Contribution to the specification and demonstration of autonomous vehicle safety, based on situations and usage scenarios and their probabilistic assessment

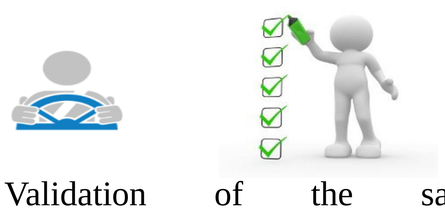
PhD student: Tchoya Florence KONE
tchoyaflorence.kone@mpsa.com/tchoya-florence.kone@univ-lorraine.fr

Thesis directors: Eric LEVRAT eric.levrat@univ-lorraine.fr,
Eric BONJOUR eric.bonjour@univ-lorraine.fr,
Stéphane GERONIMI stephane.geronimi@mpsa.com

Context

Standard vehicle engineering

- ❑ The driver is responsible of the control of the vehicle



- ❑ Validation of the safety requirements (related to critical Hazardous Events)

Autonomous vehicle (AV) engineering

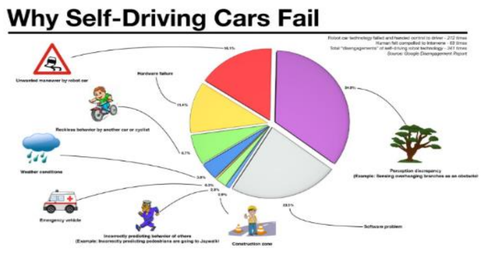
- ❑ Driver out of the loop of decision

- ❑ Vehicle control responsibility (total or partial) to the manufacturer
- ❑ Demonstration of safety performance at least equal to those of the human

Issues & challenges

❖ Statement

1. High Safety performance assigned to AV



2. Conventional validation methods are insufficient

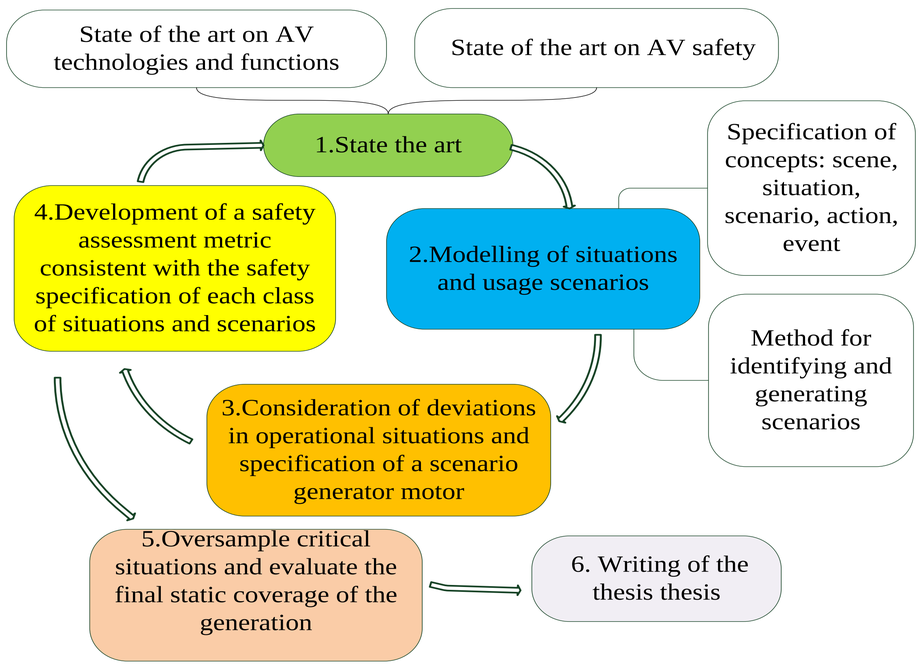
3. Use of additional solutions to ensure safety validation

- ❑ Ensure a "Safety of the Intended Functionality": PAS 21448 SOTIF
  - Setting up rules for the proper operation of the vehicle and the interaction with the driver and systematic use of (massive) simulation

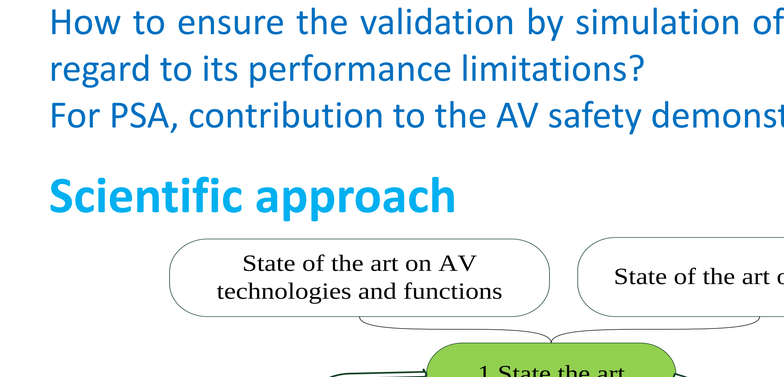
❖ Scientific issue of the thesis

How to ensure the validation by simulation of the safety of the AV with regard to its performance limitations?
For PSA, contribution to the AV safety demonstration.

Scientific approach



State of the art



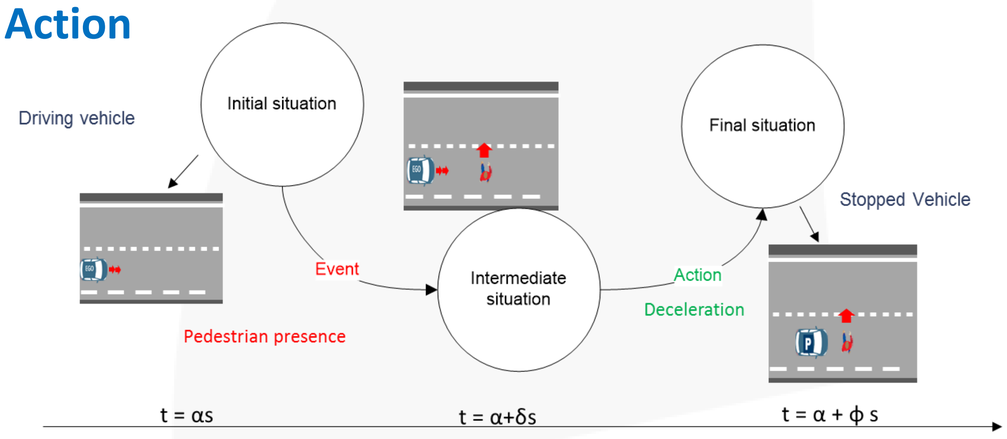
❖AV architecture & Technological issues

❖ISO 26262 vs ISO/PAS 21448 SOTIF

Source : CertX

Specification of key concepts for scenario generation

- ❖ **Input for generation:** Concept of "Situation", Identification of entities of the operational environment and their parameters, Behaviours of the AV and the other road users
- ❖ **Key concepts proposals: Situation, Scenario, Event and Action**

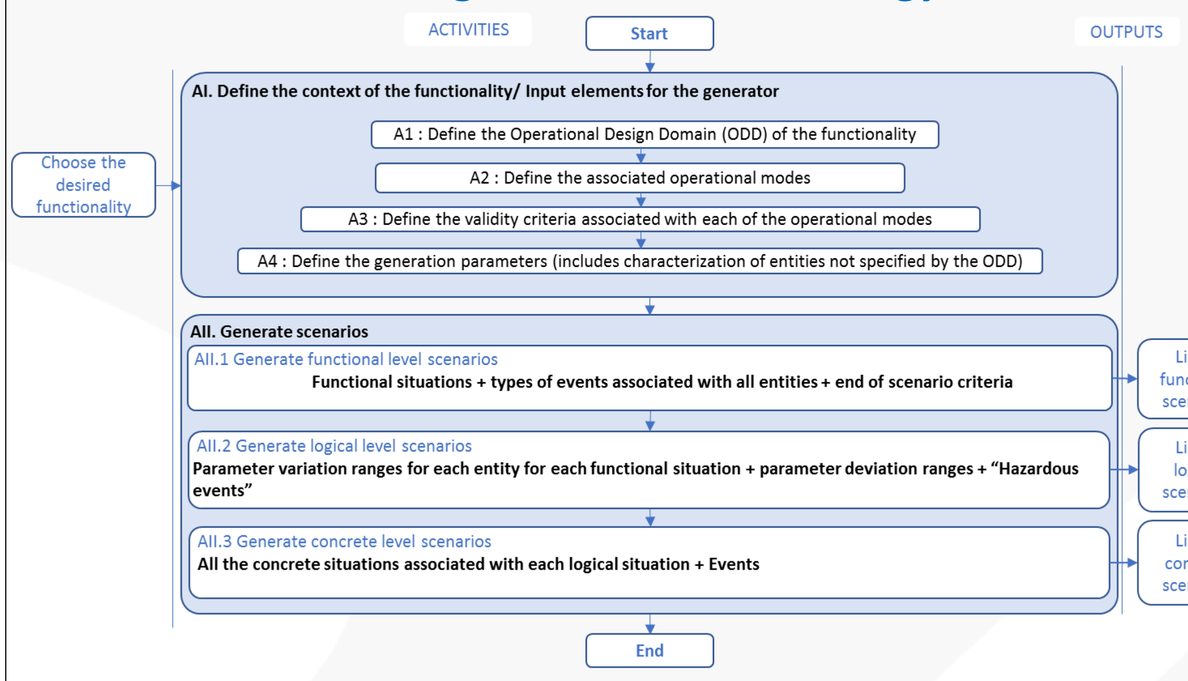


❖ Events identification and deviation concept

- ❑ Integration of factors that impact AV performances (incl. Safety issues)
- ❑ Use of HAZOP (HAZard and OPerability analysis)

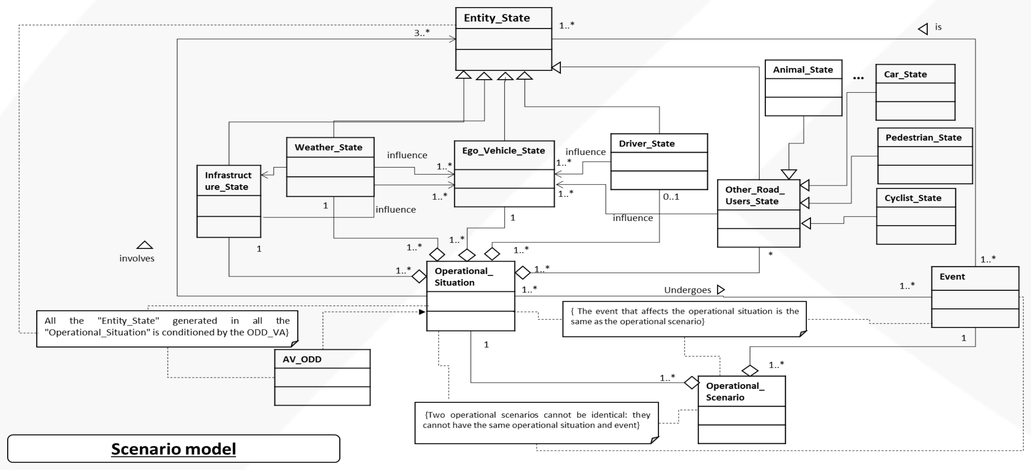
Generation specification

❖ Overview of the generation methodology



❖ Conceptual model

- ❑ Use of an MBSE methodology (Harmony-SE, SysML)



Scenario model

Perspectives: Safety analysis of scenarios, their probabilistic assessment and coverage

- ❑ Definition of the criticality of a scenario
- ❑ Probabilistic assessment of the criticality of a scenario (Uncertainty consideration)
- ❑ Over-sampling of critical scenarios during generation and statistical coverage evaluation

Publications:

- ❑ « Safety demonstration of Autonomous vehicles: a review and future research questions » (Accepted), CSDM Paris 2019.
- ❑ Challenges for Autonomous Vehicles (AVs) engineering: Safety validation of functional performance limitations, INSIGHT INCOSE (International Council on Systems Engineering)

Date of starting: 1st February 2018
Doctoral school: IAEM/University of Lorraine-Nancy

Bibliography

Koopman, P. and al. 2016. "Challenges in Autonomous Vehicle Testing and Validation.
Raffaëlli and al. 2016. 'Facing ADAS Validation Complexity with Usage Oriented Testing.'
Ulbrich, S. et al. (2014) 'Graph-Based Context Representation , Environment Modeling and Information
Kalra, Nidhi, and Susan M Paddock. 2016. "Driving to Safety." RAND Corporation - Www.Rand.Org.