PROJECT of the PEGASUS FAMILY

VERIFICATION VALIDATION METHODS

Final Event 21 / 22 November 2023

The VVM Overall Methodology

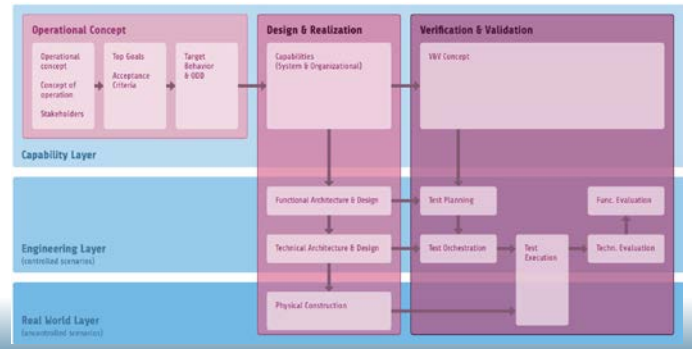
Helmut Schittenhelm, Mercedes-Benz

Supported by:

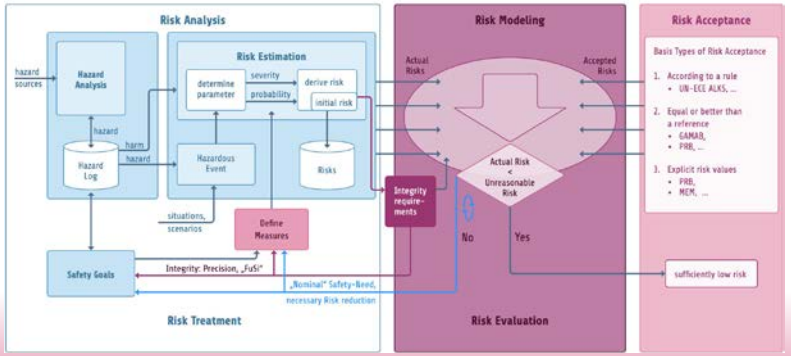
Federal Ministry for Economic Affairs and Climate Action

on the basis of a decision by the German Bundestag

Solution: Assurance Framework

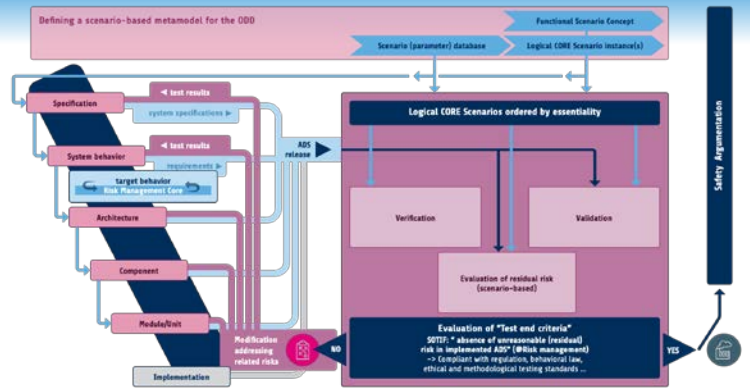


Develpment & Operation | Global

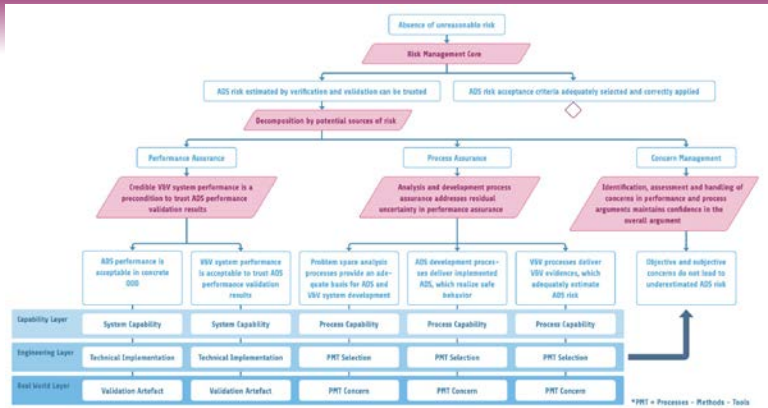


Risk Management

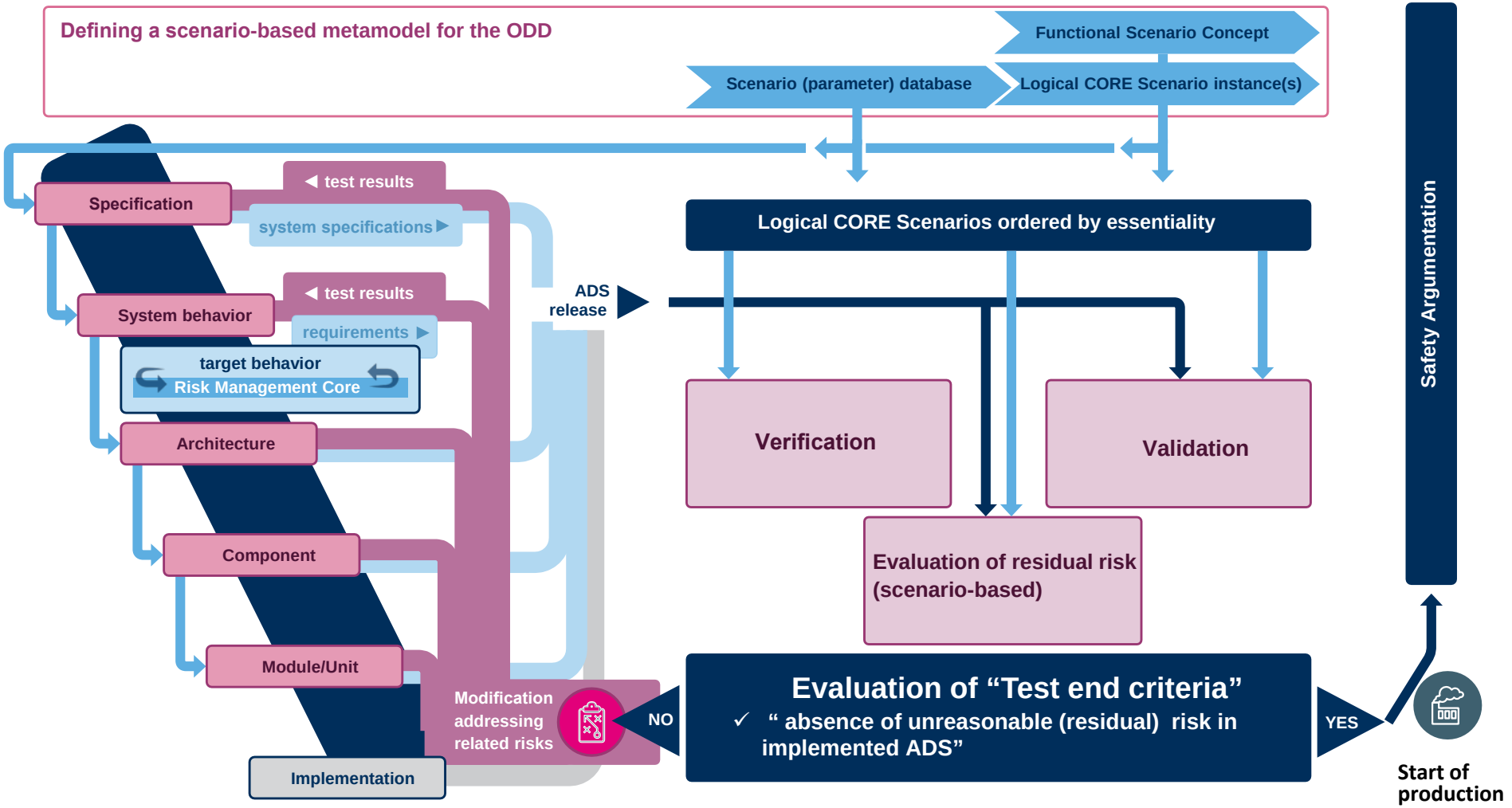
Develpment & Operation | Scenarios



Argumentation



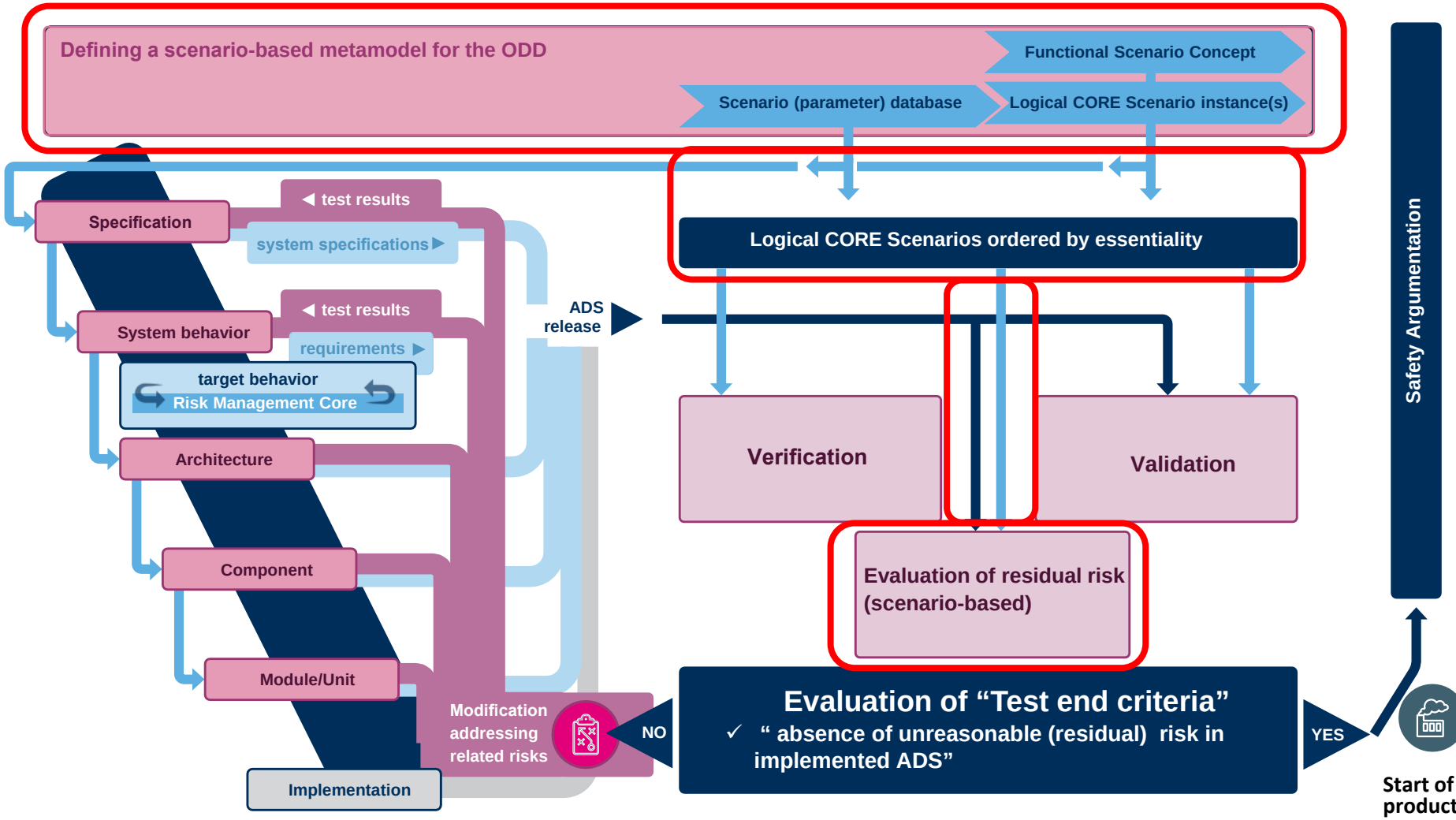
“Development & Operation “ | Scenario



VERIFICATION
VALIDATION
METHODS

Initial Situation: PEGASUS

“Development & Operation “ | Scenario – PEGASUS VIEW



Methodical Steps: PEGASUS

ODD-model:

- 6 Layer Scenario model,
- Set of Logical Scenarios

Testing:

- Scenario-based testing with risk evaluation in V&V

use of test instances:

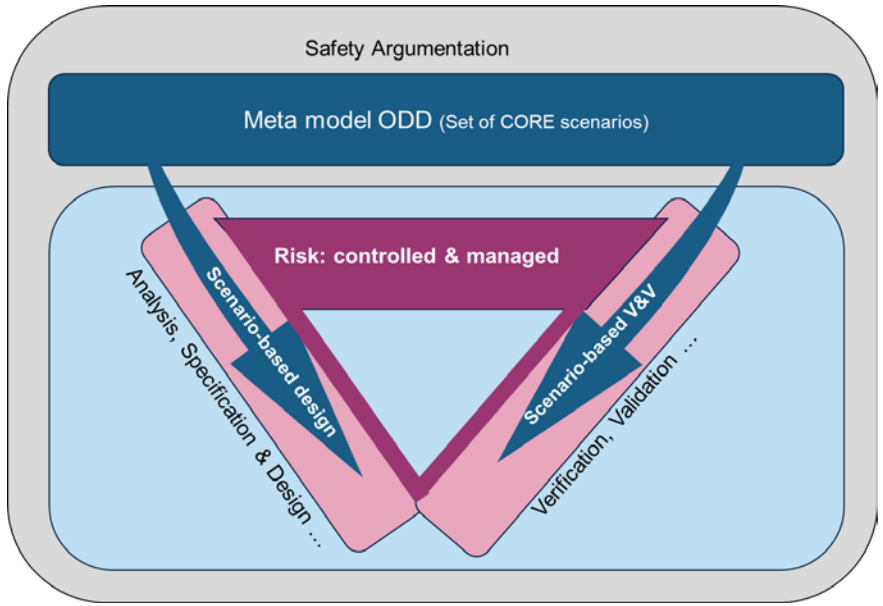
- simulation first,
- PG confirms simulation,
- endurance run assures stochastic aspects & complex situation, Task: finding “surprises”

- GSN-based argumentation

Basic idea

VVM extends the PEGASUS Approach with a holistic view of the development process and integrates elements included in current standards

- **Early alignment of the artifacts and requirements** that hold to them which the safety argumentation demands and the way they are built as requirements in the design and later provided as evidence through the validation and verification process (Argumentation–based V&V)
- **Controlled & managed risk** (derived from top safety goals) broken down in the design (to system behavior and components) controlled in the V&V process
- **Use of strategies that specifically rely on decomposition in development and V&V** in order to be able to specify behavior and limits of system and components in a systematic manner as well as to be able to evaluate and prove them
- **Consistent use of a sufficiently complete Metamodel for the ODD** and a scenario database as a tool providing exposure in the system design as well as in the V&V process



VERIFICATION
VALIDATION
METHODS

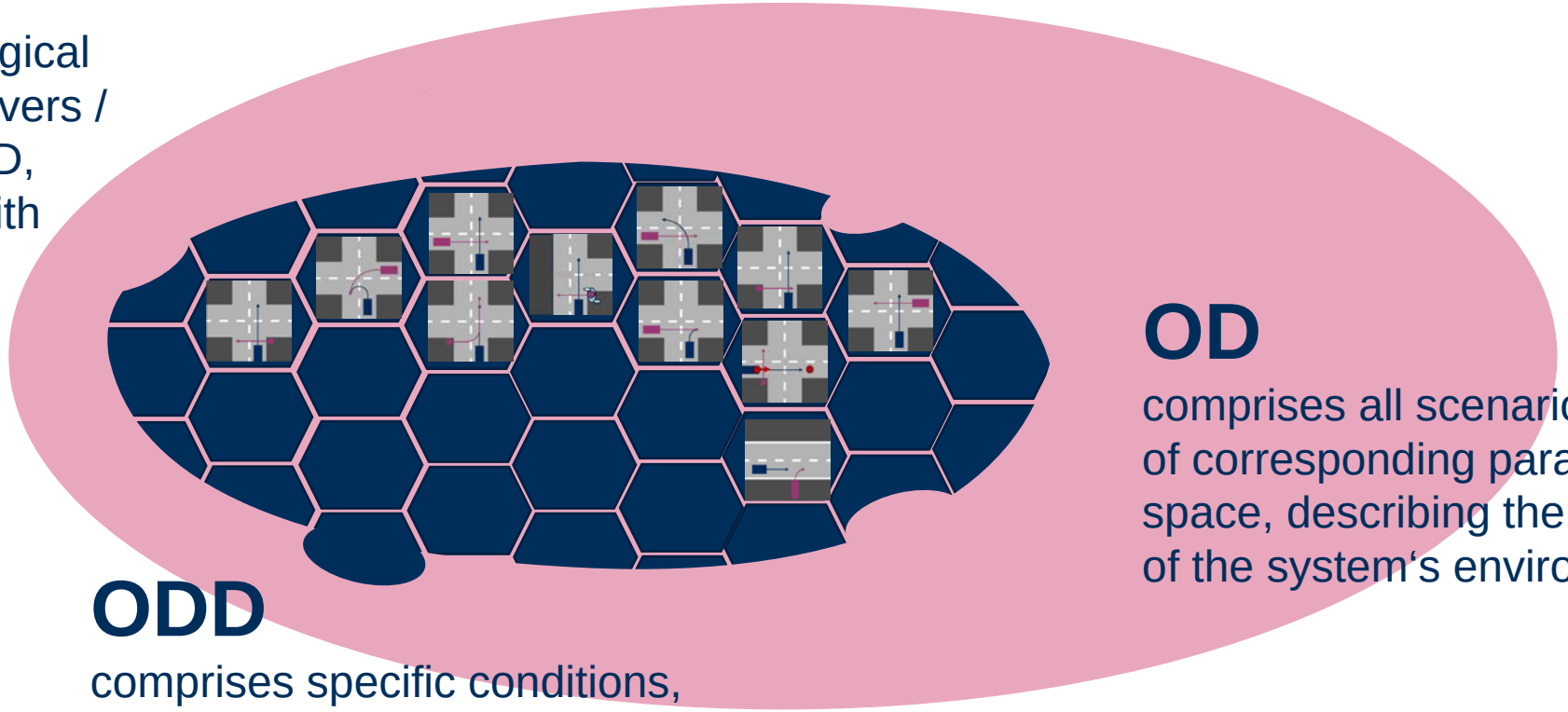
Scenario, OD, ODD Metamodel

Defining an ODD Metamodel – a sufficient complete coverage

The set of logical CORE scenarios is defined as a set of logical scenarios that have certain properties:

- Minimum set of logical scenarios, that covers / represent the ODD,
- Free of overlap with the underlying BASE scenarios,
- …

- **The Operational Domain OD can be the Full World or a Subset**



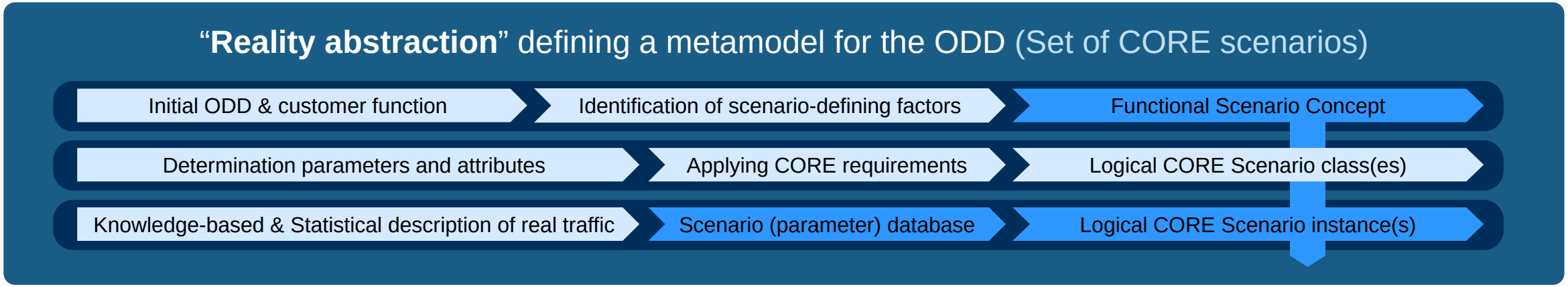
OD

comprises all scenarios of corresponding parameter space, describing the context of the system‘s environment …

ODD

comprises specific conditions, ADS is designed to function

- A **logical scenario class** is created out of a logical scenario by defining / declaring **relevant parameters.**
- A logical scenario class becomes an **instance** when the **parameters of the class have value ranges defined** or have been instantiated.



- The ODD Metamodel consist of:
  1. Set of functional scenarios,
  2. Set of logical CORE Scenarios,
  3. Scenario (parameter) Data-Base

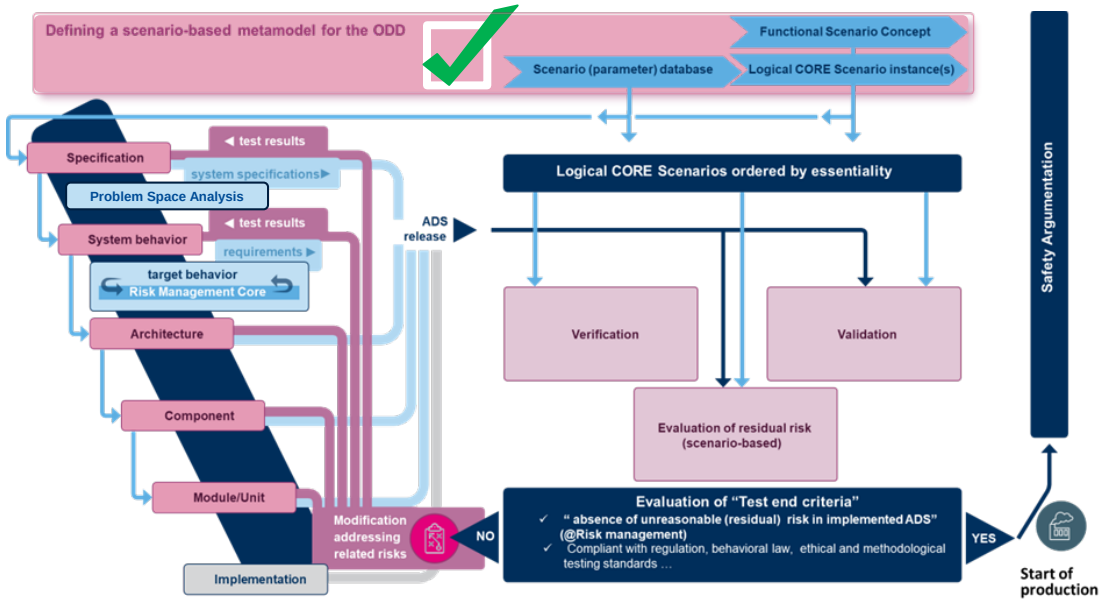
VERIFICATION
VALIDATION
METHODS

Additional Elements in ADS-Design

Things to add to the design process –
for managing risk and keeping it below an accepted level

Three Things are added in the Design Process:

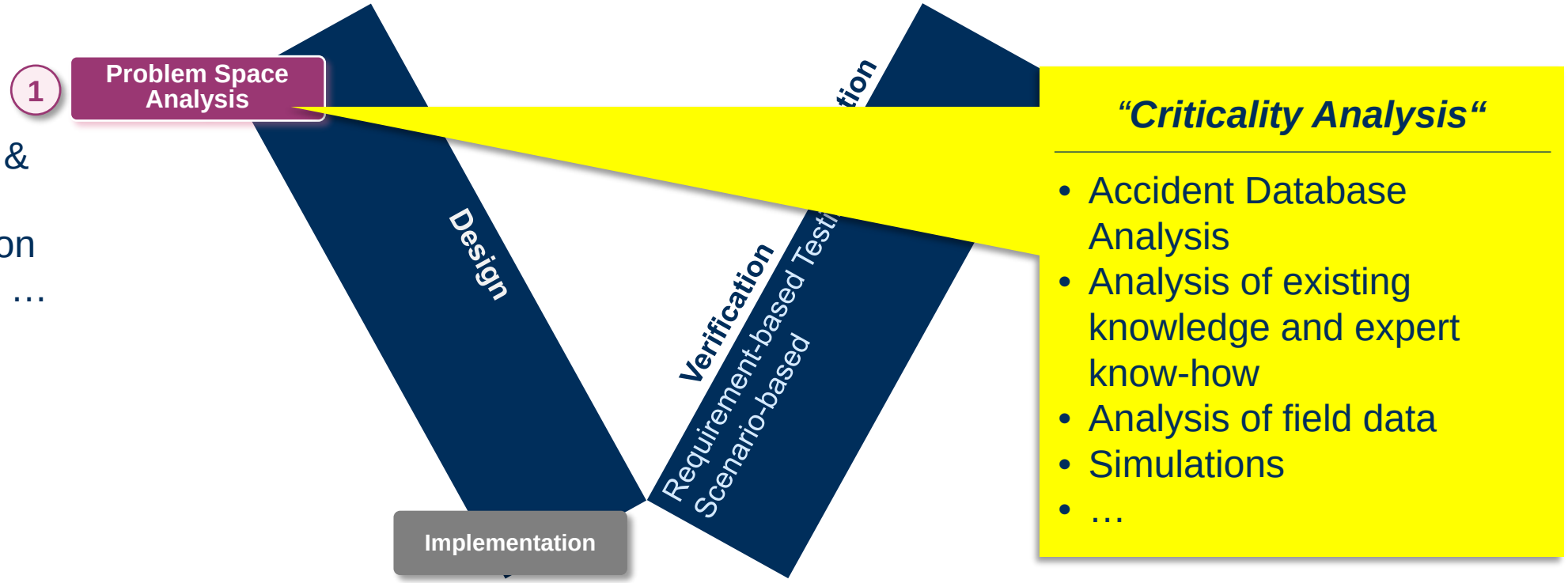
- The **ODD Metamodel**
- The **Problem Space analysis** gives a deep understanding of the problem space and is basis for the SOTIF hazard and risk analysis and definition of safety goals.
- The **Risk management Core** (RMC) is added because it defines a process framework for managing risk.



Overall Methodology

- … Problem Space Analysis …

  … basis for SOTIF hazard & risk analysis and for definition of safety goals …

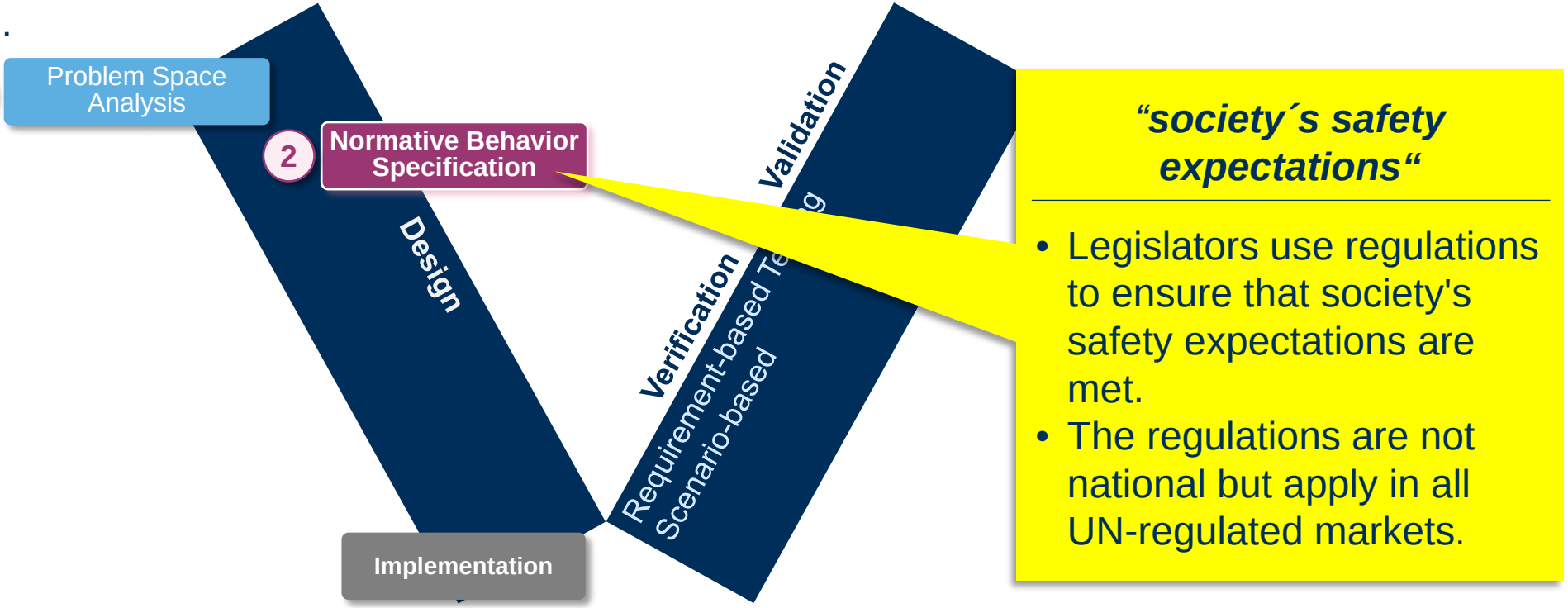


… a systematic **Analysis of the Problem Space** provides the basis for a **deep understanding of the operational environment** and identifies the **dominant characteristics**, **risks, relationships and scenario** classes that are **relevant to the safe operation** of an automated driving system…

Overall Methodology

- … normative System Behavior…

… Compliance with certification, legal, society´s, and ethical expectations…



"society´s safety expectations"

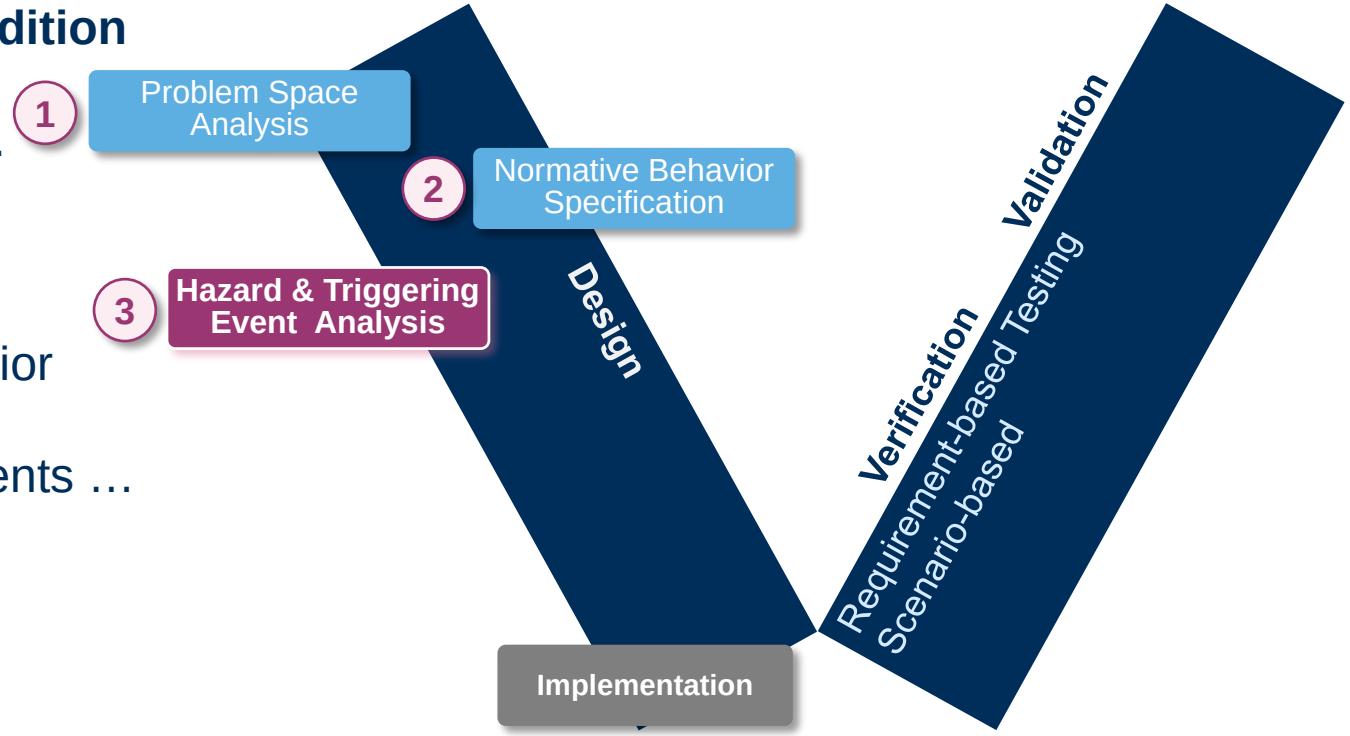
- Legislators use regulations to ensure that society's safety expectations are met.
- The regulations are not national but apply in all UN-regulated markets.

… during the specification of the **normative system behavior**, a set of requirements is defined. These requirements represent the legal (e.g. behavioral law), societal, and ethical expectations regarding the automated driving system. Clear definitions of the boundaries of ADS behavior with respect to these constraints are defined …

Overall Methodology

- … Hazard and triggering **Condition** Identification and Analysis…

  … Basis for designing System Behavior to cover all hazardous Events …

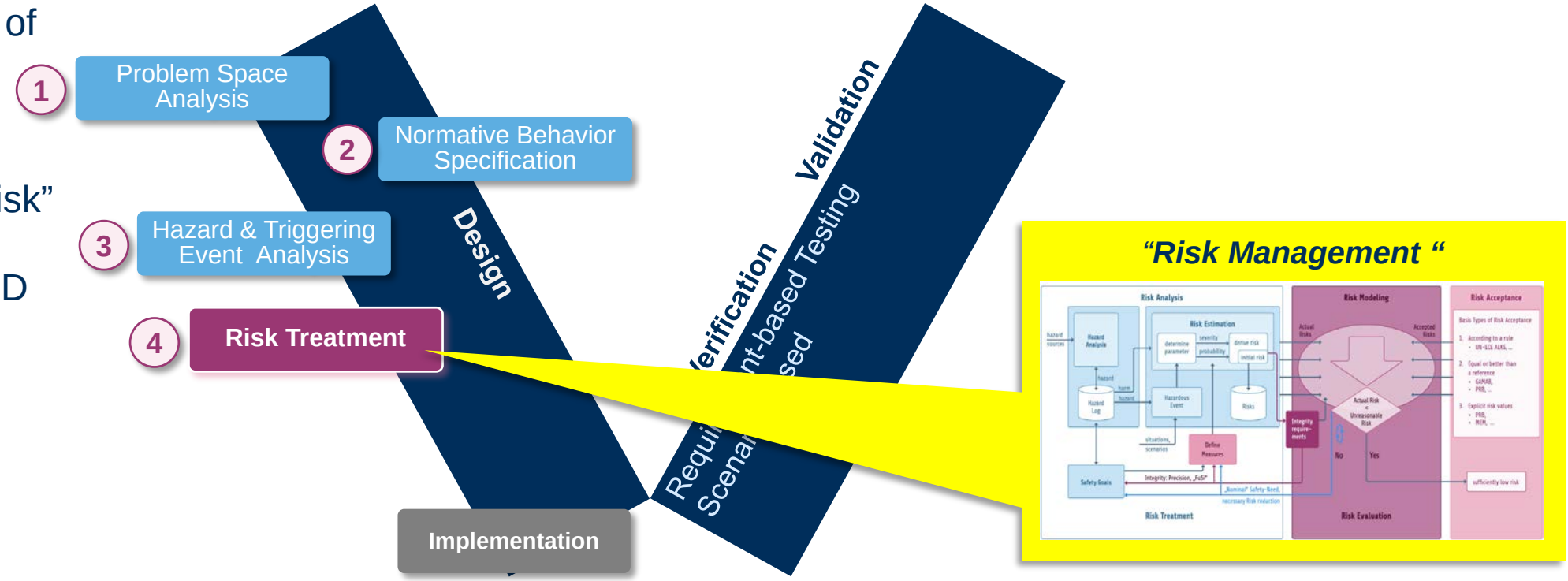


… based on the ODD Metamodel and an understanding of the proposed customer function, a **systematic hazard and risk identification and analysis** is performed for SOTIF. This includes a consideration of a failure in the function together with a systemic view of intrinsically hazardous conditions within the interaction between the ADS equipped vehicle and its environment that need to be avoided….

Overall Methodology

- … Management and treatment of Risk …

  … ensures “acceptable Risk” within System Design for ODD Metamodel…



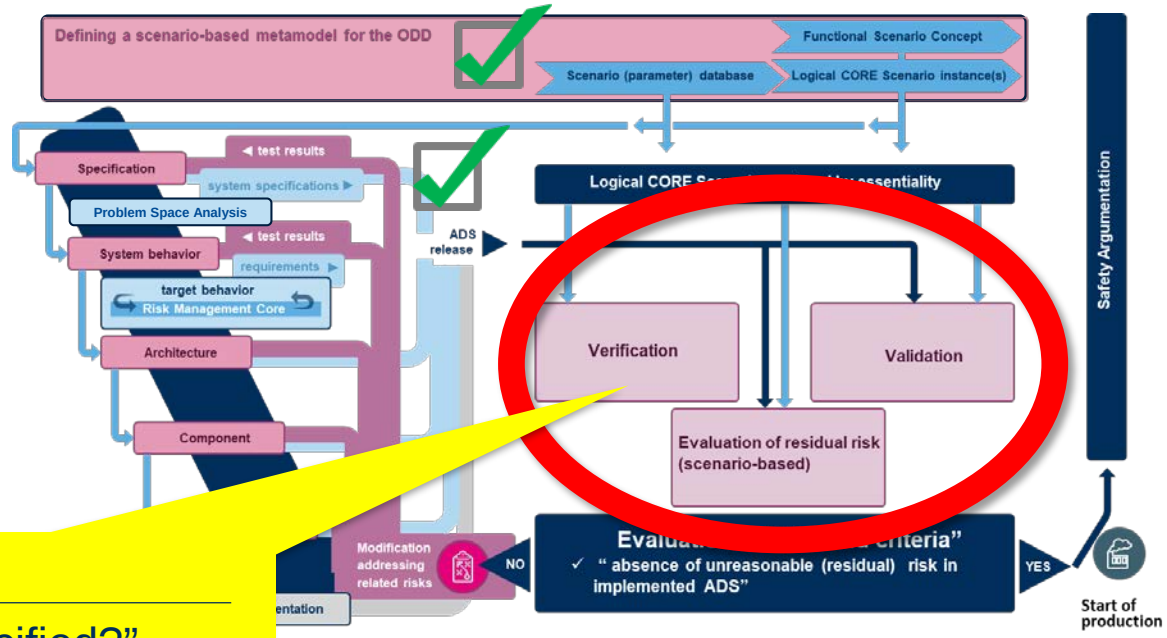
… In risk management, **safety measures are defined that result in an acceptable residual risk for the automated driving system in hazardous events systemically identified in CORE scenarios and their triggering conditions**.
For this purpose, the "Risk Management Core" (RMC) is proposed as a process tool.
The RMC is an iterative process for aligning actual risk with accepted risk using safety measures. …

Things to add to the V&V process
for delivering evidences that the safe behavior could be argued ...

VERIFICATION
VALIDATION
METHODS

Three Things are added in the Design Process:

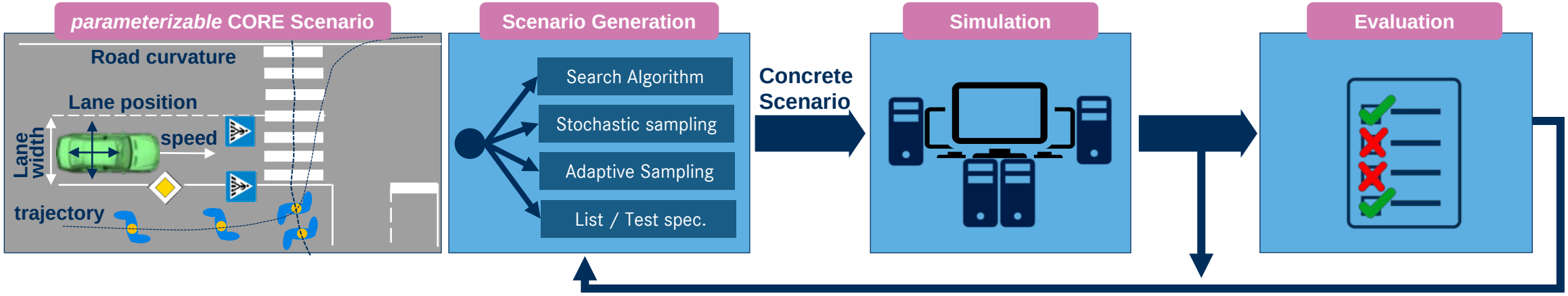
- The **ODD Metamodel** is added, allowing "Validation & Verification on the same ODD Metamodel as Hazard and Risk Analysis and System Design".
- The **Evaluation of the Residual Risk** is added, while it is essential to prove that the system behaves safely in its ODD.
- The **V&V concept** gets an additional focus on an assurance related organization of V&V.



"Scenario based"

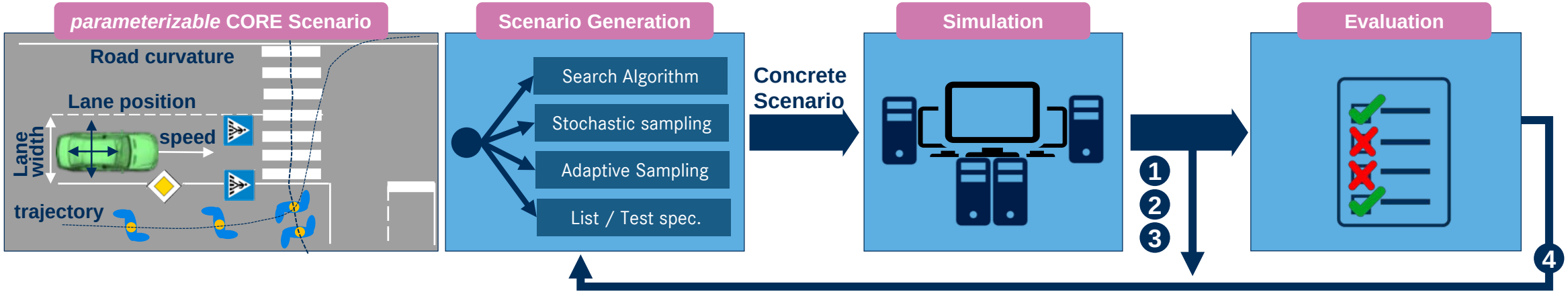
- **Verification**: "Implemented as specified?"
- **Validation:** "Specified correctly / sufficiently?"
  "Stakeholder approval available?"
- **Evaluation** of Residual Risk "Safe enough?"

Scenario-based Testing - different characteristics, one approach



	Requirement-based Testing	Adaptive Sampling Testing	Monte Carlo-based Testing	Search-based Testing
Generation of sets of parameter for parametrize concrete scenarios	Concrete scenarios for fixed parameters, Requirement-based Scenario Creation	predefined plan for Sampling, systematic coverage of parameter Sub-space	Random sampling of the parameter space (open sampling loop)	Optimizer algorithm samples parameter space (closed sampling loop)
Number of scenarios	few	some *up to* large	(very) large	immense
Parameter distributions from real-world	-		Parameter distribution (Scenario Data-Base)	Parameter distribution (Scenario Data-Base)
Used in / for	Verification (of Requirement in related scenario)	Verification (of Requirement in related scenario)	Exploration of *unsafe* (areas of) unknowns	Residual Risk evaluation

Scenario-based Testing - fields of application

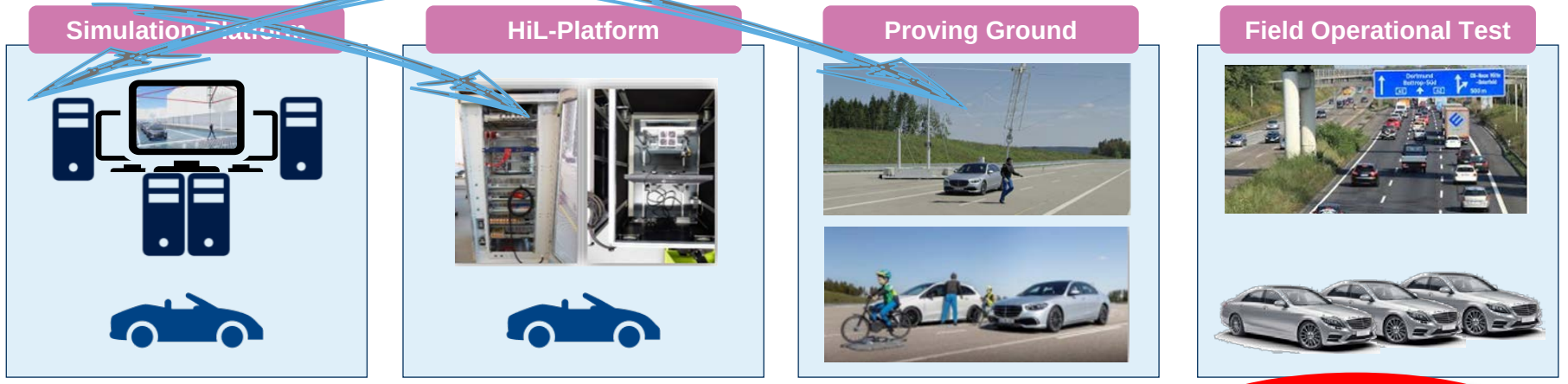


Test Object | Platform	SIL	HIL	Proving Ground	Field Operational Test
Sense: Perception	-	(X)	X	X
Sense: Fusion	X	X	X	X
Plan: behavior	X	X	X	X
Sense / Plan / Act	X / X	X	X	X
Type of use	scenario-based closed loop tests scenario-based with random traffic closed loop	scenario-based open and closed- loop & integration tests	scenario-based open and closed- loop tests with ADS equipped vehicles	random real-world closed loop

Coordinated collaboration of test platforms for scenario-based testing

“Shift to Simulation”

Seamless exchange of Test Cases



Test Objective | Platform	SIL	HIL	Proving Ground	Field Operational Test
Scenario-based testing				
Validation	becoming increasingly important for **ADS driving strategy**	Especially for Components		

Workhorse for mass processing

becoming increasingly important

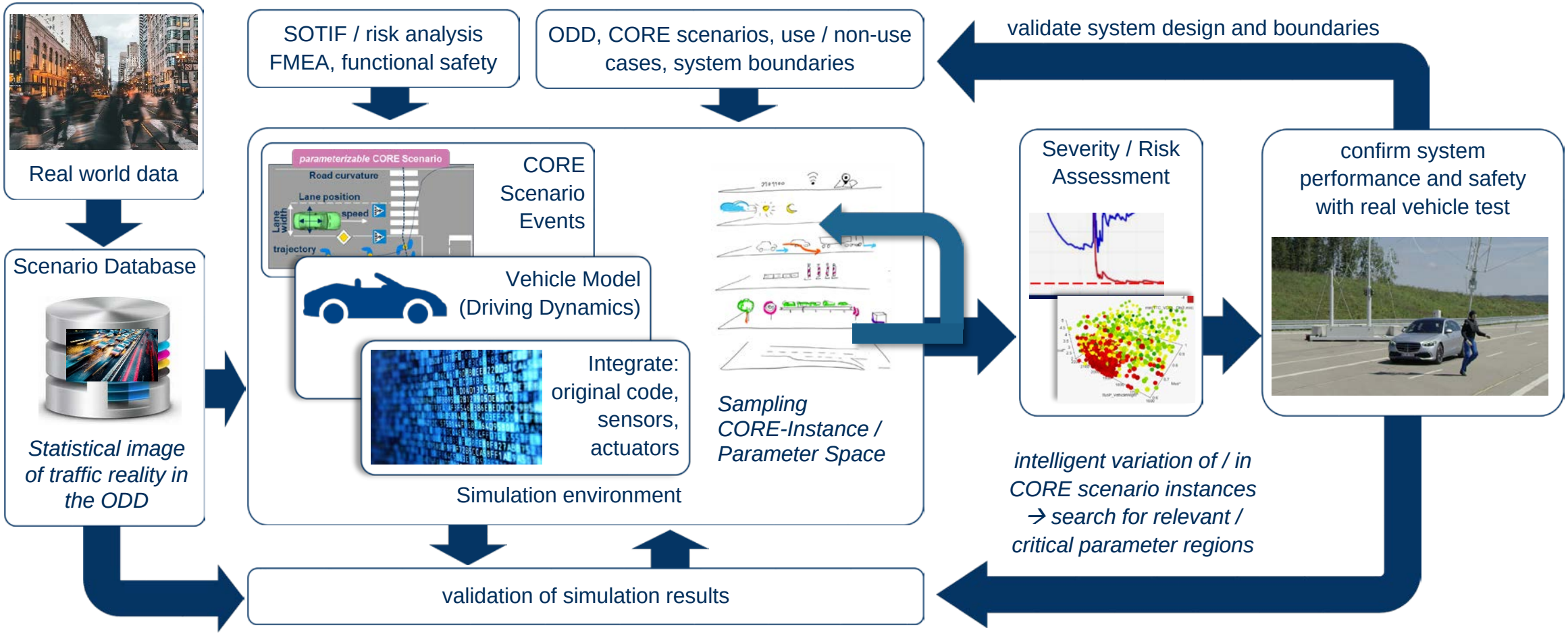
Specialist for confirming simulation results

Strategy to build equivalent class & selecting representants for CHECKING Simulation results

Test objective:
“Specified correctly / sufficiently?”
“Stakeholder approval available?”

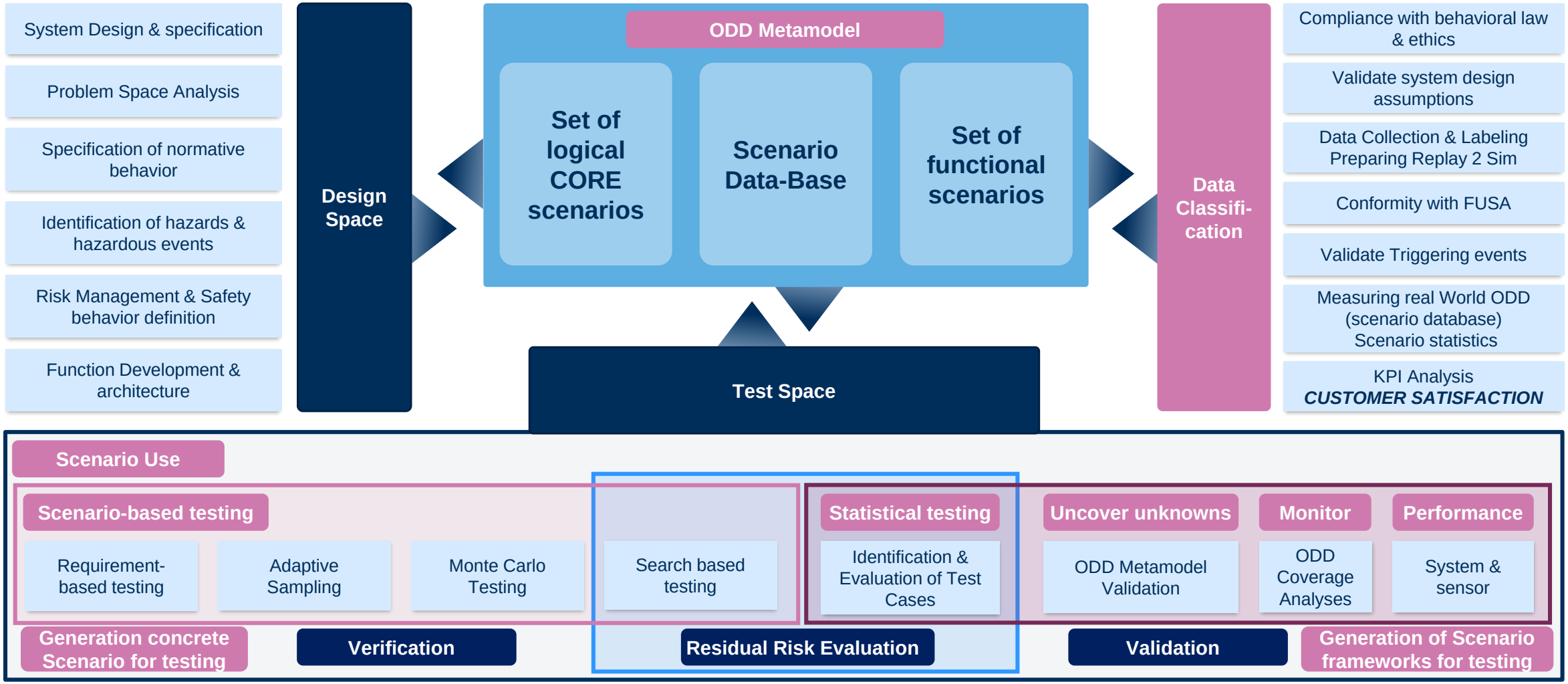
Risk Acceptance criteria & validation targets must fit!

Search-base testing – residual risk evaluation



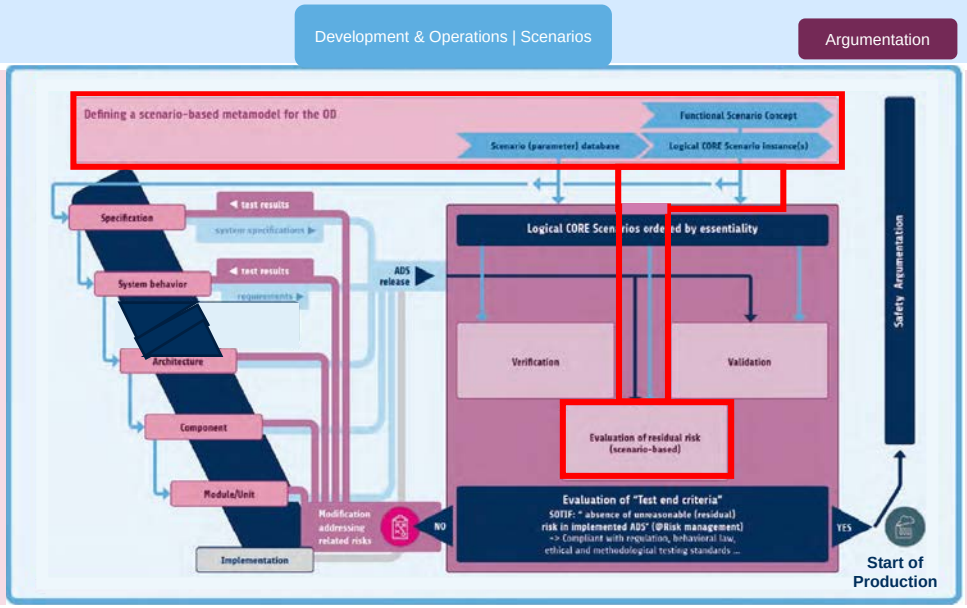
ODD Metamodel - one common, consistent ODD description –

“ADS is designed and tested on a valid model of the (real World) ODD”



PEGASUS Approach – vs – VVMethods Approach

PEGASUS



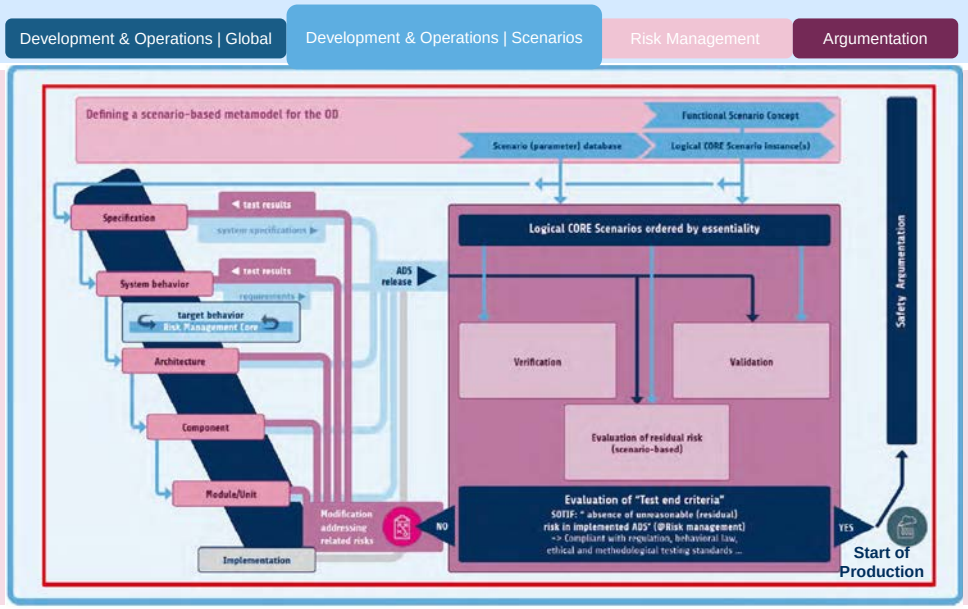
GSN-based argumentation

6 Layer Scenario model, Set of Logical Scenarios

Scenario-based testing with *risk evaluation in V&V*

Use of test instances: Simulation first, PG confirms simulation, endurance run assures stochastic aspects & complex situation

VVMethods



Framework-based Argumentation including *risk management*

6 Layer Model *& ODD Metamodel* (set of CORE scenarios)

Scenario-based behavior specification (ADF / ADS design)

Scenario-based verification & validation

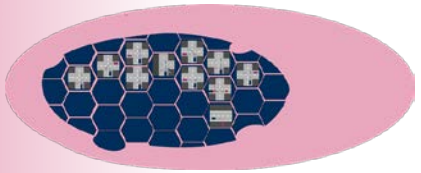
Scenario-based risk evaluation in V&V

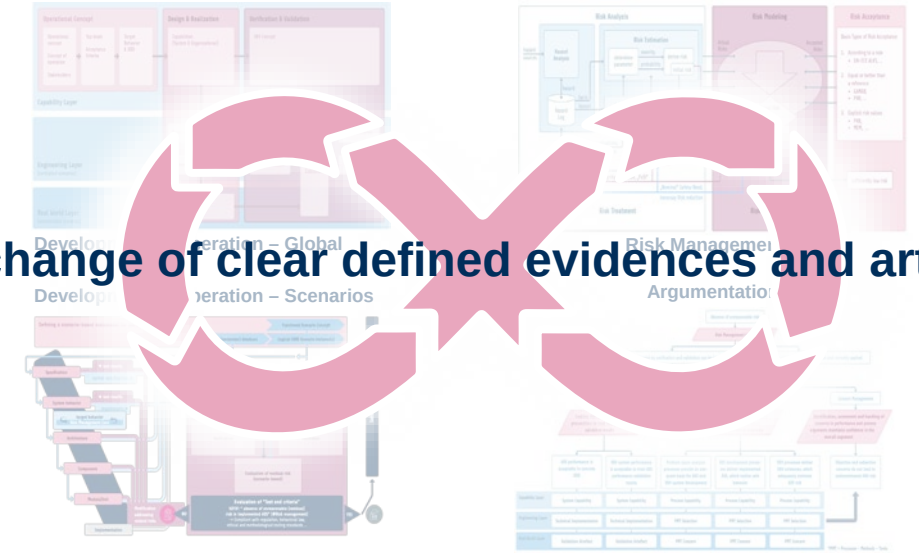
Simulation first, PG confirms simulation, endurance run assures stochastic aspects & complex situation & validates Metamodel

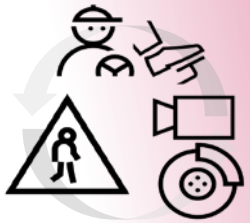
Summary

The necessary evidence to argue that the ADS is free of undue risk can be provided with a few additions to the classical development process.

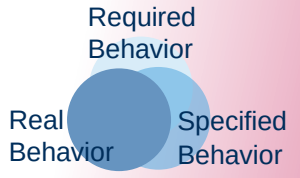
- The consistent use of a valid ODD metamodel in design and V&V.
- Risk control & management is included in design and V&V







Exchange of clear defined evidences and artefacts.



- Scenario-based validation & verification supplemented by evaluated residual risk
- Gap are closed by including Monitoring-reviews in process .

Argumentation

VERIFICATION
VALIDATION
METHODS

Thank you!

Helmut Schittenhelm, Mercedes-Benz
helmut.schittenhelm@mercedes-benz.com

PROJECT of the PEGASUS FAMILY

VDA LEITINITIATIVE

A project developed by the VDA Leitinitiative
autonomous and connected driving

Supported by:

Federal Ministry
for Economic Affairs
and Climate Action

on the basis of a decision
by the German Bundestag