Application Story of ODD as part of Safety Assurance

The significance of a well-structured ODD specification for the AD Safety and SOTIF Process

Dr. Bernhard Kaiser

ANSYS

June 2021

What are the new safety aspects of Automated Driving?

Traditional Functional Safety (FuSa) considers hazards caused by failures of E/E systems

BUT

Misfit between system assumptions / specification and actual environment

Limited Sensor Performance / Impairment by environmental conditions

Inpredictable behavior of Machine Learning Algorithms

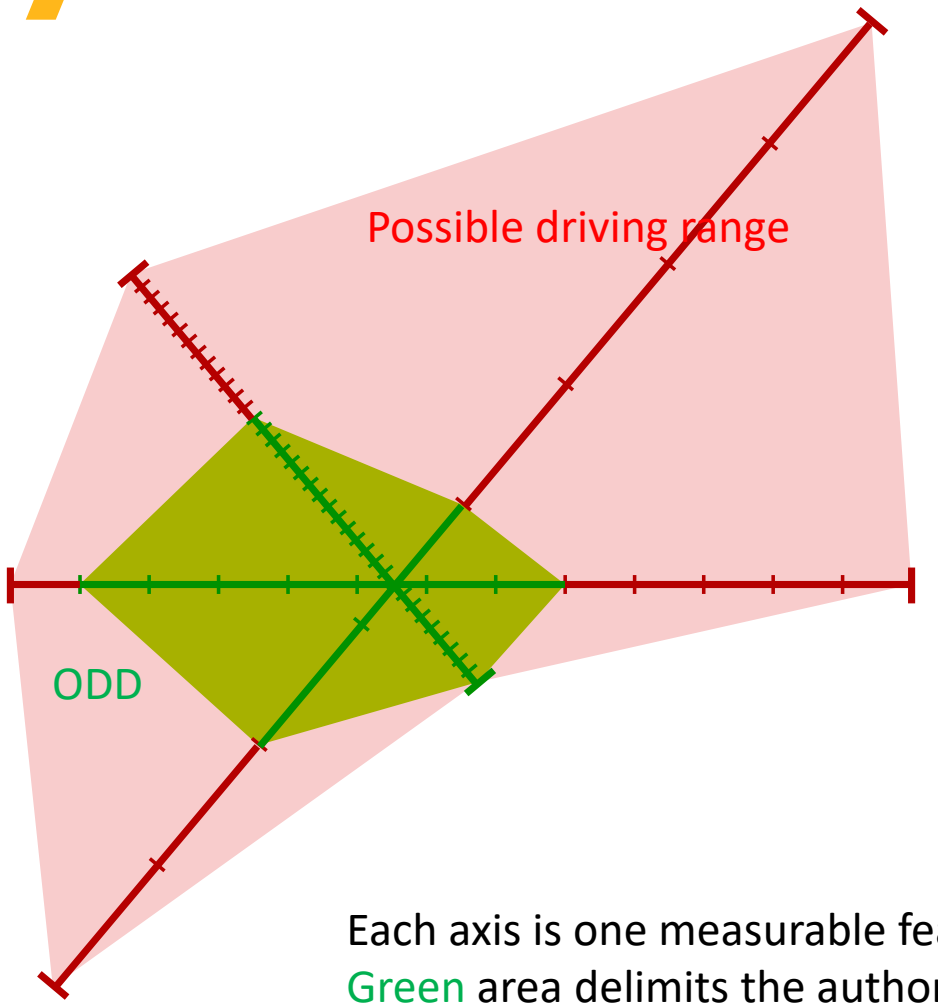
Misunderstandings, Mode Confusion, Overburdening and Misuse

FuSa
ISO 26262

SOTIF
ISO 21448

NEW!

What is an ODD?



Operational Design Domain (ODD) :=

"specific conditions under which a given driving automation system is designed to function"

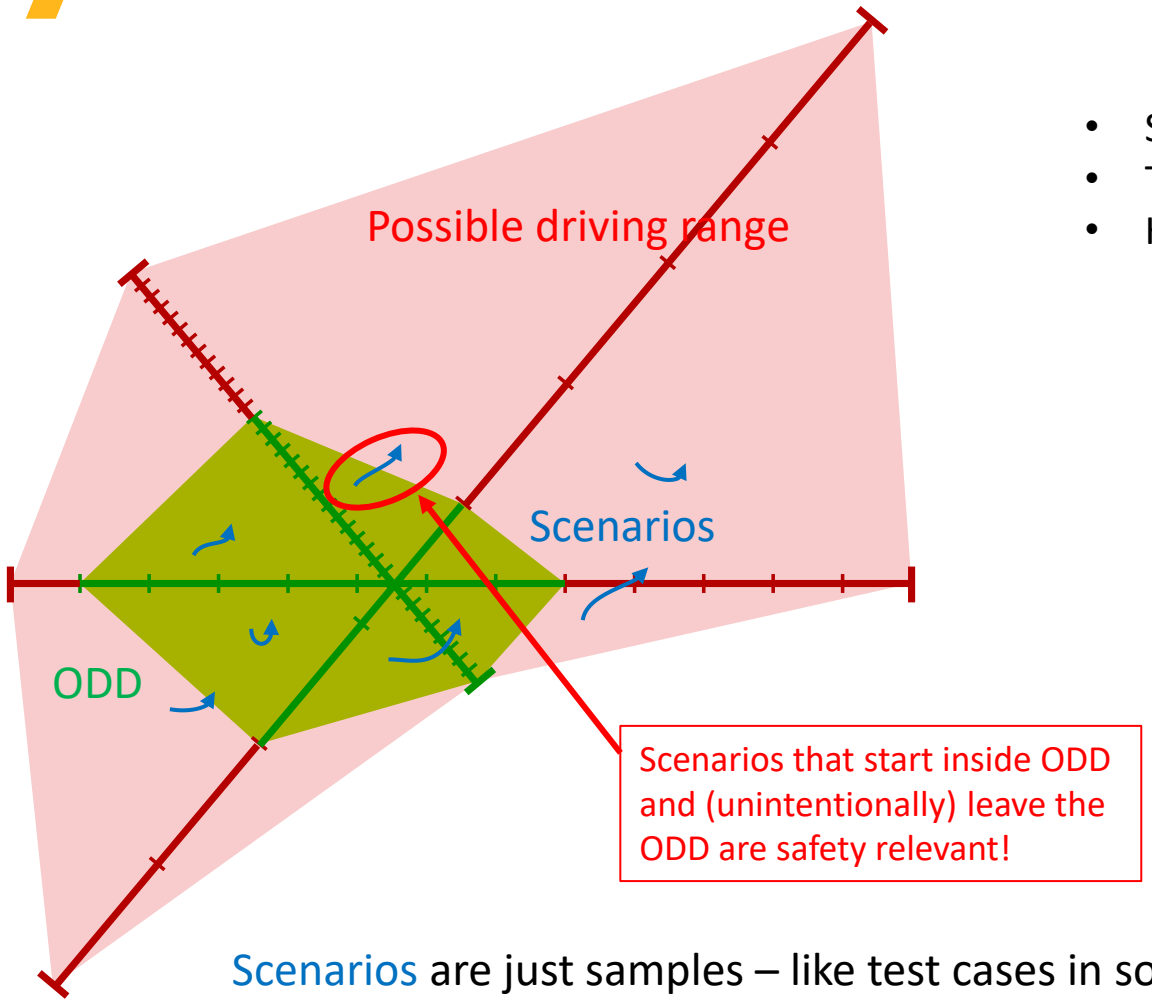
ISO DIS 21448

"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 characteristics."

SAE J 3016

Each axis is one measurable feature or parameter of the operating conditions
Green area delimits the authorized operating conditions (ODD)
Red parts are operating conditions not intended for AD operation (i.e. outside ODD)

How does the ODD relate to scenarios?



- Some people believe that a list of typical scenarios defines an ODD
- This is not correct – scenarios happen in the context of the ODD
- However, there is a close relation between ODDs and scenarios:
  1. The ODD provides the context for the driving/test scenarios
  2. The ODD (and possible situations therein) provides input to the AD function specification – which then serves as the basis (expected behavior of the AD function / pass fail criteria) for the test scenarios
  3. For each scenario it can be checked for each point in time whether the subject vehicle is inside or outside its ODD
  4. Sufficient coverage of the ODD (with all of its aspects, egde cases and rare events) will eventually have to be shown

Scenarios are just samples – like test cases in software testing.
Finally, they must *sufficiently* (i.e. by equivalence classes) cover the whole ODD

Possible Representations of ODDs: Tabular Notations

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	
		Cycle lane	
		Tram lane	
		Emergency la	
		Other special lane	
	Direction of travel	Right-hand tr	
		Left-hand traf	

ODD Definition (based on checklist)

type filter text

Feature / Condition	Value
Target Vehicle Types	Passenger cars up to 8 persons, up to 3 tons gross weight
Applicable Road Types for AD Function	Highways in industrialized countries (forbidden for cyclists and horse carriages etc.)
Vehicle speed range during AD operation	0 ... 80 km/h, only forward direction
Allowable number of lanes for ego vehicle' direction	>= 2
Must have road shoulder for emergency stop?	yes
May have pedestrian sidewalk or cycle lane?	no
Allowable time of day / light conditions during AD operation	daytime, night (no streetlamps)
Allowable weather / visibility conditions during AD operation	visibility not less than 500 m, with reduced speed no less than 100 m (no heavy rain, no dense fog, no heavy snowfall)
Allowable road surface conditions during AD operations	paved road, dry or wet, no slippery conditions (like ice, snow covered, leaves, oil)
VRUs around during AD operation	not in the regular case, but in exceptional cases (after accident / car breakdown, in construction site, illegal walkers etc.)
Opposite traffic around during AD operation	no (solid separation required)
Crossing traffic around during AD operation	no
Traffic lights possible during AD operation	not in the regular case, but in exceptional cases (e.g. drawbridge, tunnel, traffic management scheme, construction site)
Required road infrastructure (e.g. guardrails)	yes (unless there is a solid wall or at least 50 m of lateral free drivable space to the respective side of the road)
Restriction on certain traffic situations (e.g. traffic jam)	not in construction sites where traffic priority is signalled by humans
Excluded behavior of other traffic participants (e.g. vehicle in front backing up must end AD operation)	any vehicle around backing up or not aligning with traffic scheme (e.g. standing crosswise after skidding) must end AD operation.
Excluded situations for AD operation (e.g. construction sites)	not in the proximity of tool plazas and border police barriers
Driver must be constantly supervisiong AD operation	no
Driver allowed to perform side tasks during AD operations	yes
Expected emergency take over time by driver	30 s

Possible Representations of ODDs: Formal Languages

Drivable area

For drivable area type, we allow [motorways, radial roads, distributor roads].
We do not allow [minor roads].

Drivable area lane specification

For lane specification we allow at least [two] lanes with at least [3.7 m] width.
For lane type we allow [traffic lane].
We do not allow [bus lane, cycle lane, tram lane, emergency lane].
For direction of travel, we allow [left hand traffic].

Environmental

For wind, we allow [up to 15 m/s].
For rainfall, we allow [up to 10 mm/h].
For snowfall, we allow [light snow, moderate snow].
For illumination, we allow [day, night, cloudiness, artificial illumination].

Dynamic elements

For agent types, we allow [vulnerable road users, animals, non-motorized agents].

Exceptions

In rainfall we do not allow [motorways].

Formalizing an ODD language requires a syntax definition (grammar) and an ontology (terminology and possible relations between objects)

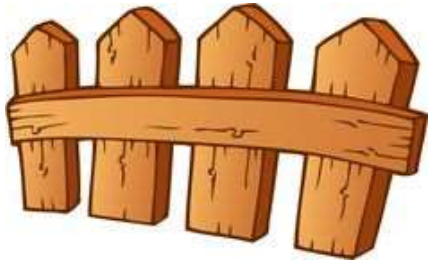
An ODD language can (and should) be human-readable.

The ASAM OpenODD Initiative aims at defining a formal and exchangeable specification format for ODDs.

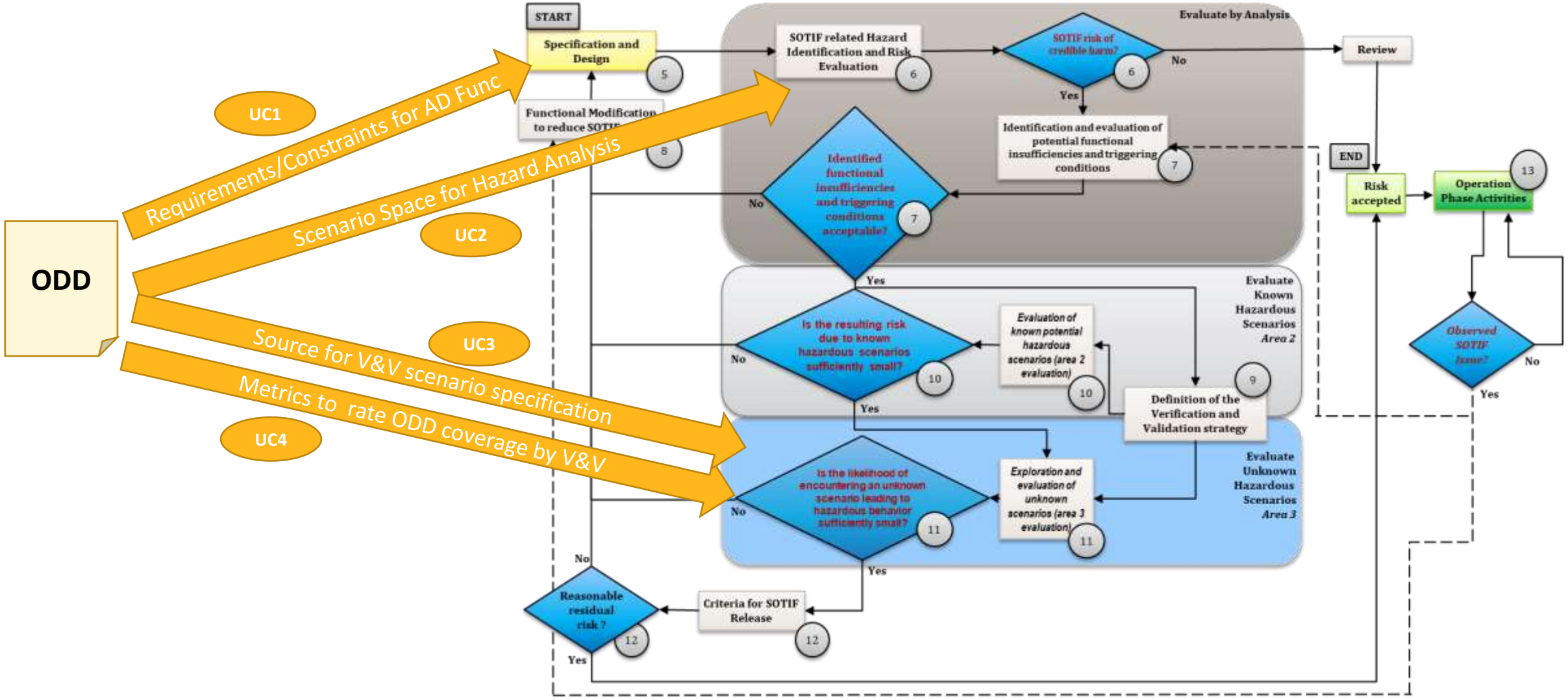
Why a structured definition of ODD is important

- Aspect 1: Know what is in your universe (i.e. everything you have to master)
  - An automated vehicle must be designed and validated to safely operate **under any conditions within ODD**
  - The **remaining risk** of unforeseen conditions that are in the real ODD but not in the specficiation or test cases must be estimated („edge cases“)
  - The ablity to accurately describe **all aspects inside the ODD** (all road types, objects, environmental conditions, expectable maneuvers etc.) is key to an accurate and complete **requirements specification**, **safety analysis** and **test/simulation scnenario set** for the AD function

- Aspect 2: Know where your universe ends (i.e. continuing outside is unsafe)
  - The capability of an automated vehicle to **determine where it is safe to operate and where not**
  - The challenge is that the automated vehicle must detect the ODD edges **onboard** (i.e. onboard sensors, HD maps and self-localization, V2X) and **in real time** to base safety-critical decisions on it
    - E.g. when to forbid activation of a function, when to call for driver-takeover or stop the vehicle, when to modify behavior, e.g. by disabling subfunctions or limiting the speed
  - The ability to accurately describe the conditions that determine **the limits of the ODD** is key to design safe ODD sensing and decision making algorithms, and corresponding test cases to validate these



The significance of the ODD for the SOTIF Process



ODD as Requirements/Constraints for AD Function

UC1

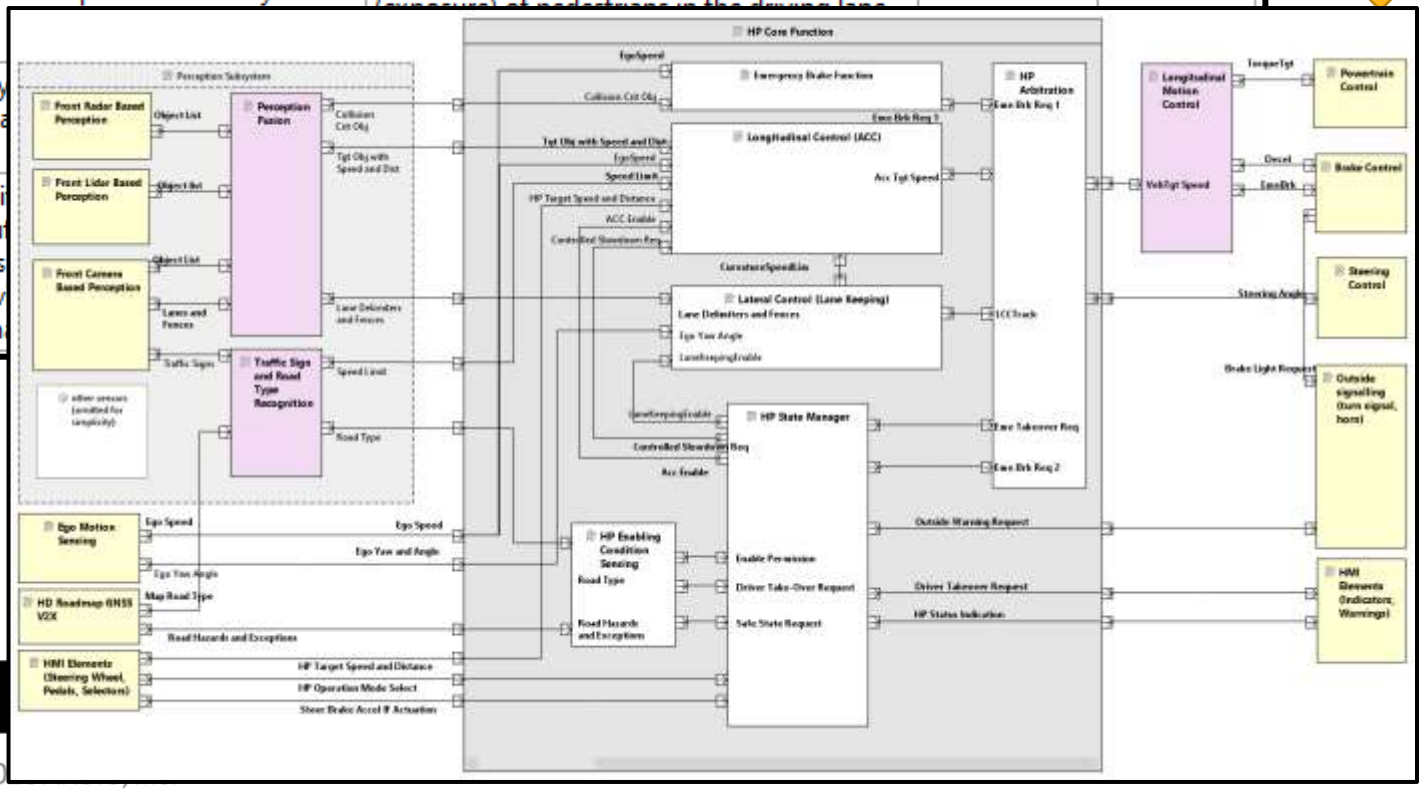
Requirements Editor

type filter text

Name	Description	Comment	Kind	Status
Sensor Range 150 m	To support highway operation at a speed up 120 kph, the sensor set shall be able to perceive a standard vehicle target from a distance of at least 150 m.	Distance is calculated from max speed ac.. ODD based on achievable processing times and brake capabilities.	FUNCTIONAL	PROPOSED
Pedestrian detection capability	To ensure safety of sporadic pedestrians on the highway, the sensor set shall be able to detect standard pedestrian targets from a distance of 150 m with at least 99.9% true positive rate under all specified visibility and weather conditions.	Required true positive rate is calculated from acceptable risk of hitting a pedestrian in the driving corridor and expected occurrence rate	FUNCTIONAL	PROPOSED
Ability to work at night	To support operation at any time of the day suitable sensors to detect vehicles, people a distance range even at night.			
	To support operation under reduced visibili shall be able to guarantee su vehicles, people and obstacles ility conditions with > 50 m v is not greater than [speed_m			

ODD

Aspect	Value Range
Road types	Highway
Speed range	<= 120 kph
Time of day	any
Visibility	>= 50 m
Pedestrian	sproradicly



Requirement with regard to „Leaving the ODD“

UC1

ODD Example

Highway Pilot is only allowed
- On highways
- At bright daylight

Scenario Example

- I‘m driving through the city
- I‘m entering a highway
- I‘m switching on Highway Pilot
- After 2 h, it starts to get dark

Danger!
Leaving ODD!

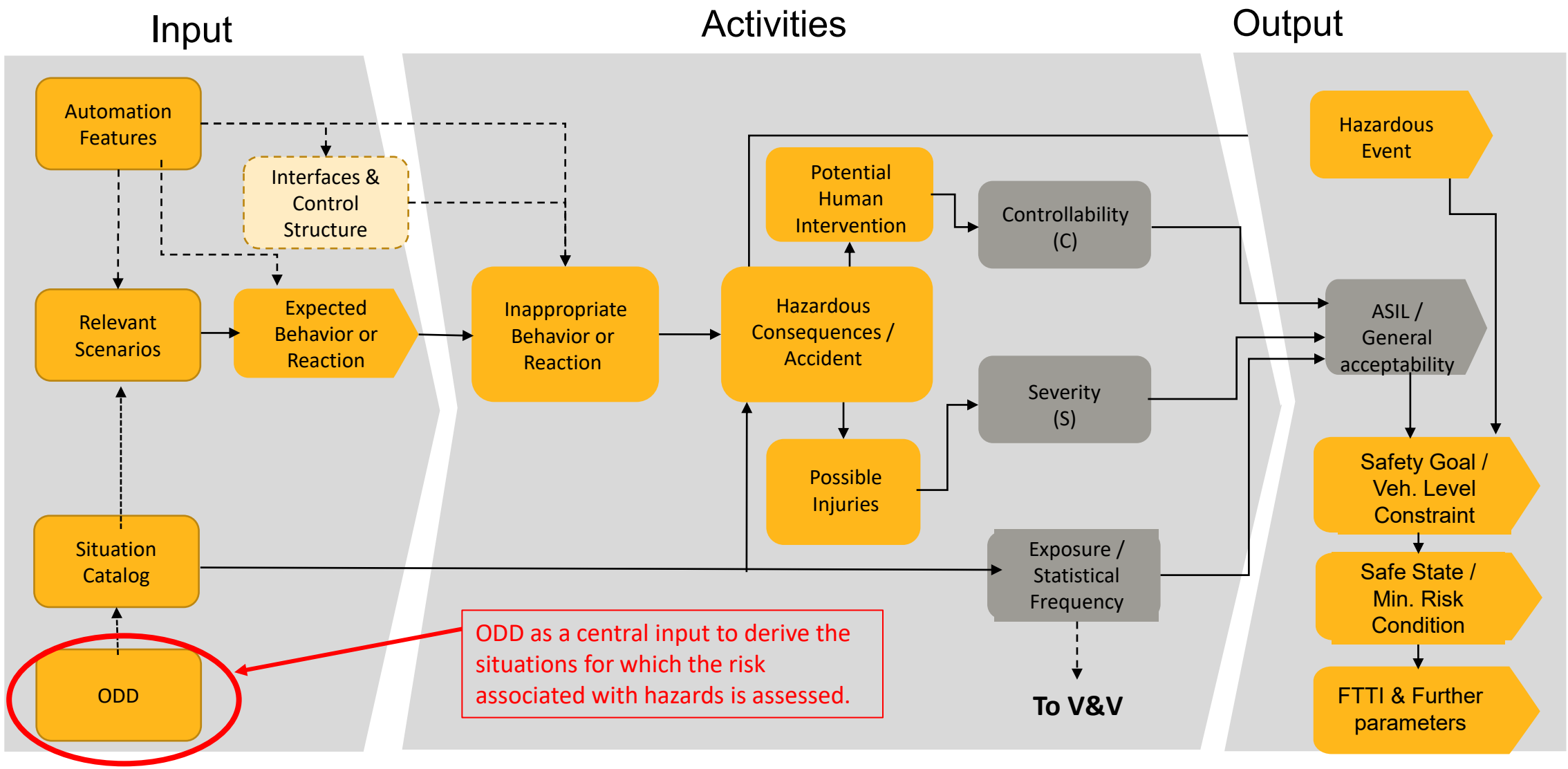
Requirements Editor

type filter text

N°	ID	Name	Description	Comment	Kind	Status
1	REQ010	Function abort on declining light conditions	The AD function shall continuously monitor if the exterior light conditions fall below 1000 lx and in this case prompt the driver to take over control.	Acc. to ODD the function is specified for daytime only, so supposedly the sensors won't work with the required accuracy and reliability if light conditions are worse than that. So we need to recognize at runtime that we are leaving the safet ODD, and safetly abort the AD function in this case.	FUNCTIONAL	PROPOSED

HARA Procedure for Highly Automated Driving (Level 3 - 5)

UC2



ODD as Scenario Space for Hazard Analysis

UC2

Operational Situations Catalogs

Select a catalog in the upper table and define its details in the lower table!

type filter text

Operational Situations Catalogs

Basic Driving Situations

type filter text

Additional Exposure Parameter for Risk Assessment

Location	tem Usage	Vehicle Speed	Traffic and People	Road Conditions	Environment	pecific Details	Exposure	Exposure Comment	Exposure I
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	typical motorway speed (<=130 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	dry	daylight, clear visibility		E4	>10 % of average operating time	Duration
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	typical motorway speed (<=130 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	dry	night (with streetlamps or some remaining light) or dusk/dawn, clear visibility		E4	>10 % of average operating time	Duration
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	speed adapted to weather conditions (<= 50 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	dry	reduced visibility (e.g. dense fog, heavy rain)		E2	<1 % of average operating time	Duration
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	typical motorway speed (<=130 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	wet	daylight, clear visibility		E4	>10 % of average operating time	Duration
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	typical motorway speed (<=130 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	wet	night (with streetlamps or some remaining light) or dusk/dawn, clear visibility		E4	>10 % of average operating time	Duration
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	speed adapted to weather conditions (<= 50 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	wet	reduced visibility (e.g. dense fog, heavy rain)		E2	<1 % of average operating time	Duration
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	speed adapted to weather conditions (<= 50 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	slippery, (partially) covered with snow or ice	daylight, clear visibility		E2	<1 % of average operating time	Duration
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	speed adapted to weather conditions (<= 50 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	slippery, (partially) covered with snow or ice	night (with streetlamps or some remaining light) or dusk/dawn, clear visibility		E2	<1 % of average operating time	Duration
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	speed adapted to weather conditions (<= 50 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	slippery, (partially) covered with snow or ice	reduced visibility (e.g. dense fog, heavy rain)		E2	<1 % of average operating time (Note: snow/ice and bad visibility are not independent, so no further reduction)	Duration
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	very fast (> 130 km/h and <180 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	any	any		E2	<1 % of average operating time (for Germany E3 may be appropriate)	Duration
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	extremely fast (> 180 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	any	any		E1	insignificant fraction of overall driving (Only relevant for specific vehicles and specific countries)	Duration
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	typical motorway speed (<=130 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	dry	any	erson standing / walking / tepping on road / driving lane	E1	Occurs less often than once a year for the great majority of drivers (pedestrians are illegal on motorways - for roadworkers see separate case)	Frequency
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	typical motorway speed (<=130 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	wet	any	erson standing / walking / tepping on road / driving lane	E1	Occurs less often than once a year for the great majority of drivers (pedestrians are illegal on motorways - for roadworkers see separate case)	Frequency

ODD as Scenario Space for Hazard Analysis

Combinatorial Explosion – Keeping the HARA manageable

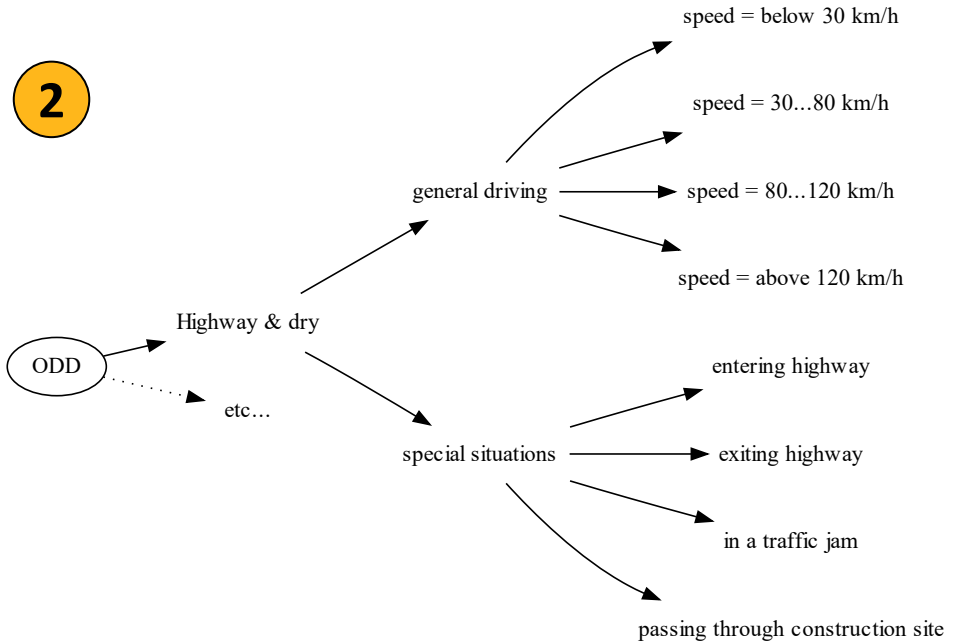
UC2

1

		Weather		
		dry	rainy	icy
Road Type	City Street			
	Country Rd			
	Highway			

+

2



+

3

Decoration:

- Bridge
- Tunnel
- Guardrails
- Traffic Signs

Explicit List of Extra Decoration

Exceptional situations:

- emergency braking
- animal on highway
- fallen motorcyclist

Full factorial of a few basic features (e.g. road type)

Unbalanced refinement for more details, as appropriate (where not needed put: „any“)

On-demand addition / or separate analysis of special or rare side conditions

Ansys

Hazard Analysis (FuSa & SOTIF) based on Situation Catalog

UC2

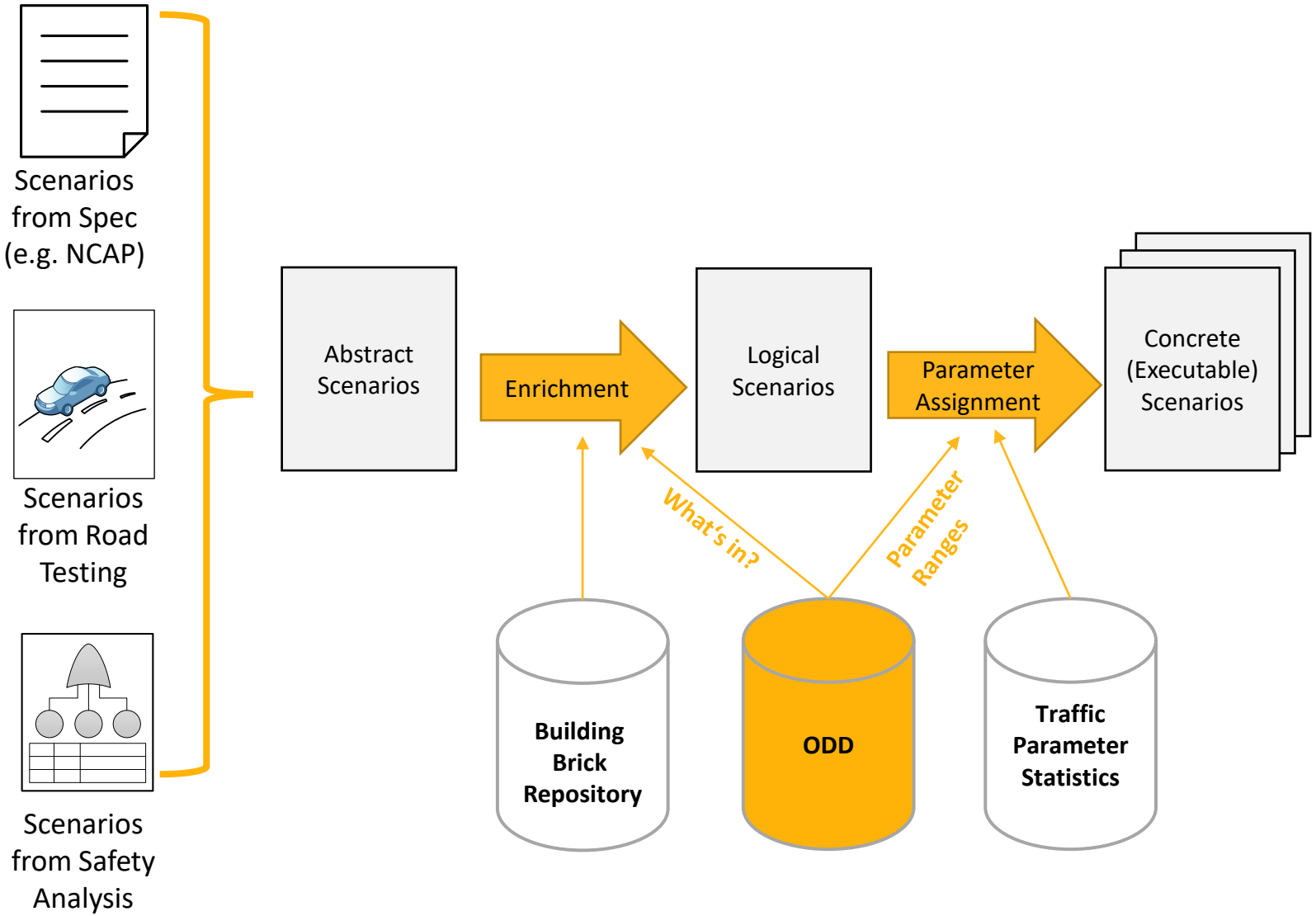
FuSaSOTIF HARA Longitudinal Control (Excerpt) Note: table layout changes will not be persisted in this read-only editor

type filter text

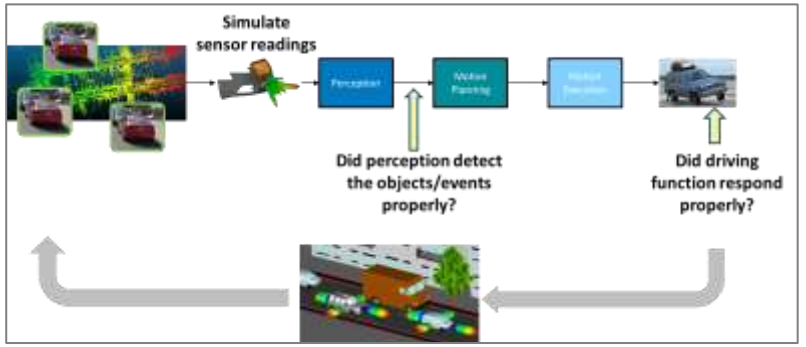
Location	Item Usage	Vehicle Speed	Traffic and People	Road Conditions	Environment	Specific Details	In ODD	Automation active	Expected Behavior	Malfunctioning Behaviour	Hazard
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	typical motorway speed (<=130 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	dry	daylight, clear visibility		yes	yes	Keep distance to predecessor vehicle Keep speed	[MF41] Driving at too close distance to predecesor	[H3] Collision or danger short distance to motor
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	typical motorway speed (<=130 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	dry	daylight, clear visibility		yes	yes	Keep distance to predecessor vehicle Keep speed	[MF49] Unjustified emergency braking	[H1] Unjustified Strong Deceleration (rear collisi
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	typical motorway speed (<=130 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	wet	daylight, clear visibility		yes	yes	Keep distance to predecessor vehicle Keep speed	[MF41] Driving at too close distance to predecesor	[H3] Collision or danger short distance to motor
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	typical motorway speed (<=130 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	wet	daylight, clear visibility		yes	yes	Keep distance to predecessor vehicle Keep speed	[MF49] Unjustified emergency braking	[H1] Unjustified Strong Deceleration (rear collisi
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	speed adapted to weather conditions (<= 50 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	wet	reduced visibility (e.g. dense fog, heavy rain)		yes	yes	Keep distance to predecessor vehicle Keep speed	[MF41] Driving at too close distance to predecesor	[H3] Collision or danger short distance to motor
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	very fast (> 130 km/h and <180 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	any	any		no	no	Be passive (don't influence any actuator)	[MF49] Unjustified emergency braking	[H1] Unjustified Strong Deceleration (rear collisi
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	typical motorway speed (<=130 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	dry	clear visibility (day or night)	vehicle in front performs strong braking maneuver o is involved in accident / loss of control	yes	yes	Perform Emergency Braking	[MF50] Failing to brake (strong and timely enough) for collision-critical motorvehicle	[H3] Collision or danger short distance to motor
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	speed adapted to weather conditions (<= 50 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	wet	reduced visibility (e.g. dense fog, heavy rain)	vehicle in front performs strong braking maneuver o is involved in accident / loss of control	yes	yes	Perform Emergency Braking	[MF50] Failing to brake (strong and timely enough) for collision-critical motorvehicle	[H3] Collision or danger short distance to motor
motorway / divided road	general driving (includes moderate accelerating, braking and curves)	typical motorway speed (<=130 km/h)	light or dense motorway traffic (cars, trucks, busses, sporadic motorcycles)	dry	daylight, clear visibility	Unexpected obstacle (e.g. rock, lost cargo) or big animal on driving lane	yes	yes	Perform Emergency Braking Evade / Change lane if possible	[MF52] Failing to brake (strong and timely enough) for collision-critical solid object	[H4] Collision with solic on driving lane or nearb

ODD as a source for SOTIF V&V scenario specification

UC3

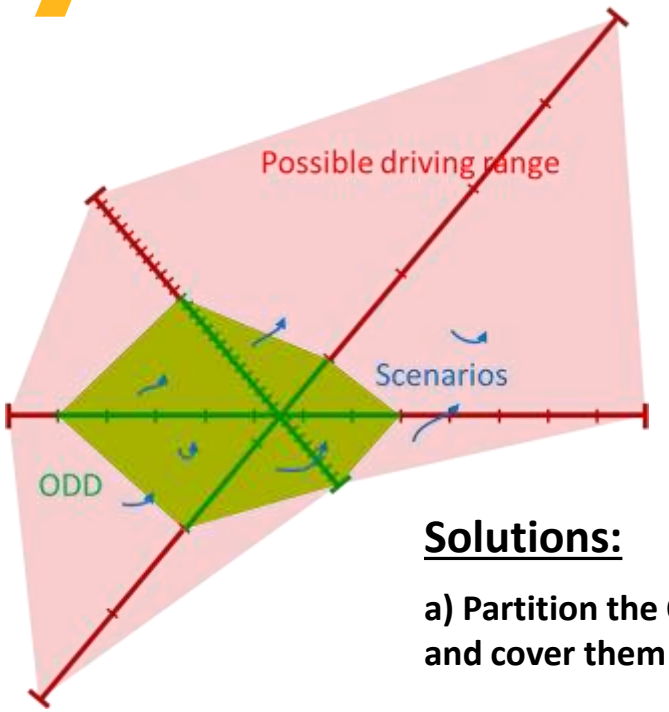


Simulation Environment with SuT



How to measure coverage of the ODD with test scenarios?

UC4

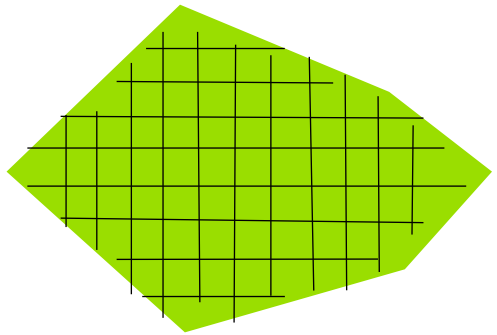


- Scnenarios are similar to test cases in software testing:
  They sample just a few representatives from a large and dense input space
  - The ODD has a huge combinatorics of enumerative attributes.
  - The ODD also contains attributes from continuous value space (e.g. lane width).
- Scenarios are „infinitely thin lines“ – even a large number of them cannot really cover the ODD

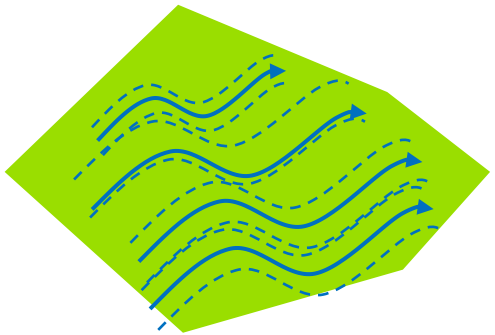
=> A notion of *sufficient coverage* must be found (i.e. risk of overlooked hazardous scenario sis acceptably low)

Solutions:

a) Partition the ODD into equivalence classes and cover them with representative scenarios



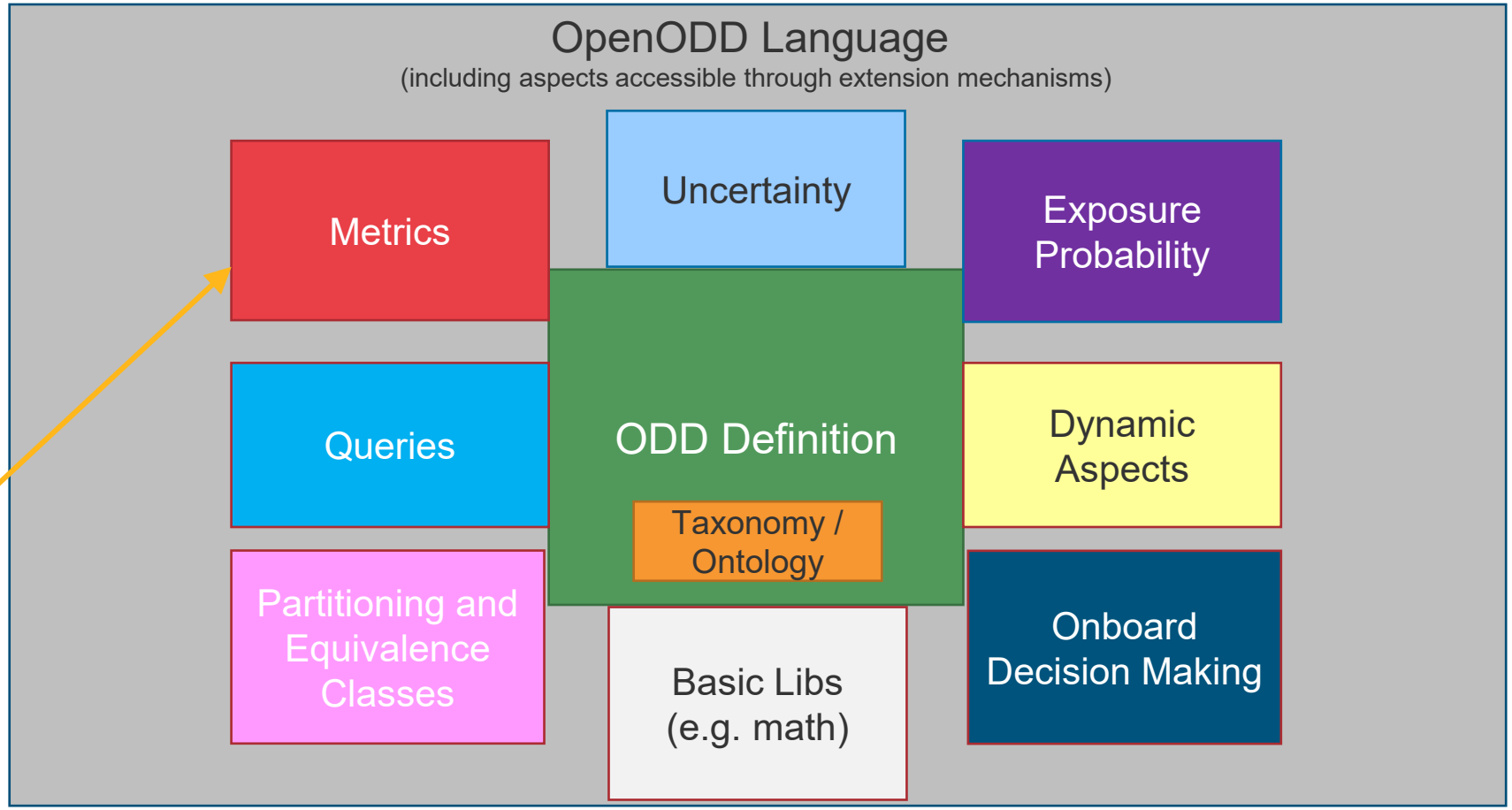
b) Use logical scenarios that cover a range of values for each parameters and vary them



Risks:
- Missing egde cases / „black swans“
- Strongly nonlinear behavior of ML

Metrics to rate ODD coverage by V&V scenarios

UC4



Metrics are not restricted to metrics about ODDs.
Also in scope: metrics about how well an ODD is covered by a set of test scenarios

Summary

- Safety (FuSa, SOTIF, etc.) are a key property of AD functions to be accepted by the society
- Safety processes (e.g. ISO 21448) require a variety of activities
- Many of them are based on a stringently defined ODD
- Examples:
  - Specification of Requirements, design of architecture and algorithms based on the ODD
  - Situation catalog for Hazard Analysis based on the ODD
  - ODD as an important source for deriving concrete V&V scenarios for test and simulation
  - Coverage metrics to enable to judge test completeness and residual risk
- ASAM OpenODD will provide a notation for ODDs and related information, e.g. metrics about ODDs