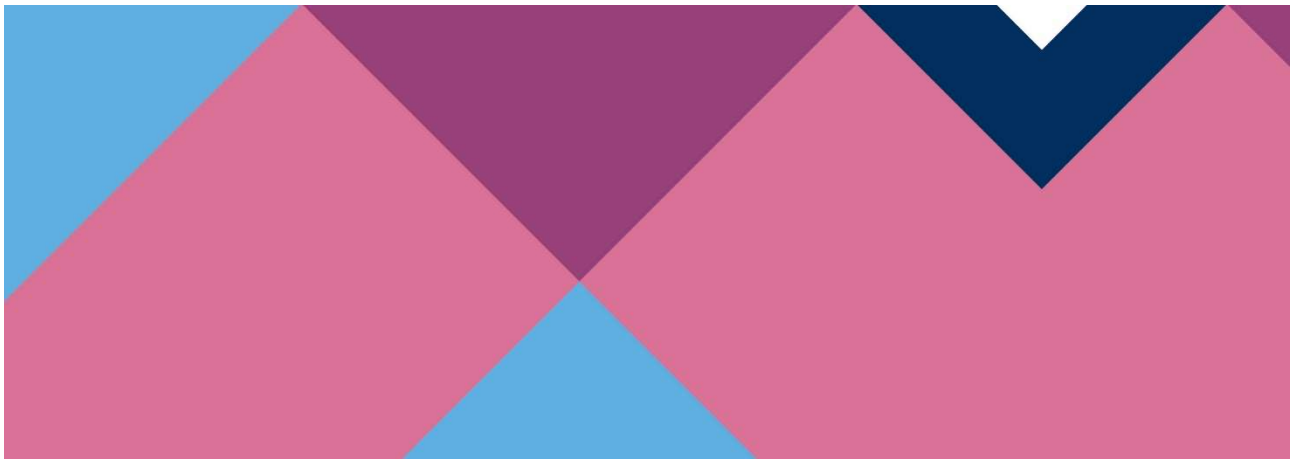
VERIFICATION
VALIDATION
METHODS

VV Methods Safety Assurance Position Paper



Version 1.0

Editors: Roland Galbas, Marcus Nolte, Ulrich Eberle, Hardi Hungar, Henning Mosebach, Nayel Fabian Salem, Helmut Schittenhelm, Jan Reich, Thomas Kirschbaum, Lukas Westhofen

Projectcoordination Robert Bosch GmbH und BMW AG

Publishing date: 15.06.2024

PEGASUS FAMILY

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Table of Content

1 Introduction

1.1 Executive summary

Developing an Automated Driving System (ADS) is a complex task involving many stakeholders from different domains. Taking up this challenge, the VV Methods project (VVM) https://www.vvm-projekt.de/en/ has developed a general methodology that is proposed as a new common basis to develop and ensure the safety of future Automated Driving Systems (ADS). The methodology enables the analysis, monitoring and control of the risk resulting from operating the ADS in its desired Operational Domain[1] for driver, passengers and other traffic participants during the development to ensure that the result maintains an acceptable level of risk. The methodological framework proposed by VVM also integrates key aspects needed to provide evidence of this in a safety case. The framework is explicitly designed for industrial application. It builds on the PEGASUS method (https://www.pegasusprojekt.de/en/) for scenario-based testing and addresses the particular challenges of operating an ADS in and coping with the complexity of urban traffic.

The main overall approach of the VVM methodology is represented in Figure 1. It combines argumentation concepts (pink) establishing the coverage of the operational design domain (ODD) and the operational domain (OD) by scenarios with an assurance framework (light blue) defining the processes and means to develop the ADS for that ODD within the OD. While the argumentation concepts are not fully formalized, the assurance framework is based on formal formats and tool-based procedures, in particular for verification and validation tasks, that can be directly integrated into industrial practice.

The project's approach and achievements can be summarized in the following theses.

- The safety of complex automated driving systems can only be established by integrating a wide range of technical and social perspectives. As a key element, VVM proposes an approach that brings these perspectives together.
- A system can be trusted only if we are convinced that it is safe. The safety argument is a central concern of the VVM methodology. The VVM approach now enables to convincingly prove the safety of an automated driving system.
- A development process implementing the VVM methodology will provide the basis for verifying the safety of automated vehicles. All OEMs adopting the methodology would use the same structures for the verification and validation of automated driving systems in urban areas. This may lead to industry-wide standards that could make road traffic even safer for all road users.

[1] The term "Operational Domain" is equivalently used to the term "Target Operational Domain" according to ISO 34503.

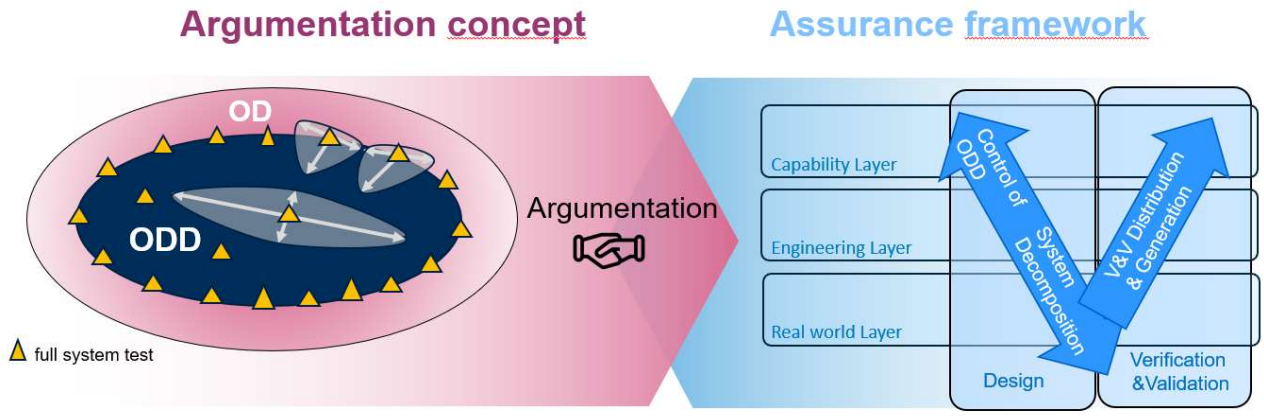


Figure 1: Overall VVM design space: Argumentation concept and assurance framework

This positioning paper starts with an introduction and a summary of general AD safety assurance challenges, and the top goals chosen by VVM to address these challenges in Chapter 1.

Chapter 2 presents and discusses the main VVM position towards a central VVM thesis statement and four subtheses with related argumentations, see Figure 2. These subtheses capture the relation between the identified challenges and the chosen top goals. They delineate the solution space and summarize how the VVM methodology addresses the challenges. Future research and development activities, which further develop and complement the project results, can also orient themselves within this framework.

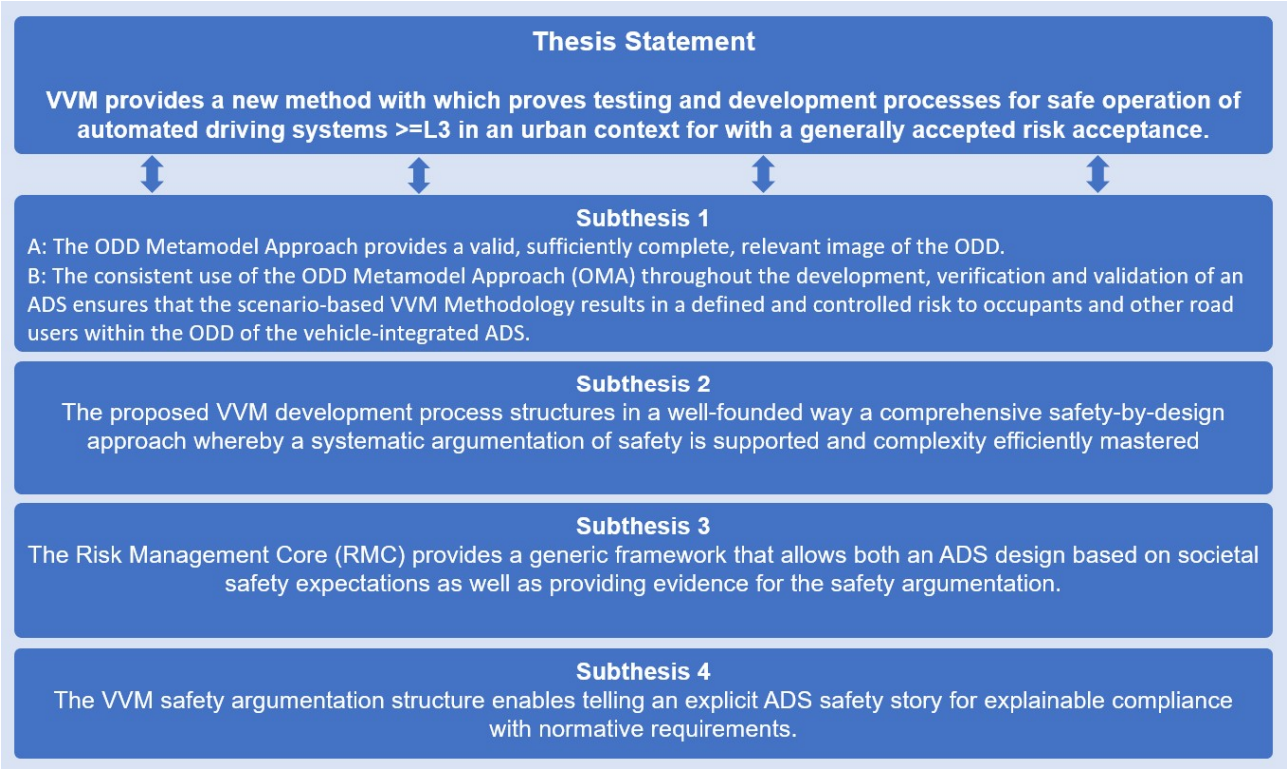


Figure 2: VVM general thesis statement and according subtheses

In Chapter 3 the main VVM result is presented by building up a tangible solution space based on the theses and their supporting argumentation and contrasted by the given challenges and top-goals of

the project. This positioning paper closes with an overview of remaining research needs in Chapter 4, supplemented by recommendations how scenario-based testing methodologies can be applied.

1.2 Status VV Methods and scenario-based safety assurance

Scenario-based testing methodologies for demonstrating the safety of ADS, the associated need for coherent measurement values, formats, procedures, and parameter ranges, as well as the necessary shift of the test space into simulation environments (or virtual environments), are the focus of many global research and development initiatives. The crucial factors behind this are the required reduction of the unlimited parameter space associated with the challenges of development, test and type approval of an ADS functionalities as well as with the latest regulations in the member states of the European Union for a certain Operating Domain (OD).

These initiatives from research, industry, test design, standardization, regulation, and large-scale deployment share a common center: scenario-based development and validation procedures and the associated shift of the design and test space into simulation-based methods.

The VV Methods (https://www.vvm-projekt.de/en/) project provides fundamental and scalable approaches towards a comprehensive overall methodology for scenario-based safety verification and validation in automated driving.

VVM in combination with the SET Level project (https://setlevel.de/) as part of the PEGASUS project family have developed an overall argumentation structure for the safety verification and validation of ADS using design and implementation methods of scenario-based approaches.

In addition to the systematical derivation of initial test situations through the definition of criticalities and the OD-describing ontologies, the VVM overall approach provides a methodical and technically applicable structure enabling an overall safety argumentation. The overall approach at the beginning was to shift the common V-model structure and its according development and validation elements and processes as much as possible into simulation-based methods in order to reduce work on physical components and full prototypes to a manageable minimum. Nevertheless, physical testing and data capturing from the real-world will always remain a key part of the development and validation process.

VV Methods has defined the overall methodology based on the PEGASUS project and is aligned with corresponding standardization initiatives. The integrated SET Level project has provided the appropriate simulation architecture with which individual components such as sensor models or driving functions can be tested so that they can then be subjected to a safety verification in accordance with regulations.

The intended area of application is urban driving, including the typical complex conditions that occur there. Methodologies for formal scenario descriptions, the optimization of parameter spaces as well as parameter sampling methods and the integration of real data collected in the field into the simulation-based verification are at the heart of both projects.

VVM and SET Level propose approaches to map the infinite parameter space (complex traffic scenarios are made efficiently manageable by examining the interdependencies) into a still large but

finite set of specific logical scenarios with certain properties, covering representatively the Operational Design Domain (ODD). Furthermore, tests can be performed both on system and on subsystem level. In this context, real testing is shifted to simulative methods wherever possible, which leads to an increase in cost and time efficiency. Also such simulative approaches, ranging from model/software-in-the-loop to hardware- and even prototype/vehicle-in-the-loop methods, enable development and validation work that would not be accessible for physical testing for reasons of sheer size of the parameter variation or safety implications. To demonstrate the feasibility, a complete test chain from model-in-the-loop to test bench (Hardware-in-the-Loop) to real driving is set up as an example. With regard to industrialization, working on the proof of safety becomes also part of the development process via systematic approaches (and a "design for testability"). This is ensured by binding and connecting coherent interfaces and processes to industrial automotive processes.

The core of both projects is developing a development and validation structure for safe automated driving, including the necessary methods for parameter variation, so that the test coverage derived from these results in a representative number of simulable scenarios, variations and eventualities, complemented by physical testing. Both VVM and SET Level are purely pre-competitive R&D projects funded by the German Ministry for Economic Affairs and Climate Action. In addition to the methodological approaches, the focus is also on the operational concretization of test scenarios, the structuring of the data bases, the use of open definitions and tools as well as example implementation of results of the two interlinked projects.

The work within VVM and SET Level was performed in close interaction with worldwide partner initiatives and projects as well as standardization bodies, through cooperation and joint expert workshops of the PEGASUS family. A unique point of VVM and SET Level projects was to develop an overall methodology covering both sides of the V-model and spanning over many abstraction layers from pure model-in-the-loop simulation to real-world driving and data capturing, as well as addressing the complexities of driving in an urban environment for AD systems

1.3 VVM goals, challenges and solution space

At the very beginning of the VVM project, four top goals were defined as guiding and target corridors for all levels of complexity within VVM (see Figure 3). These goals set out the requirement to reduce the unlimited test space for automated driving to a manageable and balanced finite number and to shift test efforts as much as possible into a means of virtual validation and assessment by simulation. Beside the technological challenges the need to include boundary conditions such as rules, laws or the social definition of safety into the test space in a formalizing way was shaping these top goals as well.

The systematic decomposition of the OD was chosen as on one access instrument to solve this challenge as defined by top **goal 1 “Systematic control of test space”**. The systematic decomposition of OD incorporating relevant hazardous phenomena, involvement of traffic-law perspective and the identification and description of a target behavior within the ODD were the main drafting lines for the argumentation concept. Applying this approach means to reduce the unlimited options in reality and parameters to an infinite and practicable size. **Goal 2** - the demand for

"Consistent Interfaces" emphasizes the need to break down the various definition and process steps of the argumentation into technically applicable test and verification procedures. The argumentation and verification chain is thus subjected to a real feasibility test. Using virtualized components and parameter spaces associated with **goal 3** "Shift to simulation", the simulation space is enhanced with more degrees of freedom to integrate further virtual elements and opportunities to mix them with real artefact data to perform an almost unlimited range of test space

Goal 4 "Explainable safety" means the constant requirement to all process steps of the argumentation being explainable, traceable and consistent to relevant stakeholders. One main challenge here is that an enormous number/variety of input variables must be taken into account and that some of these are of a non-technical, non-formal nature, but ultimately the technical proof must be very well explainable and must also be able to be carried out according to social criteria.

Figure 3: VV Methods management top goals of project

In addition to these top goals at management level, the following challenges in Table 1 were decisive for the development of the VVM overall method. These challenges are also valid beyond VVM and can significantly define future projects for the applied proof of safety.

The deployment of ADS can be accelerated by linking theses 6 thematic challenge corridors with the relevant stakeholders under the presence of growing and open innovative data- and scenario ecosystems.

These challenges (see Table 1) are the result of both project-internal investigations as well as the result of various liaisons between VVM and experts and stakeholders worldwide. Additionally, a detailed version of this overview table with further details and explanations is presented in Annex A.

Table 1: Challenges as accompanying framework for the thematic VVM project corridors

Challenge		Details
C1	**We have to develop a definition of safety and safe systems on the road**	**The society expects just safety, thus** safety and generally compliance must be **argued to the stakeholders of society** before introduction. The absence of unreasonable risk is argued via several societal claims – following laws and standards. Using quantified risk helps threefold: for defining design taged values, for a robust safety argumentation, and for comprehensible approval decisions. The expectation of society is a safety argumentation including **quantification of risk**.. The expectation of society is a safety argumentation including **quantification of risk**.
C2	**ODD-decomposition by scenarios and argumentation of ODD-coverage are key to master open world**	The **argumentation of a representative ODD-coverage** by specifically designed logical scenarios is the key for a systematic control of the development and validation space (main result VVM), thus the argumentation of a sufficient ODD-coverage using the VVM ODD meta model is essential for the overall VVM method The **VVM ODD meta model** is in that sense an appropriate and sufficient model of the ODD by introducing a structured methodology for the reality abstraction by using independent logical scenarios with special properties, the so-called base scenarios.
C3	**Safety argumentation and development process have to correspond**	**Safety argumentation and development process have to correspond** in all layers and in the whole complexity. In order to master this complexity, the Argumentation, Design and V&V should start with an **abstract perspective** i.e. using **capabilities and target behavior** of the system and should be followed by **formal decomposition** to prove integrity and safety of sub-systems. Legacy quality processes have to consider metrics of formal decomposition along the argumentation.
C4	**Virtualization is mandatory**	Despite of all systematic structuring, the challenge for systems **operating in an open context** impose a tremendous demand of tests and data. **Virtualization** of models and data on all relevant layers is mandatory. Of course, there is a significant number of residual real-world tests remaining for completion.
C5	**Tools and Formats need to be coherent and support argumentation**	Seamless toolchains from simulation to proof-in-field should base on open specifications, **open (data)-formats** as i.e. ontologies should support ODD-coverage. Interfaces should support quality metrics of technical systems and sub-systems.

		Common effort is needed to develop standardized formats and metrics for the complete toolchain including a proof-of-concept implementation.
C6	**Continuous integration between verification and validation ecosystems has to be enabled**	Data-driven approaches to **continuously feed** growing data and scenario pools into industrial useable and evolving tool chains are a key (and required) success factor to enhance legacy safety case chains with future data and adapted scenarios. The development and application of qualifiable, **implementable and certifiable processes and tools** requires systematic approaches to accessibility and interoperability, such as those being developed by new approaches in the **open data / open source** community.

2 The VV Methods position by theses and argumentation

Once the problem space and derived objectives have been clearly identified, the next step is to draw up a list of theses and an argument describing why a solution space can be mapped to the problem space on the basis of the theses. The following 4 central theses are set against the 6 challenges whereby the respective theses and their arguments address one or more challenges.

Thesis Statement

VVM provides a new method with which proves testing and development processes for safe operation of automated driving systems >=L3 in an urban context for with a generally accepted risk acceptance.

Figure 4: General thesis statement

With the VVM general method, we ensure that the target behavior of the ADS and its architecture is designed in such a way that systematic hazards and triggering events are addressed. Addressing safety measures were chosen in such a way that they reduce risk to an acceptable level.

With the VVM overall method, we ensure that the ADS to be developed is safe in such a way that it operates in its ODD with an acceptable risk.

2.1 Subthesis 1 – Consistent usage of an ODD Metamodel Approach

Pegasus has anchored the role of simulation for automated driving system manufacturers through scenario-based testing. The integration of the overall system and the integration of the ADS into the vehicle are essentially verified on digital platforms based on simulation methods. The evidence resulting from simulations are confirmed by a few coordinated tests performed on proving grounds as well as in real world driving,

In the established ADS development process in the automotive industry, the 6-layer scenario model for scenario-based testing founded in PEGASUS was one of several scenario models used alternatively and in parallel for problem/domain analysis, behavior specification, and architecture design. The existing model diversity is the starting point for VVM's new ODD metamodel approach.

VVM extends this with a holistic view of the development process and integrates elements included in current standards, for example from FUSA and SOTIF.

The metamodel approach for the ODD (OMA) established in VVM support the requirement for decomposition: on the modeling level (functional, logical, ...), on the scenario level, on the level of the 6-layer and on the level of the chosen descriptive parameters. The demand for decomposition capability results from different requirements in the development process, such as hazard

identification, decomposition of the customer function into sub-functions and effect chains, and in verification, such as testing functionalities in partial parameter spaces, managing the validation process, and determining the residual risk of the ADS in relation to scenarios.

Some new terms and definitions:

The **logical scenario class** is a logical scenario for which the descriptive parameters have been selected.

The **logical scenario instance** is a filled in logical scenario class. Each parameter has a range of values.

The **set of CORE scenarios** is defined as a set of logical scenarios that have certain properties: minimum set of logical scenarios, free of overlap with the underlying BASE scenarios, capable of representing ADS use cases and hazards, satisfying at least one system requirement, sufficiently complete representation of the ODD, ordered by essentiality.

Subthesis 1

A: The ODD Metamodel Approach provides a valid, sufficiently complete, relevant image of the ODD.

B: The consistent use of the ODD Metamodel Approach (OMA) throughout the development, verification and validation of an ADS ensures that the scenario-based VVM Methodology results in a defined and controlled risk to occupants and other road users within the ODD of the vehicle-integrated ADS.

Figure 5: Subthesis 1

Argument 1	We have developed a method with which we can describe (all) elements of the **ODD sufficiently complete**. By pointing to development steps exemplified by VVM. (Recommend that process XY is applied)
Argument 2	We have developed a formal proof with which we can show that we can generate a sufficiently complete **model of the ODD**
Argument 3	We have built a control step into our actual method that shows us that argument 2 is true within the validation, a validation step that shows that we do not find a new unknown scenario

The VVM General Methodology:

In an inertial step, a set of functional and, based on them, a set of logical CORE scenarios are defined for a target ODD and a customer function. These scenarios are complemented by a scenario parameter database. Together they form the ODD metamodel or the ODD meta model approach (OMA)

Based on the ODD metamodel, a systematic problem space analysis is performed. It provides an in-depth, fundamental understanding of the environment and risks the AD system must address.

A systematic hazard and risk analysis identifies both the events within the core scenarios in which a failure of the ego-vehicle function may occur, as well as systemically inherently hazardous conditions within the interaction between the ADS and its environment that must be avoided. ADS behavior and architecture are derived based on the ODD meta model approach (OMA).

The implementation is verified and validated in the next step. At the level of the components, the integrated system, and the integration into the vehicle, the ODD metamodel is used for scenario-based verification and validation. Scenario-based testing and statistical analysis of durability runs are based on the same scenario model that was used during the problem space analysis and specification of the target (safety) behavior of the ADS.

An additional validation step is the validation of the ODD metamodel. The ODD metamodel is used as a data filter or as a means to transfer real-world observations into this model for coverage measurement or gap identification. Therefore, the ODD metamodel is validated in the real world to ensure that the ODD metamodel we use in design and V&V is a valid representation of the real-world target ODD with respect to the set of CORE scenarios and their declared parameters. This step reduces the epistemic uncertainty or "unknown knowns" in the ODD metamodel. The recursive approach within design and V&V reduces hazards or hazardous situations.

The safety argument being built within the VVM general methodology is based on the ability of the selected ADS architecture and vehicle integration to minimize the risk of behavioral insufficiency, detection, and component failures caused by ODD complexity.

The ODD Metamodel Approach (OMA) provides a valid, sufficiently complete, relevant image of the ODD. The use of OMA consistently ensures a representative problem/domain analysis, adequate ADS design and vehicle integration, and appropriate evidence from the extended scenario-based verification and validation process as described in the VVM general method.

2.2 Subthesis 2 – Mastering complexity by safety-by-design-approach

Safety by design is only possible on the basis of a coherent approach that combines design and verification and validation (V&V). This coherence is made possible by, among other things, a systematic integration of requirements and their V&V, digital traceability of work products including a data strategy. However, a systematic argumentation and explanation of the safety by design approach only succeeds if the essential argumentation steps correspond directly with the design and V&V artefacts and thus supports the safety argumentation. Thus, these theses and their argumentation address C3: "Safety argumentation and development process must correspond" and C6 "Continuous integration between verification and validation ecosystems must be enabled".

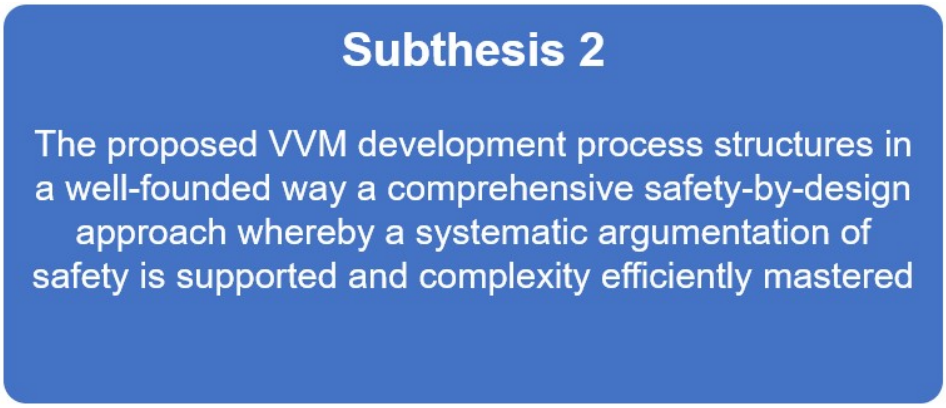


Figure 6: Subthesis 2

Argument 1	**The VVM development process structure corresponds to the perspectives of argumentation:** The central argumentation principle is the application of different perspectives of system-behavior for the systematic analysis of risks/gaps. The Layers of the VVM process structure is set up in accordance to these perspectives: capability layer - required behavior, engineering layer - implemented behavior and real-world layer - real-world behavior. Thus, the evidences generated by the design and V&V domains effectively and efficiently support the argumentation of safety.
Argument 2	**Semantic reproducibility of the central process artifacts enables chains of argumentation:** Each central process artifact generated by the VVM developments framework represents the relevant requirements (qualities) of the preceding process artifact. This way the argumentation chain and the development flow are synchronized so that a continuous chain of reasoning (argumentation) regarding safety is made possible across the system hierarchies and avoids therefore an "explosion of argumentation-paths".
Argument 3	**Consistent use of metrics enables transferability of requirements:** The traceability and transferability of quantitative requirements of central process artifacts based on the consistent use of metrics and thus enables quantitative argumentation chains across the entire range of system hierarchies.

2.3 Subthesis 3 – The Risk Management Core

Showing safety for a system in very different aspects while at the same time mastering increasing complexity requires a holistic approach, that is generic enough but is still precise for all of its applications. The Risk management Core forms this framework to address both challenge 1 “to develop a definition of safety and safe systems on the road” and challenge 3 “Safety argumentation and development process have to correspond” that are detailed in chapter 1.3 VVM goals, challenges and solution space. This is because the safety argumentation can directly follow the structure and the evidence resulting from the output of the Risk Management Core.

The Risk Management Core is designed along the solution space elements “Explainable fulfilment of Societal Safety Expectations” and “End-to-end Risk Management” that are explained in chapter .

Subthesis 3

The Risk Management Core (RMC) provides a generic framework that allows both an ADS design based on societal safety expectations as well as providing evidence for the safety argumentation.

Figure 7: Subthesis 3

Argument 1	The Risk Management Core is **a systematic approach to assess and treat risks** that are potentially introduced during operation of an ADS so that **the threshold of an "absence of *unreasonable risk*" is satisfied.** According to established industry standards, this is a necessary criterion to prove system safety.
Argument 2	This RMC has the **benefit of being applicable in all lifecycle phases,** e.g., during ADS operational design, target behavior definition, technical design, release and operation.
Argument 3	The RMC increases feasibility of assuring safety by reducing complexity by: • **accounting for hazards and manages the risk from multiple safety perspectives** such as Safety of the Intended Functionality (SoTIF), Functional Safety (FuSa) and others. • **aggregating system risk of the same type or from the same scenario set**. • **combining Risk Acceptance Criteria** from different sources and stakeholders, if they are of the same type.
Argument 4	The RMC includes a **control loop that iteratively specifies and evaluates safety measures (including nominal risk reduction and integrity)**. In this turn the RMC **aligns the estimated *actual system risk* with *accepted risk* explicitly**. Thus, the RMC **reduces the systems risk to an accepted level by applying *Risk Acceptance Criteria (RAC)* to determine the *accepted risk***, where the RACs are defined in line with societal expectations.
Argument 5	The RMC serves as **common communication and explanation structure** for different stakeholders for developers as well as authorities. Common understanding on safety and risk is a necessary criterion for the homologation of ADS equipped vehicles.

2.4 Subthesis 4 – The VVM Safety argumentation

ADS safety assurance presents a complex challenge and methods like the ones addressed by sub theses 1-3 are able to generate a multitude of development as well as verification and validation artifacts. Each of these artifacts plays a critical role in certifying the safety of ADS, yet their abundance, intricate detailing, and the complex interrelations among them pose a significant challenge. The primary issue is not solely the generation of these artifacts but weaving them into a coherent narrative that answers the fundamental question: "Why is this ADS safe enough?" This challenge underscores the necessity for a structured approach to safety argumentation, which not only organizes the available evidence into a comprehensive safety story but also ensures explainable compliance with normative requirements. The VVM safety argumentation structure, is designed to articulate an explicit ADS safety story, aligning seamlessly with the overarching goal of demonstrating and explaining how an ADS meets stringent safety benchmarks through a systematic, understandable, and stakeholder-inclusive process. In the following, six arguments are provided to substantiate sub thesis 4.

Subthesis 4

The VVM safety argumentation structure enables telling an explicit ADS safety story for explainable compliance with normative requirements.

Figure 8: Subthesis 4

Argument 1	The argumentation structure allows to **address all important aspects to demonstrate the absence of unreasonable risks**: functional safety, safety of the intended functionality, laws and regulation as well as ethics and safety performance.
Argument 2	The argumentation structure is **tightly integrated with the three pillars of the VVM assurance framework**: the risk management core, the VVM development process and the scenario-based assurance approach. Thus, the claim of the "absence of unreasonable risk" is systematically operationalized by balancing potential and actual risks with concrete safety measures to fulfill defined risk acceptance criteria.
Argument 3	The argumentation structure is **built up respecting established argumentation principles**. Therefore, it argues about claims regarding product performance, process performance, and confidence in product and process arguments. The approach for structuring the argument adds a dialectic perspective, which refutes potential counterarguments to the validity of the provided argument, systematically managing uncertainty with respect to this validity.
Argument 4	The **product performance argumentation** branch is **decomposed along the VVM scenario-based assurance approach** and considers the **credibility of the technical V&V toolchain** as a first-class argumentation need given the complexity of ADS V&V toolchains.
Argument 5	The **process argumentation** requires a justification for adequate **process, method and tool definition with respect to problem space analysis, ADS design & development and verification & validation**.
Argument 6	The provided **GSN pattern** for the VVM safety argumentation structure provides a **starting point for safety argumentation teams to efficiently create safety cases in concrete ADS projects**.

The proposed VVM development process structure enables a consistent separation of domain perspectives by combining **scenario-based testing**, **safety-by-design** and **risk management** with the perspective of **systematic reasoning** to develop and operate safety-related automotive systems. In this way, security becomes explainable and therefore **understandable for society** as well. The key to mastering this complexity is to consistently bring all aspects of the individual perspectives back together by maintaining clearly **defined interfaces** between them. This allows all aspects to be effectively integrated into **established automotive processes**.

3 VVM solution structure

The development of ADS is a complex task involving many stakeholders. PEGASUS supported the establishment of scenario-based testing across all test levels. VVM extended PEGASUS by including the development process, among other things. VVM proposes a framework integrating four perspectives to comprehensively develop a safe ADS.

Ensuring safe behavior within the operational design domain (ODD) is paramount. The framework emphasizes systematic integration of safety from the initial design stages to qualification. Three layers of system behavior guide the argumentation: the required capability, the specified engineering solution, and the real-world behavior of the integrated AD System. The framework's goal is to ensure a solid foundation for arguing safe system behavior. It also explicitly distinguishes between autonomous driving (AD) design and the verification and validation (V&V) processes.

The VVM overall method comprises four interconnected processes areas or global "perspectives" to mitigate unreasonable risk. It connects scenario-based development and testing with overarching risk management, rendering the open-world context tangible. The systematic integration of safety into the development and testing process is a key aspect.

Enhanced transparency contributes to heightened societal acceptance of Automated Driving Systems (ADS), offering companies a decisive competitive advantage.

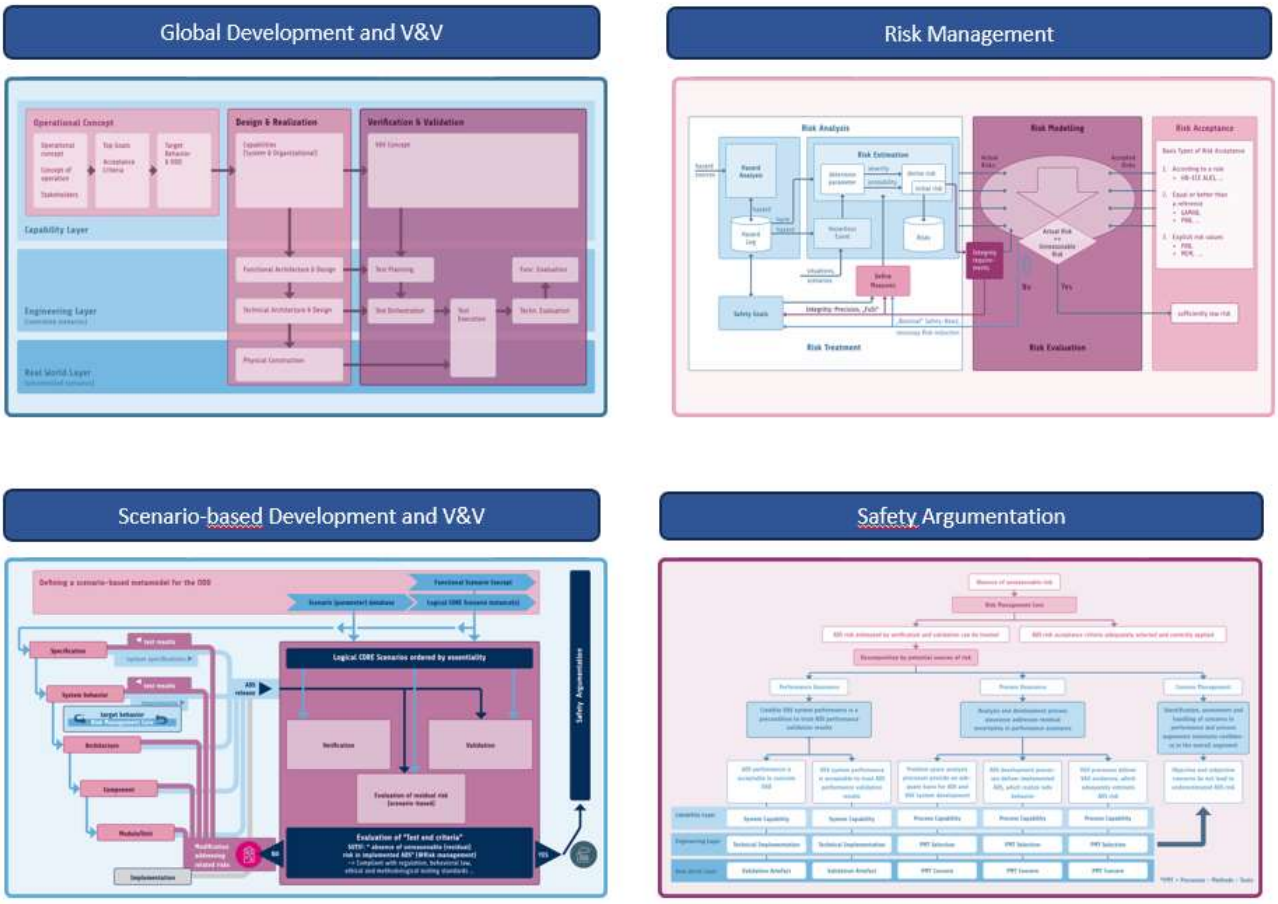


Figure 9: Four methodological processes to reach the goal: Assurance of a **safe** AD System by demonstrating the absence of **unreasonable risk**

PEGASUS, the predecessor project of VVM focused on testing. It established scenario-based testing in interconnected simulation in combination with proving ground tests and real driving to demonstrate a positive balance, respectively a reduced accident risk of an ADS in its ODD. PEGASUS also introduced a scenario database as an information basis. VVM extends this approach including the development process, with its dependencies like current standards (e.g. FUSA and SOTIF) towards a comprehensive view on the safety of ADS. At its core, VVM structures the complex requirements of the operational design area in a level of detail that a function can be developed adequately so that it can be operated safely in this domain. Additionally, VVM allows for argumentation of safety towards society. VVM proposes a framework that comprises of four perspectives:

The Global Development and V&V Perspective focusing on safety by design approach, enabling the process of design and V&V for argumentation and Dev-Ops ensuring the use of evidences from the design- and V&V-process within the argumentation.

The Scenario-based Development and Testing Perspective focusing on the process from development, especially the use of scenarios to ensure safe behavior, within design and V&V. It extends the established process by an approach to consistently use the same scenario meta model throughout the whole process.

The Risk Management Perspective focusing on a comprehensive and holistic concept of safety assessment and integration .

The Safety Argumentation Perspective focusing on a safety systematically argumentation how the safety of an ADS can be reasoned towards stakeholders of society.

3.1 Global Development and V&V perspective

The Global Development and V&V perspective focuses on the conceptual blocks present in the development process of an ADS and links these to the three layers, according to the views for safety argumentation, see Figure 10.

The argumentation of safety can essentially only be based on evidence of the development processes. Since the main idea of reasoning is to argue through different perspectives of behavior [required, specified and real] and the goal of reasoning is to systematically reduce gaps between these perspectives, these perspectives of behavior must be taken into account fundamentally in the development process. This is determined by three layers corresponding to the perspectives of the bahavior. The horizontal layers (of behavioral perspectives) represent development and operating modes for the vertical domains design and verification and validation (V&V).

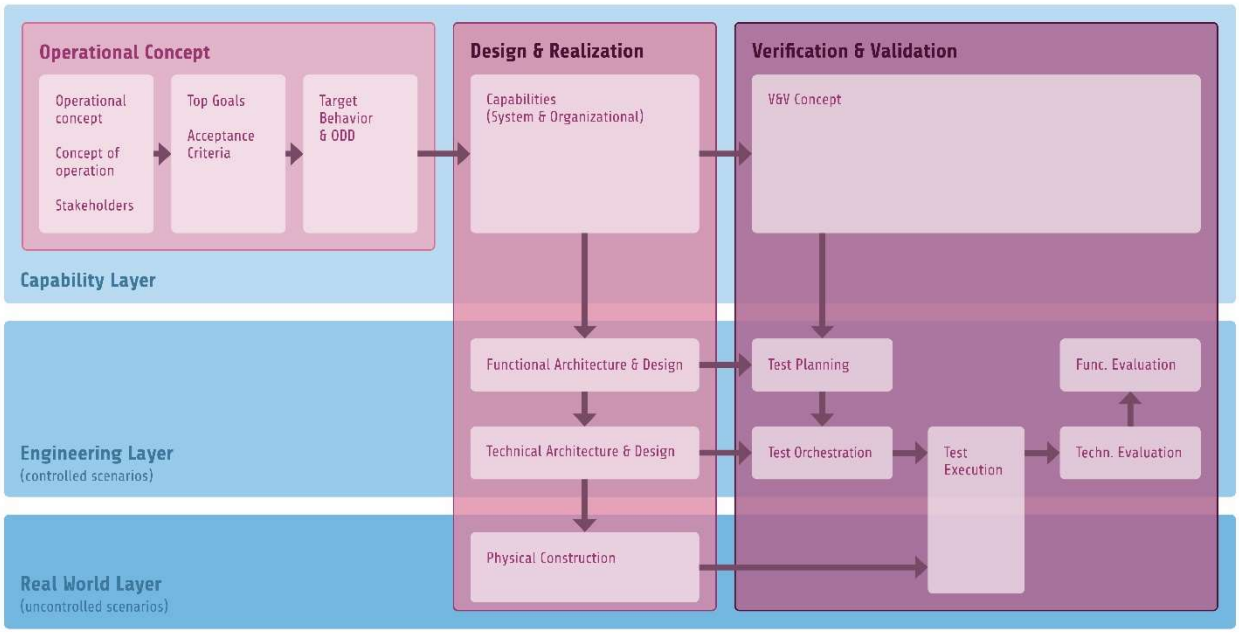


Figure 10: Global Development and V&V method

- The Capability Layer focuses on the composition of abstract requirements. Relevant claims e.g. societal, laws, standards or intended functions are transferred into ADS behavior according to its ODD and into related capabilities, including capabilities necessary for V&V.

- The Engineering Layer focuses on the system specification, structuring the decomposition of abstract requirements for the design specification of the ADS and the tests to validate and verify the ADS.
- The Real World Layer focuses on the interaction of the final implementation with the real world, thus enabling the validation of the ADS behavior within an uncontrolled environment.

These three horizontal layers and the vertical domains [as design and V&V] provide an efficient and traceable decomposition of design and V&V enabling a coherent "safety-by design" approach according to the V-Model. Thus, each horizontal layer provide specific evidences of behavior, needed to argue behavioral safety of the system. The decomposition of design and V&V is also led by the risk-model and the ODD-meta-model and its scenario decomposition. Thus, Design and V&V are structured to support reasoning of system safety expressed by a purposefully argumentation and fulfilling the challenge 3: "Safety argumentation and development process must correspond" as also challenge 6: "Continuous integration between verification and validation ecosystems must be enabled".

3.2 Scenario-based Development and Testing perspective

Complementing the conceptual view, the Scenario-based Development and Testing perspective (Figure 11) focuses on the approach, how scenario-based methods can be applied to complement the development, confirmation and assurance process of a safe ADS. VVM proposes to extend the development process towards an early alignment of artifacts and safety requirements derived from safety arguments, and an alignment of the formulation of the requirements to be used as evidence through the validation and verification process later on.

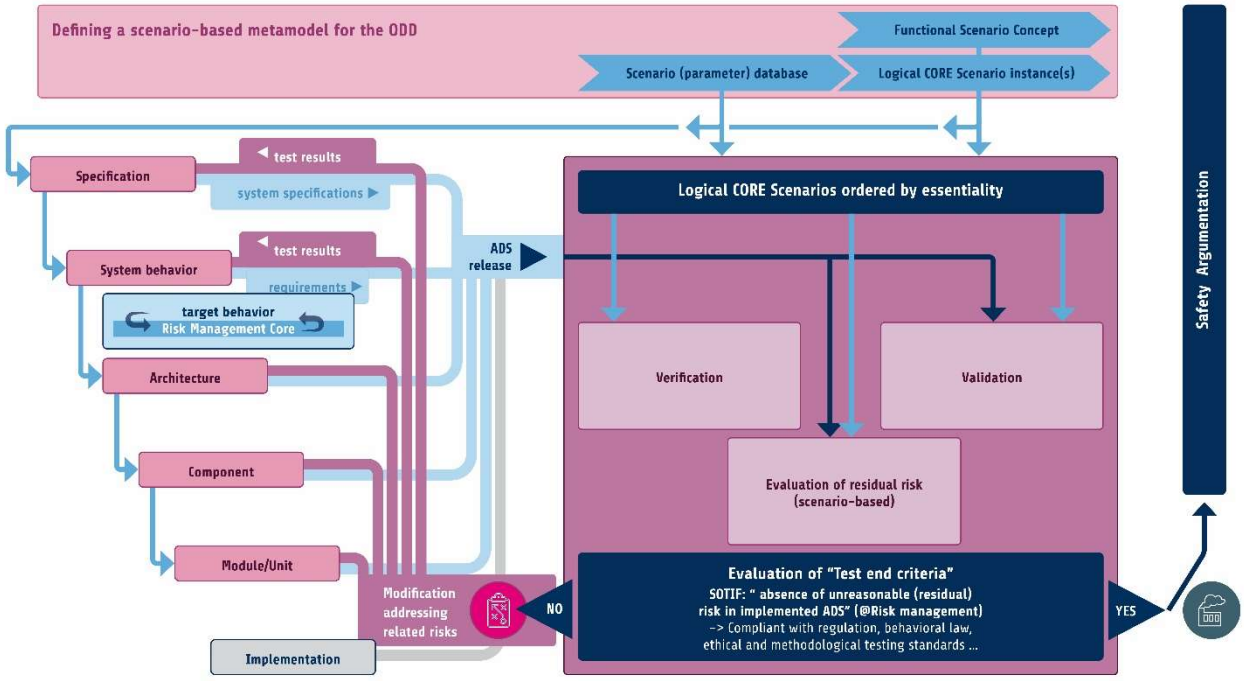


Figure 11: Scenario-Based Testing and Development method

Having safety argumentation in mind, the ODD meta model comprising of a set of core scenarios is introduced as a new tool that can be used in the design as well as the V&V process.

In the design process: The introduction of the ODD meta model allows to perform problem space analysis, System Design, and Safeguarding of the System on the same set of scenarios representing the ODD. The problem space analysis provides a deep understanding of the problem space: It can serve as the basis for the hazard and risk analysis, the definition of safety goals as well as for the integration of stakeholder needs (e.g. legal, society or ethical) in the system behavior and design. Furthermore, the Risk Management Core which defines a process framework for managing risk especially in the context of specifying system behavior and handling hazardous events serves to consistently use of controlled and managed risk throughout design and safeguarding.

During Validation and Verification: Using the ODD meta model allows for V&V on the same ODD meta model from Hazard and Risk Analysis as well as System Design. This results in the new V&V task of validating the sufficient validity of the current set of CORE scenarios. In this task evidence must be provided that validates that the CORE scenario and associated properties provide adequate coverage of the real scenarios from the target domain. The evaluation of the measures resulting from risk managed system behavior is added, which it is essential to prove that the system behaves at least in such a way that the risk acceptance criteria are met in its ODD. And the V&V concept gets a focus on an assurance related organization of V&V: test objectives, test levels, test platforms and test strategies are linked by the V&V concept and aligned with the need for artifacts and evidence of building the safety assurance argument.

Introducing the meta-model ODD, the requirements of the system are pre-structured enabling an intelligent integration of simulation strategies, proving grounds and on-road tests as well as a holistic, feasible validation, which starts early in the development and is an integral part of the development process.

3.3 Risk Management Perspective

The Risk Management perspective Figure 12 is introduced as part of the VVM framework as it can serve as basis for multiple purposes. The Risk Management perspective collects all hazards and safety goals of the ADS allowing creation of safe target behavior definition, the alignment of system risks with acceptance criteria, the risk estimation of specific system elements as well as the risk evaluation at start of production.

The multitude of necessary safety considerations, whether it is safety of the intended function, functional safety and other needs to be managed. For this purpose, the Risk Management Core (RMC) perspective is proposed within the VVM framework. The RMC represents the continuous processing of actual risks to align with acceptable risks. It establishes risk as the leading measure for safety, aggregates all system risk aspects and aligns the system risk with risk acceptance criteria.

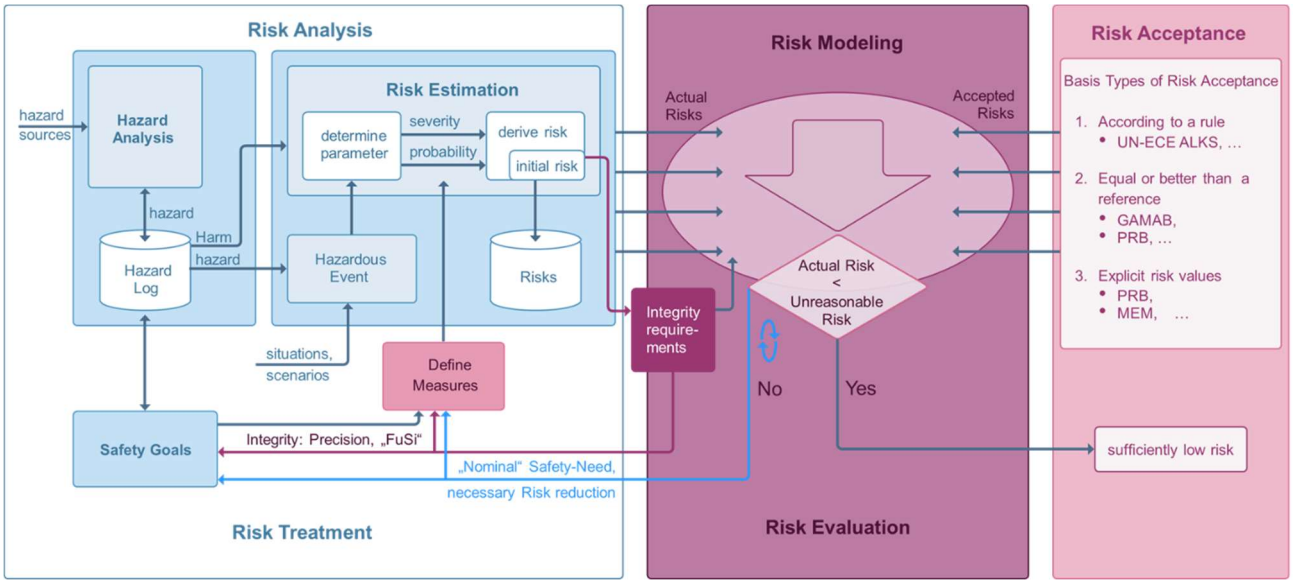


Figure 12: The Risk Management Core method

The Risk Management Core supports the both challenge 1 “to develop a definition of safety and safe systems on the road” and challenge 3 “Safety argumentation and development process have to correspond” that are detailed in chapter 1.3 VVM goals, challenges and solution space. This is because the safety argumentation can directly follow the structure and the evidence resulting from the output of the Risk Management Core. The Risk Management Core is designed along the solution space elements “Explainable fulfilment of Societal Safety Expectations” and “End-to-end Risk Management”.

3.4 Safety Argumentation Perspective

The Safety Argumentation perspective is introduced within the VVM framework to reason why an ADS is safe, i.e. why unreasonable risks are absent during operation. This perspective is proposed to hold all sources of ADS risks and structure the way Figure 13 to decompose the top safety claim “absence of unreasonable risk” into manageable sub claims. Evidence from all perspectives of the VVM assurance framework are used in the safety argumentation process, see Figure 13.

The Risk Management Core is used as a reference model to reason alignment of estimated risk with accepted risk, the Scenario-based Development and Testing approach serves as a reference model to reason that the ADS development and V&V provides confidence. The Global Development and V&V serves to reason that the specification of required capabilities, their engineering and validation in controlled and uncontrolled real-world conditions are completed.

The VVM Safety Argumentation perspective structures the argumentation needs for ADS risk prediction based on assumptions about relevant development and V&V artifacts. It serves as a starting point for argument development in concrete ADS projects considering company-specific assurance methods and V&V.

layers in-line with the relevant standards, corresponding to existing or future tooling and must be systematically integrated into the fleet operation entities.

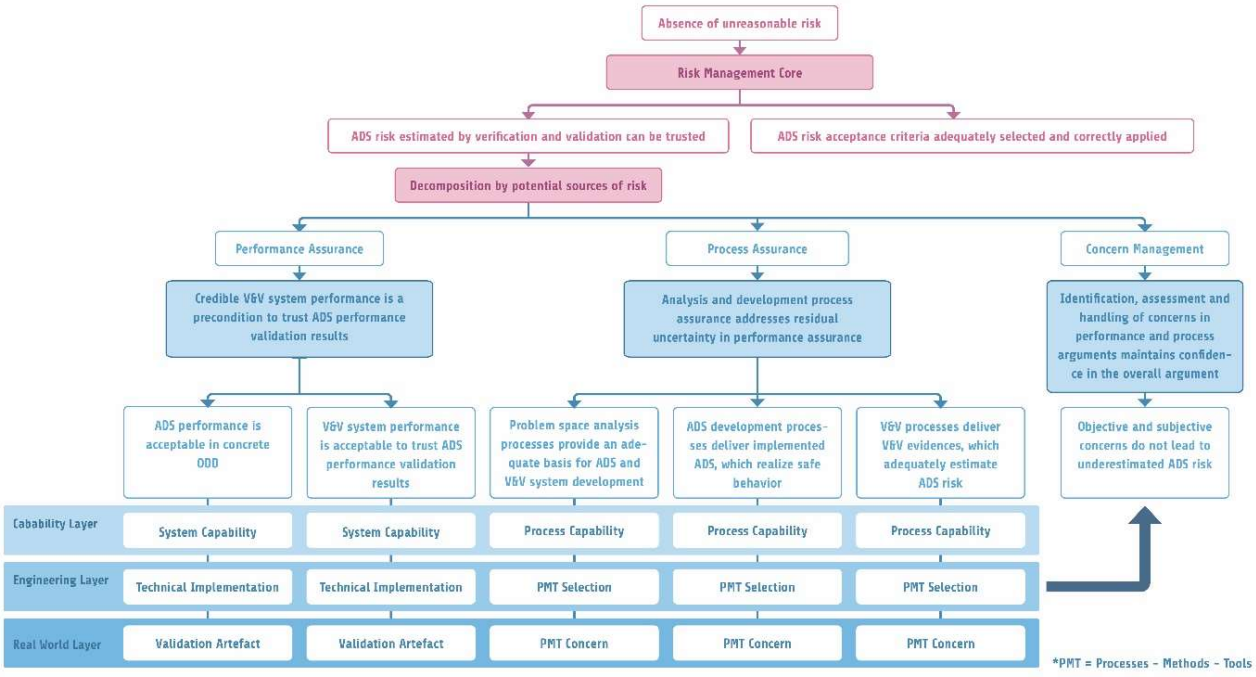


Figure 13: The VVM Safety Argumentation structure method

3.5 Enabler, Premises and Summary of Solution

Consistent use of metrics

The traceability and transferability of quantitative requirements of central process artifacts is based on the consistent use of metrics and thus enables quantitative argumentation chains across the entire range of system hierarchies. One of the biggest outcomes of the VVM-method consists of the separation and also of the linking of the four perspectives - mentioned above. Thus, the complete system of links between the perspectives as also the decomposition of process artifacts at each layer of the perspectives should base on a consistent use of metrics. Only in this way the power of the overall VVM methodology will be unfolded.

Adaptivity to ODD changes

VV Methods has made significant steps towards safeguarding Automated Driving Systems when presented with a given ODD. In the long run, we must expect the given ODD to change. For example, traffic rules are adapted and new types of traffic participants arise. Therefore, systems must be updated. A full re-run of all safeguarding procedures at every update would lead to economic infeasibility of the product. An important step towards applicability is therefore updating safety cases such that only evidence for the relevant parts are re-generated, which eventually establishes economic feasibility. This implies a complete and harmonized formally described ODD on its several layers in-line with the relevant standards, corresponding to existing or future tooling and must be systematically integrated into the fleet operation entities.

Summary

All four perspectives of the VVM overall framework bring together the most important aspects to ensure that an ADS does not pose any unreasonable risk. Thus, VVM contributes to increasing the transparency and acceptance of the safety ensuring process through this comprehensive method. The application of a safety argumentation requires a consistent alignment of scenario-based development and testing comprehensive risk management and argumentation as well as an explicit definition of their linking interfaces in order to make the open-world context tangible. This approach directly strengthens competitiveness, as companies can gain a decisive advantage by systematically integrating safety into the development and testing process.

Finally VVM has developed a methodology as common basis to develop future Automated Driving Systems (ADS) integrating societally accepted risk management. The VVM framework integrates all perspectives needed to develop a safe ADS integrating simulation strategies with proving grounds and on-road tests, enabling feasible validation and verification (V&V) procedures into comprehensive, structured, integrable in established industrial processes.

4 Conclusions, recommendations and future perspectives

The VVM overall method combines the perspectives of **scenario-based testing, safety-by-design** and **risk management** with the approach of a **systematic argumentation** in order to develop **safety assured mobility systems** whereby safety can be **explained to the society**. Key to mastering complexity is given by consequent **separation of perspectives** and their **seamless interaction** by clearly defined links as well as effective integration of established automotive processes.

The following thematic pathways are considered as further enabler for scenario-based safety verification and validation to the next level.

4.1 Outlook: Scenario-based testing and virtualization

4.1.1 Upscaling critical scenarios

While it can be justified to assume there being only a finite and manageable number of safety-critical factors to consider, testing all their possible combinations still leads to a combinatorial explosion easily exceeding any realistic testing budget. While scenario-based testing delivers promising results, in practice, ODDs are ever-increasing. In this case, practical applicability of scenario-based testing is directly related to the ability of incorporating these individually improbable but collectively relevant edge cases methodically into safety cases. Hence, how do we efficiently generate evidence, e.g., as test data, for system safety in these scenarios? A specific research approach dedicated to critical scenario generation anticipating edge cases covering the increasing ODD space may be a relevant and necessary answer to upscaled automated driving deployment.

4.1.2 Application of ODD modeling

The structuring of the Operational Domain and the Operational Design Domain as initiated by PEGASUS and VV Methods needs to be enhanced with description languages for the ODD, especially for simulation use cases. For many applications of L4 automated driving, it would also be highly relevant to have improved on-board algorithms available whether the vehicle is still inside its ODD. Approaches concerning the usage of core scenarios for a database of safe scenarios and the combination of these “atoms” for larger ODDs combined from stored standard pieces need to be investigated further, especially in case the Core Scenarios do not only cover geometric descriptions like “straight-road” or “t-shaped junction” or a “roundabout” structure. This is especially important in case traffic- and/or weather-related effects come into play which might affect the safe operation of an ADS in a given traffic area that would be considered “safe” under standard conditions.

4.1.3 Reality abstraction, virtual environments and corresponding tooling

Systematic approaches transferring the reality into versatile virtual elements s.a. models, complementary datasets mixing real and virtual data as well as the corresponding and harmonized virtual test facilities are necessary for large scale application of the VVM scenario-based testing methodology. While current abstraction processes are more-or-less based on data-driven reality abstraction in selected pilots, new (and scalable) model-based procedures calibrating and validating the models could launch the next step in applying scenario-based testing methodologies to industrial use.

Virtual environments play a crucial role in verification and validation (V&V), particularly when considering simulation as a service. The effective integration of diverse test facilities and environments, such as virtual environments, Hardware-in-the-Loop (HiL)/Vehicle-in-the-Loop (ViL), proving grounds, and field tests, is essential to accumulate comprehensive evidence.

4.1.4 Innovative data- and data-service ecosystems

Virtual safety assurance linking high-quality and traceable data and data services (partly based on open data, synthetic (AI-based) data, abstract test and pilot site elements) with industrial R&D and V&V processes is required to fulfill all requirements of safety case methodologies. Innovative ecosystems e.g. as currently are provided by several open marketplaces require to be linked to continuous data- and scenario pipelines with at least TRL 7 maturity. One specific example would concern the continuous updating of high-definition maps, and equipping these with the urgently needed information about sensor-relevant material data (e.g., reflection and refraction properties for radar and lidar). Such continuous integration chains are needed to reach the required levels of quality of the whole data supply chain for verification and validation

4.1.5 Updated and harmonized scenario DBs

Scenario-based testing methods as initialized by the PEGASUS family projects have stimulated the development of several scenario database projects and even first scenario marketplaces designed especially for the safety case. These scenario databases to some extent are already harmonized by the corresponding standardization activities e.g. process views by ISO and technical specifications by ASAM and also others. With the finalization of relevant standards for scenario-based testing in 2024 and the existing 2022 regulations in Europe new scenario DB harmonization efforts may be necessary to support the intended deployment of automated driving.

Such a database could be governed by an independent body and structured similarly to the German GIDAS accident database and should include logical scenarios and the required parameter types as well as bandwidths for the parameter and additional metrics. Such a database has to combine existing scenario DBs, updated with the recent results from the mentioned initiatives above and has to integrate all relevant stakeholder needs from industry, regulation and academia.

4.2 Outlook: Risk Handling and safety case application

4.2.1 Application of risk modeling

Within VV Methods, we developed a process framework with the goal of explicit representation and management of risk – the Risk Management Core. The conceptual framework is based on existing safety standards and applied to the specific challenge of refining a behavior specification of an Automated Driving System. While we illustrated this application of the Risk Management Core in a research publication[2], there are open questions regarding further applications of the framework. Especially, the application of the "risk modeling" step within the Risk Management Core holds multiple challenges. For example, methods are needed to aggregate estimated risks from multiple scenarios to an estimation at the ODD-level. Additionally, risk acceptance criteria will need to be applied both at the ODD-level as well as at the scenario-specific level.

4.2.2 The role of risk management for Security / Cybersecurity

The different safety requirements as well as the effects of the respective risk-reducing measures have a differentiated effect on the risk posed by the vehicle. In the Risk Management Core, an essential element of the VVM method, the semantic abstracted requirements are merged and compared with the requirement classes and its labels. Here, for example, risks from functional safety and SOTIF can be combined. Therefore, requirements of security/cybersecurity can be merged and evaluated with this approach in the same way. However, it is essential that the risks from safety and security are aggregated in a common consideration. Accordingly, conflicts of objectives of safety and security measures must also be clarified via further rule sets (usually by including an extended context).

4.2.3 Applying the safety case on concrete ODDs

Safety-by-design based on virtual elements comes with very high demands on modeling procedures, data quality and traceability, systems engineering approaches for test orchestration and interoperability of all involved elements. "Elements" also means modeling uncertainties. Uncertainties should be quantified in order to improve the process of V&V as well as the to improve the safety of AD. Handling of uncertainties is key to enable industrialization of AD and even of SAE L2 functions. Systematic national and also multi-national approaches how to transfer scenario-based testing methodologies based on uncertainties into industrial application stimulates the required transformation from scientific into industrial processes. At the same time this transformation effort incorporates all and maybe new relevant actors enables would serve as linking element between existing testing capacities and facilities.

4.3 Outlook: Technological Challenges

4.3.1 Explicit Specification of Target Behavior

ISO 21448 provides initial guidelines for the specification of safe intended behavior, an Automated Driving System shall exhibit in its context. However, there are no methods referenced by the standard

[2] N. F. Salem u. a., „Risk Management Core – Towards an Explicit Representation of Risk in Automated Driving", IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3372860.

that can be applied in an industrial setting. Thus, VV Methods proposed approaches to generate a behavior specification that can be used to support safety analyses in the context of SOTIF (but also in the context of functional safety according to ISO 26262). While these approaches were applied in a limited scope of example scenarios, further investigation is necessary how the proposed methods perform in larger scale setting. Additionally, the interrelation between behavior specification and technical design was considered conceptually as VV Methods did not focus on technical design. Future work could focus on how a behavior specification can support a traceable specification of technical requirements.

4.3.2 The role of AI in the safety case

How do future AI-elements s.a. training data, virtually generated data, models and Ai-generated functionalities as well as AI-based decision algorithms correspond to the overall safety case and how can they be integrated in the safety case?

In principle, each relevant AI-system element in terms of a functional chain of effects is included in the VVM overall method with regards to its influence on safety (in the same way as classic elements). Within the overall method each element, whether classic-design or AI-design, must provide its systemic reference to function, risk, data and their reasoning in an argumentation. The AI-specific handling is well described via the focus areas of ISO PAS 8800:

- AI lifecycle processes as e.g. new data lifecycle
- AI safety requirements and AI safety measures as e.g. new safety analyses and new data and model safety properties.
- Safe AI development & evaluation as e.g. new AI safety analysis or field operation monitoring

The challenge of and also the key path for integration of AI-elements into the safety case argumentation lies in the comparability of its performance-metrics and AI-safety methods.

4.3.3 Concernmanagement

In VVM the term concern management was assigned to the handling of “cross-cutting concerns”, whereby “cross-cutting concern” in terms of VVM signifies aspects or phenomena that have a relevant influence on claims or top goals, usually on safety and performance of the system, but their effects or causes cannot be separated arbitrarily far or there is a significant uncertainty about this. Therefore, within the framework the cross-cutting concern needs to be coordinated between different domains. Cross-cutting concerns can originate from technical nature such as the influence of the shaking of a camera on the recognition quality, for example due to potholes (technical emergencies). Cross-cutting concerns can also arise at the requirements level, such as conflicts upcoming from safety and security requirements contradictions.

The VVM concept of concern-management is an assignment of cross-cutting concerns towards a proprietary cross-domain structure (e.g. data-structures), which links known influence of cross-cutting concerns to the different domains, such the influence of solar-glare (aspect of ODD domain) towards the testing of optical sensors (aspect of V&V domain). Concern-management thus supplements the interfaces between meta-layers, domains and their hierarchies with a store of cross-domain development challenges or problem spaces. The aim of these structures is not to create parallelism but to store knowledge and later analyze and develop the cross-cutting concerns to the extent that their influences can be transferred to measures in the domains and their interfaces until the risks they are posing is sufficiently limited. Concerns are also addressed by the argumentation

structure. The concerns of argumentation comprise the impact of the cross cutting concerns and also general concerns of argumentation.

4.3.4 Remote Operation

Remote operation as a bridge technology between human-driven vehicles and full automation could implies its own validation & verification challenges that consequentially has to be handled by scenario-based testing methodologies. In contrast to the scope of VVM, the involvement of a human driver and in particular the connectivity between vehicle and tele-operation infrastructure needs to be addressed. In case of a loss or severe degradation of connectivity, a minimum risk maneuver would needed to be executed autonomously via on-board systems. In addition, the maximum driving times of a remote operator and that impact on his/her capabilities as well as the effects of round-trip latency from the vehicle to the tele-operation center and back (including human reaction times) need to be evaluated. Many tools proposed in VVM could be used for this analysis, like the ODD meta model, the ontology approaches, data formats, scenario data bases, and the proposed test methods like Adaptive Replay-to-Sim, and Vehicle/Prototype-in-the-Loop.

4.3.5 Collective learning and adjustment concepts from in-field operations

Currently, in-field testing or operation of automated driving systems is accelerated and conducted in various countries. A systematic sharing of non-proprietary data and knowledge gained in these activities can drastically reduce efforts of all parties involved and can thus act as a catalyst for improvements. Ideally, this leads to increased safety even before systems enter field tests, as parties have the possibility to access safety-relevant factors and their underlying causalities for their target ODD. How to collectively learn from field data? Here, an open and system-independent knowledge base and its according specifications in-line with the latest standardization parameters and metrics are a valuable tool. A cross country systems-engineering approach collecting, evaluating and transferring relevant data and experiences into the safety case as well as into the product development driven value chains is a promising approach to increase safety and reduce efforts.

5 Epilogue: Product driven safety assurance

Merely concentrating on the product is insufficient; equal emphasis should be placed on the entire process landscape, the array of methods, tool chains, and their seamless interaction – advocating for a "DevOps" approach. Ensuring security and establishing trustworthiness are paramount concerns in this context. Trusted data spaces or ecosystems for data and services must be created for V&V, with potential links or meshes with other data spaces. Recognizing the limitations of current artificial intelligence, especially in adapting or adjusting goal structures, underscores the importance of human decision-makers. Adequate Human-in-the-Loop concepts need to be developed to harness human intelligence effectively in the V&V process.

“The work leaves behind joy in the face of creation and humility in the face of the task”.

We would like to thank the entire VVM team and all supporters for their enormous diligence, effort, strength and perseverance and of course the fun we had.