PROJECT of the PEGASUS FAMILY

VERIFICATION
VALIDATION
METHODS

Final Event 21 / 22 November 2023

# How the VVM overall methodology supports the safety case

Helmut Schittenhelm, Mercedes-Benz

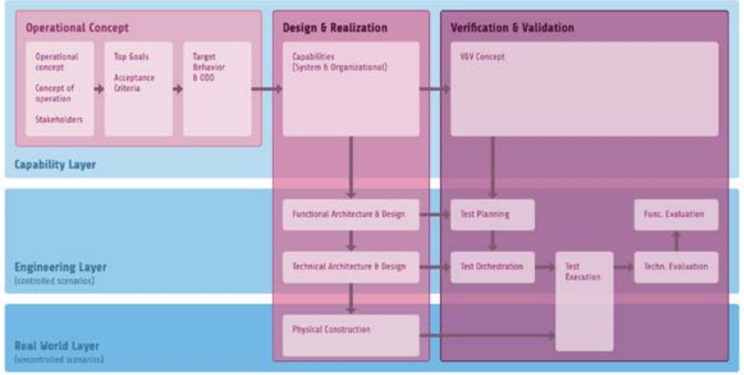
Supported by:

Federal Ministry
for Economic Affairs
and Climate Action

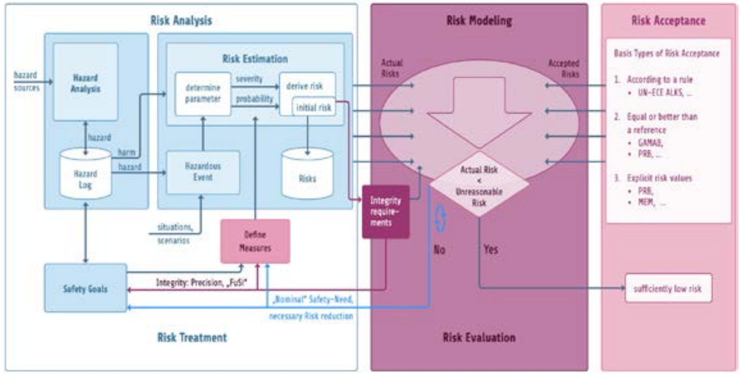
on the basis of a decision
by the German Bundestag

# The four Elements of the VVM Methology

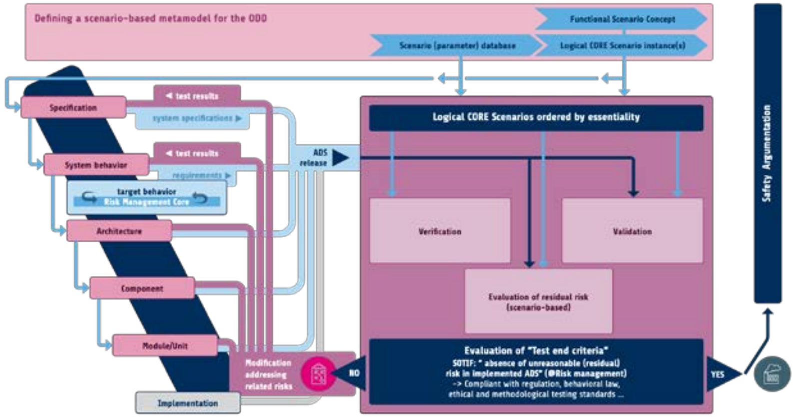
VERIFICATION
VALIDATION
METHODS



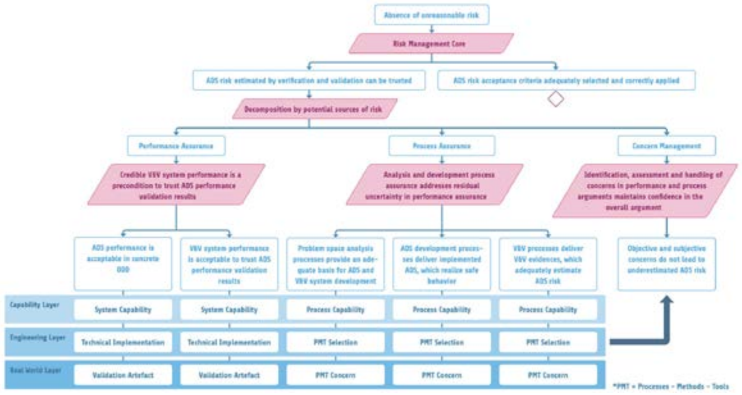
Development & Operation | Global



Risk Management

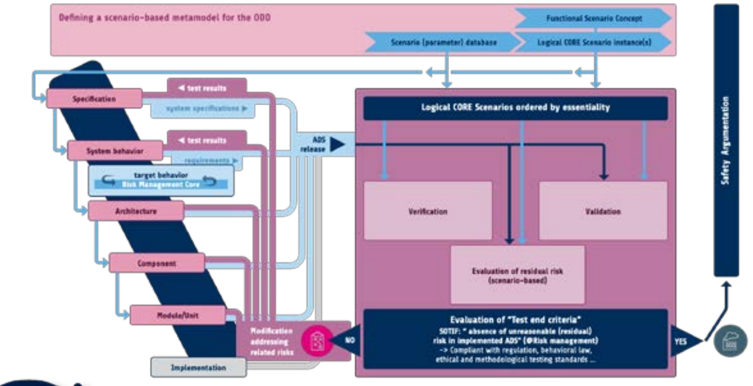

Defining a scenario-based metamodel for the ODD
Functional Scenario Concept
Scenario (parameter) database
Logical CORE Scenario instance(s)
Specification
◄ test results
system specifications ►
System behavior
◄ test results
requirements ►
target behavior
Risk Management Core
Architecture
Component
Module/Unit
Implementation
ADS release
Modification addressing related risks
NO
Logical CORE Scenarios ordered by essentiality
Verification
Validation
Evaluation of residual risk (scenario-based)
Evaluation of "Test end criteria"
SOTIF: " absence of unreasonable (residual) risk in implemented ADS" (@Risk management)
-> Compliant with regulation, behavioral law, ethical and methodological testing standards ...
YES
Safety Argumentation

Development & Operation | Scenarios

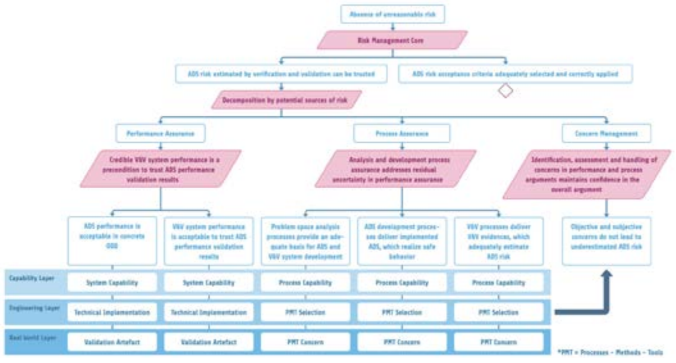

Absence of unreasonable risk
Risk Management Core
ADS risk estimated by verification and validation can be trusted
ADS risk acceptance criteria adequately selected and correctly applied
Decomposition by potential sources of risk
Performance Assurance
Process Assurance
Concern Management
Credible V&V system performance is a precondition to trust ADS performance validation results
Analysis and development process assurance addresses residual uncertainty in performance assurance
Identification, assessment and handling of concerns in performance and process arguments maintains confidence in the overall argument
ADS performance is acceptable in concrete ODD
V&V system performance is acceptable to trust ADS performance validation results
Problem space analysis processes provide an adequate basis for ADS and V&V system development
ADS development processes deliver implemented ADS, which realize safe behavior
V&V processes deliver V&V evidences, which adequately estimate ADS risk
Objective and subjective concerns do not lead to underestimated ADS risk
Capability Layer
System Capability
System Capability
Process Capability
Process Capability
Process Capability
Engineering Layer
Technical Implementation
Technical Implementation
PMT Selection
PMT Selection
PMT Selection
Real World Layer
Validation Artefact
Validation Artefact
PMT Concern
PMT Concern
PMT Concern
*PMT = Processes - Methods - Tools

Safety Argumentation

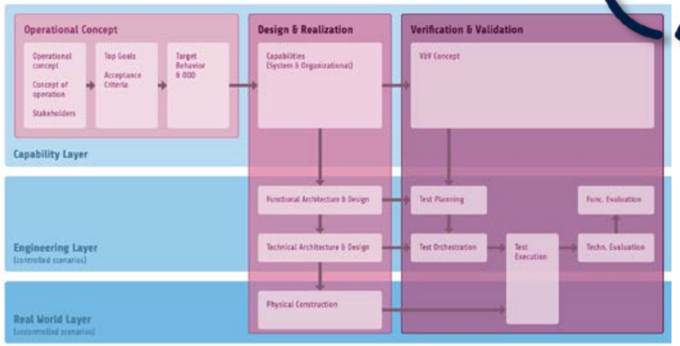
# The four Elements of the VVM Methology


Defining a scenario-based metamodel for the ODD
Functional Scenario Concept
Scenario (parameter) database
Logical CORE Scenario instance(s)
Specification
◀ test results
system specifications ▶
System behavior
◀ test results
requirements ▶
target behavior
Risk Management Core
Architecture
Component
Module/Unit
Implementation
ADS release
Modification addressing related risks
Logical CORE Scenarios ordered by essentiality
Verification
Validation
Evaluation of residual risk (scenario-based)
Evaluation of "Test end criteria"
SOTIF: " absence of unreasonable (residual) risk in implemented ADS" (@Risk management)
-> Compliant with regulation, behavioral law, ethical and methodological testing standards ...
NO
YES
Safety Argumentation

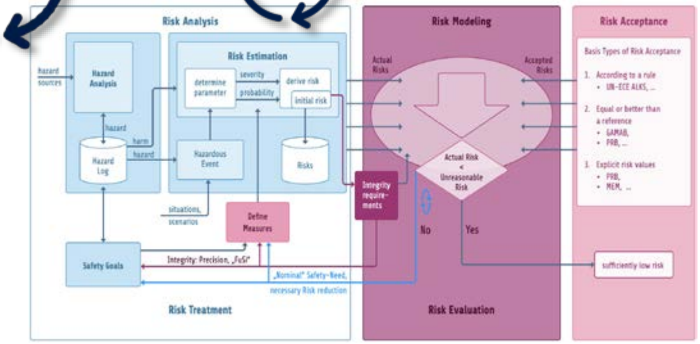
## Development & Operation | Scenarios


Absence of unreasonable risk
Risk Management Core
ADS risk estimated by verification and validation can be trusted
ADS risk acceptance criteria adequately selected and correctly applied
Decomposition by potential sources of risk
Performance Assurance
Process Assurance
Concern Management
Credible V&V system performance is a precondition to trust ADS performance validation results
Analysis and development process assurance addresses residual uncertainty in performance assurance
Identification, assessment and handling of concerns in performance and process arguments maintains confidence in the overall argument
ADS performance is acceptable in concrete ODD
V&V system performance is acceptable to trust ADS performance validation results
Problem space analysis processes provide an adequate basis for ADS and V&V system development
ADS development processes deliver implemented ADS, which realize safe behavior
V&V processes deliver V&V evidences, which adequately estimate ADS risk
Objective and subjective concerns do not lead to underestimated ADS risk
Capability Layer
System Capability
System Capability
Process Capability
Process Capability
Process Capability
Engineering Layer
Technical Implementation
Technical Implementation
PMT Selection
PMT Selection
PMT Selection
Real World Layer
Validation Artefact
Validation Artefact
PMT Concern
PMT Concern
PMT Concern
*PMT = Processes - Methods - Tools

## Safety Argumentation



## Development & Operation | Global

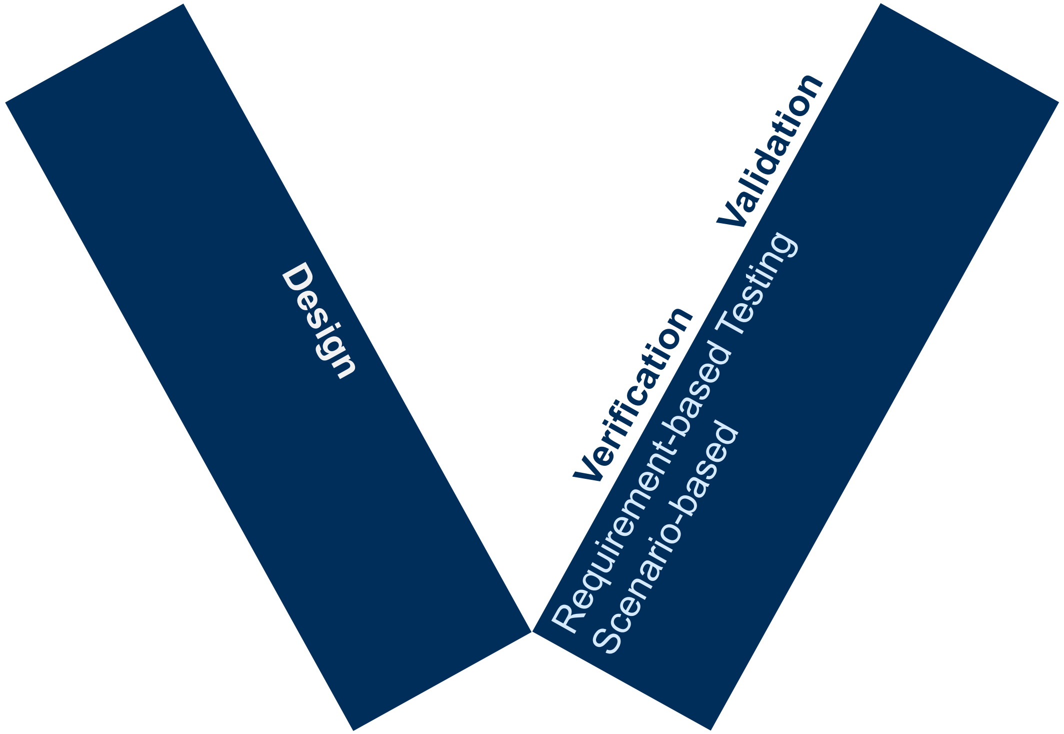


## Risk Management

# Overall Methodology – focus: “System Behavior with *acceptable Risk*”

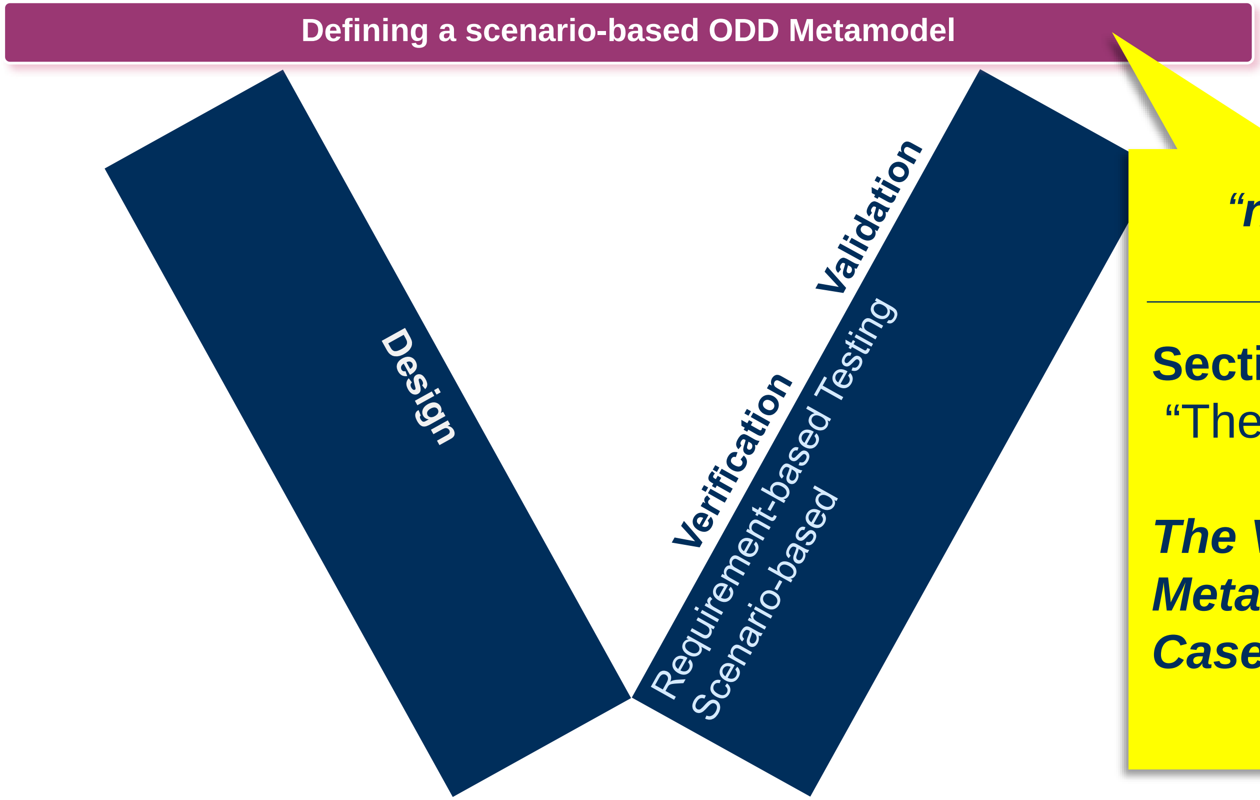
# Overall Methodology

- Starting with the V-Model …



# Overall Methodology

- … adding an ODD model …


Defining a scenario-based ODD Metamodel
Design
Verification
Validation
Requirement-based Testing
Scenario-based

***"not discussed here, but…"***

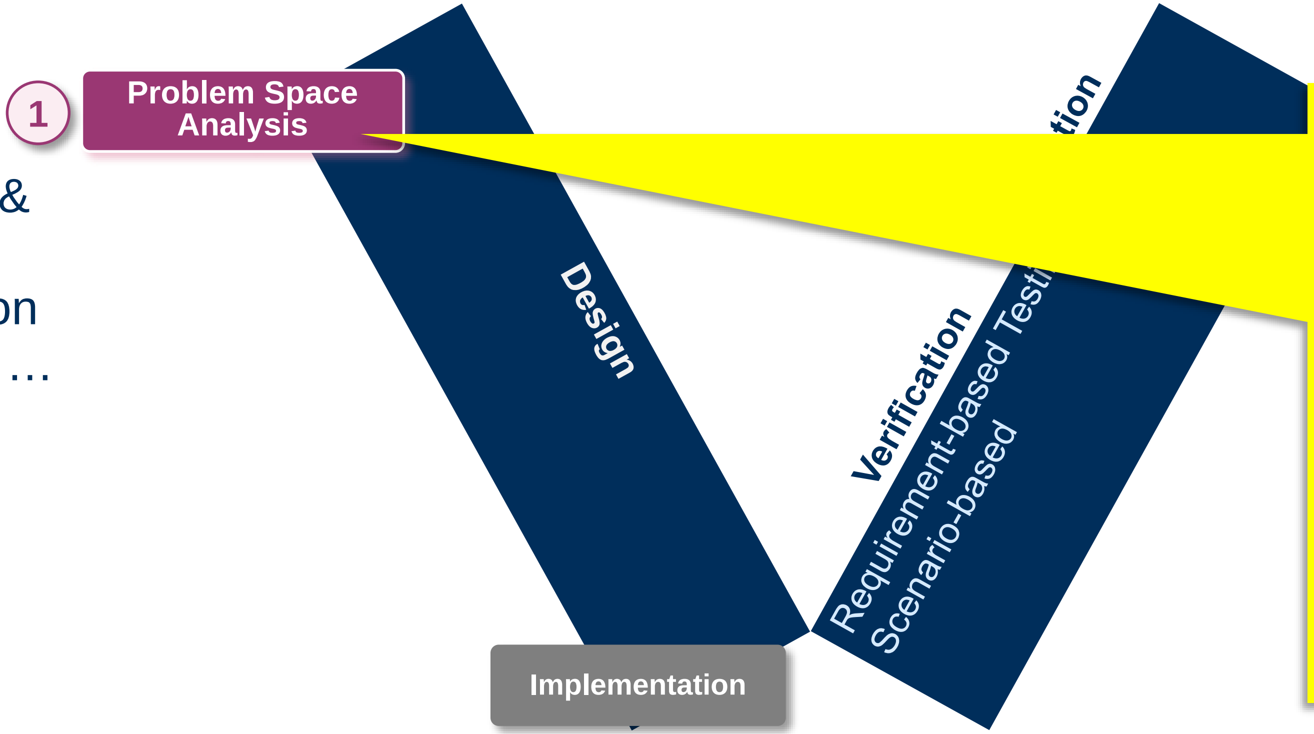
**Section 3**:
"The Role of the ODD"

***The VVM view on the ODD Metamodel in the Safety Case***

# Overall Methodology

- … Problem Space Analysis …

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



***"Criticality Analysis"***

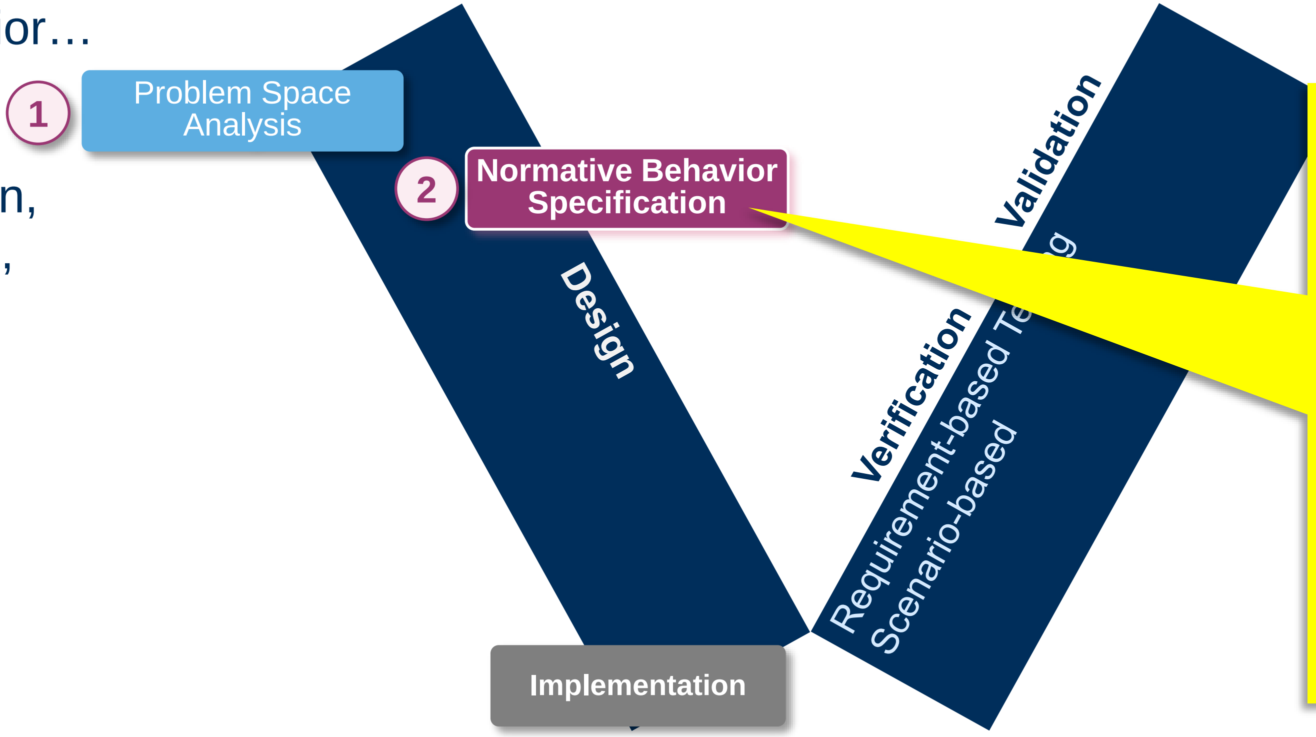
- Accident Database Analysis
- Analysis of existing knowledge and expert know-how
- Analysis of field data
- Simulations
- …

… 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“***

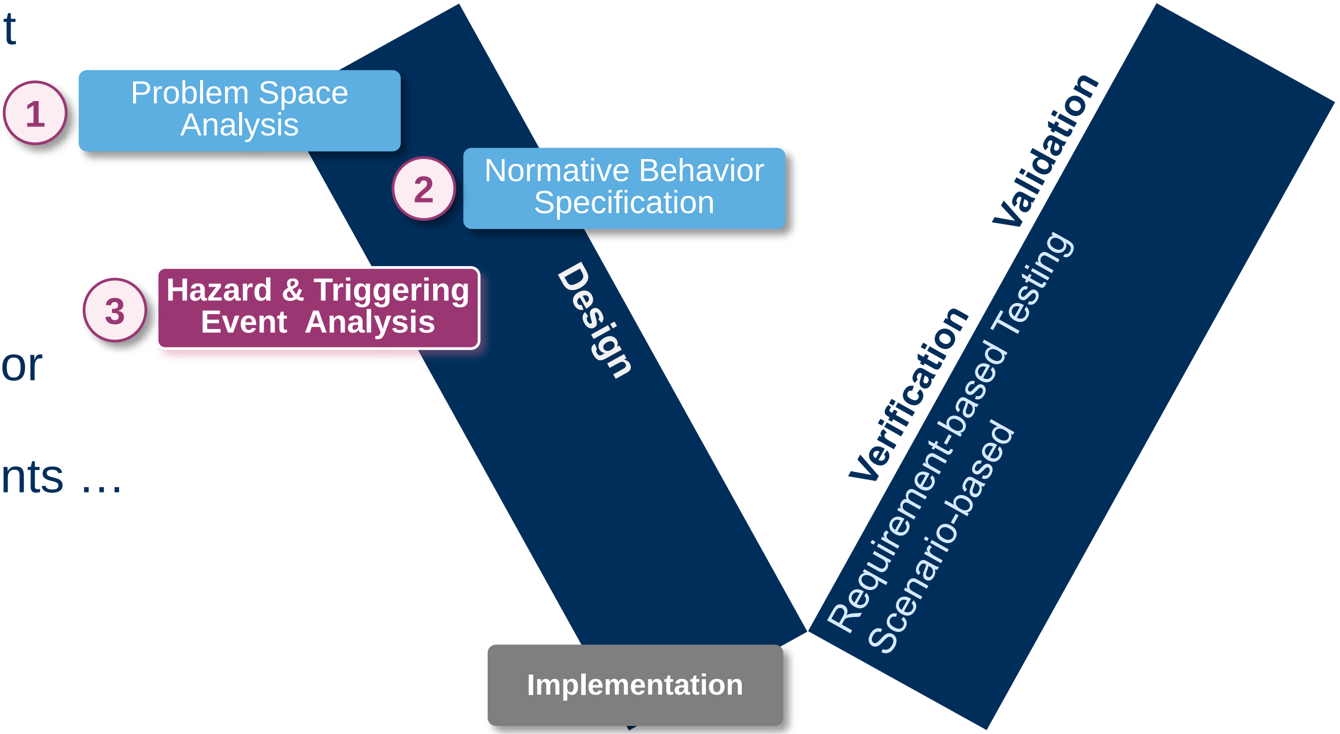
- Legislators use regulations to ensure that society's safety expectations are met.
- The regulations are not national but apply in all UN-regulated markets.

… 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 Event Identification and Analysis…

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

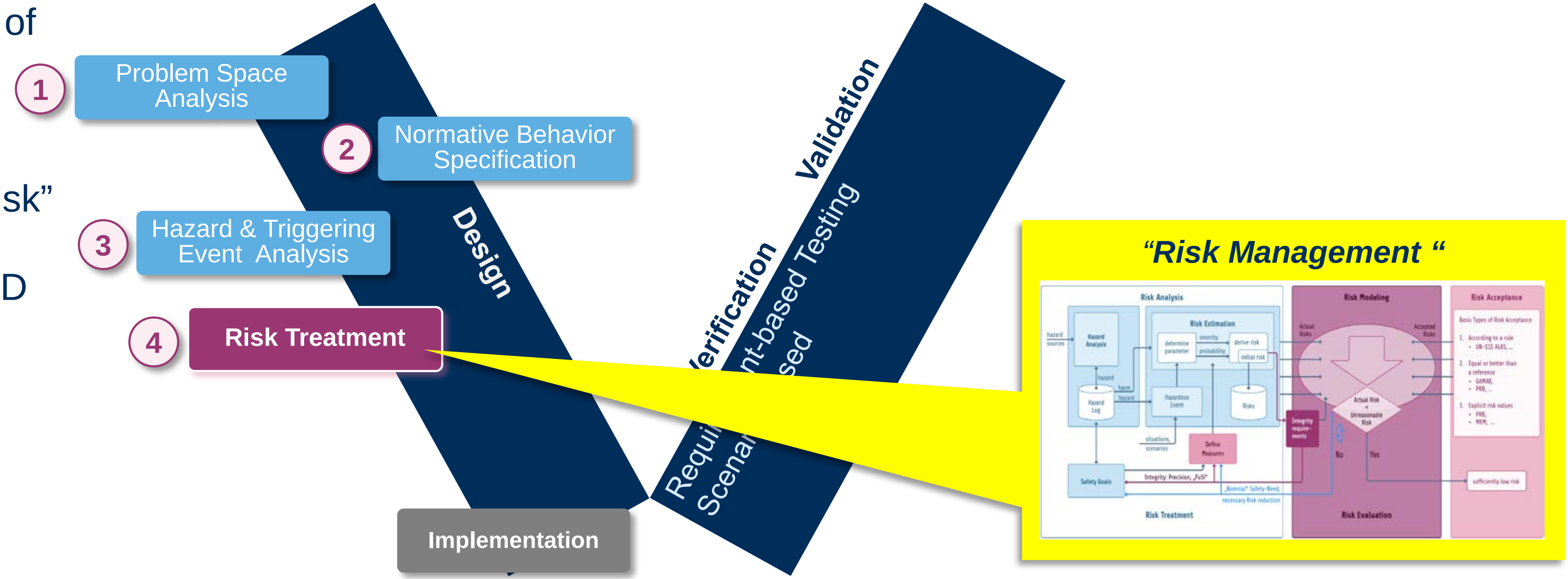

1
Problem Space Analysis
2
Normative Behavior Specification
3
Hazard & Triggering Event Analysis
Design
Implementation
Validation
Verification
Requirement-based Testing
Scenario-based

… 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 …

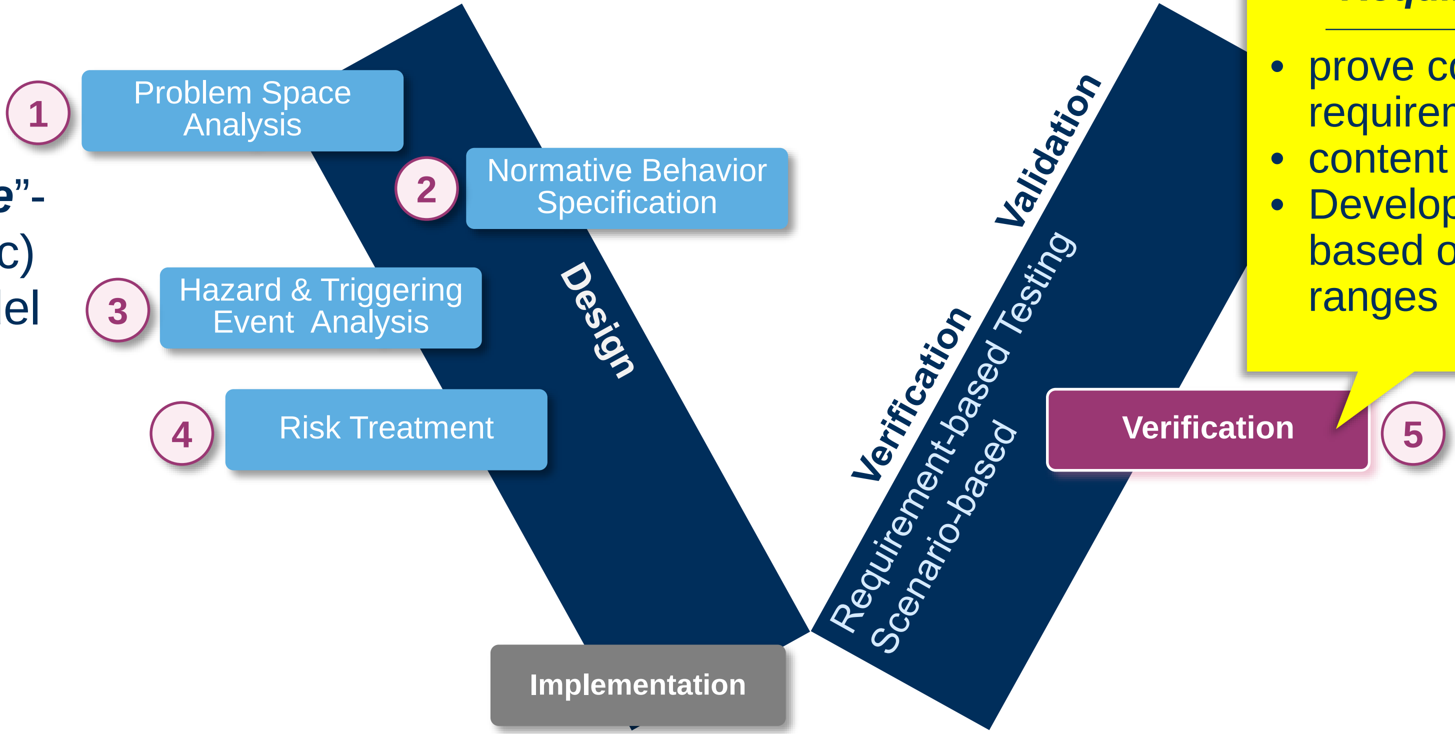
  … ensures "acceptable Risk" within System Design for ODD Metamodel…



… 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. …

# Overall Methodology

- … **Verification**…
- … System behaves as specified -“***safe***”- in (deterministic) ODD Metamodel …



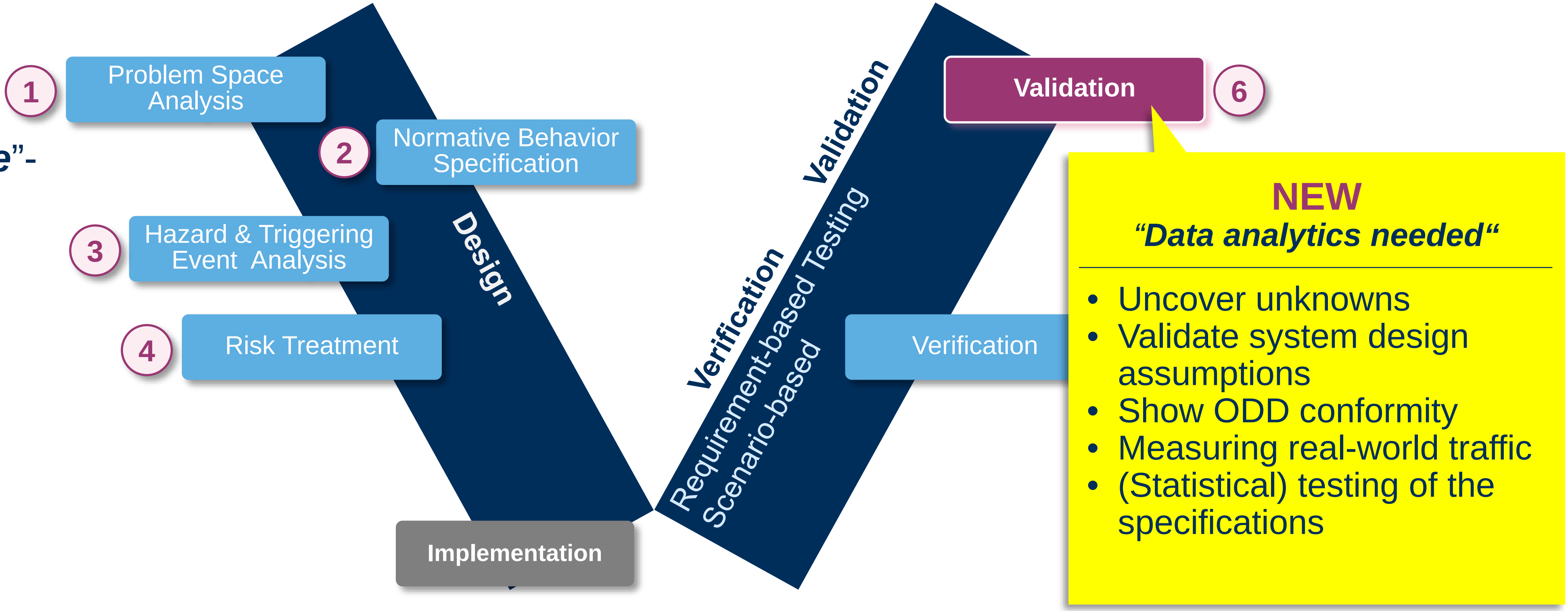
***“Requirement-based Testing“***

- prove correct implementation of requirements & specification
- content Deployment and testing
- Development & approval of tests based on implemented functional ranges

…the **automated driving system** and its components are ***verified in order to show that they behave as specified in the ODD Metamodel*** especially in known but unsafe (near misses/pot. collisions) regions of all CORE scenarios. Furthermore, it must be proven that the **system** and its **components *do not contain any undesired functionality or show operation characteristics which might violate safety objectives*** in its ODD…

# Overall Methodology

- … **Validation**…
- … System behaves as specified -“***safe***”- in (stochastic) ODD …



NEW

***“Data analytics needed“***

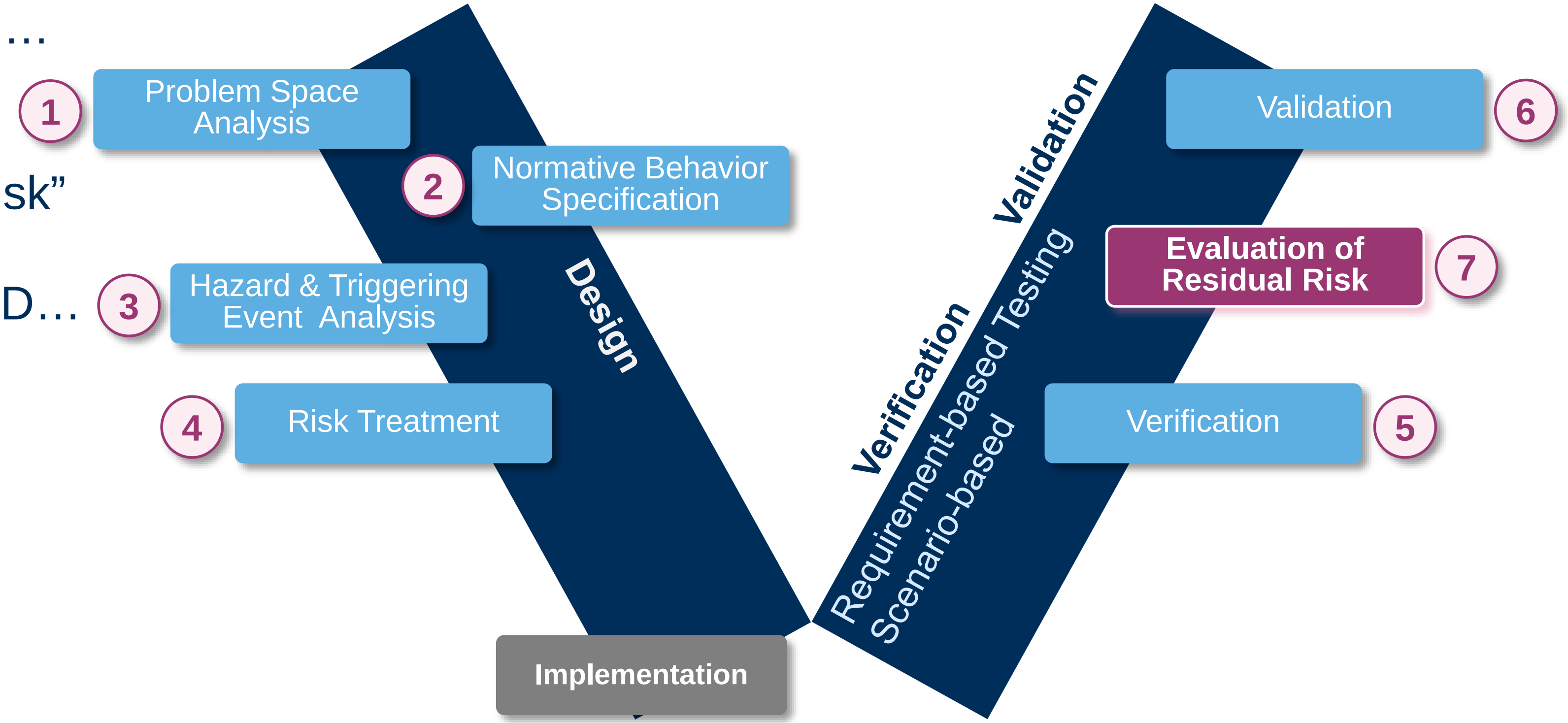
- Uncover unknowns
- Validate system design assumptions
- Show ODD conformity
- Measuring real-world traffic
- (Statistical) testing of the specifications

… validation proves “Is the specification correct and sufficient?” respectively “Are Stakeholder especially customer approvals available?”. Beyond safety and law compliant behavior, Usability, Controllability and acceptability are validation objectives. Validation includes the validation of the ODD Metamodell …

# Overall Methodology

- … Evaluation of Residual Risk …

  … validates "acceptable Risk" within System Design for ODD…



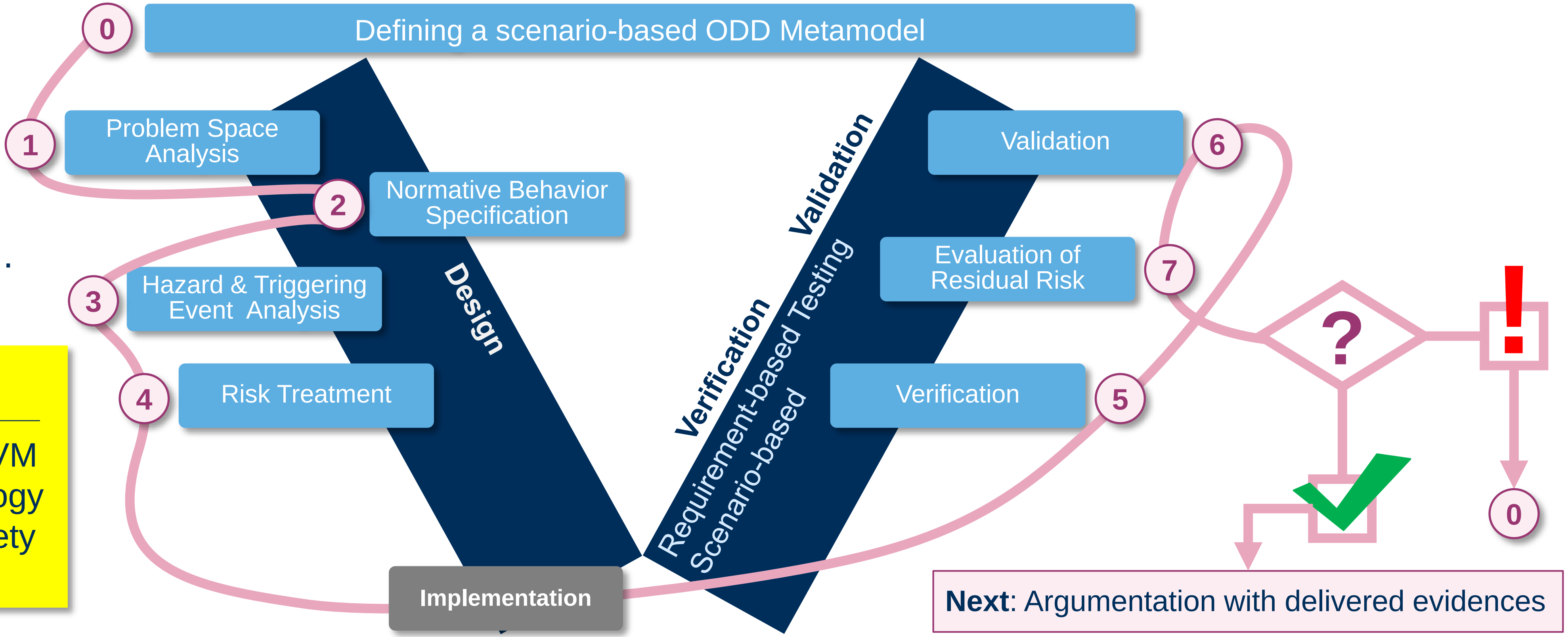
… Evaluation of potential safety risks & compliance with legal requirements consists of three components, the simulation to verify the functional correctness and safe behavior of the driving function in the ODD Metamodel, the evaluation of the sensor performance in real traffic, and an assessment regarding acceptable residual risk and legal compliance. …

# Overall Methodology

- VVM overall Approach argues with evidences provided by this structure …

**“*Resumee*”**

How does the VVM overall methodology supports the safety case?



0
Defining a scenario-based ODD Metamodel
1
Problem Space Analysis
2
Normative Behavior Specification
3
Hazard & Triggering Event Analysis
4
Risk Treatment
Design
Implementation
Verification
Validation
Requirement-based Testing
Scenario-based
Validation
6
Evaluation of Residual Risk
7
Verification
5
?
!
0

**Next**: Argumentation with delivered evidences

… For **each method selected to provide confirmation of a particular quality attribute in the VVM overall approach, a set of criteria has been defined that assesses the contribution** of the analysis, verification or test method to the associated quality attribute as directly as possible. The **achievement of these criteria is then the "reason" for the corresponding statements in the safety case**…

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