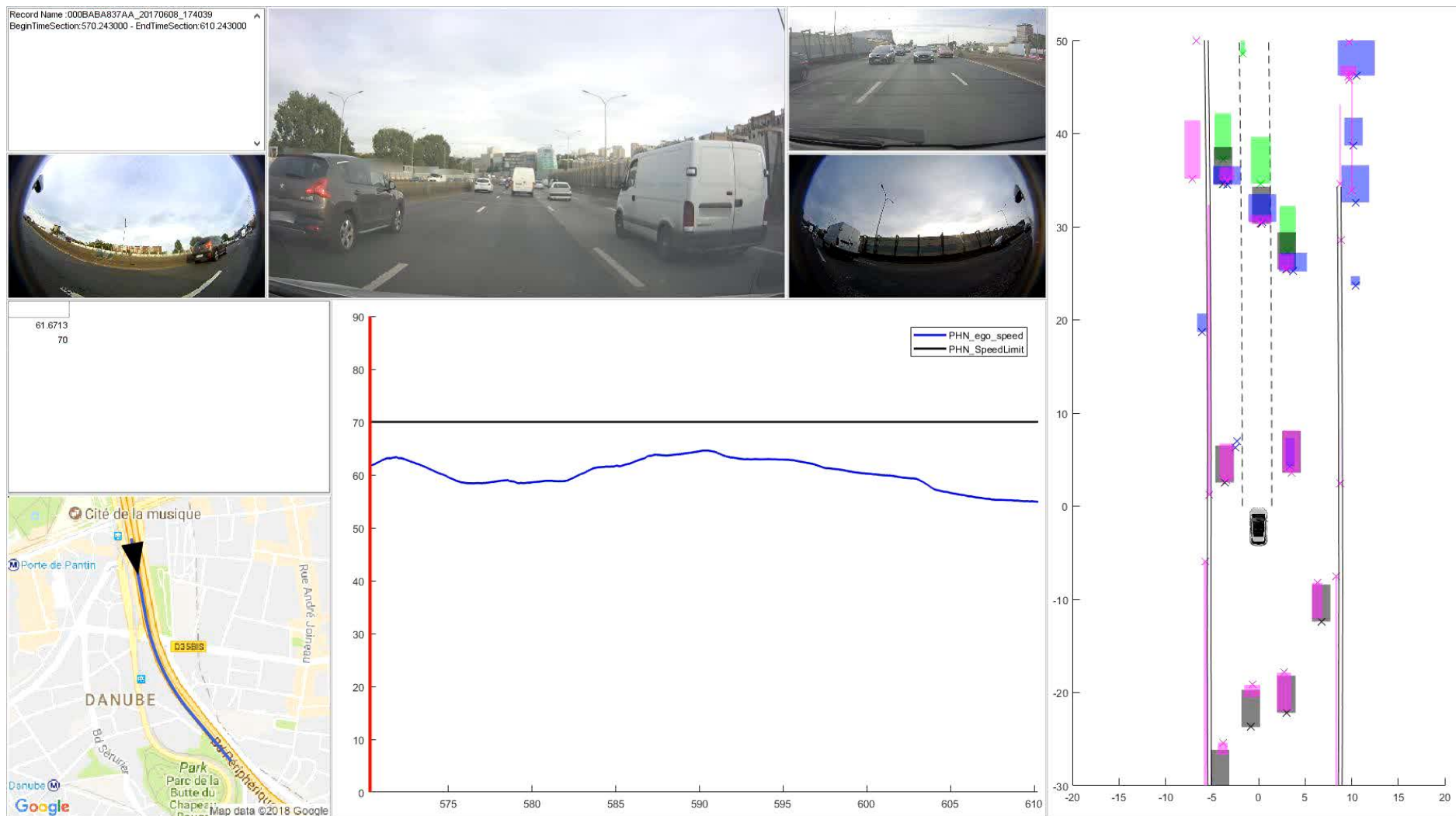


Analyses Collaboratives

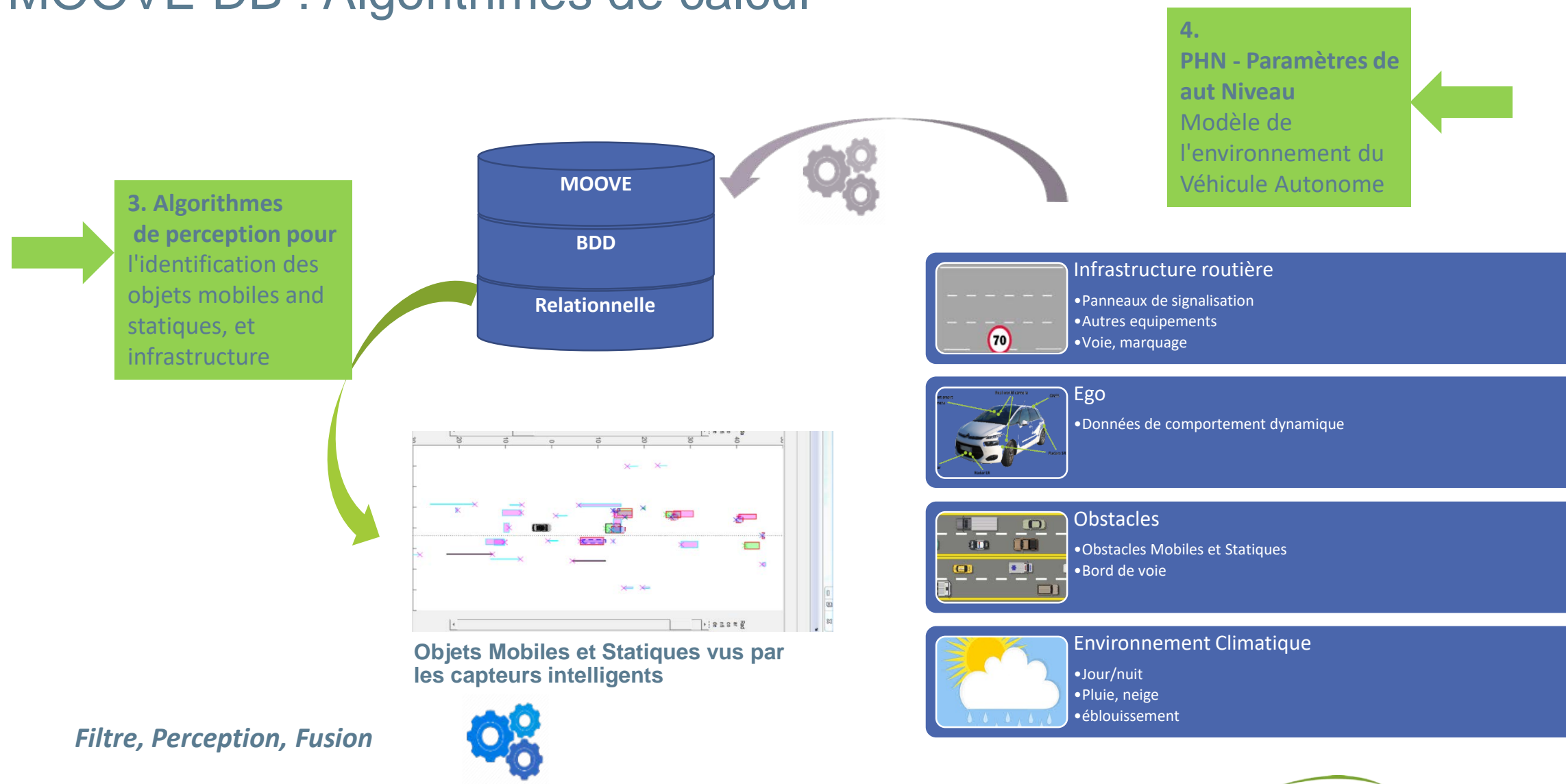
Des Fichiers Brutes A une Base de Données Relationnelle



Visualisation



MOOVE DB : Algorithmes de calcul



Classes des Paramètres de Haut Niveau

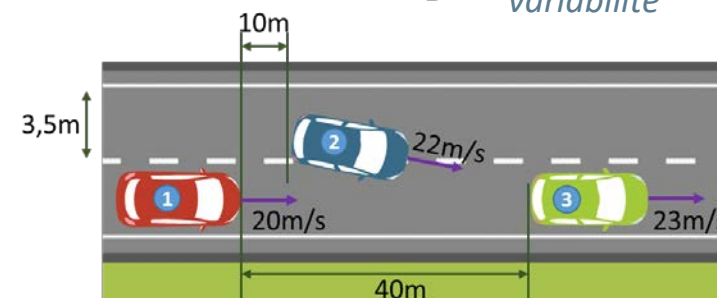
5.
 Recherche des
 Scenarios :
 évènements de
 safety, variabilité
 (PHN) et
 Statistiques

PHN - Parametres de haut Niveau
HLP_OriginalMultiplexor
HLP_UniqueID
HLP_AgeMax
HLP_AbsoluteSpeed
HLP_LaneShift
HLP_LengthCorrection
HLP_MobileObjectClassification
HLP_FixedObjectClassification
HLP_TimeBetweenVehicles
HLP_TimeToCollision
...

Annotation Manuelle



*Analyses de données,
 Scenarios
 identification,
 extraction,
 variabilité*



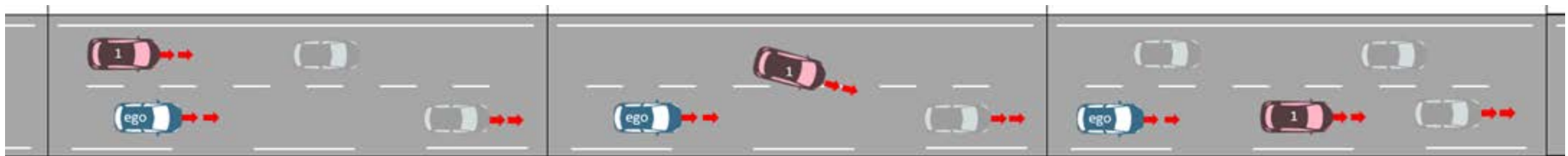
Data Visualisation



Detection Scenarios avec les PHN

5. Recherche des Scenarios : évènements de safety, variabilité (PHN) et Statistiques

- Règles Logiques appliquées aux PHN définissent les évènements
- Sequences temporelles des événements construisent chaque scenario

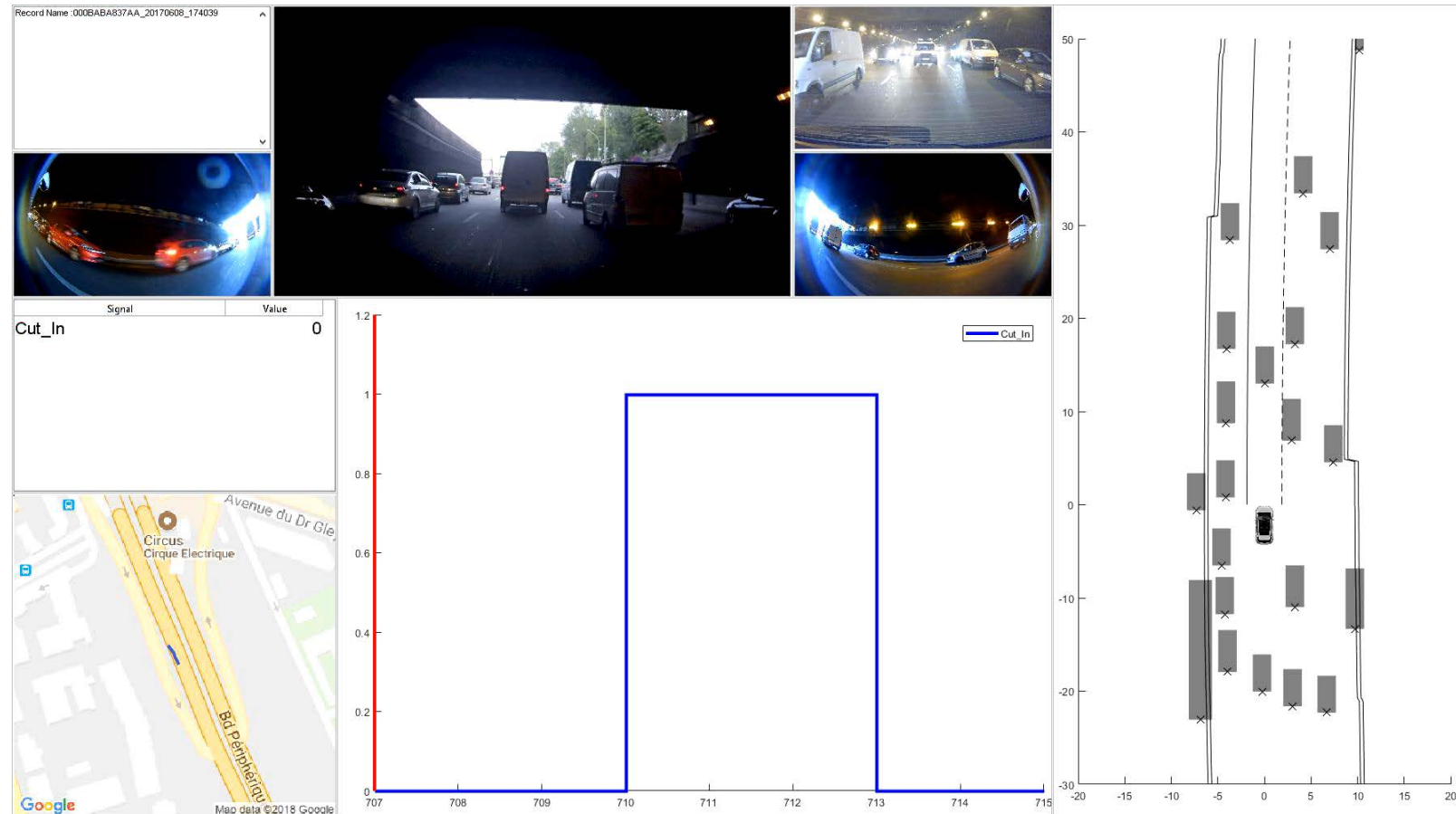


1 est dans la voie adjacente

1 franchit la ligne de marquage

1 est la nouvelle cible
dans la voie de l'ego

Detection Scenarios avec les PHN



MERCI



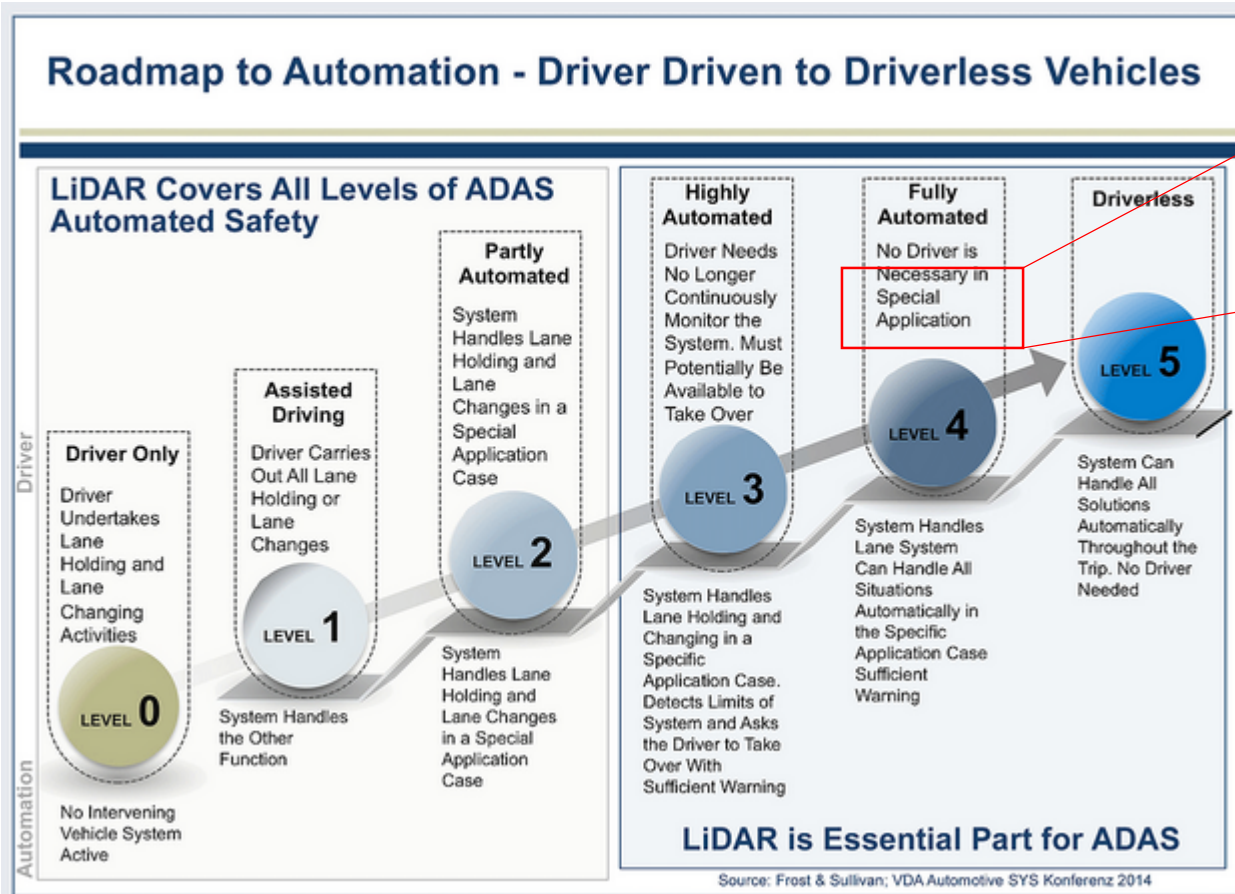
SURETÉ DE FONCTIONNEMENT ET TRANSPORT PUBLIC

JEAN-MARC PAGLIERO, ALSTOM



ALSTOM

Spécificités des transports collectifs : Les 6 niveaux SAE



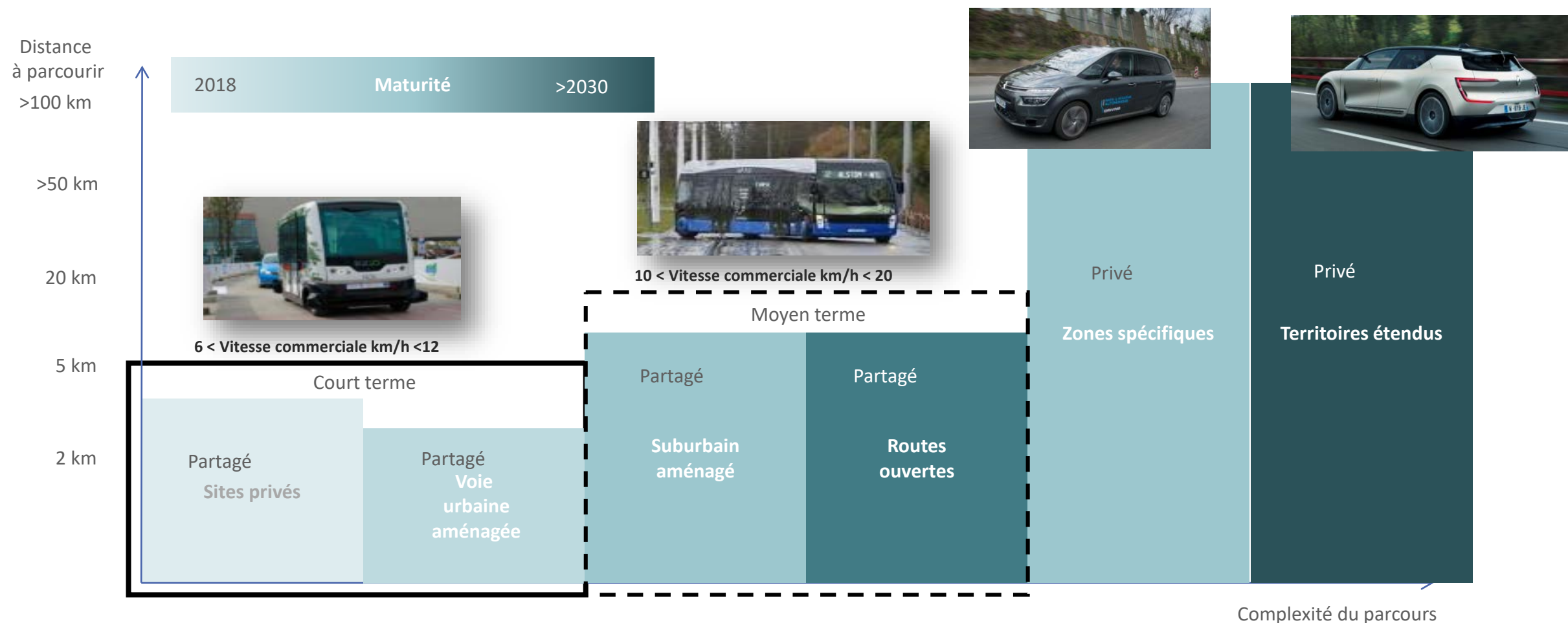
Special Application

Niveau 4 accessible des 2019 en Driverless

- ✓ Parcours limité à des tracés bien délimités
- ✓ Possibilité d'aménager les zones critiques
- ✓ Vitesse maximum limitée
- ✓ Supervision structurée
- ✓ La standardisation n'est pas un préalable

**BUT : démontrer l'apport de ces systèmes aux transports collectifs traditionnels,
Valider l'acceptation du public, et les orientations technologiques**

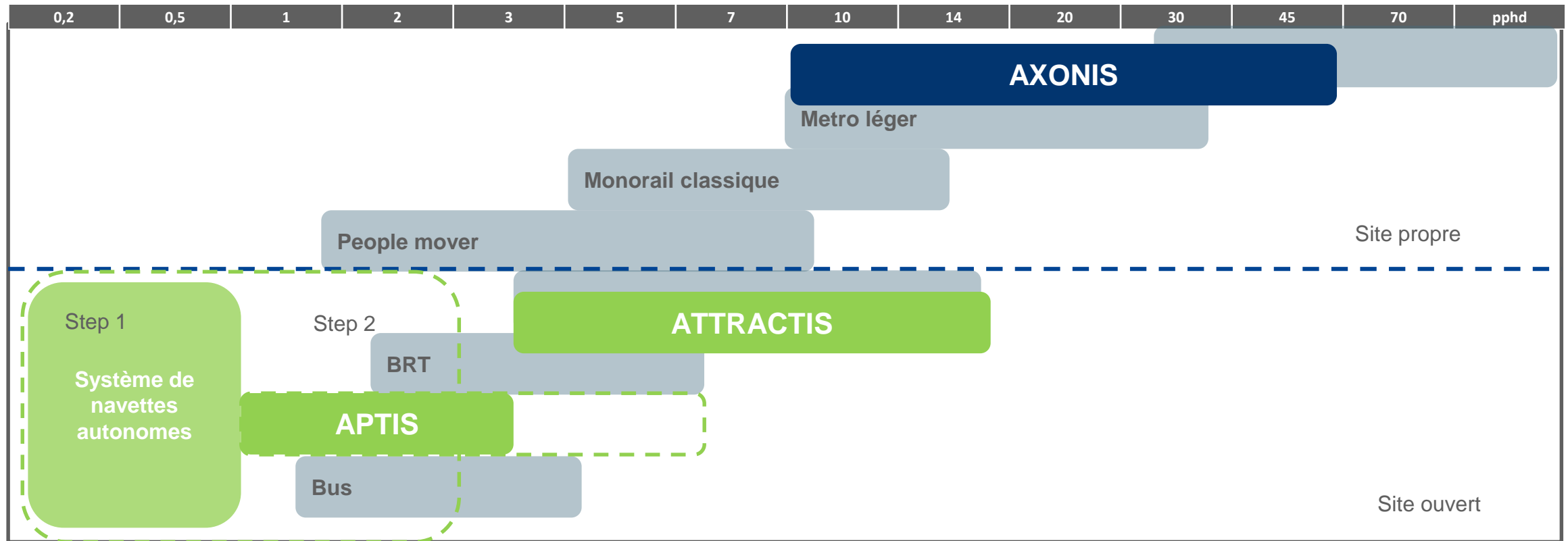
Véhicules autonomes : Maturité fonction de la complexité



Transport partagé sur courte distance en voies prédéfinies

Transport public urbain: Positionnement des solutions de transport autonomes

Segmentation du marché transport public capacité / implantation



Les systèmes de Navettes autonomes répondent à un segment non couvert principalement pour des raisons de couts d'infrastructure et d'exploitation

Transport public urbain: Définition de système



Définition du système
et gestion de projet



Test et Intégration



Maintenance et exploitation

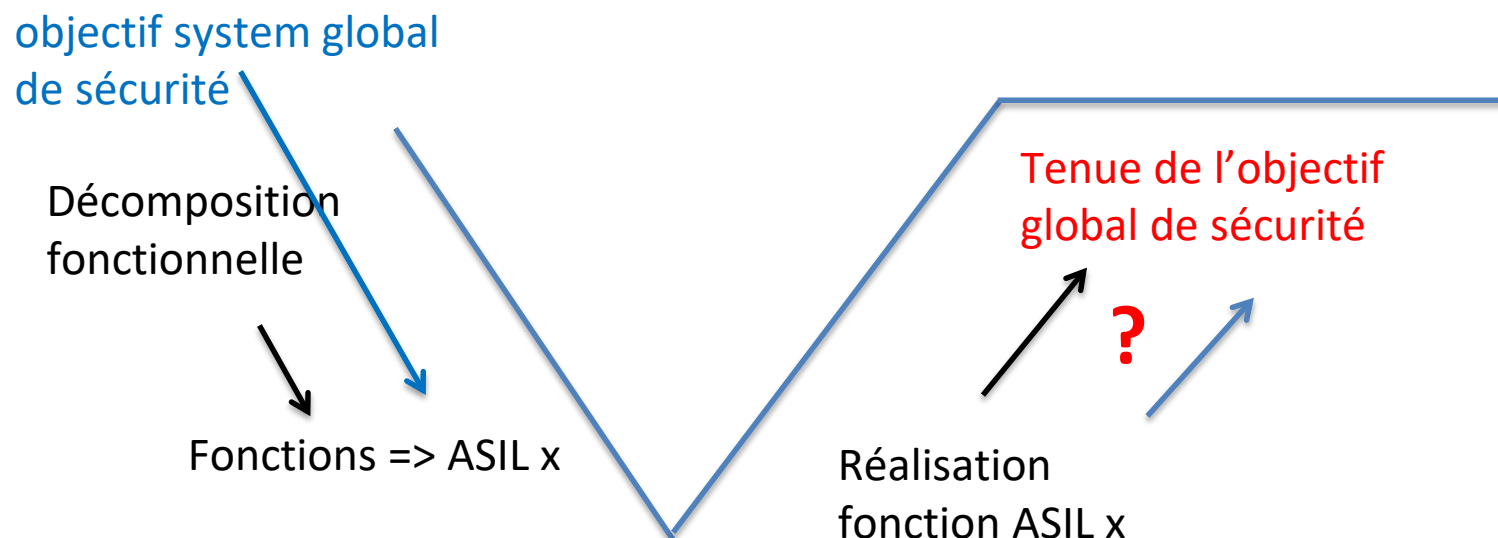
Le système comprend l'ensemble des éléments constituant la solution de transport ainsi que les prestations liées au cycle de vie

Transport Public urbain : Objectif global versus ASIL

Méthode classique automobile : Allocation d'ASIL conformément à l'ISO2626-2

=> Risque de non tenue de l'objectif global

=> Nécessité d'une approche complémentaire top-down d'allocation de l'objectif



Pour la phase d'allocation des ASIL, nécessité d'une approche complémentaire basée sur l'analyse de risques top-down

Dans un environnement moins contraint l'objectif global est plus facilement atteignable avec les technologies actuelles – (moins de SOTIF)

Quelle méthode pour définir cette approche global

STPA – Introduction

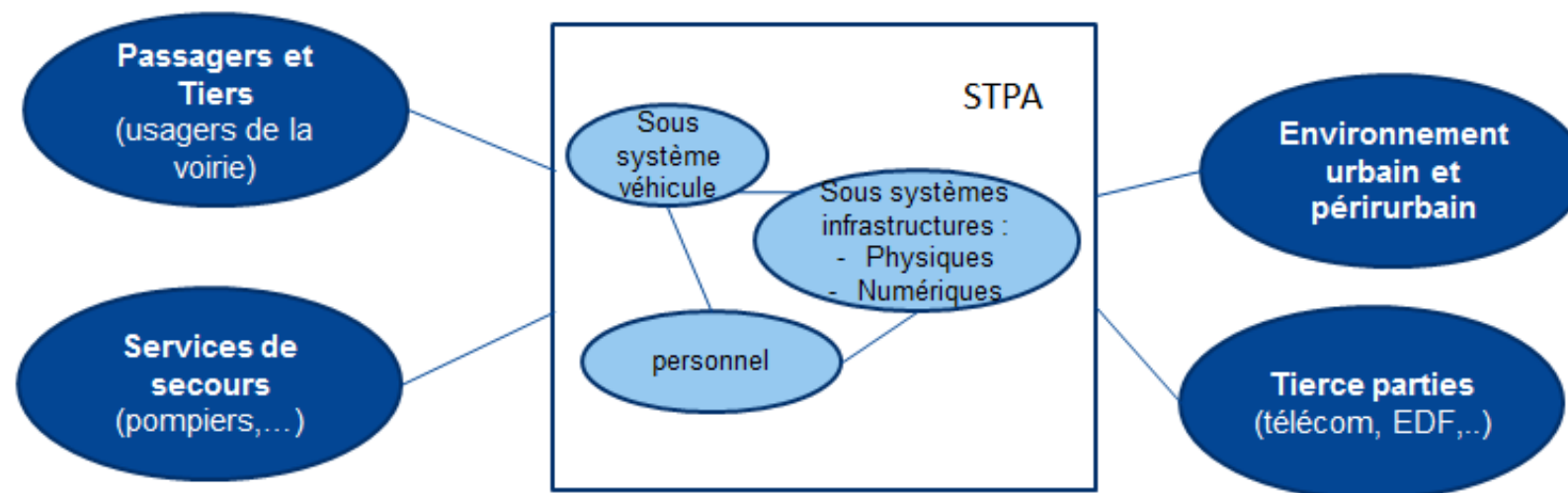
Contexte

- Besoin sécurité comme tout moyen de transport
- Pas de référentiel applicable
- Réflexion menée dans le cadre NFI-STPA au travers des groupes homologation, spécification + création d'un groupe spécifique sécurité.

Points clefs

- Processus d'homologation / Autorisation (GT homologation)
- Référentiel et objectifs de sécurité (GT sécurité)

STPA – Approche Système



Un système STPA est constitué d'une flotte de navette, d'infrastructures physiques et numériques (insertion urbaine, réseau de communication, centre de contrôle, système éventuels d'aide aux passages des carrefours,...) et de personnels dédiés.



STPA – Approche sécurité

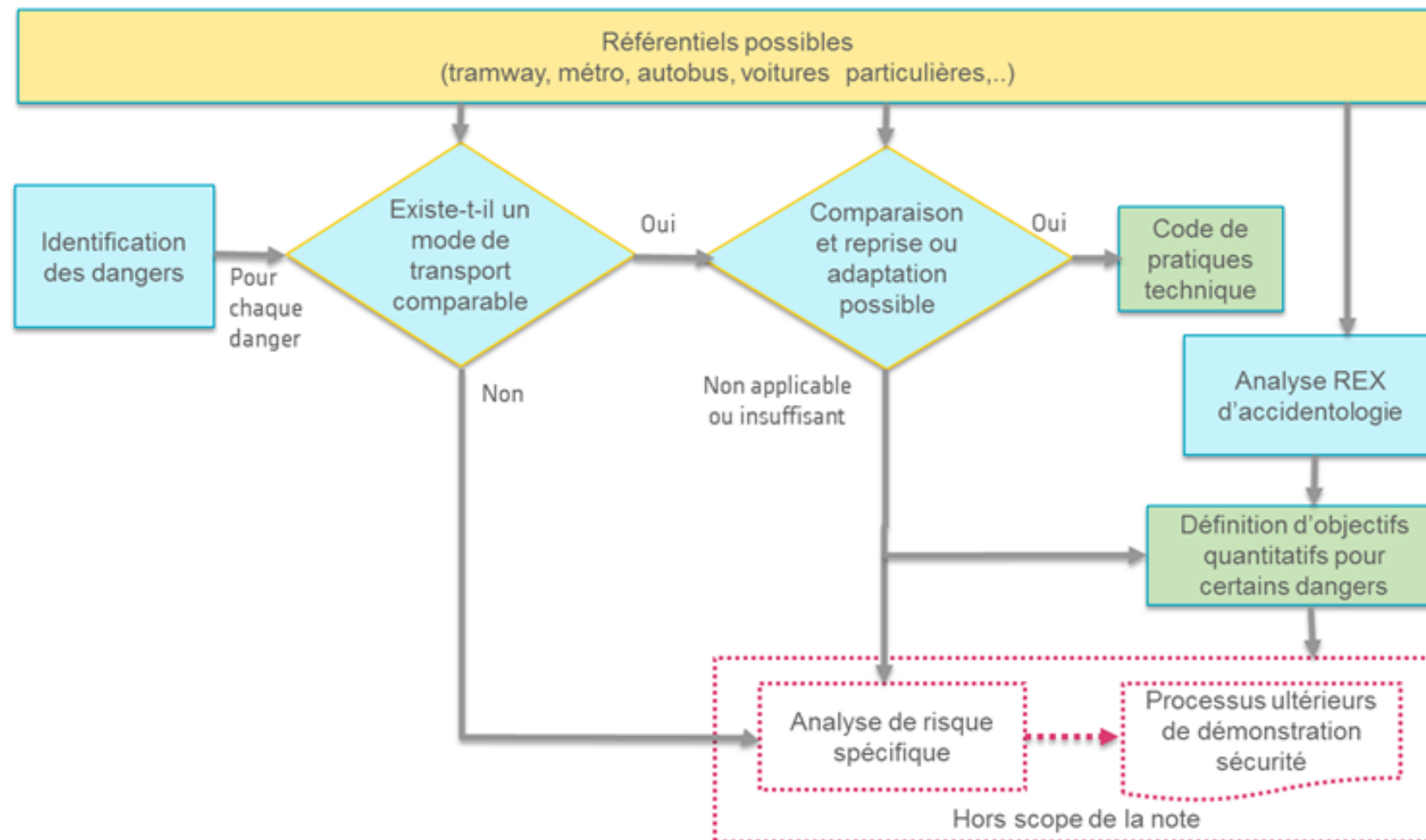
Nécessité de définir un référentiel sécurité permettant de garantir un niveau acceptable et au moins équivalent aux systèmes de transport déjà en place.



Démarche basée sur une adaptation de l'approche GAME / STPG mais non limitée à un mode de transport.



STPA - Méthodologie



Code de
pratiques
technique

STPA – Exemple « Codes de pratiques »

ER	N°ER	Détails sur l'Événement Redouté	Comparaison NA / possible systèmes de référence	Possible référentiel et/ou objectif spécifique	Remarques
Incendie / Explosion	1.1	Incendie dans une navette : asphyxie / suffocation / brulure du fait des matériaux de la navette (toxicité, <u>flammabilité</u>)	<p>Beaucoup moins de personnes que dans un bus et à fortiori que dans un tramway. Durée d'évacuation faible. => Hors zones spécifiques, exigences non supérieures à ce qui se fait pour les bus (Véhicule type M2/M3)</p> <p>L'absence de personnel pour encadrer l'évacuation peut être palliée par une assistance du PCC via les moyens de communication à considérer par comparaison avec les métros automatiques (voir ligne 1.3)</p>	<p>En l'absence de zones à risque spécifiques (tunnel, zone conduisant à des arrêts différés), application du référentiel UN R118 / UN R107</p> <ul style="list-style-type: none"> - R107: Annexe 3, Point 7.5: Prévention des risques d'incendie (obligatoire) - R118: tenue au feu des matériaux en terme de propagation flamme (non obligatoire) <p>Nécessité d'une étude du site, afin de définir les éventuelles zones ou l'évacuation pourrait être retardé du fait d'une temporisation dans l'application de la demande d'évacuation (voir ligne 3.3)</p>	<p>L'évacuation des PMR peut nécessiter une assistance comme pour le cas des métros automatiques (aides des autres passagers)</p> <p>Les dangers associés aux difficultés d'évacuation sont définis en ligne 3.1</p>

Définition d'objectifs
quantitatifs pour
certains dangers

STPA – Objectifs en terme de taux de collision

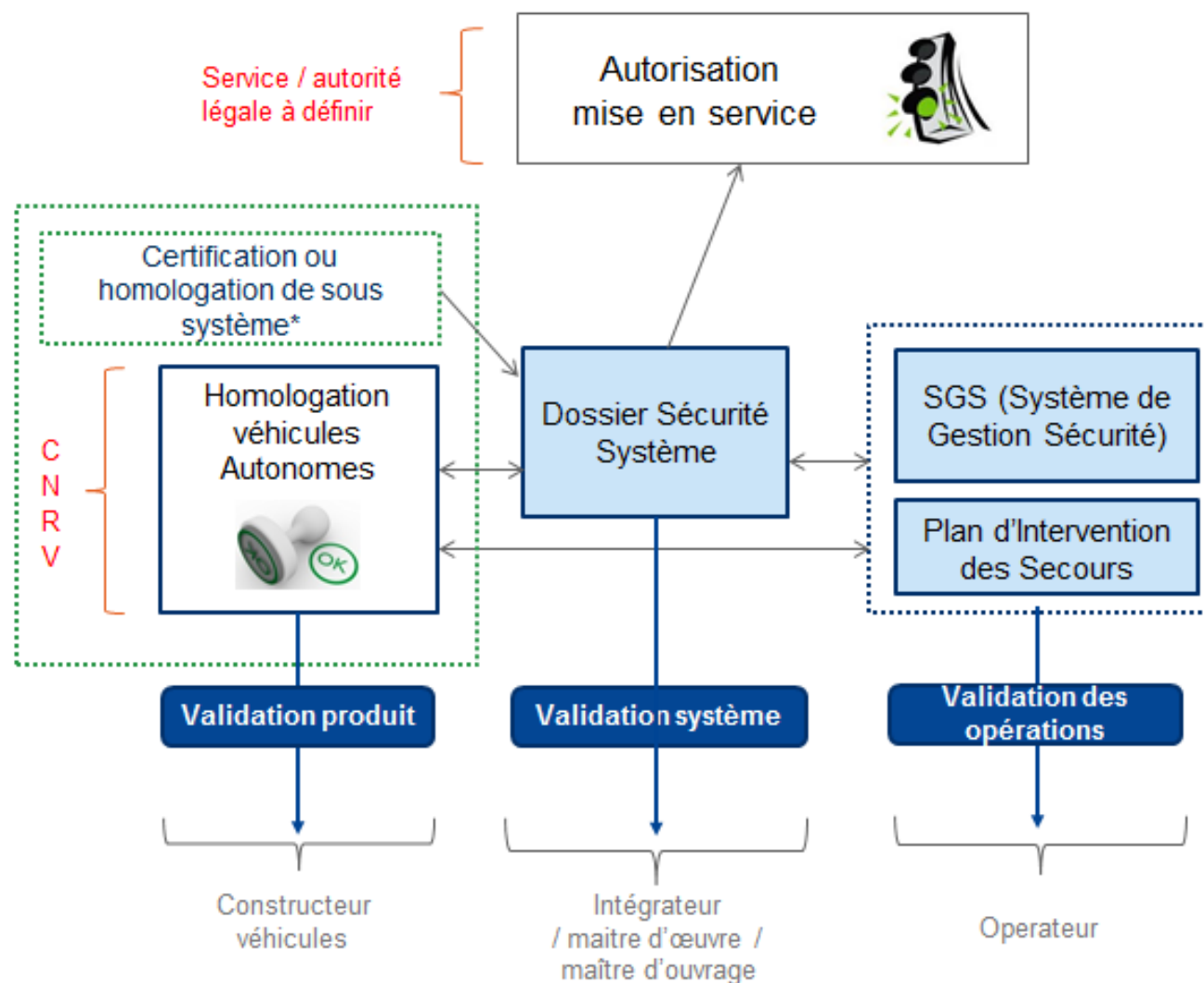
Les objectifs en termes de taux d'occurrence maximum (THR-Tolerable Hazard Rate) retenus sont :

- taux de collision mortelle : $4.10^{-8}/h$ de roulage navette
- taux de collision grave : $4.10^{-7}/h$ de roulage navette
- taux de collision avec victime : $4.10^{-6}/h$ de roulage navette

Ces objectifs sont à prendre en compte pour l'ensemble des situations et fonctions pouvant conduire aux conséquences indésirées, telles que gestion des carrefours, gestion des feux et stop, gestions des règles de priorité des circulations routières (incluant le cas des véhicules prioritaires de type police, pompier, etc.), les sorties de parking, la priorité aux passages piétons, etc



STPA – Processus d'Autorisation



Homologation véhicules
Certification / Homologation
de sous systèmes
+
Autorisation système
(pour un site/projet)



Transport public urbain : Quel suite attendue

Les Notes de recommandations transmises à la DGITM.

La validation de ces principes permettrait :

> La mise en exploitation de systèmes simple des 2019

Systèmes principalement en voies réservées, clairement formalisées, protégées d'intrusion involontaire sur la majorité de la distance.

À l'exception :

- De carrefours signalisés
- De passages piétons suffisamment espacés
- De zones piétonnières de longueurs limitées

Vitesse commerciale à produire de 8 à 12 km/h sur des distances de 1 à 5 km

> Donnerait des objectifs à atteindre pour les développements de l'ensemble de l'industrie concernée

> Donnerait un référentiel à promouvoir à l'international

MERCI

