TRUSWORTHY EMBEDDED AI

PART 1 : OOPERATIONAL DESIGN DOMAIN ODD

Asma Smaoui CEA/LIST/DILS/LSEA : asma.smaoui@cea.fr

- with contributions from **Morayo Adedjouma,** Matteo MORELLI, Ansgar RADERMACHER, Fabio ARNEZ, Guillaume OLLIER, Diana RAZAFINDRABE (CEA-LIST/DILS/LSEA); EL JIHAD Hasnaa; Huascar ESPINOZA (KDT JU)

Safety and robustness — Key factors in autonomous systems innovation

- Safety of robotics applications must be guaranteed
- Legal directives and standards compliance must be fulfilled!
- Avoid emergency stops and ensure system stability

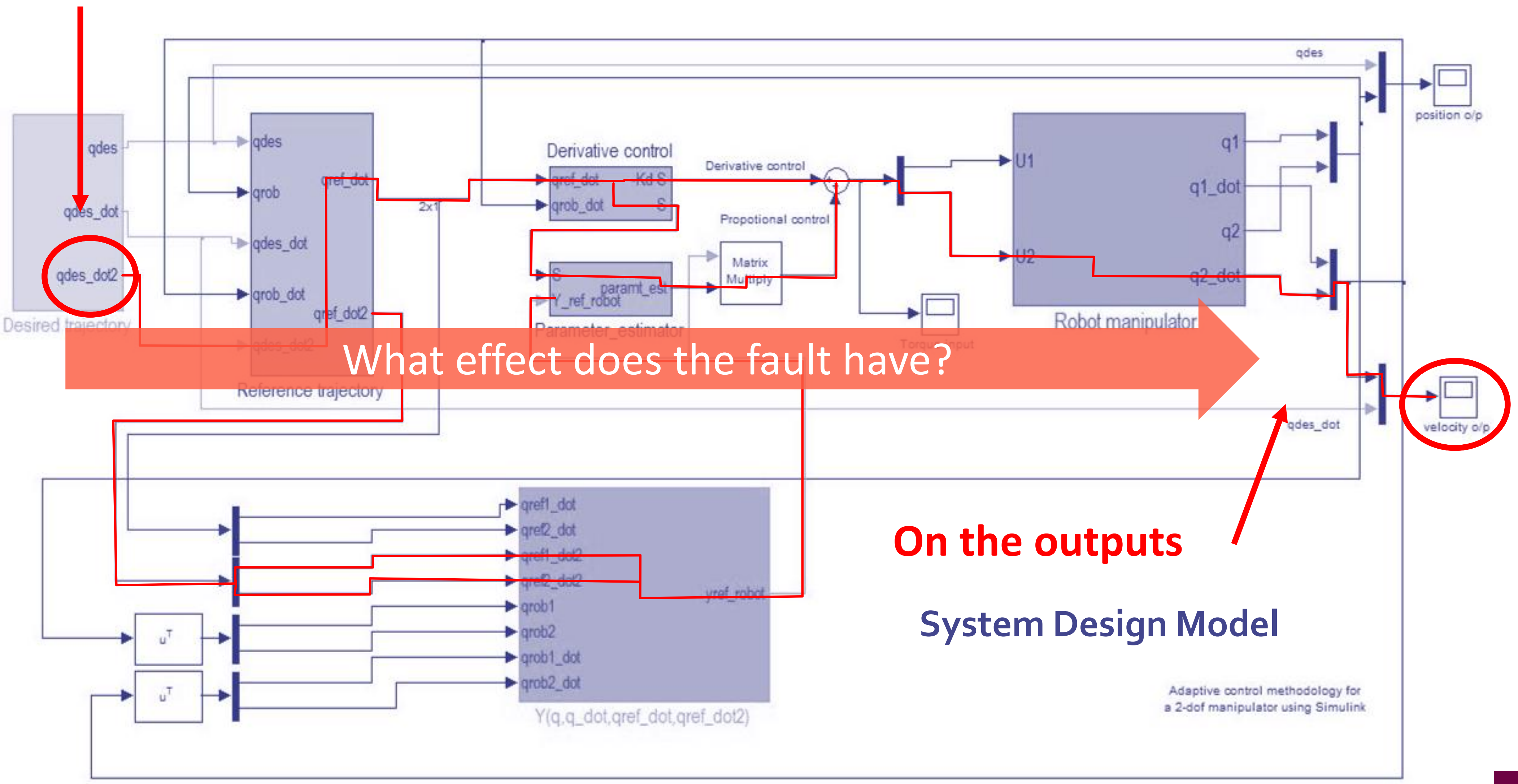
Safety is the condition of being protected from harm or other non-desirable outcomes. It can also refer to risk management.

Functional safety is the part of the overall safety of a system or piece of equipment that depends on automatic protection operating correctly in response to its inputs or failure in a predictable manner.

Safety of the Intended Functionality (SOTIF) concerns with guaranteeing the safety of a functionality that can have safety risks in the absence of a fault.

How to anticipate the fault impact on the system to ensure safety?

If a fault develops here



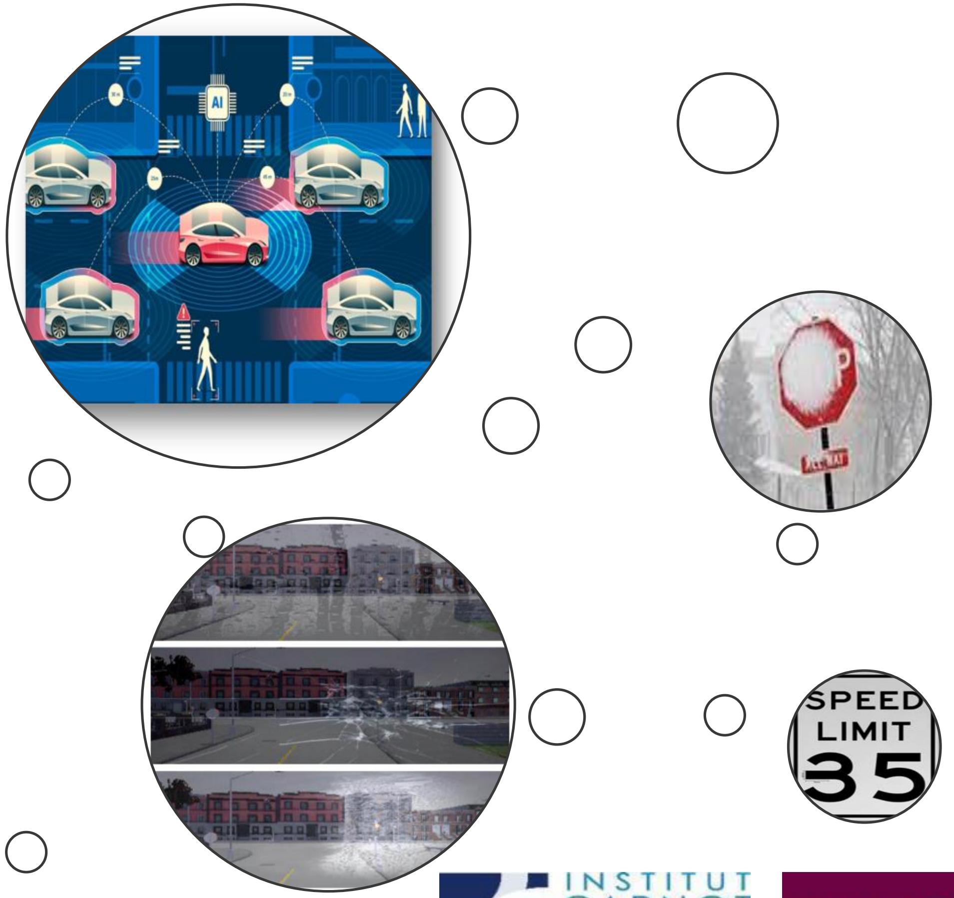
Credits: Yiannis Papadopoulos, University of Hull, U.K

How to support design, verification and validation to achieve and maintain the SOTIF?

Guidance on measures to ensure the absence of unreasonable risk due to a hazard caused by insufficiencies of functionalities where proper situational awareness is essential to safety and where such situational awareness is derived from complex sensors and processing algorithms, including AI

- **SOTIF is crucial to achieve trustworthy AI-based systems**
  e.g., autonomous shuttles for passenger transportation near activity zones, living areas open to pedestrians, etc.

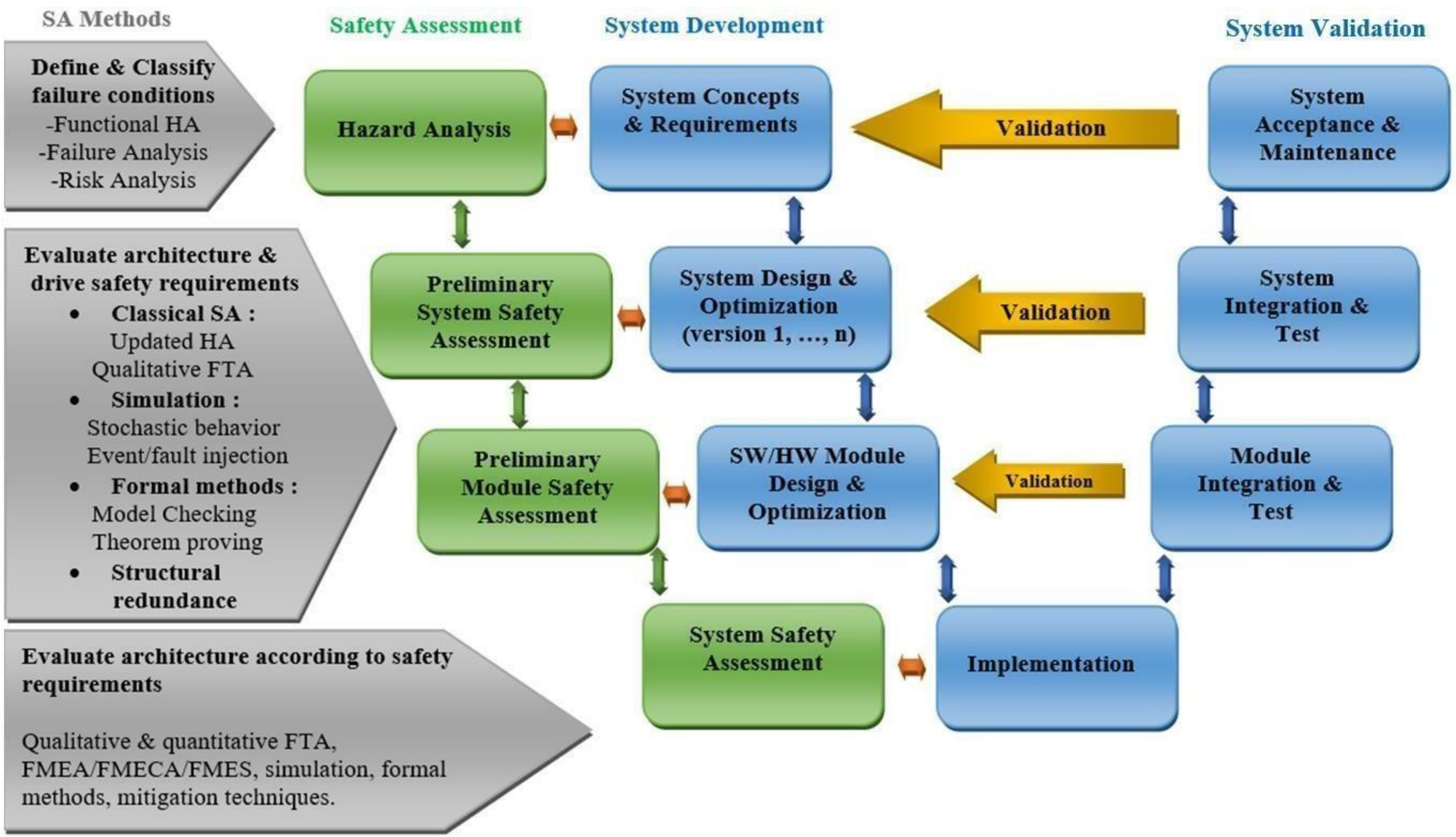
- **Challenges:**
  complex/changing operational contexts;
  data noise, ambiguous scenarios;
  degraded sensor quality and sensor failures.



Model-driven engineering as a key enabler for design and V&V of safe autonomous systems

formal process, based on models

formal process, based on models

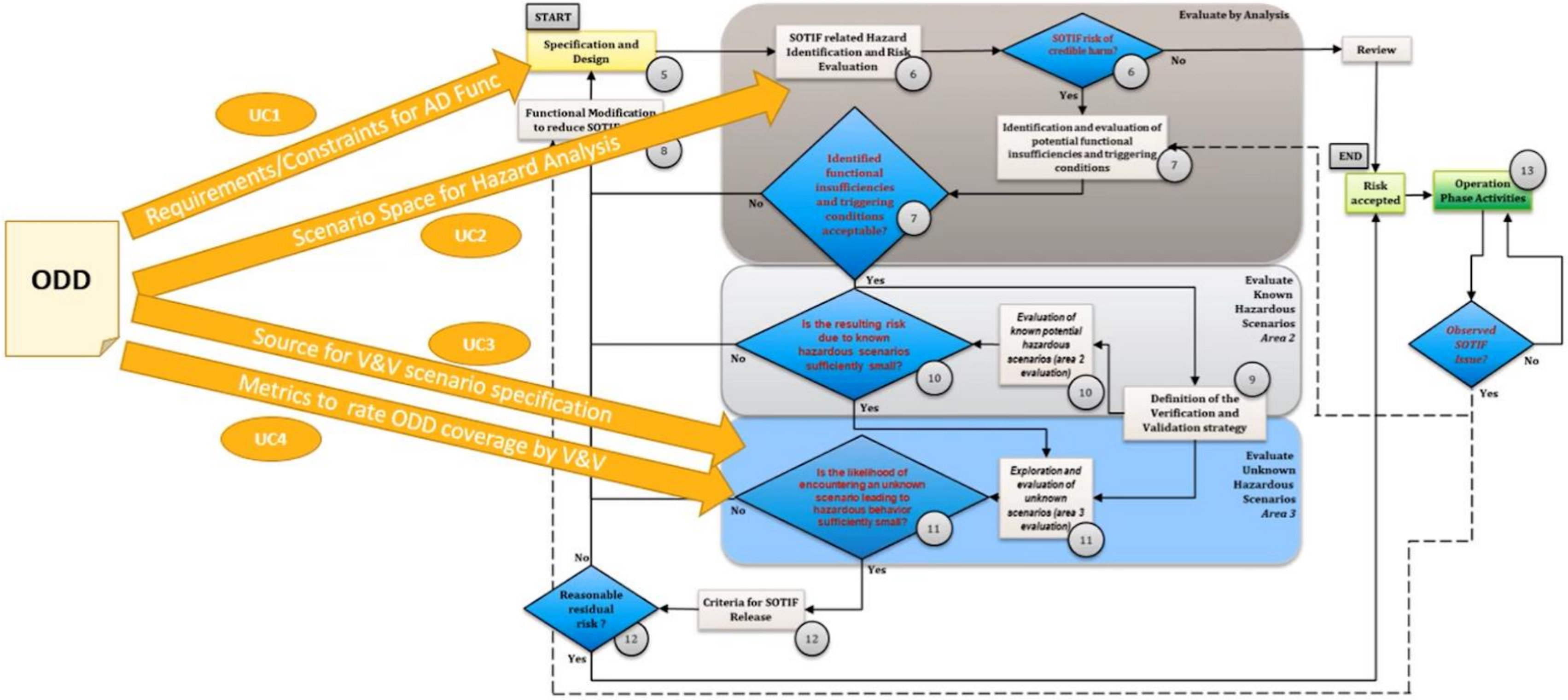


Operational Design Domain (ODD) definition

Context: In practice, the number of possible scenarios which have to be managed by an automated tends to be infinite. Because the NNs learned from data, it is impossible to ensure that these data capture the infinite number of scenarios in which automated systems must operate, which makes their safety evaluation challenging.

Goal: We need a mean to define the scenario-space in which the automated system must operate safely without having to enumerate the different scenarios individually. The scenario-space is specified through the operational design domain.

Operating conditions under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited to, **environmental**, **geographical**, and **time-of-day** restrictions, and/or the requisite presence or absence of certain **traffic** or **roadway characteristic**.



*Definition from SAE J3016

Ontology for Automated Systems

- Contains **cross-domain concepts** to **describe** the **environment** (e.g, weather, maneuvers, human operator)

Domain- specific Ontology

- Contains relevant concepts to **describe** the **environment** for a **specific domain** (e.g, automotive, avionic, railway)

Operational Domain

- Contains concepts to **describe** the **environment** for a **specific system**
- Represents the **system scenario-space**.

ODD

- Refers to the **intended ADS capability** to handle operating conditions.

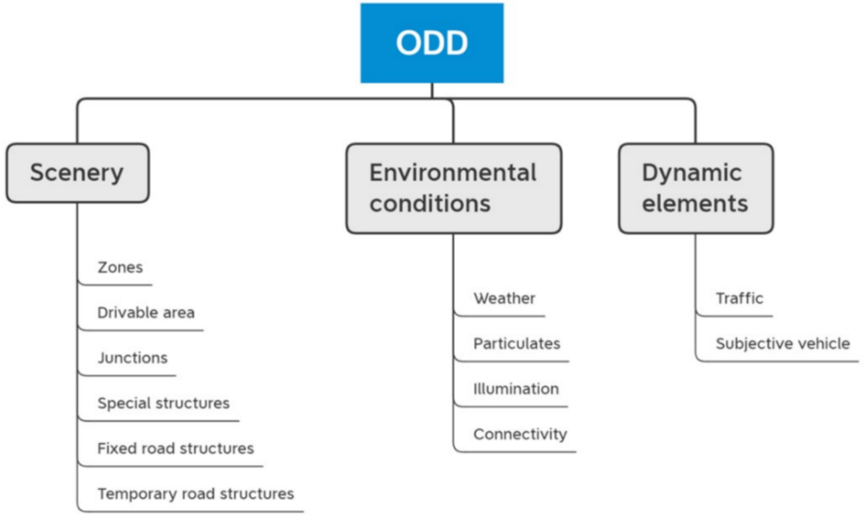
Usage Scenario

- **Expected ADS behavior** under **specific operating conditions**.

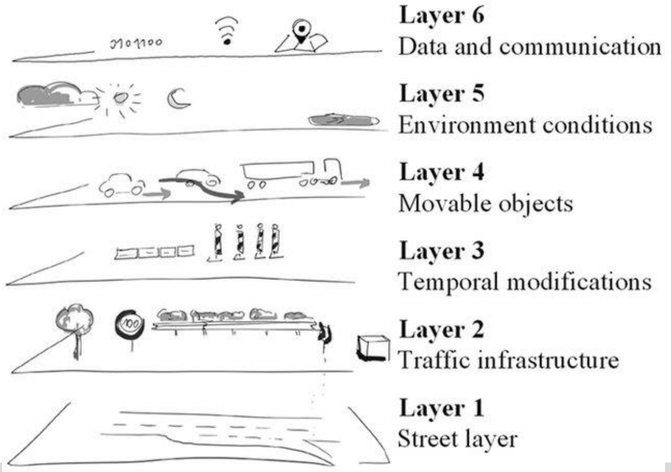
From Operational Domain to ODD and scenarios

The structuring of scenarios can be achieved following a number of approaches, e.g.:

✓ *descriptions from the <u>outside</u> of the ADS (e.g. 6-layer approach, ISO/DIS 34503, PAS 1883)*



Top-level taxonomy with ODD attributes



Attribute	Sub-attribute	Sub-attribute	Capability
Drivable area type	Motorways (M)	—	Yes
	Radial roads (A-roads)		Yes
	Distributor roads (B-roads)		Yes
	Minor roads		No
Lane specification	Number of lanes	—	Yes, minimum of two lanes
	Lane dimensions		Minimum 3.7 m
	Lane type	Bus lane	No
		Traffic lane	Yes
		Cycle lane	No
		Tram lane	No
		Emergency lane	No
		Other special purpose lane	No
	Direction of travel	Right-hand traffic	No
		Left-hand traffic	Yes

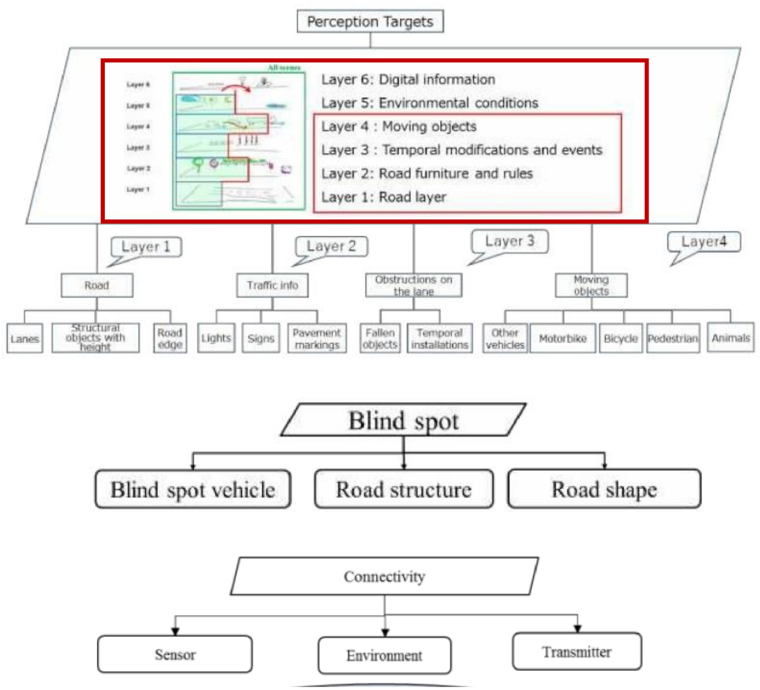
Attribute	Sub-attribute	Sub-attribute	Capability
Drivable area geometry	Horizontal plane	Straight roads	Yes
	—	Curves	Yes – up to 1/500 m (radius of curvature)
	Vertical plane	Up-slope	Yes
		Down-slope	Yes
		Level plane	Yes
	Cross-section	Divided/undivided	Divided
		Pavement	Yes
		Barrier on the edge	No
		Types of lanes together	Only traffic lane
Drivable area surface type	Asphalt	—	Yes
	Concrete		Yes
	Cobblestone		No
	Gravel		No
	Granite setts		No
Drivable area signs	Type	Regulatory	Yes
		Warning	Yes
		Information	Yes
	Time of operation	Part-time	No
		Full-time	Yes
	State	Variable	Yes
		Uniform	Yes

*Source: PAS 1883

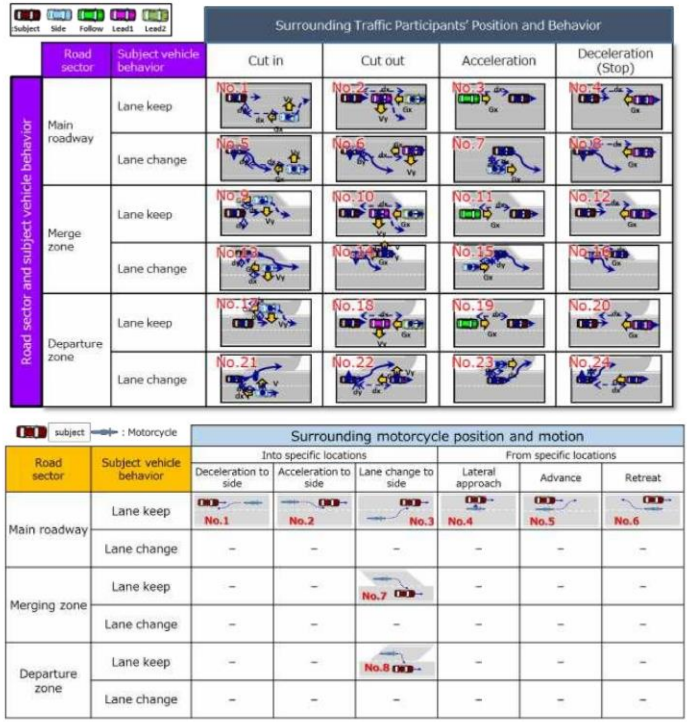
From Operational Domain to ODD and scenarios

The structuring of scenarios can be achieved following a number of approaches, e.g.:

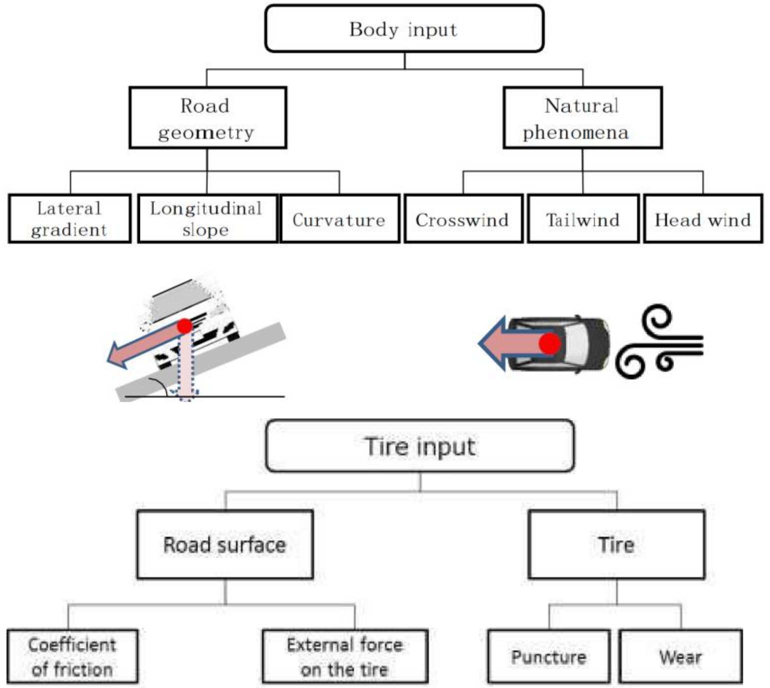
✓ *descriptions from the inside the ADS (e.g. 3-categories approach, ISO/DIS 34502 approach)*



Perception related critical scenarios



Traffic related critical scenarios



Vehicle control related critical scenarios

*Source: ISO 34502-#:####(X)-DIS draft 210908

From Operational Domain to ODD and scenarios

✓ *ODD definition and formalization using OpenODD language*

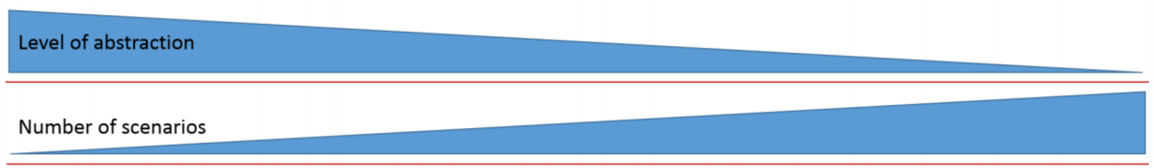

```
#Composition statements
Suitable geofenced areas is [predefined route]
Suitable regions or states is [Ottawa Canada]
Suitable zones are [regions or states, geofenced areas]
Cond_1 Conditional drivable area type are [minor roads, parking, shared space]
Cond_2 Conditional horizontal plane is [curved roads]
Unsuitable transverse plane is [divided]
Suitable types of lane together is [traffic lane]
Suitable lane dimension is [3.7,∞]
Suitable lane marking is [2,∞]
Suitable lane type is [traffic lane]
Suitable number of lanes is [2,∞]
Suitable direction of travel is [right hand travel]
Unsuitable drivable area signs is [variable]
Suitable drivable area edge is [line markers, solid barriers]
Unsuitable induced drivable area surface conditions are [flooded roadways, mirage]
Suitable drivable area surface type is [uniform]
Suitable roundabout is [normal]
Suitable normal is [non signalised]
Unsuitable intersection is [staggered, grade separated]
Suitable special structures is [pedestrian crossing]
Unsuitable temporary road structures is [construction site detours]
Unsuitable wind are [near gale, gale, strong gale, storm, violent storm, hurricane-
force]
Unsuitable rainfall is [violent rain, cloudburst]
Suitable temperature is [-30,40 C]
Suitable particulates is [non precipitating water droplets]
Suitable vehicle to infrastructure is [cellular]
Suitable positioning is [global positioning]
Suitable subject vehicle speed is [0,15 km/h]

#Conditional statements
Cond_1 Suitable speed of subject vehicle for [minor roads] is [0,15 km/h]
Cond_1 Suitable speed of subject vehicle for [parking, shared space] is [0,10 km/h]
Cond_2 Unsuitable radius of curved road is [0,5 m]
```

*Source: ISO 34503-#:####(X)-WD 34503 – r11.0

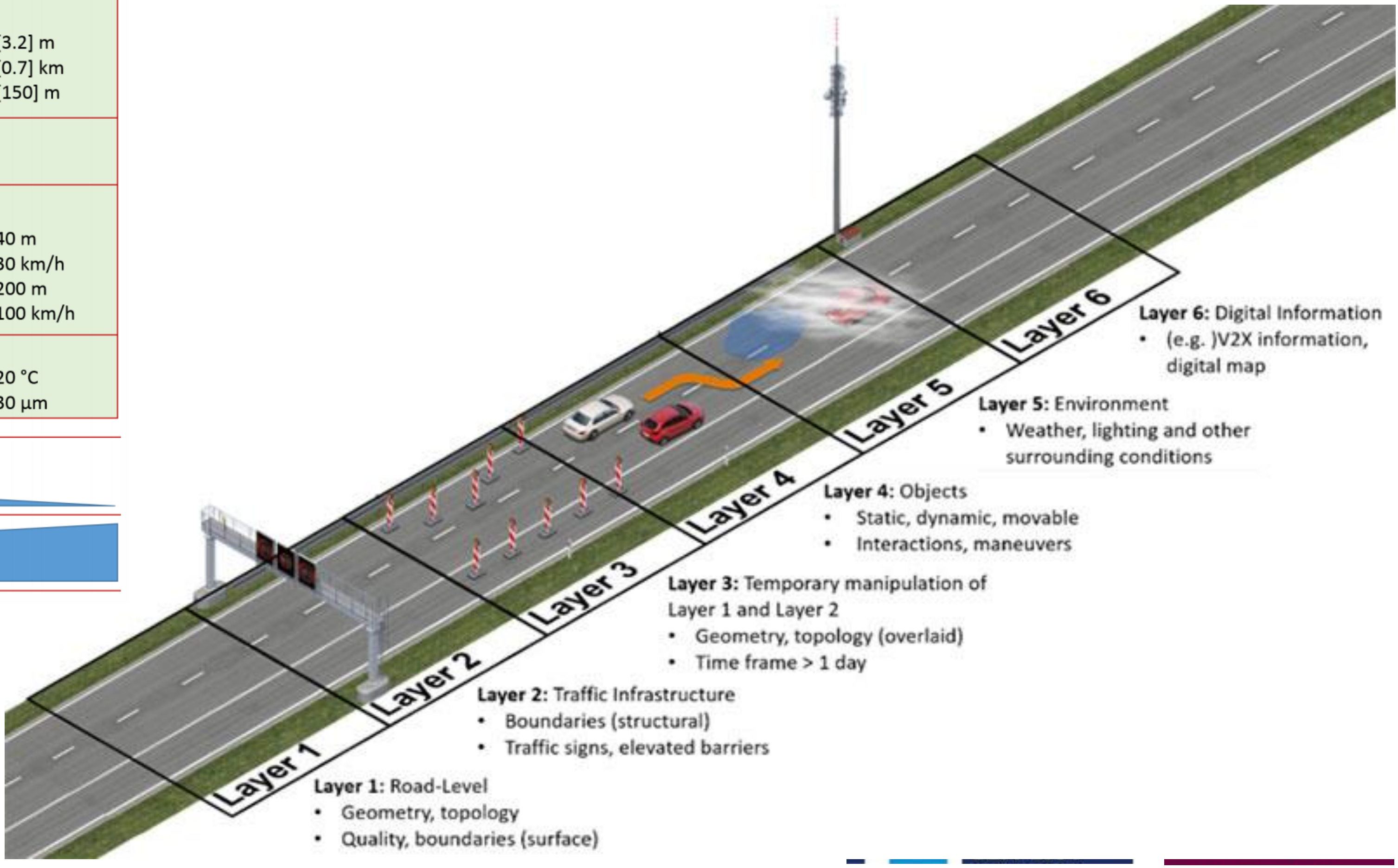
Scenario description can be done at functional, logical, concrete levels

Functional scenarios	Logical scenarios	Concrete scenarios
Base road network: three-lane motorway in a curve, 100 km/h speed limit indicated by traffic signs	Base road network: Lane width [2.3..3.5] m Curve radius [0.6..0.9] km Position traffic sign [0..200] m	Base road network: Lane width [3.2] m Curve radius [0.7] km Position traffic sign [150] m
Stationary objects: -	Stationary objects: -	Stationary objects: -
Moveable objects: Ego vehicle, traffic jam; Interaction: Ego in maneuver „approaching“ on the middle lane, traffic jam moves slowly	Moveable objects: End of traffic jam [10..200] m Traffic jam speed [0..30] km/h Ego distance [50..300] m Ego speed [80..130] km/h	Moveable objects: End of traffic jam 40 m Traffic jam speed 30 km/h Ego distance 200 m Ego speed 100 km/h
Environment: Summer, rain	Environment: Temperature [10..40] °C Droplet size [20..100] µm	Environment: Temperature 20 °C Droplet size 30 µm

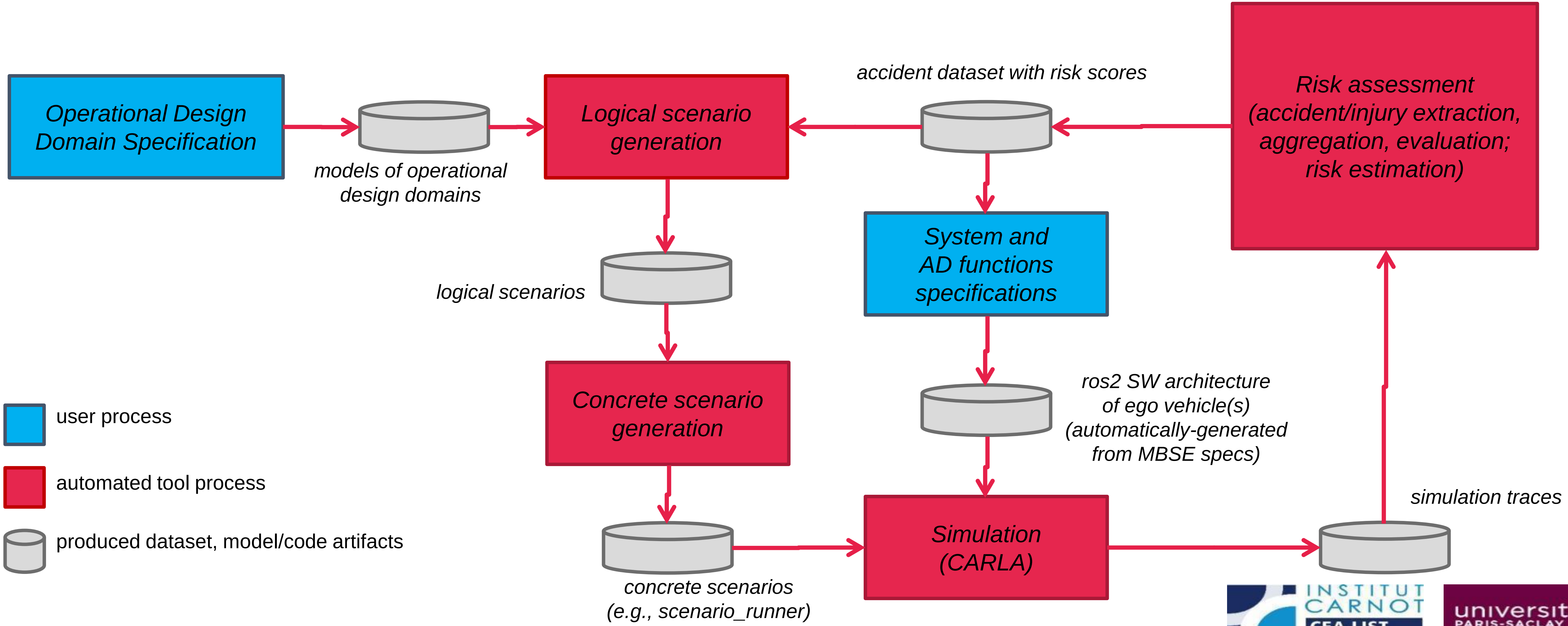


✓ *Do we need to include occupants and vehicle status?*

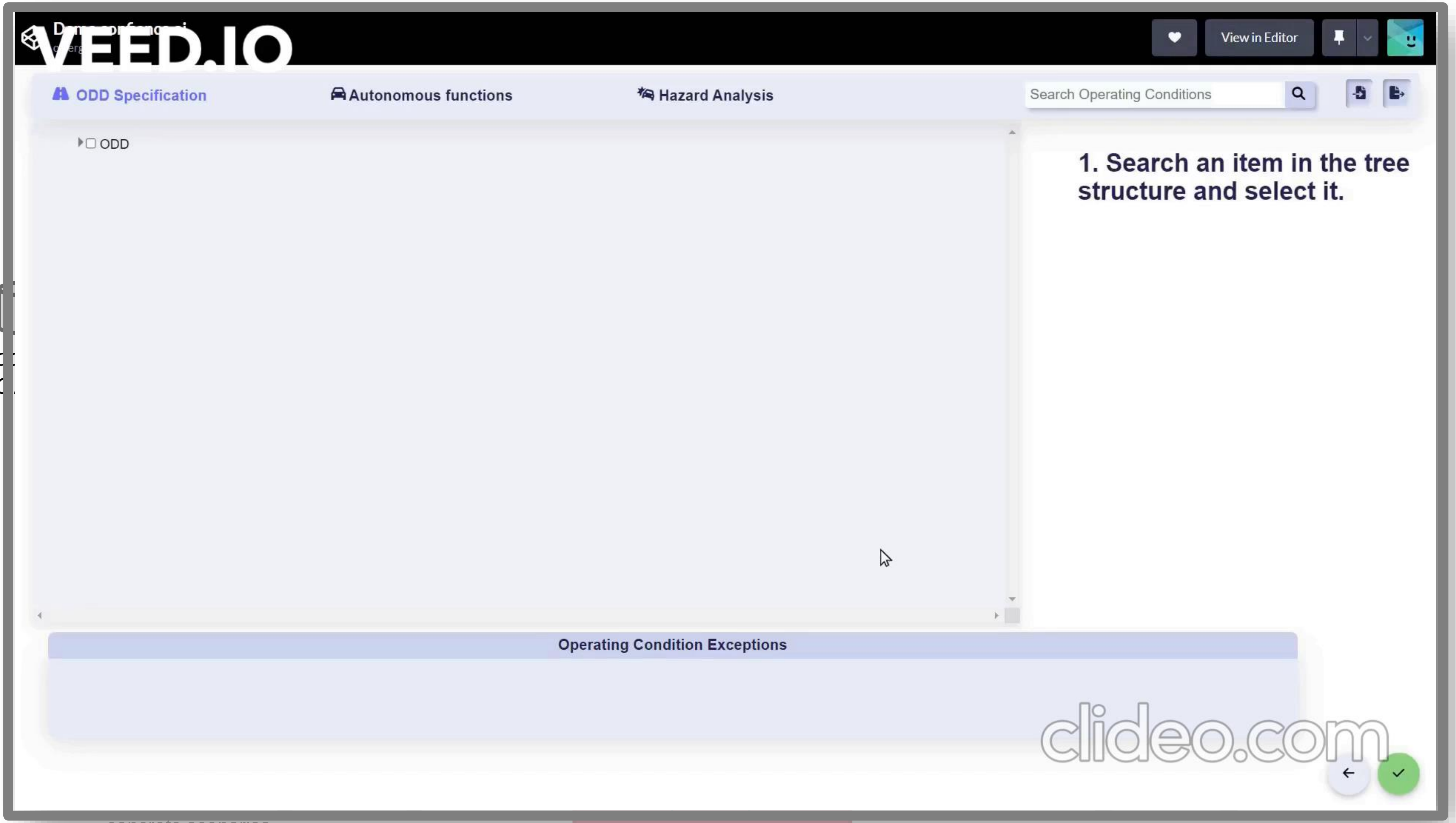
*Source: https://www.pegasusprojekt.de/de/about-PEGASUS



Combined process based on knowledge engineering and simulation for the identification and evaluation of unsafe scenarios in autonomous driving systems



Operational Design Domain Specification



concrete scenarios
(e.g., scenario_runner)

Thank you

Updated version 06-12-2024 by Asma Smaoui
asma.smaoui@cea.fr