JOURNÉE FRANCAISE DE L'INGÉNIERIE DES EXIGENCES

5 | 6 | 7

NOVEMBRE 2024

11H30 - 13H30

CFTL
Comité Français des Tests Logiciels

XSdF-Conseil

# Patrice KAHN

## Exigences sûreté et cybersécurité : qu'est-ce qui vous attend pour l'avenir

ÉVENEMENT SPONSORISÉ PAR

TELYS
SPÉCIALISTE DE LA BUSINESS ANALYSE

opentext™

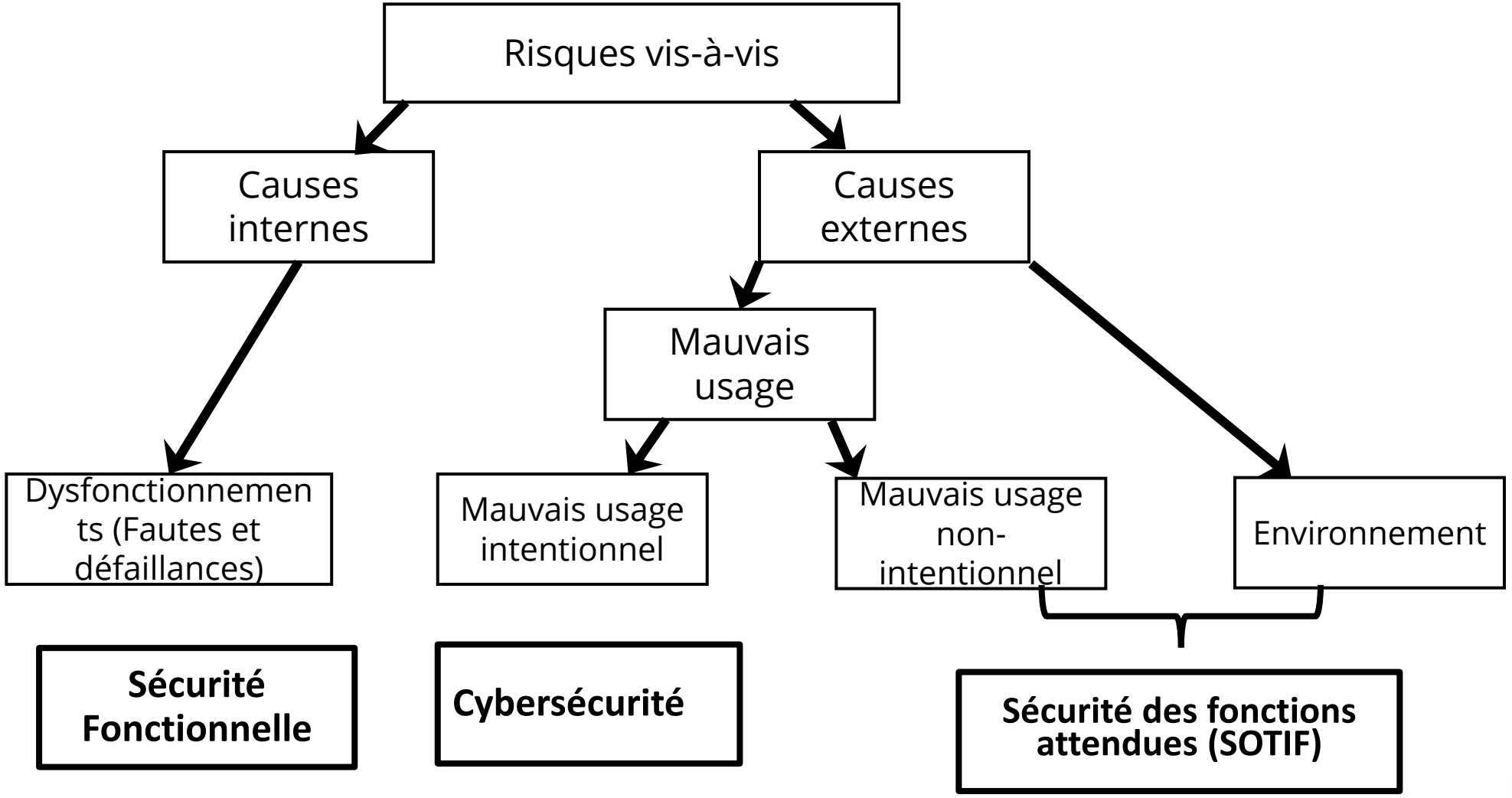
# Propriétés attendues des exigences (Rappel)



- **S**pécifique
- **M**esurable
- **A**cceptable
- **R**éaliste
- **T**emporellement défini

- **Question : Est-ce toujours possible ?**

# Maîtrise des risques




**SOTIF : Safety Of The Intended Functions (Norme ISO 21448)**

# Problématique SdF / Cyber / SOTIF



- **Sécurité Fonctionnelle** : Définir des situations qui ne doivent pas se produire face à des dysfonctionnements internes difficiles à identifier
- **Cybersécurité*** : Identifier des menaces potentielles et définir des situations qui ne doivent pas se produire face à des actions externes non définies
- **Sécurité des fonctions attendues** : Définir des exigences qui assurent la sécurité des utilisateurs dans toutes les (multiples) conditions d'utilisation possibles (environnement et/ou comportement utilisateurs)

**Question : Comment formuler et vérifier le respect d'exigences pour couvrir ce type de besoin ?**

**** : Peut aussi être étendu à des problématiques I&L***

# Exigences SdF – Sécurité Fonctionnelle



- **En réponse à un ou (plusieurs) attendu(s) :**
  - Tel(s) événement(s) ne doi(ven)t pas pouvoir arriver plus souvent que $10^{-9(x)/h}$
- **Action à mener :**
  - Essayer d'identifier toutes les causes potentielles pour chaque événement
  - Définir les moyens de réduction de risques compatibles avec tous les événements
  - Spécifier (exigences) les mécanismes à implémenter (redondance, surveillance, monitoring)
- **Comment démontrer que le besoin est satisfait :**
  - Vérifier que les exigences sont couvertes (traçabilité et résultats des tests)
  - Vérifier que les mécanismes se mettent en œuvre à bon escient
  - Evaluer le(s) risque(s) résiduel(s)
  - Faire des tests de robustesse, d'injection de fautes

# Exigences Cybersécurité



- **Face à un enjeu de cybersécurité :**
  - Identifier des menaces potentielles et définir des situations qui ne doivent pas se produire face à des actions externes non définies
- **Action à mener :**
  - Analyser les éléments à protéger
  - Identifier les vulnérabilités et les menaces potentielles
  - Définir des moyens de réduction des vulnérabilités et protection contre les menaces
  - Spécifier (exigences) les mécanismes à implémenter (cryptage, pare-feu, surveillances)
- **Comment démontrer que le besoin est satisfait :**
  - Vérifier que les exigences sont couvertes (traçabilité et résultats des tests)
  - Vérifier que les mécanismes se mettent en œuvre à bon escient
  - Evaluer le(s) risque(s) résiduel(s)
  - Faire des tests de pénétration (pentest, selon le niveau de risques cybersécurité*)

**** : La norme IEC 62443-3-3 (System security requirements and security level) définit 4 niveaux de cybersécurité***

# Liens Safety - Cybersécurité



- **Potentiel conflit :**
  - Domaine où la qualification (validation) d'un système est complexe (voir normative) :
    - Safety : une fois le système qualifié il doit être figé
    - Cybersécurité : à chaque nouvelle vulnérabilité identifiée (avec impact potentiel) : il faut mettre à jour le système
  - Problème de timing :
    - Safety : agir vite (ex. déclenchement airbag suite à détection de choc)
    - Cybersécurité : protection de l'information (encodage, transmission, décodage) pour éviter l'envoi de commande intempestive
- **Priorité définie :**
  - Exemple nucléaire : Les dispositions de cybersécurité ne doivent pas affecter de manière préjudiciable la réalisation des fonctions importantes pour la sûreté, les performances requises (y compris le temps de réponse), la fiabilité requise ou le fonctionnement requis des systèmes numériques programmables importants pour la sûreté
- **…**

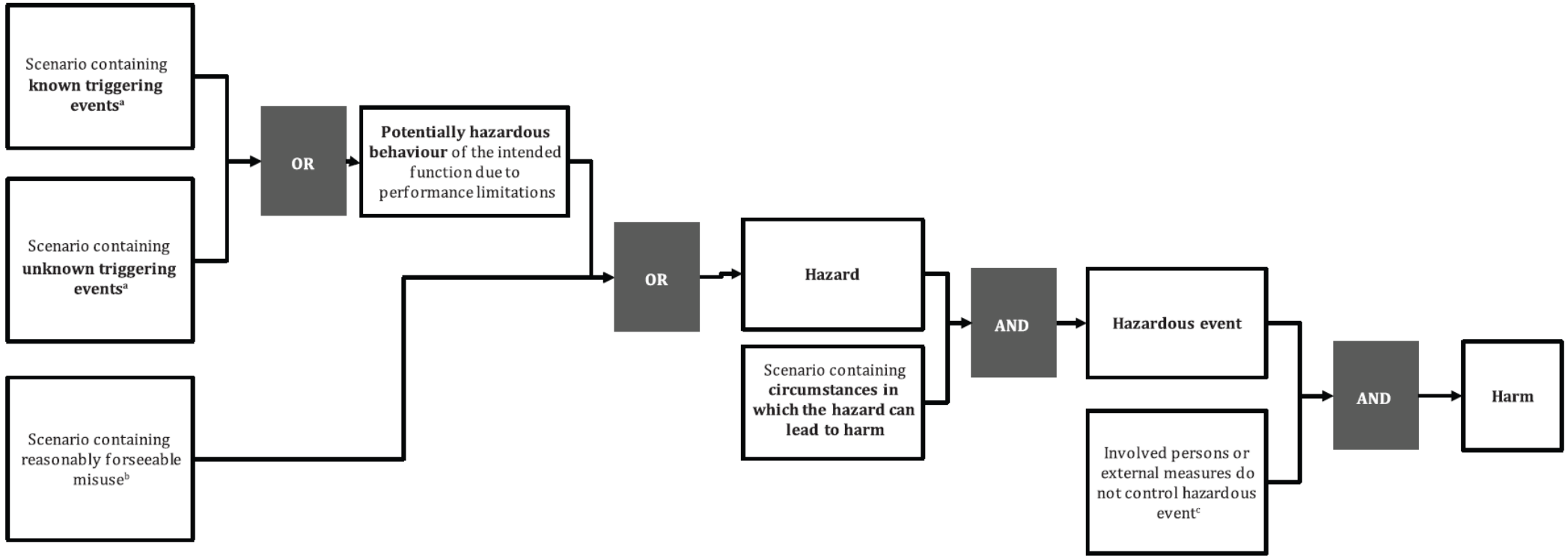
# Liens Safety - Cybersécurité



- …
- **Recherche d'arbitrage :**
  - Initiation des 2 stratégies :
    - HARA : Identification des risques Safety
    - TARA : Identification des vulnérabilités
  - Conciliation des 2 approches :
    - Identification des exigences Safety pouvant avoir un impact sur la cybersécurité ?
    - Identification des exigences cybersécurité pouvant avoir un impact sur la safety ?
    - Conciliation des moyens de réduction de risques définis (exigences) pour réduire les conflits.
    - Renforcer les tests des exigences ayant un double impact.

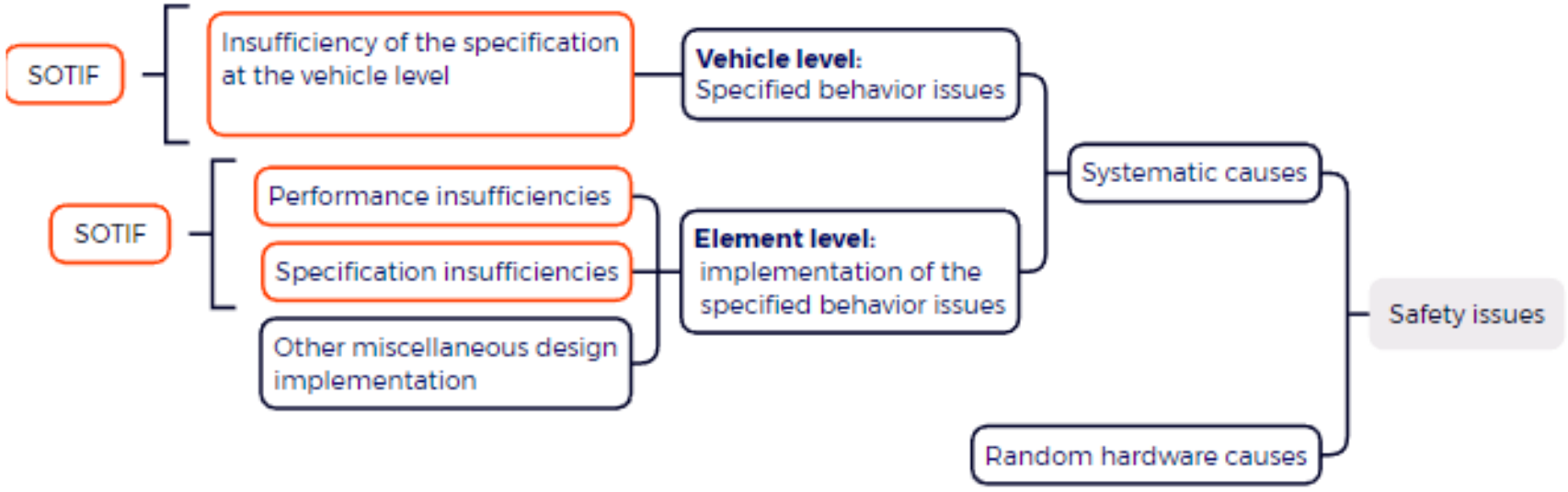
# SOTIF

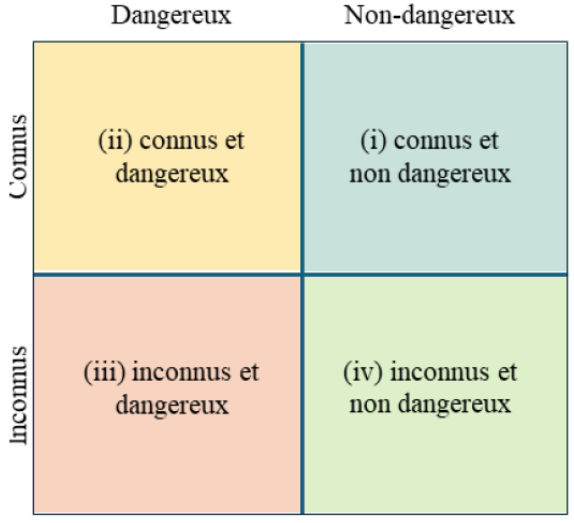
- SOTIF est la mise en œuvre de mesures de sécurité visant à prévenir ou à atténuer les événements dangereux au niveau du véhicule, causés par des insuffisances fonctionnelles, de mauvaises utilisations prévisibles des caractéristiques par un conducteur et des conditions inattendues dans le domaine de la conception opérationnelle (ODD).

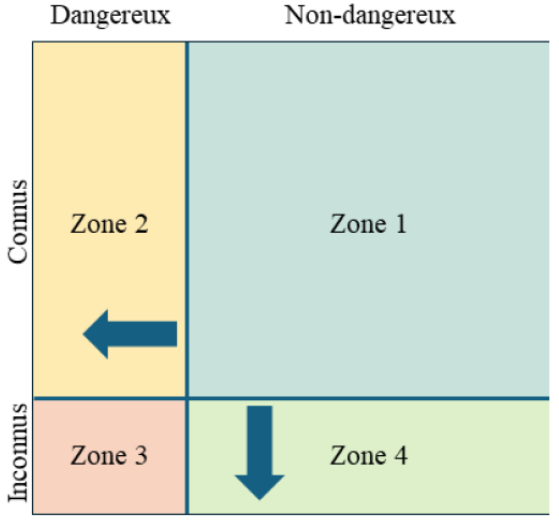


# SOTIF : Points focus






Catégorisation des scénarios opérationnels.

# SOTIF : domaine de conception opérationnelle (ODD)



Les domaines de conception opérationnelle (ODD) définissent les conditions de fonctionnement dans lesquelles les systèmes de conduite automatisée d'un véhicule peuvent être engagés en toute sécurité.

Chaque ODD est spécifique au modèle et à la fonction du véhicule. Au sein d'une même marque de véhicule, les modèles ont des niveaux variables de capacités de conduite automatisée et auront donc des ODD différents.

Quels sont les critères ODD ?

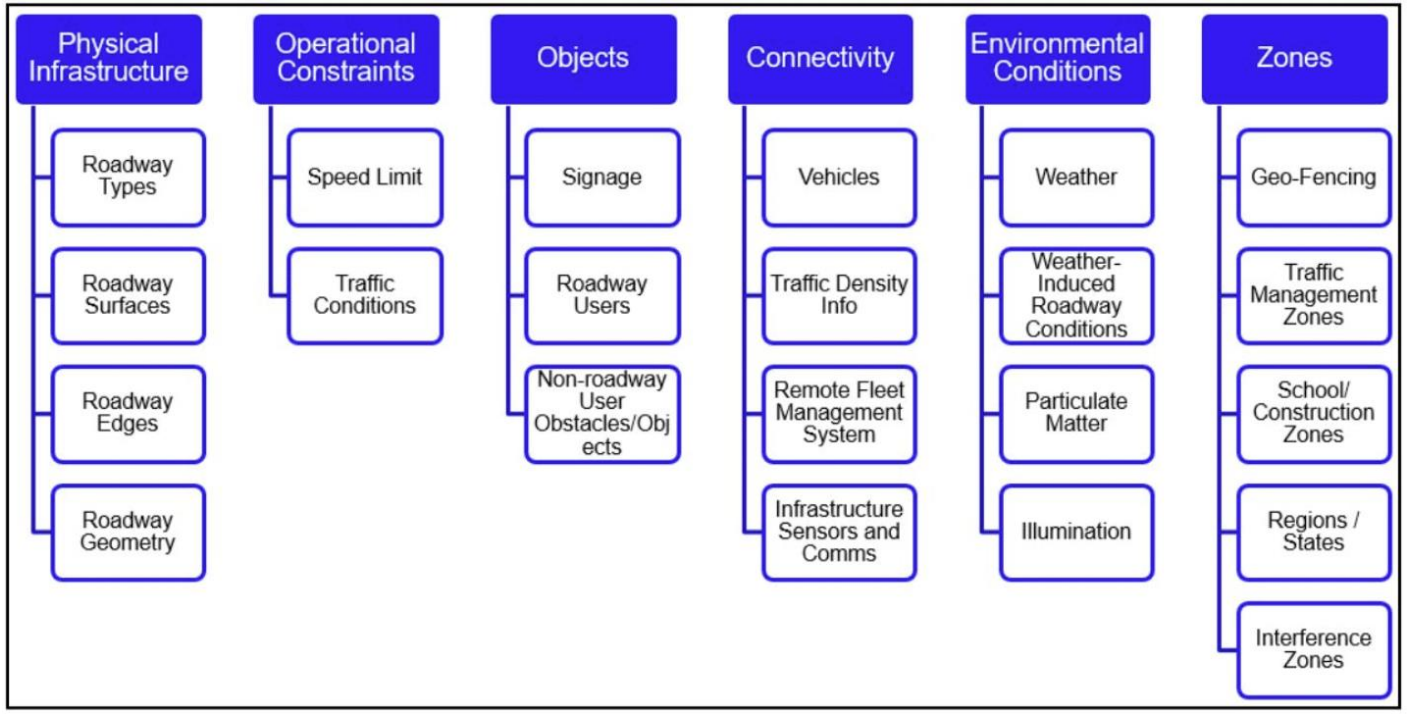
Parmi les critères ODD couramment cités figurent les caractéristiques de la route, l'heure de la journée, les conditions météorologiques et le terrain. Par exemple, un dispositif de conduite mains libres peut être conçu pour fonctionner le jour mais pas la nuit, par temps clair mais pas par forte pluie ou brouillard, ou sur un tronçon d'autoroute relativement droit mais pas dans un environnement urbain confiné.

# SOTIF : domaine de conception opérationnelle (ODD)



**Taxonomie des ODD : pour organiser et identifier les différents ODD.**

**Liste non exhaustive et nombreuses autres catégories pourraient également être utilisées pour définir un ODD.**




**National Highway Traffic Safety Administration (NHTSA)**

Exemple :

- Autopilot activable sur route 2 x 2 voies, avec terreplein central et vitesse < 60 km/h

# SOTIF : Description fonctionnelle



- **La spécification fonctionnelle et du système comprend (le cas échéant) :**

- **La fonction :**
  - Les objectifs de la fonctionnalité prévue ;
  - Les cas d'utilisation dans lesquels la fonctionnalité prévue est activée, désactivée et active ;
  - La description de la fonctionnalité prévue ;
  - Le niveau d'automatisation/d'autorité sur la dynamique du véhicule ;
  - Les dépendances et les interactions avec :
    - le conducteur, les passagers, les piétons et les autres usagers de la route ;
    - les conditions environnementales pertinentes ;
    - les interfaces avec l'infrastructure routière.

- **Le système :**
  - …

# SOTIF : Description du système

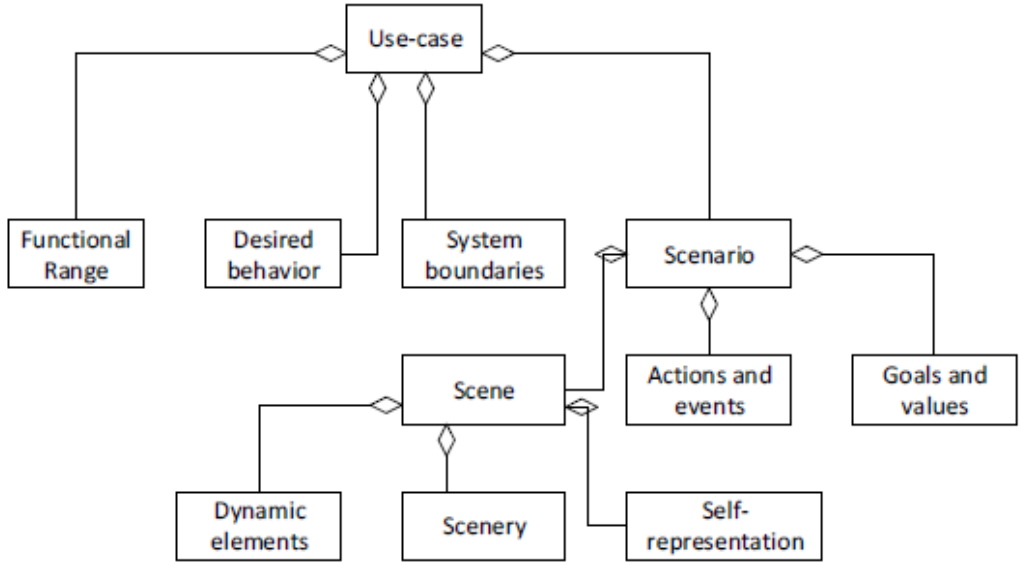


**La spécification fonctionnelle et du système comprend (le cas échéant) :**

- **La fonction :**
  - **…**
- **Le système :**
  - Description du système et des éléments mettant en œuvre la fonctionnalité prévue.
  - La description et le comportement des capteurs, contrôleurs et actionneurs installés, utilisés par la fonctionnalité prévue.
  - Les hypothèses sur la manière dont la fonctionnalité prévue utilise les entrées d'autres éléments.
  - Les hypothèses sur la manière dont d'autres éléments utilisent les sorties de la fonctionnalité prévue.
  - Les concepts et technologies pour le système et les sous-systèmes.
  - Les limitations et leurs contre-mesures.
  - L'architecture du système prenant en charge les contre-mesures.
  - Le concept de dégradation.
  - Les stratégies d'alerte.
  - Les dépendances et les interactions avec les autres fonctions et systèmes du véhicule.

# Définition des Cas d'usage






**Exemple de génération de nouveaux cas d'utilisation :**

- Les nouveaux cas d'utilisation sont obtenus via l'itération des paramètres modifiables. Les paramètres modifiables comprennent les actions et les événements, les valeurs et les paramètres de la scène.
- Afin d'éviter l'explosion du nombre de cas d'utilisation considérés, le processus d'itération requiert de la créativité. Seuls les paramètres pertinents pour la fonctionnalité choisie doivent être itérés.

- **Exemple de cas d'utilisation entièrement défini :**

1. **Gamme fonctionnelle : freinage d'urgence automatisé (AEB)**
2. **Comportement souhaité : le système active le freinage si une collision avec un obstacle est considérée comme hautement probable**
3. **Limites du système : système caméra / radar, calculateur AEB, calculateur de freinage, système de freinage.**
4. **Scénario**

**4.1. Actions et événements:**

**i) Le véhicule ego (c'est-à-dire le véhicule équipé de la fonctionnalité AEB prise en compte dans l'analyse) avance.**

**ii) Il n'y a pas d'obstacle sur le trajet du véhicule personnel dans la distance dangereuse (2 sec)**

**4.2. Objectifs et valeurs**

**i) Objectif: continuer à suivre la route, pas de changement de voie, pas de changement de direction**

**ii) Valeur: vitesse préférée, distance latérale, distance longitudinale**

**4.3. Scène**

**4.3.1. Éléments dynamiques: autres véhicules sur la route (par exemple un bus devant le véhicule de l'ego, à une distance de 3 secondes et une autre voiture derrière le véhicule de l'ego, une distance de 5 secondes)**

**4.3.2. Paysage**

**i) intra-urbain**

**ii) circulation à droite**

**iii) Route à deux voies: voie droite et voie gauche**

**iv) Piste cyclable à droite de la voie de droite**

**v) passage pour piéton à droite de la piste cyclable**

**vi) La route est symétrique (c'est-à-dire qu'elle a deux voies, une piste cyclable et un passage pour piétons dans la direction opposée)**

**4.3.3. Représentation de ego : le véhicule de l'ego est une voiture de tourisme.**

# Tests du Véhicule UBER (13/03/2018)



- Le système de détection d'obstacle a considéré à tort (mais sans défaillance) que le piéton habillé de manière sombre, dans un endroit peu éclairé, hors d'un passage protégé était un faux positif et était donc programmé dans un tel cas pour ne pas s'arrêter.
- La personne en charge de surveiller le véhicule durant les phases de tests n'a pas fait correctement son travail

- Question subsidiaire : est-ce qu'un conducteur humain aurait pu éviter l'accident ?

- https://www.challenges.fr/automobile/actu-auto/la-video-de-la-cycliste-renversee-par-une-volvo-autonome-uber-accuse-l-homme_575581

# Accident TESLA (11/10/2024)



- Collision avec un véhicule pour éviter écrasement d'un piéton

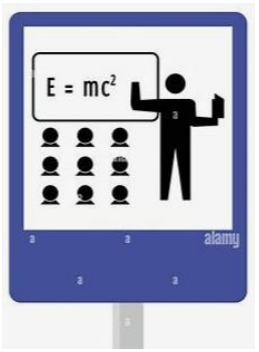
- https://www.linkedin.com/posts/fahed-hermassi-bb3a45254_tesla-autonomousdriving-ai-activity-7250786087562833920-BqtF?utm_source=share&utm_medium=member_desktop

- Difficile de savoir si cette décision est un choix d'évitement sans logique de comparaison entre les deux risques (écraser ou entrer en collision avec un véhicule venant en sens inverse et ce malgré la présence d'une ligne blanche) ou une décision résultant d'une vraie estimation des deux risques.
- Les nombreux accidents de Tesla font plutôt penser à l'application d'un scénario basique sans réelle analyse de risques.

# SOTIF

- **Comment reconnaitre toutes les situations**










# Ingénierie des exigences



- Comment s’assurer que toutes les situations définies sont couvertes et en sécurité ?

- Comment s’assurer que le système se comporte comme prévu lors des essais ?

# Merci

# Quel est votre avis ?